FORTINET

Fortinet

Security Services

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and networking and security convergence. Our network security solutions are the most deployed, most patented, and among the most validated in the industry. Our broad, complementary portfolio of cybersecurity solutions are built from the ground up with integration and automation in mind, enabling more efficient, self-healing operations and a rapid response to known and unknown threats

Click Your Industry

Education | Government

Nonprofit

Public Sector

- K-12 Education
- Higher Education
- State & Local Government

Fortinet secures the lasrgest enterprise, service provider, and government organizations and is available on a competitively solicited, publicly awarded cooperative contract through OMNIA Partners.

- **IT Security and Data Protection Solutions**
  Region 14 ESC - TX | 01-154

VIEW CONTRACT DOCUMENTATION

CONTACT US

Fortinet Contract Documentation

U.S. Communities, National IPA, & NCPA are wholly-owned subsidiaries of OMNIA Partners, dba OMNIA Partners, Public Sector. All public sector participants already registered with National IPA, U.S. Communities, or NCPA continue to have access to all contracts, with certain exceptions, in the portfolio and do not need to re-register to use a legacy National IPA, legacy U.S. Communities, legacy NCPA, or new OMNIA Partners contract. U.S. Communities, National IPA, and NCPA remain separate legal entities and lead agency contracts completed under each brand are effective and available for use through the contract's approved term. In the event we believe re-registration is necessary for any reason, OMNIA Partners will let you know.

IT Security and Data Protection Solutions

Region 14 ESC - TX
Contract Number: 01-154

Initial Term: December 1, 2022 to November 30, 2025
Renewal Options: Option to renew for two (2) additional one (1) year periods through November 30, 2027.

Region XIV Education Service Center

1850 Highway 351
Abilene, TX 79601-4750
325-675-8600
FAX 325-675-8659

Thursday, December 1st, 2022

Fortinet, Inc.
ATTN: Jerilyn Bailey
899 Kifer Road
Sunnyvale, CA 94086

Dear Jerilyn:

Region XIV Education Service Center is happy to announce that Fortinet, Inc. has been awarded an annual contract for IT Security Products and Data Protection Solutions on the proposal submitted to Region XIV ESC.

The contract is effective immediately and will expire on November 30th, 2025. The contract can then be renewed annually for an additional two years, if mutually agreed on by Region XIV ESC and Fortinet, Inc.

We look forward to a long and successful partnership underneath this contract.

If you have any questions or concerns, feel free to contact me at 325-675-8600.

Sincerely,

Shane Fields
Region XIV, Executive Director

PROPOSAL

SUBMITTED TO:

Region 14 Education Service Center
and
The National Cooperative Purchasing Alliance

IN RESPONSE TO:

RFP# 40-22
IT Security Products and Data Protection Solutions

SUBMITTED BY:

FORTINET, INC.
899 Kifer Road
Sunnyvale, California 94086-5205

www.fortinet.com

FOREWORD

Fortinet, Inc. is pleased to respond to this Request for Proposal (RFP) for IT Security Products and Data Protection Solutions issued by the Texas Region 14 Education Service Center (ESC) on behalf of the National Cooperative Purchasing Alliance (NCPA).

Fortinet is one of the world's top cybersecurity brands, delivering broad, integrated, and automated protection to enable organizations to securely accelerate their digital journey. We rank number one in the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses. For over 20 years, Fortinet's mission has been to secure people, devices, and data. Fortinet has been the driving force in the evolution of cybersecurity and the convergence of networking and security.

Fortinet's network security solutions are the most deployed, most patented, and among the most validated in the industry. Fortinet secures the largest enterprises, service providers, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future.

We appreciate the opportunity to submit this response and in the event we are awarded a contract, we look forward to working with the Region 14 ESC and NCPA.

In keeping with the RFP instructions, our proposal consists of the following information:

Tabs
Tab 1 – Master Agreement / Signature Form
Tab 2 – NCPA Administration Agreement
Tab 3 – Vendor Questionnaire
Tab 4 – Vendor Profile
Tab 5 – Products and Services / Scope
Tab 6 – References
Tab 7 – Pricing
Tab 8 – Value Added Products and Services
Tab 9 – Required Documents

Should you have any questions about our proposal, please do not hesitate to contact me.

Best regards,

Jerilyn Bailey
Public Sector Contracts Manager
FORTINET
Phone: (850) 728-6504 | Email: baileyj@fortinet.com

TAB 1
MASTER AGREEMENT - GENERAL TERMS AND CONDITIONS

Customer Support
The vendor shall provide timely and accurate technical advice and sales support. The vendor shall respond to such requests within one (1) working day after receipt of the request.

Disclosures
Respondent affirms that he/she has not given, offered to give, nor intends to give at any time hereafter any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor or service to a public servant in connection with this contract.

The respondent affirms that, to the best of his/her knowledge, the offer has been arrived at independently, and is submitted without collusion with anyone to obtain information or gain any favoritism that would in any way limit competition or give an unfair advantage over other vendors in the award of this contract.

Renewal of Contract
Unless otherwise stated, all contracts are for a period of three (3) years with an option to renew for up to two (2) additional one-year terms or any combination of time equally not more than 2 years if agreed to by Region 14 ESC and the vendor.

Funding Out Clause
Any/all contracts exceeding one (1) year shall include a standard “funding out” clause. A contract for the acquisition, including lease, of real or personal property is a commitment of the entity’s current revenue only, provided the contract contains either or both of the following provisions:

Retains to the entity the continuing right to terminate the contract at the expiration of each budget period during the term of the contract and is conditioned on a best efforts attempt by the entity to obtain appropriate funds for payment of the contract.

Shipments (if applicable)
The awarded vendor shall ship ordered products within seven (7) working days for goods available and within four (4) to six (6) weeks for specialty items after the receipt of the order unless modified. If a product cannot be shipped within that time, the awarded vendor shall notify the entity placing the order as to why the product has not shipped and shall provide an estimated shipping date. At this point the participating entity may cancel the order if estimated shipping time is not acceptable.

Tax Exempt Status
Since this is a national contract, knowing the tax laws in each state is the sole responsibility of the vendor.

Payments
The entity using the contract will make payments directly to the awarded vendor or their affiliates (distributors/business partners/resellers) as long as written request and approval by NCPA is provided to the awarded vendor.

Adding Authorized Distributors/Dealers
Awarded vendors may submit a list of distributors/partners/resellers to sell under their contract throughout the life of the contract. Vendor must receive written approval from NCPA before such distributors/partners/resellers considered authorized.

Purchase orders and payment can only be made to awarded vendor or distributors/ business partners/resellers previously approved by NCPA.

Pricing provided to members by added distributors or dealers must also be less than or equal to the pricing offered by the awarded contract holder.

All distributors/partners/resellers are required to abide by the Terms and Conditions of the vendor's agreement with NCPA.

Pricing
All pricing submitted shall include the administrative fee to be remitted to NCPA by the awarded vendor. It is the awarded vendor's responsibility to keep all pricing up to date and on file with NCPA.

All deliveries shall be freight prepaid, F.O.B. destination and shall be included in all pricing offered unless otherwise clearly stated in writing

Warranty
Proposal should address the following warranty information:

- Applicable warranty and/or guarantees of equipment and installations including any conditions and response time for repair and/or replacement of any components during the warranty period.
- Availability of replacement parts
- Life expectancy of equipment under normal use
- Detailed information as to proposed return policy on all equipment

Products: Vendor shall provide equipment, materials and products that are new unless otherwise specified, of good quality and free of defects
Construction: Vendor shall perform services in a good and workmanlike manner and in accordance with industry standards for the service provided.

Safety
Vendors performing services shall comply with occupational safety and health rules and regulations. Also all vendors and subcontractors shall be held responsible for the safety of their employees and any conditions that may cause injury or damage to persons or property.

Permits
Since this is a national contract, knowing the permit laws in each state is the sole responsibility of the vendor.

Indemnity
The awarded vendor shall protect, indemnify, and hold harmless Region 14 ESC and its participants, administrators, employees and agents against all claims, damages, losses and expenses arising out of or resulting from the actions of the vendor, vendor employees or vendor subcontractors in the preparation of the solicitation and the later execution of the contract.

Franchise Tax
The respondent hereby certifies that he/she is not currently delinquent in the payment of any franchise taxes.

Supplemental Agreements
The entity participating in this contract and awarded vendor may enter into a separate supplemental agreement to further define the level of service requirements over and above the minimum defined in this contract i.e. invoice requirements, ordering requirements, specialized delivery, etc. Any supplemental agreement developed as a result of this contract is exclusively between the participating entity and awarded vendor.

Certificates of Insurance
Certificates of insurance shall be delivered to the Public Agency prior to commencement of work. The insurance company shall be licensed in the applicable state in which work is being conducted. The awarded vendor shall give the participating entity a minimum of ten (10) days notice prior to any modifications or cancellation of policies. The awarded vendor shall require all subcontractors performing any work to maintain coverage as specified.

Legal Obligations
It is the Respondent's responsibility to be aware of and comply with all local, state, and federal laws governing the sale of products/services identified in this RFP and any awarded contract and shall comply with all while fulfilling the RFP. Applicable laws and regulation must be followed even if not specifically identified herein.

Protest
A protest of an award or proposed award must be filed in writing within ten (10) days from the date of the official award notification and must be received by 5:00 pm CST. Protests shall be filed with Region 14 ESC and shall include the following:

- Name, address and telephone number of protester
- Original signature of protester or its representative
- Identification of the solicitation by RFP number
- Detailed statement of legal and factual grounds including copies of relevant documents and the form of relief requested

Any protest review and action shall be considered final with no further formalities being considered.

Force Majeure
If by reason of Force Majeure, either party hereto shall be rendered unable wholly or in part to carry out its obligations under this Agreement then such party shall give notice and full particulars of Force Majeure in writing to the other party within a reasonable time after occurrence of the event or cause relied upon, and the obligation of the party giving such notice, so far as it is affected by such Force Majeure, shall be suspended during the continuance of the inability then claimed, except as hereinafter provided, but for no longer period, and such party shall endeavor to remove or overcome such inability with all reasonable dispatch.

The term Force Majeure as employed herein, shall mean acts of God, strikes, lockouts, or other industrial disturbances, act of public enemy, orders and regulation of any kind of government of the United States or any civil or military authority; insurrections; riots; epidemics; pandemic; landslides; lighting; earthquake; fires; hurricanes; storms; floods; washouts; droughts; arrests; restraint of government and people; civil disturbances; explosions, breakage or accidents to machinery, pipelines or canals, or other causes not reasonably within the control of the party claiming such inability. It is understood and agreed that the settlement of strikes and lockouts shall be entirely within the discretion of the party having the difficulty, and that the above requirement that any Force Majeure shall be remedied with all reasonable dispatch shall not require the settlement of strikes and lockouts by acceding to the demands of the opposing party or parties when such settlement is unfavorable in the judgment of the party having the difficulty

Prevailing Wage
It shall be the responsibility of the Vendor to comply, when applicable, with the prevailing wage legislation in effect in the jurisdiction of the purchaser. It shall further be the responsibility of the Vendor to monitor the prevailing wage rates as established by the appropriate department of labor for any increase in rates during the term of this contract and adjust wage rates accordingly.

Termination
Either party may cancel this contract in whole or in part by providing written notice. The cancellation will take effect 30 business days after the other party receives the notice of cancellation. After the 30th business day all work will cease following completion of final purchase order.

Open Records Policy
Because Region 14 ESC is a governmental entity responses submitted are subject to release as public information after contracts are executed. If a vendor believes that its response, or parts of its response, may be exempted from disclosure, the vendor must specify page-by-page and line-by-line the parts of the response, which it believes, are exempt. In addition, the respondent must specify which exception(s) are applicable and provide detailed reasons to substantiate the exception(s).

The determination of whether information is confidential and not subject to disclosure is the duty of the Office of Attorney General (OAG). Region 14 ESC must provide the OAG sufficient

information to render an opinion and therefore, vague and general claims to confidentiality by the respondent are not acceptable. Region 14 ESC must comply with the opinions of the OAG. Region14 ESC assumes no responsibility for asserting legal arguments on behalf of any vendor. Respondent are advised to consult with their legal counsel concerning disclosure issues resulting from this procurement process and to take precautions to safeguard trade secrets and other proprietary information.

PROCESS

Region 14 ESC will evaluate proposals in accordance with, and subject to, the relevant statutes, ordinances, rules, and regulations that govern its procurement practices. NCPA will assist Region 14 ESC in evaluating proposals. Award(s) will be made to the prospective vendor whose response is determined to be the most advantageous to Region 14 ESC, NCPA, and its participating agencies. To qualify for evaluation, response must have been submitted on time, and satisfy all mandatory requirements identified in this document.

Contract Administration
The contract will be administered by Region 14 ESC. The National Program will be administered by NCPA on behalf of Region 14 ESC.

Contract Term
The contract term will be for three (3) year starting from the date of the award. The contract may be renewed for up to two (2) additional one-year terms or any combination of time equally not more than 2 years.

It should be noted that maintenance/service agreements may be issued for up to (5) years under this contract even if the contract only lasts for the initial term of the contract. NCPA will monitor any maintenance agreements for the term of the agreement provided they are signed prior to the termination or expiration of this contract.

Contract Waiver
Any waiver of any provision of this contract shall be in writing and shall be signed by the duly authorized agent of Region 14 ESC. The waiver by either party of any term or condition of this contract shall not be deemed to constitute waiver thereof nor a waiver of any further or additional right that such party may hold under this contract.

Price Increases
Should it become necessary, price increase requests may be submitted at any point during the term of the contract by written amendment. Included with the request must be documentation and/or formal cost justification for these changes. Requests will be formally reviewed, and if justified, the amendment will be approved.

Products and Services Additions
New Products and/or Services may be added to the resulting contract at any time during the term by written amendment, to the extent that those products and/or services are within the scope of this RFP.

Competitive Range
It may be necessary for Region 14 ESC to establish a competitive range. Responses not in the competitive range are unacceptable and do not receive further award consideration.

Deviations and Exceptions
Deviations or exceptions stipulated in response may result in disqualification. It is the intent of Region 14 ESC to award a vendor's complete line of products and/or services, when possible.

Estimated Quantities
While no minimum volume is guaranteed, the estimated (but not limited to) annual volume for Products and Services purchased under the proposed Master Agreement is $50 million dollars annually. This estimate is based on the anticipated volume of Region 14 ESC and current sales within the NCPA program.

Evaluation
Region 14 ESC will review and evaluate all responses in accordance with, and subject to, the relevant statutes, ordinances, rules and regulations that govern its procurement practices. NCPA will assist the lead agency in evaluating proposals. Recommendations for contract awards will be based on multiple factors, each factor being assigned a point value based on its importance.

Formation of Contract
A response to this solicitation is an offer to contract with Region 14 ESC based upon the terms, conditions, scope of work, and specifications contained in this request. A solicitation does not become a contract until it is accepted by Region 14 ESC. The prospective vendor must submit a signed Signature Form with the response thus, eliminating the need for a formal signing process. Contract award letter issued by Region 14 ESC is the counter-signature document establishing acceptance of the contract.

NCPA Administrative Agreement
The vendor will be required to enter and execute the National Cooperative Purchasing Alliance Administration Agreement with NCPA upon award with Region 14 ESC. The agreement establishes the requirements of the vendor with respect to a nationwide contract effort.

Clarifications/Discussions
Region 14 ESC may request additional information or clarification from any of the respondents after review of the proposals received for the sole purpose of elimination minor irregularities, informalities, or apparent clerical mistakes in the proposal. Clarification does not give respondent an opportunity to revise or modify its proposal, except to the extent that correction of apparent clerical mistakes results in a revision. After the initial receipt of proposals, Region 14 ESC reserves the right to conduct discussions with those respondent's whose proposals are determined to be reasonably susceptible of being selected for award. Discussions occur when oral or written communications between Region 14 ESC and respondent's are conducted for the purpose clarifications involving information essential for determining the acceptability of a proposal or that provides respondent an opportunity to revise or modify its proposal. Region 14 ESC will not assist respondent bring its proposal up to the level of other proposals through discussions. Region 14 ESC will not indicate to respondent a cost or price that it must meet to neither obtain further consideration nor will it provide any information about other respondents' proposals or prices.

Multiple Awards
Multiple Contracts may be awarded as a result of the solicitation. Multiple Awards will ensure that any ensuing contracts fulfill current and future requirements of the diverse and large number of participating public agencies.

Past Performance
Past performance is relevant information regarding a vendor's actions under previously awarded contracts; including the administrative aspects of performance; the vendor's history of reasonable and cooperative behavior and commitment to customer satisfaction; and generally, the vendor's businesslike concern for the interests of the customer.

EVALUATION CRITERIA

Pricing (40 points)
Electronic Price Lists

- Products, Services, Warranties, etc. price list
- Prices listed will be used to establish both the extent of a vendor's product lines, services, warranties, etc. available from a particular bidder and the pricing per item.

Ability to Provide and Perform the Required Services for the Contract (25 points)

- Product Delivery within participating entities specified parameters
- Number of line items delivered complete within the normal delivery time as a percentage of line items ordered.
- Vendor's ability to perform towards above requirements and desired specifications.
- Past Cooperative Program Performance
- Quantity of line items available that are commonly purchased by the entity.
- Quality of line items available compared to normal participating entity standards.

References and Experience (20 points)

- A minimum of ten (10) customer references for product and/or services of similar scope dating within past 3 years
- Respondent Reputation in marketplace
- Past Experience working with public sector.
- Exhibited understanding of cooperative purchasing

Value Added Products/Services Description, (8 points)

- Additional Products/Services related to the scope of RFP
- Marketing and Training
- Minority and Women Business Enterprise (MWBE) and (HUB) Participation
- Customer Service

Technology for Supporting the Program (7 points)

- Electronic on-line catalog, order entry use by and suitability for the entity's needs
- Quality of vendor's on-line resources for NCPA members.
- Specifications and features offered by respondent's products and/or services

FORTINET

TAB 1
SIGNATURE FORM

The undersigned hereby proposes and agrees to furnish goods and/or services in strict compliance with the terms, specifications and conditions at the prices proposed within response unless noted in writing. The undersigned further certifies that he/she is an officer of the company and has authority to negotiate and bind the company named below and has not prepared this bid in collusion with any other Respondent and that the contents of this proposal as to prices, terms or conditions of said bid have not been communicated by the undersigned nor by any employee or agent to any person engaged in this type of business prior to the official opening of this proposal.

Prices are guaranteed: **120 days**

Fortinet, Inc.
Company Name

899 Kifer Road
Address

Sunnyvale	California	94086
City	State	Zip

(850) 728-6504	N/A
Telephone Number	Fax Number

baileyj@fortinet.com
Email Address

Jerilyn Bailey	Public Sector Contracts Manager
Printed Name	Position

Jerilyn Bailey
Authorized Signature

TAB 2
NCPA ADMINISTRATION AGREEMENT

This Administration Agreement is made as of December 1, 2022, by and between National Cooperative Purchasing Alliance ("NCPA") and Fortinet, Inc. ("Vendor").

Recitals

WHEREAS, Region 14 ESC has entered into a certain Master Agreement dated December 1, 2022, referenced as Contract Number 01-154, by and between Region 14 ESC and Vendor, as may be amended from time to time in accordance with the terms thereof (the "Master Agreement"), for the purchase of IT Security Products and Data Protection Solutions;

WHEREAS, said Master Agreement provides that any state, city, special district, local government, school district, private K-12 school, technical or vocational school, higher education institution, other government agency or nonprofit organization (hereinafter referred to as "public agency" or collectively, "public agencies") may purchase products and services at the prices indicated in the Master Agreement;

WHEREAS, NCPA has the administrative and legal capacity to administer purchases under the Master Agreement to public agencies;

WHEREAS, NCPA serves as the administrative agent for Region 14 ESC in connection with other master agreements offered by NCPA

WHEREAS, Region 14 ESC desires NCPA to proceed with administration of the Master Agreement;

WHEREAS, NCPA and Vendor desire to enter into this Agreement to make available the Master Agreement to public agencies on a national basis;

NOW, THEREFORE, in consideration of the payments to be made hereunder and the mutual covenants contained in this Agreement, NCPA and Vendor hereby agree as follows:

General Terms and Conditions

- The Master Agreement, attached hereto as Exhibit 1 and incorporated herein by reference as though fully set forth herein, and the terms and conditions contained therein shall apply to this Administration Agreement except as expressly changed or modified by this Administration Agreement.
- NCPA shall be afforded all of the rights, privileges and indemnifications afforded to Region 14 ESC under the Master Agreement, and such rights, privileges and indemnifications shall accrue and apply with equal effect to NCPA under this Administration Agreement including, but not limited to, Contractor's obligation to provide appropriate insurance and certain indemnifications to Region 14 ESC.

- Contractor shall perform all duties, responsibilities and obligations required under the Master Agreement in the time and manner specified by the Master Agreement.
- NCPA shall perform all of its duties, responsibilities, and obligations as administrator of purchases under the Master Agreement as set forth herein, and Contractor acknowledges that NCPA shall act in the capacity of administrator of purchases under the Master Agreement.
- With respect to any purchases made by Region 14 ESC or any Participating Agency pursuant to the Master Agreement, NCPA (a) shall not be construed as a dealer, re-marketer, representative, partner, or agent of any type of Contractor, Region 14 ESC, or such Participating Agency, (b) shall not be obligated, liable or responsible (i) for any orders made by Region 14 ESC, any Participating Agency or any employee of Region 14 ESC or Participating Agency under the Master Agreement, or (ii) for any payments required to be made with respect to such order, and (c) shall not be obligated, liable or responsible for any failure by the Participating Agency to (i) comply with procedures or requirements of applicable law, or (ii) obtain the due authorization and approval necessary to purchase under the Master Agreement. NCPA makes no representations or guaranties with respect to any minimum purchases required to be made by Region 14 ESC, any Participating Agency, or any employee of Region 14 ESC or Participating Agency under this Administration Agreement or the Master Agreement.
- With respect to any supplemental agreement entered into between a Participating Agency and Contractor pursuant to the Master Agreement, NCPA, its agents, members and employees shall not be made party to any claim for breach of such agreement.
- This Administration Agreement supersedes any and all other agreements, either oral or in writing, between the parties hereto with respect to the subject matter hereof, and no other agreement, statement, or promise relating to the subject matter of this Administrative Agreement which is not contained herein shall be valid or binding.
- Contractor agrees to allow NCPA to use their name and logo within website, marketing materials and advertisement. Any use of NCPA name and logo or any form of publicity regarding this Administration Agreement or the Master Agreement by Contractor must have prior approval from NCPA.
- If any action at law or in equity is brought to enforce or interpret the provisions of this Administration Agreement or to recover any administrative fee and accrued interest, the prevailing party shall be entitled to reasonable attorney's fees and costs in addition to any other relief to which such party may be entitled.
- Neither this Administration Agreement nor any rights or obligations hereunder shall be assignable by Contractor without prior written consent of NCPA, provided, however, that the Contractor may, without such written consent, assign this Administration Agreement and its rights and delegate its obligations hereunder in connection with the transfer or sale of all or substantially all of its assets or business related to this Administration Agreement, or in the event of its merger, consolidation, change in control or similar transaction. Any permitted assignee shall assume all assigned obligations of its assignor under this Administration Agreement.
- This Administration Agreement and NCPA's rights and obligations hereunder may be assigned at NCPA's sole discretion, to an existing or newly established legal entity that has the authority and capacity to perform NCPA's obligations hereunder.

Term of Agreement

This Agreement shall be in effect so long as the Master Agreement remains in effect, provided, however, that the obligation to pay all amounts owed by Vendor to NCPA through the

termination of this Agreement and all indemnifications afforded by Vendor to NCPA shall survive the term of this Agreement.

Fees and Reporting

The awarded vendor shall electronically provide NCPA with a detailed quarterly report showing the dollar volume of all sales under the contract for the previous quarter. Reports are due on the fifteenth (15th) day after the close of the previous quarter. It is the responsibility of the awarded vendor to collect and compile all sales under the contract from participating members and submit one (1) report. The report shall include at least the following information as listed in the example below:

Entity Name	Zip Code	State	PO or Job #	Sale Amount

Total _____

Each quarter NCPA will invoice the vendor based on the total of sale amount(s) reported. From the invoice the vendor shall pay to NCPA an administrative fee based upon the tiered fee schedule below. Vendor's annual sales shall be measured on a calendar year basis. Deadline for term of payment will be included in the invoice NCPA provides.

Annual Sales Through Contract	Administrative Fee
0 - $30,000,000	2%
$30,000,001 - $50,000,000	1.5%
$50,000,001+	1%

Supplier shall maintain an accounting of all purchases made by Public Agencies under the Master Agreement. NCPA and Region 14 ESC reserve the right to audit the accounting for a period of four (4) years from the date NCPA receives the accounting. In the event of such an audit, the requested materials shall be provided at the location designated by Region 14 ESC or NCPA. In the event such audit reveals an under reporting of Contract Sales and a resulting underpayment of administrative fees, Vendor shall promptly pay NCPA the amount of such underpayment, together with interest on such amount and shall be obligated to reimburse NCPA's costs and expenses for such audit.

ACKNOWLEDGMENT OF CONTRACTOR REQUIREMENTS

National Cooperative Purchasing Alliance	Fortinet, Inc.
Organization	Vendor Name
Matthew Mackel	John Whittle
Name	Name
Director, Business Development	EVP of Corporate Development, Chief Legal Officer
Title	Title
PO Box 701273	899 Kifer Road
Address	Address
Houston, TX 77270	Sunnyvale, CA 94086
Address	Address
[signature]	DocuSigned by: John Whittle 2EBD4ABC62DE44D...
Signature	Signature
December 1, 2022	12/7/2022
Date	Date

DocuSigned by:
[signature]
12/7/2022

FORTINET

TAB 3
VENDOR QUESTIONAIRE

Please provide responses to the following questions that address your company's operations, organization, structure, and processes for providing products and services.

Locations Covered

- Bidder must indicate any and all locations where products and services can be offered.
- Please indicate the price co-efficient for each location if it varies.

☒ **All 50 States & District of Columbia** (Selecting this box is equal to checking all boxes below)			
☐ Alabama	☐ Illinois	☐ Montana	☐ Rhode Island
☐ Alaska	☐ Indiana	☐ Nebraska	☐ South Carolina
☐ Arizona	☐ Iowa	☐ Nevada	☐ South Dakota
☐ Arkansas	☐ Kansas	☐ New Hampshire	☐ Tennessee
☐ California	☐ Massachusetts	☐ New Jersey	☐ Texas
☐ Colorado	☐ Michigan	☐ New Mexico	☐ Utah
☐ Connecticut	☐ Minnesota	☐ New York	☐ Vermont
☐ Delaware	☐ Mississippi	☐ North Carolina	☐ Virginia
☐ D.C.	☐ Missouri	☐ North Dakota	☐ Washington
☐ Florida	☐ Kentucky	☐ Ohio	☐ West Virginia
☐ Georgia	☐ Louisiana	☐ Oklahoma	☐ Wisconsin
☐ Hawaii	☐ Maine	☐ Oregon	☐ Wyoming
☐ Idaho	☐ Maryland	☐ Pennsylvania	

☒ **All U.S. Territories and Outlying Areas** (Selecting this box is equal to checking all boxes below)	
☐ American Somoa	☐ Northern Marina Island
☐ Federated States of Micrones	☐ Puerto Rico
☐ Guam	☐ U.S. Virgin Islands
☐ Midway Islands	

☒ **All Canada Provinces and Territories** (Selecting this box is equal to checking all boxes below)	
☐ Alberta	☐ Prince Edward Island
☐ British Columbia	☐ Quebec
☐ Manitoba	☐ Saskatchewan
☐ New Brunswick	☐ Northwest Territories
☐ Newfoundland and Labrador	☐ Nunavut
☐ Nova Scotia	☐ Yukon
☐ Ontario	

If awarded a Master Agreement, will your company extend the terms offered in your Proposal to public agencies in Canada? If no or maybe, please explain.

☒ Yes ☐ Maybe ☐ No

If awarded a Master Agreement, will your company extend the terms offered in your Proposal to private sector customers?

☐ Yes ☐ Maybe ☒ No

Minority and Women Business Enterprise (MWBE) and (HUB) Participation
It is the policy of some entities participating in NCPA to involve minority and women business enterprises (MWBE) and historically underutilized businesses (HUB) in the purchase of goods and services. Respondents shall indicate below whether or not they are an M/WBE or HUB certified.

☐ Minority/Women Business Enterprise
Respondent Certifies that this firm a Minority / Women Business Enterprise

☐ Historically Underutilized Business
Respondent Certifies that this firm is a Historically Underutilized Business

Small Business, MWBE and HUB Growth
If Proposer is a Large, National or Multinational Organization/Corporation, what programs are in place that partners or supports the growth of small and MWEB and HUB business? If yes, please describe.

☐ N/A, we are a recognized small, MWEB or HUB organization

☐ No, we do not have any programs in place.

☒ Yes, we have programs in place.

Residency
Responding Company's principal place of business is in the city of Sunnyvale, State of California.

Felony Conviction Notice
Please Check Applicable Box (If the 3rd box is checked, a detailed explanation of the names and convictions must be attached):

☒ A publicly held corporation; therefore, this reporting requirement is not applicable.

☐ Is not owned or operated by anyone who has been convicted of a felony.

☐ Is owned or operated by the following individual(s) who has/have been convicted of a felony

Distribution Channel
Which best describes your company's position in the distribution channel:

☐ Manufacturer Direct ☐ Certified education/government reseller

☐ Authorized Distributor ☒ Manufacturer marketing through reseller

☐ Value-added reseller ☐ Other: _____

Processing Contact Information

Contact Person	Jerilyn Bailey
Title	Public Sector Contracts Manager
Company	Fortinet, Inc.
Address	899 Kifer Road
City/State/Zip	Sunnyvale, CA 94086
Phone	(850) 728-6504
Email	baileyj@fortint.com

Pricing Information
In addition to the current typical unit pricing furnished herein, the Vendor agrees to offer all future product introductions at prices that are proportionate to Contract Pricing. If answer is no, attach a statement detailing how pricing for NCPA participants would be calculated for future product introductions.

☒ Yes ☐ No

Pricing submitted includes the required NCPA administrative fee. The NCPA fee is calculated based on the invoice price to the customer.

☒ Yes ☐ No

TAB 4 VENDOR PROFILE

Please provide the following information about your company:

- Company's official registered name.

  Our company's official registered name is Fortinet, Inc.

- Brief history of your company, including the year it was established.

  Fortinet, headquartered in Sunnyvale, California, is a profitable and rapidly growing US company whose core competencies are cyber threat research; cybersecurity product research and development; and the design, implementation and support of integrated cybersecurity solutions based on our extensive portfolio of proprietary products.

  Fortinet was founded in 2000 by Ken Xie and is led by a strong management team with deep experience in networking and security. Fortinet is the only security leader to develop and build custom security processing unit (SPU) technology that offers the best performance and value in the industry with Security Compute Ratings that are much higher than other vendors that offer software-oriented or CPU-driven approaches. Each day the Fortinet FortiGuard Labs use one of the most effective and proven artificial intelligence (AI) and machine learning systems in the industry to process and analyze more than 100 billion events daily, and send actionable real-time threat intelligence to customers.

  The Fortinet Security Fabric (Attachment 1) is at the heart of the Fortinet security strategy that delivers security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. It is a platform organically built around a common operating system and management framework to enable broad visibility, seamless integration and interoperability between critical security elements, and granular control and automation.

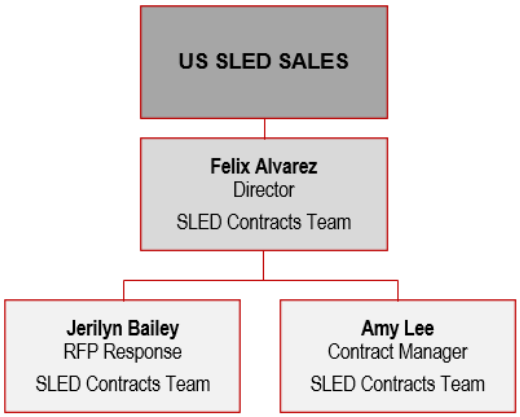
  Fortinet has its products tested by the industry's most prominent and impartial third party performance and effectiveness testing organizations and our products have achieved consistent positive test results! Fortinet is commitment to cybersecurity innovation and excellence and Fortinet has been recognized as a LEADER three years in a row on four Gartner® Magic Quadrant™ reports.

  The Fortinet market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and media outlets worldwide. Fortinet is proud to count the majority of Fortune 500 companies among its satisfied customers. See Fortinet's Corporate Brochure (Attachment 2) for additional information.

- Company's Dun & Bradstreet (D&B) number.

  Our D&B Number is 040806445.

- Company's organizational chart of those individuals that would be involved in the contract.



- Corporate office location.
  - List the number of sales and services offices for states being bid in solicitation.

If awarded a contract in response to this RFP, Fortinet's entire line of products and services will be available to NCPA customers in all 50 states, the District of Columbia, and in US territories.

Fortinet sells its products and services through its established distribution channel that includes US-based distributors and resellers across the country. Fortinet provides pre-sales guidance and account management to our customers, distributors, and resellers through strategically placed district sales teams.

SALES OFFICES	COVERAGE
North Central District	ND, SD, NE, MN, IA, WI, IL
Ohio Valley District	MI, IN, OH, KY
New England District	Upstate NY, VT, NH, ME, MA, CT, RI
Northeast District	PA, NJ, NYC, DE
Mid-Atlantic District	WV, VA, TN, NC, SC
Florida/ Georgia District	FL, GA
South Central District	KS, MO, OK, AR, LA, MS, AL
Texas District	TX
California District	CA
West District	WA, OR, MT, ID, WY, NV, UT, CO, AZ, NM
Great Lakes District	WI, IL

Fortinet supports its products and services through the following Regional Technical Assistance Centers and Supply Depots:

OFFICES	LOCATIONS
Regional Technical Assistance Centers*	Plano, Texas Ottawa, Ontario ON Canada Burnaby, BC Canada
Supply Depots	Fortinet maintains 35 hardware storage facilities worldwide and 200 regional equipment depots.

** Fortinet uses a follow-the-sun model for technical assistance. Support will therefore be provided to NCPA customers from these North American centers during regular business hours and will roll over to TACs in other regions after hours (except in the case of contracts/purchase orders that require support from US TACs only).*

- List the names of key contacts at each with title, address, phone and e-mail address.

Responsibility	Name and Contact Information
RFP Response	Jerilyn Bailey Public Sector Contracts Manager baileyj@fortinet.com
Contract Management and Reporting	Amy Lee Public Sector Contracts Manager leea@fortinet.com
Contract Administration	Fortinet SLED Contracts Team SLED_Contracts@fortinet.com

- Define your standard terms of payment.

If awarded a contract in response to this RFP, customers will make payments directly to the Fortinet-approved distributor or reseller with whom the order was placed. Payment terms are net thirty (30) days from the date of the invoice. Late fees may be charged on all amounts not paid when due at the rate of one and one half percent (1.5%) per month or the highest rate permitted by law, whichever is lower.

- Who is your competition in the marketplace?

The table below provides information on our competitors per segment within the market:

Market Segment	Competitors
Enterprise Firewalls Definition: *Purpose -built appliances for securing enterprise networks. Able to support single-enterprise firewall deployments and large and/or complex deployments. The ability to provide virtual versions for the data center is now an expectation as is the ability to deploy in cloud environments.*	• Palo Alto • Check Point
Unified Threat Management Devices Definition: *Multifunctional network security products designed for small to medium-size organizations (100 to 1,000 employees). Typical capabilities provided include enterprise firewall, intrusion prevention, remote access, secure web/email gateway, routing and wan connectivity.*	• Check Point • Sophos
Next-Generation Firewall Definition. *Deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and to bring in intelligence from outside the firewall*.	• Barracuda • Checkpoint • Cisco • Forcepoint • Palo Alto • Sophos • SonicWall • WatchGuard
Data Center Security Gateway (DCSG) Definition. *DCSGs protects data center servers and the applications that run on them (i.e., web servers, mail servers, DNS servers, application servers, etc.) from potential threats. They converge data center firewall and data center intrusion prevention system technologies and perform access control and deep packet inspection to protect server applications from remote attacks.*	• Juniper • Palo Alto • Cisco

Data Center Intrusion Protection Systems (DCIPS) Definition. *Data center network security devices are deployed to protect servers and applications hosted in the data center. Data center intrusion prevention systems (DCIPS) are deployed at critical points in the network. Their role is to identify and block sophisticated threats against web servers, application servers, and database servers without false positives or degradation of network performance.*	• Juniper • McAfee • Trend Micro
Breach Detection (or Advanced Threat Protection) Definition. *These products provide enhanced detection of advanced malware, zero-day attacks, and targeted attacks that could bypass defenses such as next generation firewalls, intrusion prevention systems, intrusion detection systems, antivirus/endpoint protection (including host IPS), and secure web gateways.*	• Trend Micro • Lastline • Check Point
Web Application Firewalls Definition: *Physical or virtual appliance to protect public and internal web applications, whether deployed on premise or remotely hosted. Should protect against a variety of attacks including injection attacks and application-layer denial of service (DoS).*	• F5 • Imperva • Akamai
Wired and Wireless LAN Access Infrastructure Definition: *This market segment consists of vendors supplying wired and wireless networking hardware and software that enables devices to connect to the enterprise wired LAN or Wi-Fi network.*	• Riverbed • Dell EMC • Juniper • New H3C
Advanced Endpoint Protection (AEP) Definition: *AEP products protect endpoints from a multitude of attack threat vectors targeting a very dynamic enterprise class endpoint attack surface. They should also be resistant to evasion techniques and provide low false positive results.*	• Sentinel One • McAfee • Symantec • Cylance • Trend Micro • ESET

- Provide Annual Sales for last 3 years broken out into the following categories:
  - Cities / Counties
  - K-12
  - Higher Education
  - Other government agencies or nonprofit organizations

- Provide the revenue that your organization anticipates each year for the first three (3) years of this agreement.

- What differentiates your company from competitors?

Fortinet offers the most cost effective networking and cyber security solutions in the market providing the best total cost per protected megabit of traffic as tested by independent sources such as NSS labs. Recognized as a leader by technology research firm Garter, Fortinet lowers total cost of ownership by integrating cyber security into all of our products and simplifying administration through near single-pane of glass management. With the added benefit of our integrated FortiGuard Services, Fortinet provides near real-time effectiveness to cyber threats by ensuring that all threats known and unknown can be identified and mitigated as close to the source and as quickly as possible. In summary, Fortinet products protect your entire digital attack surface more effectively, at lower total cost and can be managed more efficiently than any other product on the market today.

- Describe how your company will market this contract if awarded.

Fortinet provides marketing on its products and services throughout the sales lifecycle. Fortinet's marketing strategy is geared towards nurturing our relationships with our customers to grow business, lock in brand loyalty, and foster customer advocacy for our solutions.

Fortinet has created marketing materials specifically geared toward public sector customers and intends to market the NCPA contract in a multitude of ways to reach our intended audience. Each of these avenues will promote awareness of the NCPA contract and highlight our products and services.

Fortinet understands the importance of marketing NCPA contracts to public sector customers and during the life of the contract Fortinet's marketing plan will include the following:

	Website advertisement and social media awareness campaigns.
	General media exposure in various digital and print publications.
	Sales team trainings to inform them of the contract and teach them how to promote the contract to our customers.
	Customer outreach activities from our sales team, within their respective areas of operation or vertical focus, to get our current customers acquainted with the NCPA contract.
	Conference calls and webinars to inform and educate potential new customers on the value proposition of the NCPA contract.
	Participation in advisory councils, sponsored regional events, and attendance at annual public sector tradeshows to promote NCPA contract awareness.

Fortinet will also provide support on marketing efforts executed by our authorized resellers. While each reseller will operate their own marketing program, Fortinet will assist its authorized resellers by providing in depth information on its products and will also outline the value proposition of the NCPA contract.

- Describe how you intend to introduce NCPA to your company.

Fortinet understands that effective communication to our sales team regarding the awarded NCPA contract is crucial to our success as a NCPA contract holder. Our SLED Contracts Team will take the lead on introducing the NCPA contract to Fortinet Sales Account Managers responsible for sales to the SLED market. This team will also introduce the contract to Channel Managers responsible for recruiting and supporting resellers who serve this market.

Upon contract award, our SLED Contracts Team will utilize the following methods to introduce NCPA to our company:

- Group Conference Calls
- Training Webinars
- Training Materials
- Ongoing Contract Use Monitoring
- Ongoing Contract Promotion

- Describe your firm's capabilities and functionality of your on-line catalog / ordering website.

Since Fortinet uses a channel model for sales, we do not have, nor do we intend to implement, an ordering website for the NCPA contract. What we do provide is our website (www.fortinet.com) that SLED customers can use to find detailed information on our products and services and to access technical support. In addition, we have a contracts site (www.fortinet.com/resources/sled-contracts-grants) within our website that will have a dedicated page for the NCPA contract that will provide information on how to use our NCPA contract and assists customers to connect with qualified and capable authorized resellers who serve their geographic market.

- Describe your company's Customer Service Department (hours of operation, number of service centers, etc.)

To provide effective support to a customer base that spans the globe, Fortinet has made it a priority to build a best-in class global infrastructure for technical assistance and warranty/maintenance support. This infrastructure features three global Centers of Expertise (COE) supplemented by regional Technical Assistance Centers (TACs). It also includes 35 hardware storage facilities worldwide and 200 regional depots.

This infrastructure provides the foundation for FortiCare Services (Attachment 3), the program through which we will provide support for products covered by warranty and, thereafter, maintenance support for products covered by a FortiCare maintenance plan.

- Green Initiatives (if applicable)
  - As our business grows, we want to make sure we minimize our impact on the Earth's climate. We are taking every step we can to implement innovative and responsible environmental practices throughout NCPA to reduce our carbon footprint, reduce waste, energy conservation, ensure efficient computing and much more. To that effort we ask respondents to provide their companies environmental policy and/or green initiative.

Fortinet is focused on reducing the environmental footprint of our customers by innovating highly efficient, integrated appliances and cloud-based security solutions.

Product Design & Life Cycle Management: When it comes to our products, environmental sustainability is a top priority at the design stage and throughout the entire product lifecycle. This includes product energy use and efficiency, the safety of material inputs required for proper product operations (e.g., chemicals, water), ease of reuse and recycling, and proper disposal at the end of life.

All of our products comply with all globally recognized product environmental compliance directives and regulations. We are also working to eliminate PVC from Product Packaging.

Regarding compliance with the WEEE directive, Fortinet requires its distributors and resellers worldwide to perform an environmentally friendly, WEEE-compliant collection of discarded products at no charge to the user.

Energy Management: Years of dedicated innovation and the development of the industry's only security-focused processors have allowed Fortinet to integrate multiple security and networking functions into a single, energy-efficient platform. This has resulted in appliances that use less power, space, and cooling. In addition, Fortinet's family of proprietary secure processor units (SPUs) are built for power and efficiency.

As a result, Fortinet produces the most energy-efficient appliances in the industry, helping our customers and partners reduce their environmental footprint. These advanced security solutions consume as much as 3X fewer resources than traditional appliances, helping lower the ecological impact of data centers, which consume around 2% of all energy worldwide.

Climate Change and Environmental Management: Fortinet takes its responsibility to the environment seriously. We have pledged to reduce our impact on climate change and have taken steps to mitigate our environmental footprint.

From an operations standpoint, we are committed to driving an environmentally low impact business, including energy, air pollution, waste, and water, across our globally distributed offices, facilities, and data centers. This includes monitoring and managing our impact on the climate from owned operations and supply chains related to greenhouse gas emissions, energy efficiency, and renewable energy procurement; the ability to recover from and manage risks, such as the impact of more extreme weather events and natural disasters; and transition risks, such as the increasing cost of energy and customer expectations related to energy and emissions.

Fortinet invests in renewable electricity and sustainable projects. All of Fortinet’s owned facilities around the world run on 100% renewable electricity. Furthermore, Fortinet's recent headquarters expansion is a state-of-the-art 172,000-square-foot and LEED-Gold certified. This all electric, net-zero facility has implemented multiple energy efficiency measures including solar panels and radiant cooling, which uses 30% less energy than a standard building and conserves 76,800 gallons of water annually. Fortinet also incentivizes employees at its headquarters to reduce their environmental footprint by providing onsite solar-powered EV Charging Stations, preferred parking spaces for sustainable energy vehicles, and installed bike racks.

Fortinet works with supply chain and logistics service providers committed to ensuring the application and enforcement of environmental policies aimed at reducing air emissions and pollutions by promoting the use of clean fuels, transportation network optimization, and investing in fuel-saving technologies. We have local RMA depots in over 20 countries and central regional depots in North America, Europe, and Asia. These help us reduce transportation-related emissions by minimizing shipping distances and consolidating shipments, collecting defective products at centralized locations, performing local repairs, and recycling defective units in compliance with local regulations.

- Anti-Discrimination Policy (if applicable)
  - Describe your organizations’ anti-discrimination policy.

At Fortinet we believe everyone should be treated equally regardless of race, sex, gender identification, sexual orientation, national origin, native language, religion, age, disability, marital status, citizenship, genetic information, pregnancy, or any other characteristic protected by law. In support of this Fortinet strives to provide a work environment where everyone can work

together comfortably and productively. Each individual has the right to work in a professional atmosphere that promotes equal opportunity and prohibits discriminatory practices, including sexual and other forms of prohibited harassment. Fortinet's anti-discrimination and anti-harassment policy prohibits all forms of harassment based on an individual's race, color, religion, sex (including pregnancy, childbirth, breastfeeding, and related medical condition), age, national origin, disability, sexual orientation, gender (including gender identity and expression), marital status (including registered domestic partnership status), civil union status, familial status, ancestry, physical or mental disability, medical condition, genetic information or traits, caregiver status, citizenship status, Civil Air Patrol status, military or veteran status, status as a victim of domestic violence, assault, or stalking, or any other characteristic protected by applicable federal, state, or local laws. This policies applies to all employees of Fortinet, including supervisors and managers, as well as to customers, partners, vendors, and any other third parties we do business with.

- Vendor Certifications (if applicable)
  - Provide a copy of all current licenses, registrations and certifications issued by federal, state and local agencies, and any other licenses, registrations or certifications from any other governmental entity with jurisdiction, allowing respondent to perform the covered services including, but not limited to, licenses, registrations, or certifications. Certifications can include M/WBE, HUB, and manufacturer certifications for sales and service.

Fortinet is committed to innovation and excellence and we are our proud to meet and exceed a wide range of national, regional, and international requirements, and our solutions and services have earned the respect of independent third-party testing labs around the world. Fortinet's submitted Product Certifications Brochure (Attachment 4) outlines the certifications our products have received and contains access to our Certifications Resource Center that serves as the repository for product compliance reports, certifications, and independent validation results.

In addition to the product certifications outlined in our Product Certifications Brochure, we wish to make you aware of the following certifications:

- ISO 9001:2015, Quality Management System: the scope of this certificate covers the design, development, and manufacture of Network Security Products and the Delivery of Associated Security Services and Support.
- Our price list includes selected products that are certified for compliance under the US National Information Assurance Program Common Criteria Evaluation and Validation Scheme (CCEVS).
- Our price list includes selected products certified by the National Institute of Standards and Technology for compliance with FIPS 140-2, Security Requirements for Cryptographic Modules.

TAB 5 PRODUCTS AND SERVICES

Respondent shall perform and provide these products and/or services under the terms of this agreement. The supplier shall assist the end user with making a determination of their individual needs.

Fortinet's goal, if awarded a contract, is to establish a productive and mutually beneficial partnership with the Texas Region 14 ESC and NCPA. To accomplish this, Fortinet is proud to offer our entire line of products and services in response to this RFP and Fortinet agrees to work closely with customers utilizing the awarded contract to assist them in determining their individual needs for IT Security Products and Data Protection Solutions.

Warranty

Proposal should address the following warranty information:

- Applicable warranty and/or guarantees of equipment and installations including any conditions and response time for repair and/or replacement of any components during the warranty period.
- Availability of replacement parts
- Life expectancy of equipment under normal use
- Detailed information as to proposed return policy on all equipment

Fortinet's submitted EULA and Warranty Terms (Attachment 5) complies with this requirement.

Products

- Vendor shall provide equipment, materials and products that are new unless otherwise specified, of good quality and free of defects

As the manufacturer Fortinet understands that good quality is critical to satisfying customers and retaining their loyalty. In our endeavor to continuously achieve this objective, Fortinet has actively participated in third-party audits and testing since we first opened our doors. Through these third-party audits and testing we validate our design and development processes which help us guarantee that our products and solutions meet and exceed a wide range of regional, national, and international standard quality requirements.

Construction

- Vendor shall perform services in a good and workmanlike manner and in accordance with industry standards for the service provided.

Fortinet is committed to ensuring that all of our products and services consistently exceed industry benchmarks and remain compliant with public sector regulatory frameworks and standards.

The following is a list of suggested (but not limited to) IT Security Products and Data Protection Solutions categories. List all categories along with manufacturer that you are responding with:

- Security Threat Intelligence Products and Services
- Security Information and Event Management (SIEM)
- Managed Security Services
- Security awareness training
- Security Consulting Services
- Content Filtering
- Anti-Virus / Anti-Spam
- Network Forensics / Real – Time Monitoring
- Network Access Control
- Firewalls
- ~~Network Storage / Archiving~~

- Wireless Networks
- ~~Bandwidth Management~~
- Networking Hardware
- Application Security
- Cloud Security
- Email Security ~~and Archiving~~
- Data Protection
  - ~~Backup~~
  - ~~Cloud Backup~~
  - Risk Assessments
  - Encryption and Pseudonymization
  - Data Destruction
- Data Loss Prevention (DLP)
- Consulting Services

We have edited the list above to show which suggested capabilities Fortinet's products and services address. Described at a high level, our products and services include:

- **Physical and virtual cybersecurity appliances** (hardware appliances and perpetual software licenses) that provide functional capabilities in these areas:
  - Network Security
  - Cloud Security
  - Web Application Security
  - Email Security
  - Advanced Threat Protection
  - Secure Unified Access
  - Endpoint Security
  - Management and Analytics
- **FortiGuard Security Subscriptions** (term software licenses) for:
  - Application control
  - Intrusion prevention
  - Antivirus
  - Sandboxing
  - IP reputation and anti-botnet
  - Web filtering
  - Web application security
  - Credential stuffing defense
  - Database security
  - Virus outbreak protection
  - Content disarm and reconstruction
  - Security rating
- **Hardware and software maintenance plans (as described in Section 4.12)**
  - 8 x 5 support
  - 24 x 7 support
  - 360o support (24 x 7 support with proactive monitoring and health checks)
  - Premium support services
- **Professional Services**
  - Remote engineering support
  - Onsite engineering support
- **Training**
  - Onsite courses
  - Self-paced courses
  - Instructor-led virtual courses

TAB 6 REFERENCES

Provide at least ten (10) customer references for products and/or services of similar scope dating within the past three (3) years. Please provide a range of references across all eligible government entity groups including K-12, higher education, city, county, or non-profit entities.

All references should include the following information from the entity:

- Entity Name
- Contact Name and Title
- City and State
- Phone
- Email
- Years Serviced
- Description of Services
- Annual Volume

NCPA also accepts Procurated review scores to evaluate relationships with their customers. Vendors without a current Procurated score will be rated based solely on the references provided, and will not be penalized for lack of Procurated scoring. To find out your company's Procurated score please go to https://www.procurated.com.

TAB 7 PRICING

Please submit price list electronically via our online Bonfire portal (pricing can be submitted as Discount off MSRP, cost plus, etc). Products, services, warranties, etc. should be included in price list. Prices submitted will be used to establish the extent of a respondent's products and services (Tab 5) that are available and also establish pricing per item.

Price lists must contain the following:

- Product name and part number (include both manufacturer part number and respondent part number if different from manufacturers).
- Description
- Vendor's List Price
- Percent Discount to NCPA participating entities

Fortinet's submitted price list complies with this requirement.

Not To Exceed Pricing

- NCPA requests pricing be submitted as "not to exceed pricing" for any participating entity.
- The awarded vendor can adjust submitted pricing lower but cannot exceed original pricing submitted for solicitation.
- NCPA requests that vendor honor lower pricing for similar size and scope purchases to other members.

Fortinet will ensure that all resellers authorized to sell through an awarded NCPA contract understand that the prices on our price list are "not to exceed prices"; however, since size and scope are only two of multiple factors that can impact the price of a customer's unique security solution, we cannot honor the request to honor lower pricing for similar size and scope purchases.

TAB 8 VALUE ADDED PRODUCTS AND SERVICES

Include any additional products and/or services available that vendor currently performs in their normal course of business that is not included in the scope of the solicitation that you think will enhance and add value to this contract for Region 14 ESC and all NCPA participating entities.

If awarded a NCPA contract in response to this RFP, as value adds to our submitted offer of our entire line of products and services, Fortinet is proud to offer the following two **FREE** additional programs:

1. FORTINET'S FREE GRANT SUPPORT PROGRAM

Public sector organizations face unique challenges in defending against the constant changing cyber threats landscape and most public sector agencies lack adequate funding to purchase the protection resources they need. Federal and state grants can provide valuable funding to the public sector that initiates or expands purchases they otherwise would not be able to.

Through Fortinet's **free** Grant Support Program, Fortinet helps empower public sector customers to find and access grant funding to make their mission critical projects happen!

Our **FREE** Grant Support Program helps public sector agencies by:

a. Providing comprehensive grants information for entities that are understaffed or lack experience with grant applications and don't know where to start.

   Finding and applying for grants can be a daunting and complicated task, but doing so is imperative right now for the public sector since currently there are billions of dollars in funding available for cybersecurity projects and solutions. Our Grant Support Program was created to assist entities successfully find and apply for grants.

   Our Grants Support Program consultants provide extensive grant resources and services, such as: in-depth grant research, grant funding availability reports, and grant application development assistance. We of course cannot guarantee funding, but we will do everything we can to assist an entity in submitting a successful grant application.

b. Identifying all available grant funding for technology-rich projects.

   With a few specifics about an entity's needs, our Grants Support Program consultants will develop customized reports on funding opportunities that are the best fit for the project.

   The reports will identify the most relevant funders based on the project type, the organization type (or types, in the case of a consortium project), and the geographic location where the project will be deployed. Then our consultants will review their findings with the entity on a conference call scheduled at the entity's convenience.

   We will also continually monitor granting sources and will provide notifications to the entity when grants or funding opportunities are released that best serve their project.

c. Providing customized consultation services that help develop project ideas and even expand cybersecurity modernization initiatives.

   Grants tend to be awarded to projects that address a clearly identified need, either for a specific population or a defined geographic community. In addition, fundable projects

should have measurable objectives and a compelling reason for including the security technology needed to achieve those objectives.

Our Grants Support Program consultants will help entities clarify and articulate their specific technology needs, assist in the development of measurable objectives, and provide input on other elements that might further strengthen the entities project proposal, application or other information required by the grant.

Grants Support Program Frequently Asked Questions:

- ***What's the benefit of utilizing Fortinet's Grants Support Program?***

Our Grants Support Program is designed to help public sector entities overcome financial barriers that prevent our customers from purchasing Fortinet's cybersecurity solutions. We provide free support by assigning a grant expert who works with the entity throughout the entire grants process.

- ***What entities are eligible to receive grant funds?***

The public sector entities listed below are generally eligible to apply for federal or state grant funding opportunities as long as the project identified on the entity's submitted grant application meets the grant requirements.

Government Organizations
- State governments
- County governments
- City or township governments
- Special district governments
- Native American tribal governments

Education Organizations
- Independent school districts
- Public and state controlled institutions of higher education
- Private institutions of higher education

Public Housing Organizations
- Public housing authorities
- Native American housing authorities

- ***What are the top grant funding streams for cybersecurity?***

Thousands of grant opportunities are made available each year in the US, providing billions of dollars in funding. Of course, not all of these opportunities are technology-friendly; however the following grant opportunities have been identified as the top funding streams for cybersecurity:

- Infrastructure Investment and Jobs Act, including State and Local Cybersecurity Grant Program ($550B)
- Stimulus funding from the American Rescue Plan ($1.9T)
- Tying into energy and climate funding available through Inflation Reduction Act ($369B)
- Tying into annual funding available from 26 federal grant-making agencies ($700B)

- ***Where do I get more information on Fortinet's Grants Support Program?***

For more information on this program, please email us at: sled_capture@fortinet.com.

2. FORTINET'S FREE SECURITY AWARENESS AND TRAINING PROGRAM

The US education sector is in the midst of a cyber crisis. The shift to cloud-based virtual learning during COVID-19 created the perfect storm for threat actors to capitalize on. Education IT departments, already weathering a shortage of physical resources, funding, and staffing, unexpectedly faced an even greater challenge. Without the human resources and advanced solutions to secure vulnerabilities in their networks, K-12 school districts and higher-ed institutions became easy targets.

In July 2022, Fortinet participated in the White House National Cyber Workforce and Education Summit where Fortinet participated in important discussions around solutions to help address this significant challenge facing the cybersecurity industry in the United States. As a result of these discussions, Fortinet announced its commitment to expand its existing Information Security Awareness and Training program to make it available to all K-12 school districts and systems across the United States for **FREE**!

Schools that take advantage of this **free** offering will be training their staff and faculty with skillsets and knowledge that could prevent them from falling victim to popular threat methods, such as social engineering attempts, reducing the likelihood of a security breach. Fortinet's Security Awareness and Training program was developed by Fortinet's award-winning Training Institute. With content incorporating threat intelligence insights from FortiGuard Labs, this training arms faculty and staff with the latest knowledge, guidance, and tips to make smarter choices when confronted by cyberattacks and other security risks.

Security Awareness and Training Frequently Asked Questions:

- ***What key benefits will K-12 school districts and systems gain from participating in this training?***

  By participating in our Security Awareness and Training K-12 school districts and systems will:

  - Have trained faculty and staff that will prevent or recognize and report potential security threats whether in an email, online, or in a physical setting.
  - Satisfy city, county, state, and national requirements for security and awareness training across major frameworks (this training aligns to the National Institute of Standards and Technology framework -NIST 800-50 and NIST 800-16).
  - Prevent the impact of breaches caused by faculty and staff errors and/or poor judgement.
  - Ensure faculty and staff are properly trained on data privacy and security, and are motivated to protect personally identifiable information and other sensitive data.

- ***How comprehensive is this free training program?***

  We are offering the premium version of our Information Security Awareness and Training program **free** of charge to K-12 school districts and systems. This premium training consists of 23 Base Modules, 10 Re-engagement Modules and 18 Reinforcement Modules and is delivered in multiple formats, including video, text, audio, imagery, and animation, which appeals to different learning styles to ensure that the training is understood and applied.

- ***Where do I get more information on this training?***

  For more information on this program visiting our website at http://fortinet.com/K12trainingUS, or to register for this training, please email us at k12trainingUS@fortinet.com.

TAB 9 REQUIRED DOCUMENTS

- Federal Funds Certifications
- Clean Air and Water Act & Debarment Notice
- Contractors Requirements
- Required Clauses for Federal Assistance by FTA
- Federal Required Signatures
- Antitrust Certification Statements Texas Government Code § 2155.005
- State Notice Addendum

FEDERAL FUNDS CERTIFICATIONS

Participating Agencies may elect to use federal funds to purchase under the Master Agreement. The following certifications and provisions may be required and apply when a Participating Agency expends federal funds for any purchase resulting from this procurement process. Pursuant to 2 C.F.R. § 200.326, all contracts, including small purchases, awarded by the Participating Agency and the Participating Agency's subcontractors shall contain the procurement provisions of Appendix II to Part 200, as applicable.

APPENDIX II TO 2 CFR PART 200

(A) Contracts for more than the simplified acquisition threshold currently set at $250,000, which is the inflation adjusted amount determined by the Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) as authorized by 41 U.S.C. 1908, must address administrative, contractual, or legal remedies in instances where contractors violate or breach contract terms, and provide for such sanctions and penalties as appropriate.

- Pursuant to Federal Rule (A) above, when a Participating Agency expends federal funds, the Participating Agency and Offeror reserves all rights and privileges under the applicable laws and regulations with respect to this procurement in the event of breach of contract by either party.

(B) Termination for cause and for convenience by the grantee or subgrantee including the manner by which it will be effected and the basis for settlement. (All contracts in excess of $10,000)

- Pursuant to Federal Rule (B) above, when a Participating Agency expends federal funds, the Participating Agency reserves the right to terminate any agreement in excess of $10,000 resulting from this procurement process in the event of a breach or default of the agreement by Offeror as detailed in the terms of the contract

(C) Equal Employment Opportunity. Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 CFR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

- Pursuant to Federal Rule (C) above, when a Participating Agency expends federal funds on any federally assisted construction contract, the equal opportunity clause is incorporated by reference herein.

(D) Davis-Bacon Act, as amended (40 U.S.C. 3141-3148). When required by Federal program legislation, all prime construction contracts in excess of $2,000 awarded by non-Federal entities must include a provision for compliance with the Davis-Bacon Act (40 U.S.C. 3141-3144, and 3146-3148) as supplemented by Department of Labor regulations (29 CFR Part 5, "Labor Standards Provisions Applicable to Contracts Covering Federally Financed and Assisted Construction"). In accordance with the statute, contractors must be required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. In addition, contractors must be required to pay

wages not less than once a week. The non-Federal entity must place a copy of the current prevailing wage determination issued by the Department of Labor in each solicitation. The decision to award a contract or subcontract must be conditioned upon the acceptance of the wage determination. The non- Federal entity must report all suspected or reported violations to the Federal awarding agency. The contracts must also include a provision for compliance with the Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States"). The Act provides that each contractor or subrecipient must be prohibited from inducing, by any means, any person employed in the construction, completion, or repair of public work, to give up any part of the compensation to which he or she is otherwise entitled. The non-Federal entity must report all suspected or reported violations to the Federal awarding agency.

- Pursuant to Federal Rule (D) above, when a Participating Agency expends federal funds during the term of an award for all contracts and subgrants for construction or repair, offeror will be in compliance with all applicable Davis-Bacon Act provisions
- Any Participating Agency will include any current and applicable prevailing wage determination in each issued solicitation and provide Offeror with any required documentation and/or forms that must be completed by Offeror to remain in compliance the applicable Davis-Bacon Act provisions.

(E) Contract Work Hours and Safety Standards Act (40 U.S.C. 3701-3708). Where applicable, all contracts awarded by the non-Federal entity in excess of $100,000 that involve the employment of mechanics or laborers must include a provision for compliance with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5). Under 40 U.S.C. 3702 of the Act, each contractor must be required to compute the wages of every mechanic and laborer on the basis of a standard work week of 40 hours. Work in excess of the standard work week is permissible provided that the worker is compensated at a rate of not less than one and a half times the basic rate of pay for all hours worked in excess of 40 hours in the work week. The requirements of 40 U.S.C. 3704 are applicable to construction work and provide that no laborer or mechanic must be required to work in surroundings or under working conditions which are unsanitary, hazardous or dangerous. These requirements do not apply to the purchases of supplies or materials or articles ordinarily available on the open market, or contracts for transportation or transmission of intelligence.

- Pursuant to Federal Rule (E) above, when a Participating Agency expends federal funds, offeror certifies that offeror will be in compliance with all applicable provisions of the Contract Work Hours and Safety Standards Act during the term of an award for all contracts by Participating Agency resulting from this procurement process.

(F) Rights to Inventions Made Under a Contract or Agreement. If the Federal award meets the definition of "funding agreement" under 37 CFR §401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

- Pursuant to Federal Rule (F) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (F) above

(G) Clean Air Act (42 U.S.C. 7401-7671q.) and the Federal Water Pollution Control Act (33 U.S.C. 1251-1387), as amended— Contracts and subgrants of amounts in excess of $150,000 must contain a provision that requires the non- Federal award to agree to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401- 7671q) and the Federal Water Pollution Control Act as amended (33 U.S.C. 1251- 1387). Violations must be reported to the Federal awarding agency and the Regional Office of the Environmental Protection Agency (EPA).

- Pursuant to Federal Rule (G) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency member resulting from this procurement process, the offeror agrees to comply with all applicable requirements as referenced in Federal Rule (G) above

(H) Debarment and Suspension (Executive Orders 12549 and 12689)—A contract award (see 2 CFR 180.220) must not be made to parties listed on the government wide exclusions in the System for Award Management (SAM), in accordance with the OMB guidelines at 2 CFR 180 that implement Executive Orders 12549 (3 CFR part 1986 Comp., p. 189) and 12689 (3 CFR part 1989 Comp., p. 235), “Debarment and Suspension.” SAM Exclusions contains the names of parties debarred, suspended, or otherwise excluded by agencies, as well as parties declared ineligible under statutory or regulatory authority other than Executive Order 12549.

- Pursuant to Federal Rule (H) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term of an award for all contracts by Participating Agency resulting from this procurement process, the offeror certifies that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency. If at any time during the term of an award the offeror or its principals becomes debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation by any federal department or agency, the offeror will notify the Participating Agency

(I) Byrd Anti-Lobbying Amendment (31 U.S.C. 1352)—Contractors that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award.

- Pursuant to Federal Rule (I) above, when federal funds are expended by Participating Agency, the offeror certifies that during the term and after the awarded term of an award for all contracts by Participating Agency resulting from this procurement process, the

offeror certifies that it is in compliance with all applicable provisions of the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352). The undersigned further certifies that:

- No Federal appropriated funds have been paid or will be paid for on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with the awarding of a Federal contract, the making of a Federal grant, the making of a Federal loan, the entering into a cooperative agreement, and the extension, continuation, renewal, amendment, or modification of a Federal contract, grant, loan, or cooperative agreement.
- If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying”, in accordance with its instructions.
- The undersigned shall require that the language of this certification be included in the award documents for all covered sub-awards exceeding $100,000 in Federal funds at all appropriate tiers and all subrecipients shall certify and disclose accordingly.

RECORD RETENTION REQUIREMENTS FOR CONTRACTS INVOLVING FEDERAL FUNDS

When federal funds are expended by Participating Agency for any contract resulting from this procurement process, offeror certifies that it will comply with the record retention requirements detailed in 2 CFR § 200.334. The offeror further certifies that offeror will retain all records as required by 2 CFR § 200.334 for a period of three years after grantees or subgrantees submit final expenditure reports or quarterly or annual financial reports, as applicable, and all other pending matters are closed.

CERTIFICATION OF COMPLIANCE WITH THE ENERGY POLICY AND CONSERVATION ACT

When Participating Agency expends federal funds for any contract resulting from this procurement process, offeror certifies that it will comply with the mandatory standards and policies relating to energy efficiency which are contained in the state energy conservation plan issued in compliance with the Energy Policy and Conservation Act (42 U.S.C. 6321 et seq.; 49 C.F.R. Part 18).

CERTIFICATION OF COMPLIANCE WITH BUY AMERICA PROVISIONS

To the extent purchases are made with Federal Highway Administration, Federal Railroad Administration, or Federal Transit Administration funds, offeror certifies that its products comply with all applicable provisions of the Buy America Act and agrees to provide such certification or applicable waiver with respect to specific products to any Participating Agency upon request. Participating Agencies will clearly identify whether Buy America Provisions apply in any issued solicitation. Purchases made in accordance with the Buy America Act must still follow the applicable procurement rules calling for free and open competition.

CERTIFICATION OF ACCESS TO RECORDS

Offeror agrees that the Inspector General of the Agency or any of their duly authorized representatives shall have access to any non-financial documents, papers, or other records of offeror that are pertinent to offeror's discharge of its obligations under the Contract for the purpose of making audits, examinations, excerpts, and transcriptions. The right also includes timely and reasonable access to offeror's personnel for the purpose of interview and discussion relating to such documents. This right of access will last only as long as the records are retained.

CERTIFICATION OF APPLICABILITY TO SUBCONTRACTORS

Offeror agrees that all contracts it awards pursuant to the Contract shall be bound by the foregoing terms and conditions.

CLEAN AIR AND WATER ACT AND DEBARMENT NOTICE

By the signature below (Under Federal Required Signatures), I, the Vendor, am in compliance with all applicable standards, orders or regulations issued pursuant to the Clean Air Act of 1970, as Amended (42 U.S. C. 1857 (h), Section 508 of the Clean Water Act, as amended (33 U.S.C. 1368), Executive Order 117389 and Environmental Protection Agency Regulation, 40 CFR Part 15 as required under OMB Circular A-102, Attachment O, Paragraph 14 (1) regarding reporting violations to the grantor agency and to the United States Environment Protection Agency Assistant Administrator for the Enforcement.

I hereby further certify that my company has not been debarred, suspended or otherwise ineligible for participation in Federal Assistance programs under Executive Order 12549, “Debarment and Suspension”, as described in the Federal Register and Rules and Regulations.

CONTRACTOR REQUIRMENTS

Contractor Certification
Contractor's Employment Eligibility
By entering the contract, Contractor warrants compliance with the Federal Immigration and Nationality Act (FINA), and all other federal and state immigration laws and regulations. The Contractor further warrants that it is in compliance with the various state statues of the states it is will operate this contract in.

Participating Government Entities including School Districts may request verification of compliance from any Contractor or subcontractor performing work under this Contract. These Entities reserve the right to confirm compliance in accordance with applicable laws.

Should the Participating Entities suspect or find that the Contractor or any of its subcontractors are not in compliance, they may pursue any and all remedies allowed by law, including, but not limited to: suspension of work, termination of the Contract for default, and suspension and/or debarment of the Contractor. All costs necessary to verify compliance are the responsibility of the Contractor.

The offeror complies and maintains compliance with the appropriate statutes which requires compliance with federal immigration laws by State employers, State contractors and State subcontractors in accordance with the E-Verify Employee Eligibility Verification Program.

Contractor shall comply with governing board policy of the NCPA Participating entities in which work is being performed.

Fingerprint & Background Checks
If required to provide services on school district property at least five (5) times during a month, contractor shall submit a full set of fingerprints to the school district if requested of each person or employee who may provide such service. Alternately, the school district may fingerprint those persons or employees. An exception to this requirement may be made as authorized in Governing Board policy. The district shall conduct a fingerprint check in accordance with the appropriate state and federal laws of all contractors, subcontractors or vendors and their employees for which fingerprints are submitted to the district. Contractor, subcontractors, vendors and their employees shall not provide services on school district properties until authorized by the District.

The offeror shall comply with fingerprinting requirements in accordance with appropriate statutes in the state in which the work is being performed unless otherwise exempted.

Contractor shall comply with governing board policy in the school district or Participating Entity in which work is being performed.

Business Operations in Sudan, Iran
In accordance with A.R.S. 35-391 and A.R.S. 35-393, the Contractor hereby certifies that the contractor does not have scrutinized business operations in Sudan and/or Iran.

REQUIRED CLAUSES FOR FEDERAL ASSISTANCE PROVIDED BY FTA

ACCESS TO RECORDS AND REPORTS

Contractor agrees to:

a) Maintain all non-financial books, records, accounts and reports required under this Contract for a period of not less than two (2) years after the date of termination or expiration of this Contract or any extensions thereof except in the event of litigation or settlement of claims arising from the performance of this Contract, in which case Contractor agrees to maintain same until the FTA Administrator, the U.S. DOT Office of the Inspector General, the Comptroller General, or any of their duly authorized representatives, have disposed of all such litigation, appeals, claims or exceptions related thereto.

b) Permit any of the foregoing parties to inspect all non-financial work, materials, and other data and records that pertain to the Project, and to audit the non-financial books, records, and accounts that pertain to the Project and to reproduce by any means whatsoever or to copy excerpts and transcriptions as reasonably needed for the purpose of audit and examination. The right of access detailed in this section continues only as long as the records are retained.

FTA does not require the inclusion of these requirements of Article 1.01 in subcontracts.

CIVIL RIGHTS / TITLE VI REQUIREMENTS

1) Non-discrimination. In accordance with Title VI of the Civil Rights Act of 1964, as amended, 42 U.S.C. § 2000d, Section 303 of the Age Discrimination Act of 1975, as amended, 42 U.S.C. § 6102, Section 202 of the Americans with Disabilities Act of 1990, as amended, 42 U.S.C. § 12132, and Federal Transit Law at 49 U.S.C. § 5332, Contractor or subcontractor agrees that it will not discriminate against any employee or applicant for employment because of race, color, creed, national origin, sex, marital status age, or disability. In addition, Contractor agrees to comply with applicable Federal implementing regulations and other applicable implementing requirements FTA may issue that are flowed to Contractor from Awarding Participating Agency.

2) Equal Employment Opportunity. The following Equal Employment Opportunity requirements apply to this Contract:

   a. Race, Color, Creed, National Origin, Sex. In accordance with Title VII of the Civil Rights Act, as amended, 42 U.S.C. § 2000e, and Federal Transit Law at 49 U.S.C. § 5332, the Contractor agrees to comply with all applicable Equal Employment Opportunity requirements of U.S. Dept. of Labor regulations, “Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor, 41 CFR, Parts 60 et seq., and with any applicable Federal statutes, executive orders, regulations, and Federal policies that may affect construction activities undertaken in the course of this Project. Contractor agrees

to take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without regard to their race, color, creed, national origin, sex, marital status, or age. Such action shall include, but not be limited to, the following: employment, upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation; and selection for training, including apprenticeship. In addition, Contractor agrees to comply with any implementing requirements FTA may issue that are flowed to Contractor from Awarding Participating Agency.

b. Age. In accordance with the Age Discrimination in Employment Act (ADEA) of 1967, as amended, 29 U.S.C. Sections 621 through 634, and Equal Employment Opportunity Commission (EEOC) implementing regulations, "Age Discrimination in Employment Act", 29 CFR Part 1625, prohibit employment discrimination by Contractor against individuals on the basis of age, including present and prospective employees. In addition, Contractor agrees to comply with any implementing requirements FTA may issue that are flowed to Contractor from Awarding Participating Agency.

c. Disabilities. In accordance with Section 102 of the Americans with Disabilities Act of 1990, as amended (ADA), 42 U.S.C. Sections 12101 *et seq.*, prohibits discrimination against qualified individuals with disabilities in programs, activities, and services, and imposes specific requirements on public and private entities. Contractor agrees that it will comply with the requirements of the Equal Employment Opportunity Commission (EEOC), "Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act," 29 CFR, Part 1630, pertaining to employment of persons with disabilities and with their responsibilities under Titles I through V of the ADA in employment, public services, public accommodations, telecommunications, and other provisions.

d. Segregated Facilities. Contractor certifies that their company does not and will not maintain or provide for their employees any segregated facilities at any of their establishments, and that they do not and will not permit their employees to perform their services at any location under the Contractor's control where segregated facilities are maintained. As used in this certification the term "segregated facilities" means any waiting rooms, work areas, restrooms and washrooms, restaurants and other eating areas, parking lots, drinking fountains, recreation or entertainment areas, transportation, and housing facilities provided for employees which are segregated by explicit directive or are in fact segregated on the basis of race, color, religion or national origin because of habit, local custom, or otherwise. Contractor agrees that a breach of this certification will be a violation of this Civil Rights clause.

3) Solicitations for Subcontracts, Including Procurements of Materials and Equipment. In all solicitations, either by competitive bidding or negotiation, made by Contractor for work to be performed under a subcontract, including procurements of materials or leases of equipment, each potential subcontractor or supplier shall be notified by Contractor of Contractor's obligations under this Contract and the regulations relative to non-discrimination on the grounds of race, color, creed, sex, disability, age or national origin.

4) Sanctions of Non-Compliance. In the event of Contractor's non-compliance with the non-discrimination provisions of this Contract, Public Agency shall impose such Contract sanctions as it or the FTA may determine to be appropriate, including, but not limited to: 1) Withholding of payments to Contractor under the Contract until Contractor complies, and/or; 2) Cancellation, termination or suspension of the Contract, in whole or in part.

Contractor agrees to include the requirements of this clause in each subcontract financed in whole or in part with Federal assistance provided by FTA, modified only if necessary to identify the affected parties.

DISADVANTAGED BUSINESS PARTICIPATION

This Contract is subject to the requirements of Title 49, Code of Federal Regulations, Part 26, "*Participation by Disadvantaged Business Enterprises in Department of Transportation Financial Assistance Programs"*, therefore, it is the policy of the Department of Transportation (DOT) to ensure that Disadvantaged Business Enterprises (DBEs), as defined in 49 CFR Part 26, have an equal opportunity to receive and participate in the performance of DOT-assisted contracts.

1) Non-Discrimination Assurances. Contractor or subcontractor shall not discriminate on the basis of race, color, national origin, or sex in the performance of this Contract. Contractor shall carry out all applicable requirements of 49 CFR Part 26 in the award and administration of DOT-assisted contracts. Failure by Contractor to carry out these requirements is a material breach of this Contract, which may result in the termination of this Contract or other such remedy as public agency deems appropriate. Each subcontract Contractor signs with a subcontractor must include the assurance in this paragraph. (See 49 CFR 26.13(b)).

2) Prompt Payment. Contractor is required to pay each subcontractor performing Work under this prime Contract for satisfactory performance of that work no later than thirty (30) days after Contractor's receipt of payment for that Work from public agency. In addition, Contractor is required to return any retainage payments to those subcontractors within thirty (30) days after the subcontractor's work related to this Contract is satisfactorily completed and any liens have been secured. Any delay or postponement of payment from the above time frames may occur only for good cause following written approval of public agency. This clause applies to both DBE and non-DBE subcontractors. Contractor must promptly notify public agency whenever a DBE subcontractor performing Work related to this Contract is terminated or fails to complete its Work, and must make good faith efforts to engage another DBE subcontractor to perform at least the same amount of work. Contractor may not terminate any DBE subcontractor and perform that Work through its own forces, or those of an affiliate, without prior written consent of public agency.

3) DBE Program. In connection with the performance of this Contract, Contractor will cooperate with public agency in meeting its commitments and goals to ensure that DBEs shall have the maximum practicable opportunity to compete for subcontract work, regardless of whether a contract goal is set for this Contract. Contractor agrees to use good faith efforts to carry out a policy in the award of its subcontracts, agent agreements, and procurement contracts which will, to the fullest extent, utilize DBEs consistent with the efficient performance of the Contract.

ENERGY CONSERVATION REQUIREMENTS

Contractor agrees to comply with mandatory standards and policies relating to energy efficiency which are contained in the State energy conservation plans issued under the Energy Policy and Conservation Act, as amended, 42 U.S.C. Sections 6321 *et seq.* and 41 CFR Part 301-10.

FEDERAL CHANGES

Contractor shall at all times comply with all applicable FTA regulations, policies, procedures and directives, listed directly or by reference in the Contract between Public Agency and the FTA, and those applicable regulatory and procedural updates that are communicated to Contractor by Public Agency, as they may be amended or promulgated from time to time during the term of this contract. Contractor's failure to so comply shall constitute a material breach of this Contract.

INCORPORATION OF FEDERAL TRANSIT ADMINISTRATION (FTA) TERMS

The provisions include, in part, certain Standard Terms and Conditions required by the U.S. Department of Transportation (DOT), whether or not expressly set forth in the preceding Contract provisions. All contractual provisions required by the DOT and applicable to the scope of a particular Contract awarded to Contractor by a Public Agency as a result of solicitation, as set forth in the most current FTA Circular 4220.1F, published February 8th, 2016, are hereby incorporated by reference. Anything to the contrary herein notwithstanding, all FTA mandated terms shall be deemed to control in the event of a conflict with other provisions contained in this Contract. Contractor agrees not to knowingly perform any act, knowingly fail to perform any act, or refuse to comply with any reasonable public agency requests that would directly cause public agency to be in violation of the FTA terms and conditions.

NO FEDERAL GOVERNMENT OBLIGATIONS TO THIRD PARTIES

Agency and Contractor acknowledge and agree that, absent the Federal Government's express written consent and notwithstanding any concurrence by the Federal Government in or approval of the solicitation or award of the underlying Contract, the Federal Government is not a party to this Contract and shall not be subject to any obligations or liabilities to agency, Contractor, or any other party (whether or not a party to that contract) pertaining to any matter resulting from the underlying Contract.
Contractor agrees to include the above clause in each subcontract financed in whole or in part with federal assistance provided by the FTA. It is further agreed that the clause shall not be modified, except to identify the subcontractor who will be subject to its provisions.

PROGRAM FRAUD AND FALSE OR FRAUDULENT STATEMENTS

Contractor acknowledges that the provisions of the Program Fraud Civil Remedies Act of 1986, as amended, 31 U.S.C. §§ 3801 et seq. and U.S. DOT regulations, "Program Fraud Civil Remedies," 49 CFR Part 31, apply to its actions pertaining to this Contract. Upon execution of the underlying Contract, Contractor certifies or affirms, to the best of its knowledge, the truthfulness and accuracy of any statement it has made, it makes, it may make, or causes to me

made, pertaining to the underlying Contract or the FTA assisted project for which this Contract Work is being performed.

In addition to other penalties that may be applicable, Contractor further acknowledges that if it makes, or causes to be made, a false, fictitious, or fraudulent claim, statement, submission, or certification, the Federal Government reserves the right to impose the penalties of the Program Fraud Civil Remedies Act of 1986 on Contractor to the extent the Federal Government deems appropriate.

Contractor also acknowledges that if it makes, or causes to me made, a false, fictitious, or fraudulent claim, statement, submission, or certification to the Federal Government under a contract connected with a project that is financed in whole or in part with Federal assistance originally awarded by FTA under the authority of 49 U.S.C. § 5307, the Government reserves the right to impose the penalties of 18 U.S.C. § 1001 and 49 U.S.C. § 5307 (n)(1) on the Contractor, to the extent the Federal Government deems appropriate.

Contractor agrees to include the above clauses in each subcontract financed in whole or in part with Federal assistance provided by FTA. It is further agreed that the clauses shall not be modified, except to identify the subcontractor who will be subject to the provisions.

FEDERAL REQUIRED SIGNATURES

Offeror certifies compliance with all provisions, laws, acts, regulations, etc. as specifically noted in the pages above. It is further acknowledged that offeror agrees to comply with all federal, state, and local laws, rules, regulations and ordinances as applicable.

Offeror	Fortinet, Inc.
Address	899 Kifer Road
City/State/Zip	Sunnyvale, CA 94086
Authorized Signature	Jocelyn Bailey
Date	11/15/2022

ANTITRUST CERTIFICATION STATEMENTS
TEXAS GOVERNMENT CODE § 2155.005

I affirm under penalty of perjury of the laws of the State of Texas that:

(1) I am duly authorized to execute this contract on my own behalf or on behalf of the company, corporation, firm, partnership or individual (Company) listed below;

(2) In connection with this bid, neither I nor any representative of the Company has violated any provision of the Texas Free Enterprise and Antitrust Act, Tex. Bus. & Comm. Code Chapter 15;

(3) In connection with this bid, neither I nor any representative of the Company has violated any federal antitrust law; and

(4) Neither I nor any representative of the Company has directly or indirectly communicated any of the contents of this bid to a competitor of the Company or any other company, corporation, firm, partnership or individual engaged in the same line of business as the Company.

Company Name	Fortinet, Inc.
Address	899 Kifer Road
City/State/Zip	Sunnyvale, CA 94086
Telephone Number	(850) 728-6504
Fax Number	N/A
Email Address	baileyj@fortinet.com
Printed Name	Jerilyn Bailey
Title	Public Sector Contracts Manager
Authorized Signature	Jerilyn Bailey

STATE NOTICE ADDENDUM

The National Cooperative Purchasing Alliance (NCPA), on behalf of NCPA and its current and potential participants to include all county, city, special district, local government, school district, private K-12 school, higher education institution, state, tribal government, other government agency, healthcare organization, nonprofit organization and all other Public Agencies located nationally in all fifty states, issues this Request for Proposal (RFP) to result in a national contract.

For your reference, the links below include some, but not all, of the entities included in this proposal:

http://www.usa.gov/Agencies/State_and_Territories.shtml

https://www.usa.gov/local-governments

ATTACHMENTS

1. Fortinet Security Fabric
2. Fortinet Corporate Brochure (Q3 2022 – Convergence of Networking and Security)
3. Fortinet Support Services
4. Fortinet Product Certifications Brochure
5. Fortinet EULA and Warranty

INTERACTIVE INFOGRAPHICS

Icons on this document link to additional information

Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Security-Driven Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protect LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

Linksys HomeWRK
Enterprise networking solution for remote and hybrid workers

FortiSASE
Scalable, Simple, and Secure Access for Remote Workforce

FortiProxy
Enforce internet compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiDDoS
Machine-learning quickly inspects traffic at layers 3, 4, and 7.

FortiCWP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during unexpected network downtime

FortiMail
Secure mail gateway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

Zero Trust Access

FortiNAC
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

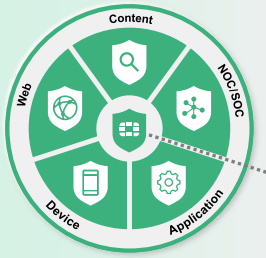
FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiConnect
Simplified guest access, BYOD, and policy management

FortiGuard Threat Intelligence

Powered by FortiGuard Labs



Threat Map

LABS

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
SaaS w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage, and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOps Tools & Scripts
Fortinet & community-driven

Fabric API Integrations
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC as a Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

FortiCare Support Services

FortiCare Essentials
15% of hardware, FG-80 & below

FortiCare Premium* 20% of hardware

FortiCare Elite** 25% of hardware*

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for FortiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

Free Assessments
Validate existing network controls for NGFW, Email, and SD-WAN

FortiOS
The Heart of the Fortinet Security Fabric

FortiCamera
Centrally-managed HDTV-quality security coverage reliability

FortiFone
Robust IP Phones w/ HD Audio with centralized management

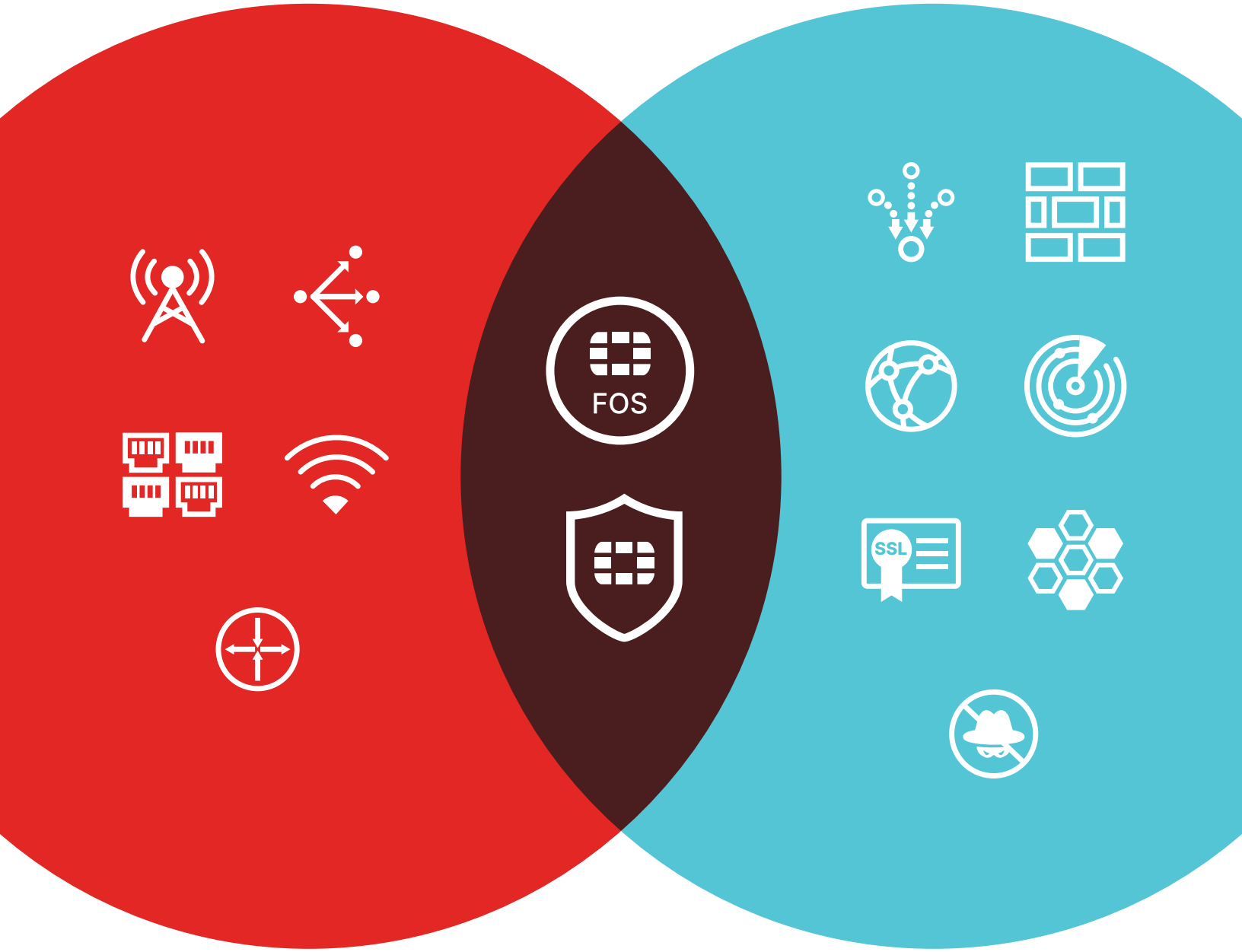
Revised June 1, 2022

FORTINET

Q3 / 2022

Convergence of Networking and Security

Digital Security, everywhere you need it.



FORTINET

FY 2021 Results

Revenue: $3.34 B

Billings: $4.18 B

Q2 2022 Results

Revenue: $1.030 B

Billings: $1.304 B

Op. Margin (GAAP): 19.0%

EPS (GAAP): $0.21/share

Cash + Investments: $1.943 B

Market Cap: $44.6 B (As of June 30, 2022)

Customers

595,000+

Cumulative Units Shipped

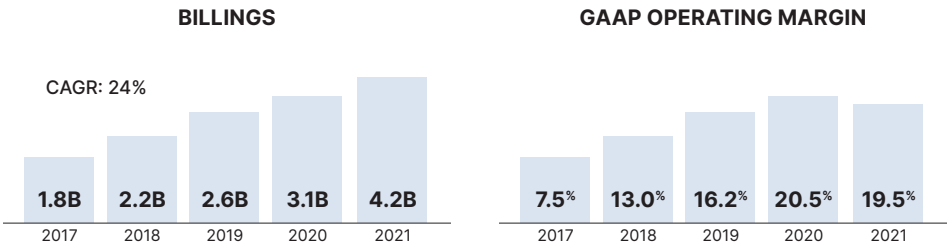
8.8+ Million

Headcount By Region

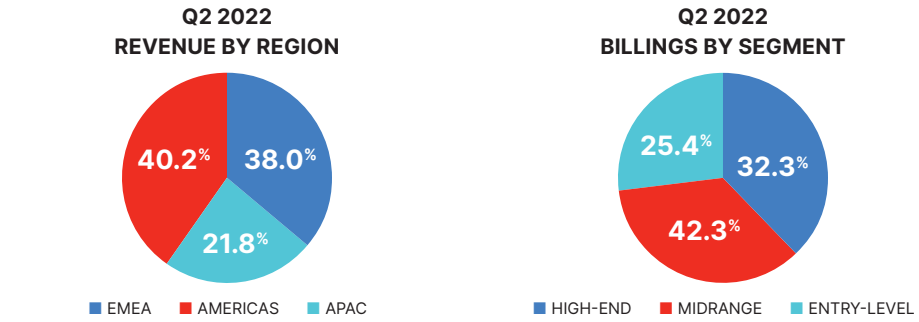
AMERICAS	US	3,413
	CANADA	2,162
	REST OF AMERICAS	784
EMEA	FRANCE	468
	UK	382
	REST OF EMEA	1,939
APAC	INDIA	585
	JAPAN	513
	REST OF APAC	1,262
TOTAL		11,508

ALL INFORMATION AS OF JUNE 30, 2022

Strong Growth in Annual Billings and Profitability

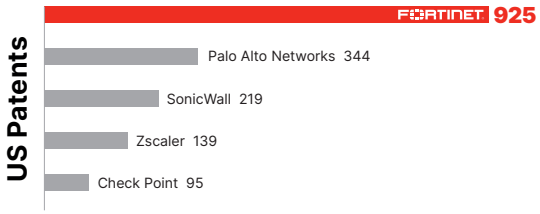


Highly Diversified Across Regions and Segments



Technological Leadership

Nearly 3X more patents than comparable Network Security companies



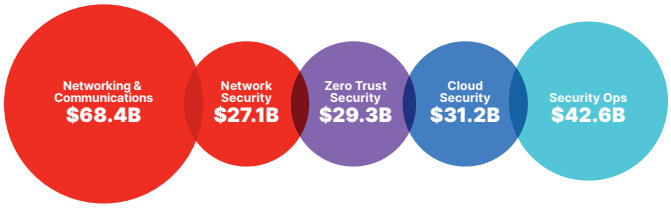
Source: US Patent Office, As of June 30, 2022

1279
Global Patents

925 U.S. Patents
354 International Patents
(247 Pending Patents)

A Large and Growing Total Available Market

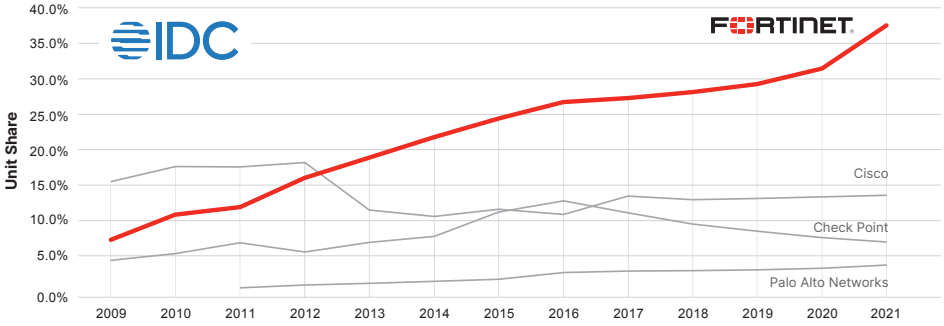
Total Addressable market of $138B in 2022 growing to $199B by 2026



Source: Fortinet estimates based on recent analyst research. 2026 opportunity shown.

The Most Deployed Network Security Solution

Over One-Third of All Firewall Shipments



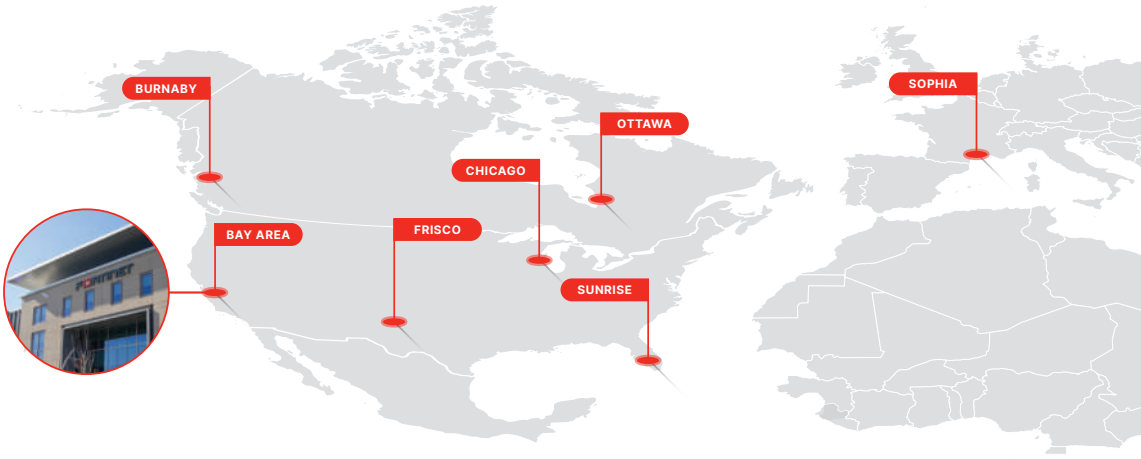
Source: IDC Worldwide Security Appliance Tracker, February 2022 (based on unit shipments of Firewall, UTM, and VPN appliances)

Fortinet – Making possible a digital world you can always trust

For over 20 years, Fortinet has been a driving force in the evolution of cybersecurity and the convergence of networking and security. Our network security solutions are the most deployed, most patented, and among the most validated in the industry. Our broad, complementary portfolio of cybersecurity solutions are built from the ground up with integration and automation in mind, enabling more efficient, self-healing operations and a rapid response to known and unknown threats.

Investing In Global Scale

- With over 2M square feet of real estate owned, we are investing in long term economic growth.
- Commitment to carbon neutral by 2030.
- New state-of-the-art LEED-Gold Certified 172,000 sqft HQ building.



Mission: to secure people, devices and data everywhere

Founded: October 2000

Headquarters: Sunnyvale, CA

Fortinet IPO (FTNT): November 2009

NASDAQ 100 and S&P 500:
Only cybersecurity company in both

Investing in the future **$10B** billings by **2025**

Corporate Social Responsibility

Learn more at **Fortinet.com/CSR**

A digital world you can always trust is essential to achieving just and sustainable societies. At Fortinet, we believe it is our corporate social responsibility to deliver on that vision by innovating sustainable security technologies, diversifying cybersecurity talent, and promoting responsible business across our value chain.

Innovative for a Safe Internet

Growing an Inclusive Cybersecurity Workforce

Respecting the Environment

Promoting Responsible Business

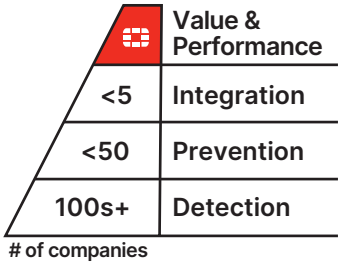
Key Fortinet Advantages

Security Fabric

Organically developed, highly integrated and automated cybersecurity platform

Security Processors

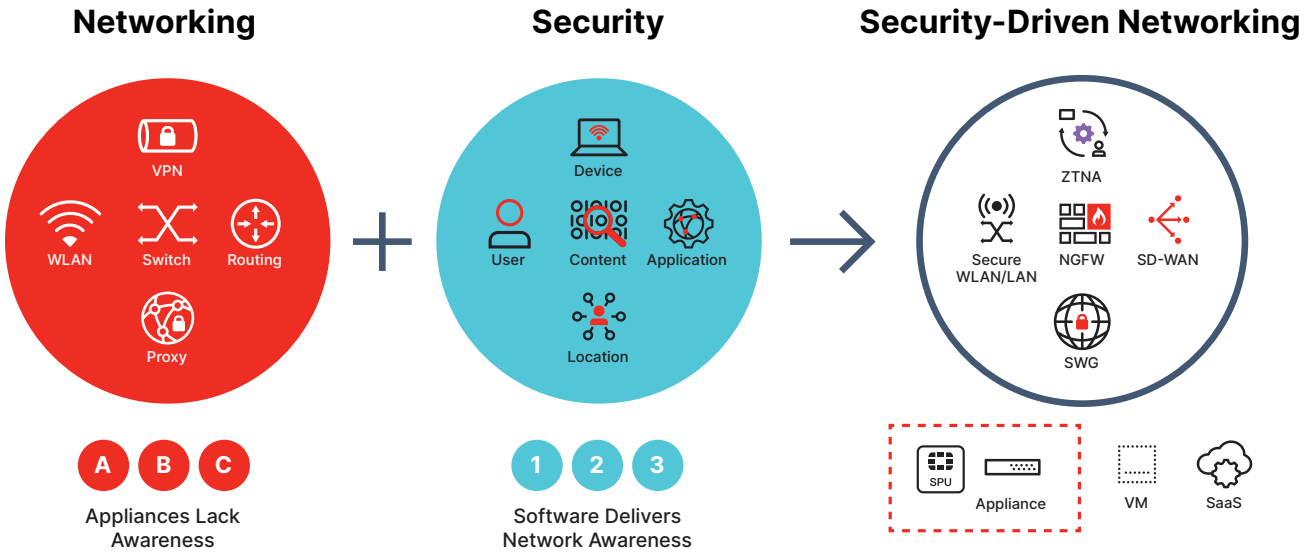
Superior NGFW and SD-WAN performance and efficiency



The only company to excel at all key stages of network security

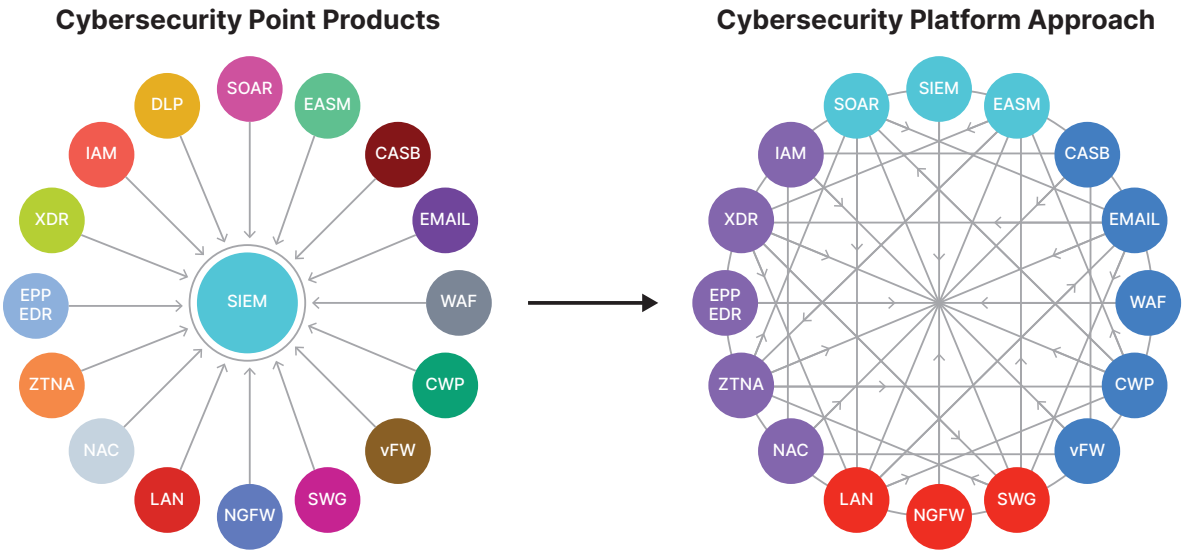
The Convergence of Networking and Security

Traditional networking lacks awareness of content, applications, users, devices, location and more. Organizations have overlaid security solutions on to the network later to account for this shortcoming — but doing so has led to increased management complexity, performance bottlenecks, poor user experience, and the potential introduction of new exploitable gaps or vulnerabilities. A better Security-driven Networking approach converges networking and security into a single, accelerated solution. A specially designed operating system and security processors work in concert to greatly improve network performance and security posture, adding greater awareness while also improving user experience, easing management complexity, and decreasing footprint and power consumption.



Consolidation of Vendors and Point Solutions to a Platform

Cybersecurity has traditionally been deployed one solution at time, in response to each emerging problem or challenge. However, individual security solutions — typically from a new vendor — are not designed to work well with the other deployed solutions. With meaningful levels of cross-vendor integration and automation proving difficult to achieve, management complexity is massively increased, and effective response to new threats is simply too slow. A more effective approach is to consolidate point product vendors into a cybersecurity platform, allowing for much tighter integration, increased automation, and a more rapid, coordinated, and effective response to threats across the network.



The Fortinet Security Fabric

The Fortinet Security Fabric is at the heart of the Fortinet security strategy. It is a platform organically built around a common operating system and management framework to enable broad visibility, seamless integration and interoperability between critical security elements, and granular control and automation.

Broad

visibility and protection of the entire digital attack surface to better manage risk.

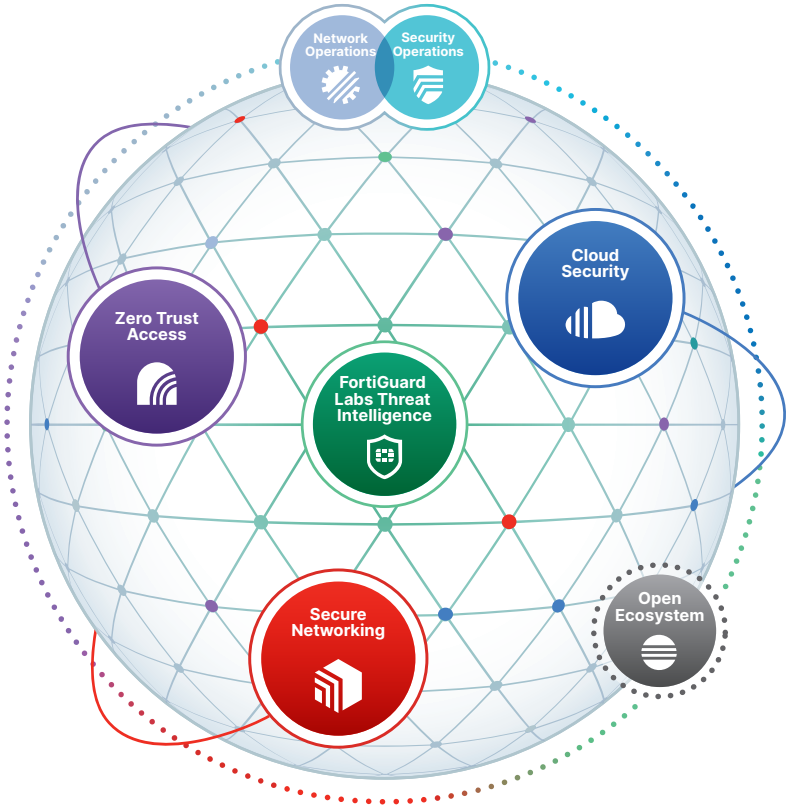
Integrated

solution that reduces management complexity and shares threat intelligence.

Automated

self-healing networks with AI-driven security for fast and efficient operations.

Learn more at **Fortinet.com/SecurityFabric**



Broad Portfolio of Solutions to Protect Your Digital Attack Surface

Zero Trust Access

- ZTNA Agent
- Authentication
- MFA/Token
- SASE

Secure Networking

- Network Firewall
- SD-WAN
- SD-Branch
- Web Proxy
- Wi-Fi
- Switching
- 5G/LTE
- Network Access Control
- And More...

Cloud Security

- Cloud-native Protection
- DevSecOps
- Cloud Firewall
- SD-WAN for Multi-cloud
- WAF
- Email Security
- ADC / GSLB
- Anti-DDOS
- CASB

Network Operations

- Network Management
- Network Orchestration
- Network Monitoring
- Cloud Management
- Digital Experience Monitoring

Security Operations

- Endpoint (EDR/ XDR)
- Automation: SIEM/ SOAR
- Managed SOC & MDR
- DRPS, EASM
- Deception

Open Ecosystem

- Fabric Connectors
- Fabric API
- Fabric DevOps
- Extended Ecosystem
- 490+ Open Ecosystem
- Integrations

LABS

FortiGuard Labs – Industry-leading Threat Intelligence

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. Partnering with law enforcement agencies, government organizations, and security vendor alliances worldwide to fight emerging global security risks. FortiGuard labs maintain real-time threat intelligence and innovative prevention tactics and tools across the Fortinet Security Fabric in three key categories:

Trusted ML and AI

Stop unknown faster with Powerful combination of actionable local learning and AI & ML models on large-scale cloud-driven data lakes.

Real-Time Threat Intelligence

Proactive security posture through continuous security updates based on in-house research and collaboration.

Threat hunting and Outbreak Alerts

Faster remediation with Alerts, analysis and detection, prevention and remediation tools including outbreaks.

Global Leadership & Collaboration: Cyber Threat Alliance, World Economic Forum, INTERPOL, NCI Agency

FortiGuard AI-Powered Security

Rich set of industry leading security capabilities unified into one security framework. Delivering coordinated, context-aware policy for hybrid deployments across networks, endpoints, and clouds. The services continually assess the risk and automatically adjust the prevention to counter known and unknown threats in real-time.

Market Leading Security as a Service

ML-enabled security, deployed close to the protected assets powered by FortiGuard Labs

Consistent Context Aware Policy

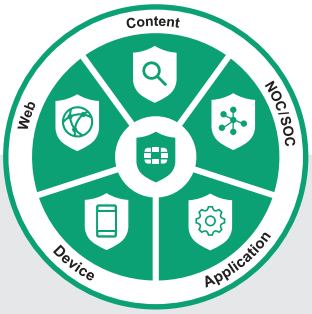
Centralized detection and prevention delivered from the cloud built for hybrid environments

Coordinated Real-Time Prevention

Continuously assess the risks and automatically respond and counter known and unknown threats

FortiGuard Security Integration Across the Security Fabric

		FortiGate (HW/VM/SASE)	Proxy	FortiTrust	XDR	FortiWeb	FortiMail	FortiADC	SOC Platforms	FortiNDR
Content Security	Antivirus	✓	✓	✓	✓	✓	✓	✓		✓
	IL SBX	✓			✓	✓	✓	✓		
	Credential Stuffing	✓	✓			✓		✓		
Web Security	URL	✓	✓	✓	✓	✓	✓			✓
	DNS	✓	✓	✓	✓					
	IP-REP	✓				✓	✓			
Device Security	DVC PROT	✓								
	IPS	✓	✓	✓						✓
	BOT/C2	✓	✓	✓	✓		✓			
Application Security	WAF SIG					✓				
	ANN							✓		
	AntiSpam						✓			
Soc Security	MITRE ATT&CK				✓				✓	
	Threat Hunting				✓				✓	
	Auto IR				✓				✓	
	Outbreak							✓	✓	✓
	IoC				✓				✓	✓



New in FortiOS 7.2

NEW FortiSandbox Inline Blocking

NEW IoT/ IT Device protection

NEW Dedicated IPS

NEW SOC as a Service

NEW Outbreak Detection

Enhanced Web Security

More FortiGuard subscription services are available across our broad Security Fabric portfolio of solutions

Learn more at **Fortinet.com/fortiguard**

FortiOS – The Foundation of the Security

Learn more at **Fortinet.com/fortiOS**

FortiOS is the foundation of the Fortinet Security Fabric, converging and consolidating many security and networking technologies and use cases into a simplified, single policy, and management framework.

What's New In FortiOS 7.2

FortiGate SD-WAN
Automated Overlay Orchestration and Large Scale Zero Touch Provisioning

FortiGate Firewall
FortiGate is the first next-generation firewall to support HTTP/3.0

SD-Branch
Automation, simplified Deployment, and Orchestration for Global Scale management

LAN Edge
Zero Touch Provisioning Campus and Large-Scale SD-Branch

ZTNA
Unified Policy Configuration in a Single GUI

FortiToken / FortiToken Cloud
Fido-based passwordless Authentication

SASE
Automated provisioning of ZTNA agents & Apps from FortiSASE

Identity
Zero Touch Provisioning Campus and Large-Scale SD-Branch

FortiTrust – Redefining the Future of Security Services

FortiTrust provides user-based licensing across all networks, endpoints and clouds

- **Access:** Add ZTNA to your FortiGate-based network.
- **Identity:** Cloud-based subscription across enterprise hybrid environments.

FortiCare – Expertise At Your Service

Learn more at **Fortinet.com/support**

FortiCare Services help thousands of organizations every year to get the most out of their Fortinet Security Fabric solutions. We have over 1,400 experts providing accelerated implementation, reliable assistance, and proactive care through advanced support and professional services to maximize your security and performance.

1400+ EXPERTS

24×7 TECHNICAL SUPPORT

23 GLOBAL SUPPORT CENTERS

Adopting new technologies is not a project with a start and a finish. Instead, it is a journey from design and implementation to optimization, operations, and ongoing management of the solution. Fortinet has you covered every step of the way, freeing up your resources to focus on your business needs.

Design
Business Alignment
- High-level design
- Low-level design
- Product-agnostic workshops

Deploy
Accelerated Implementation
- Migration
- Configuration
- Implementation
- Validation
- Knowledge Transfer

Operate
Reliable Assistance
- 24×7 Support
- Premium hardware replacement
- Technical account management
- Proactive Incident avoidance
- Dedicated resources

Optimize
Performance Excellence
- Health checks
- Software upgrade recommendation
- Incident readiness
- Penetration testing

Evolve
Personalized Care
- Product upgrade assistance
- Transformation readiness
- Migration & replacement
- Software upgrade

The SPU Advantage

Fortinet's Security Processors (SPUs) radically increase the speed, scale, efficiency and value of Fortinet solutions while greatly improving user experience, reducing footprint and power requirements. From entry-level to high-end solutions, SPU-powered Fortinet appliances deliver superior Security Compute Ratings versus industry alternatives.

Network Processor 7
NP7

Network Processors operate in-line to deliver unmatched performance for network functions and hyperscale for stateful firewall functions.

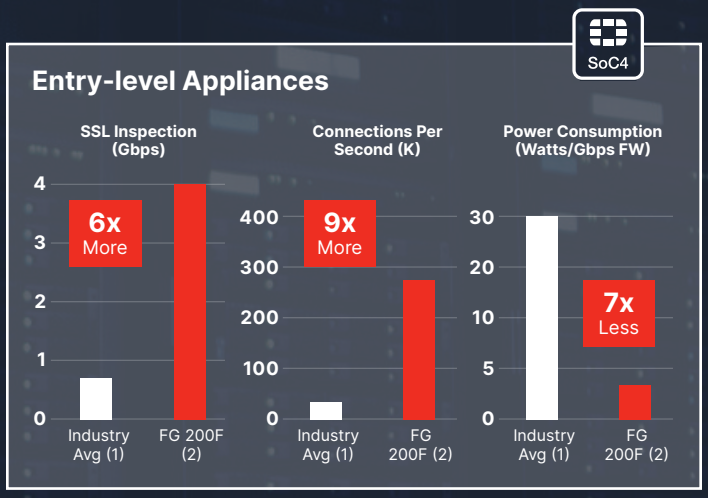
Content Processor 9
CP9

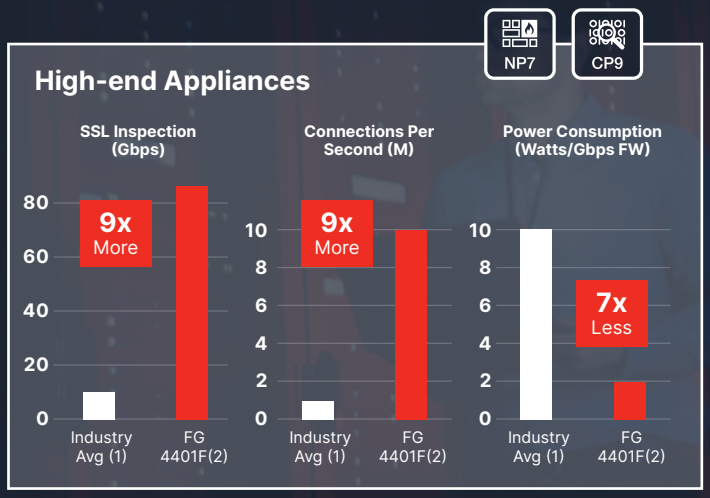
As a co-processor to the main CPU, Content Processors offload resource-intensive processing and drive content inspection to accelerate security functions.

System-on-a-Chip 4
SoC4

The System-on-a-Chip consolidates network and content processing, delivering fast application identification, steering, and overlay performance.

Security Compute Ratings are benchmarks that compare the performance metrics of Fortinet SPU-based next-generation firewalls to similarly priced solutions from vendors that utilize generic processors for networking and security.





[1] Industry average (entry-level) is calculated as the average of the similarly priced PAN-820, Cisco FPR-1120, Juniper SRX-345, and Check Point SG-3600. Industry average (high end) is calculated as the average of the similarly priced PAN-7050, Cisco FPR-9300, Juniper SRX-5400, and Check Point SG-28000. All data from public datasheets.
[2] Fortinet metrics from public datasheets.

New Product Spotlight: FortiGate 4800F series

Deliver ultra-high performance to secure Hyperscale data centers and 5G

Ultra-scalable and high-performance Security

Flexible, scalable dynamic, segmentation

Secure, ultra-high-performance DCI with 400G support

Specification	FortiGate 4801F[1]	Security Compute Rating	Industry Average[2]	PAN PA-5450[3]	Check Point Quantum 28000	Cisco FPR-4145	Juniper SRX-5400[4]
Firewall	2.4 Tbps	15x	158 Gbps	136.4 Gbps	145 Gbps	80 Gbps	270 Gbps
IPsec VPN	800 Gbps	19x	42 Gbps	34.8 Gbps	49 Gbps	23 Mbps	60 Gbps
Threat Prevention	70 Gbps	1.5x	46 Gbps	61.8 Gbps	30 Gbps	N/A	N/A
SSL Inspection	55 Gbps	5.5x	10 Gbps	N/A	N/A	10 Gbps	N/A
Concurrent Sessions	280M/1760M[2]	34x	51M	40M	32M	40M	91M
Connections per second	900K/25M[2]	19x	1.3M	1.45M	615K	1.5M	1.7M

Notes:
1. Fortinet: Enabled by a Hyperscale License
2. PAN: Calculated with 2xNC and 2xDPC cards, no services and support. PAN Application Firewall used as they don't publish stateful FW
3. Juniper: SRX5400E-B2

Training and Certifications

Fortinet NSE Certification Program

The Fortinet Network Security Expert (NSE) Certification Program is an 8-level training and assessment program designed for customers, partners, and employees to help close the cybersecurity skills gap. With over 840,000 security certifications to date, Fortinet delivers expert-level training in local languages in 136 countries and territories worldwide through our ecosystem of Authorized Training Centers, academic partners, and a variety of online options (many of them free of charge).

Fortinet Training & Education Partner Programs

The Fortinet Training Institute's ecosystem of public and private partnerships help Fortinet address the skills gap by increasing the access and reach of our cybersecurity certifications and training. The Academic Partner program works with academic institutions including K-12 and higher education. The Education Outreach program partners with industry, academia, government, and nonprofits to reach a broad population, in 94 countries and territories, while also focusing on recruiting women, minorities, veterans, and other underrepresented groups.

930,000+
CERTIFICATIONS

471
ACADEMIES PARTNERS

29
EDUCATION OUTREACH PARTNERS

Information Security Awareness
Learn about today's cyberthreats and how you can secure your information.

Security Associate
Learn about security solutions that have been created to address security problems faced by organizations.

Security Associate
Learn about the key Fortinet products and the cybersecurity problems they address.

Professional
Develop the knowledge required to manage the day-to-day configuration, monitoring, and operation of FortiGate devices to support corporate network security policies.

Analyst
Develop a detailed understanding of how to implement network security management and analytics.

Specialist
Develop an understanding of the Security Fabric products that augment FortiGate, providing deeper and more comprehensive network security.

Architect
Develop the knowledge required to integrate Fortinet products into network security solution deployment and administration.

Expert
Demonstrate the ability to design, configure, install, and troubleshoot a comprehensive network security solution in a live environment.

Learn more at **Fortinet.com/nse-training**

Figures as of June 30, 2022

New Fortinet Security Awareness and Training Service

The Security Awareness and Training service offers every organization the ability to further protect their critical digital assets from cyber threats by building employee cybersecurity awareness and creating a cyber-aware culture.

Free cybersecurity awareness and training for all U.S. School Districts

At the National Cyber Workforce and Education Summit at the White House on July 19, 2022, Fortinet announced it is offering a customized academic version of its Security Awareness and Training service free to all U.S school districts starting with more than 8 million staff and faculty. This offering is part of Fortinet's mission to help close the cybersecurity skills gap.

Our Pledge to Train 1 Million People by 2026

Fortinet has pledged to train 1 million people globally over 5 years through its Training Advancement Agenda (TAA) and Fortinet Training Institute programs to help close the cybersecurity skills gap. January 2022 marked the start of this five-year pledge that will use Fortinet's award-winning certification program content as the basis for meeting this goal. The Fortinet Training Institute has been recognized by various organizations for our contribution to excellence in cybersecurity training and certification as well as our many programs that help close the cybersecurity skills gap.

Our Global Partner Commitment

Fortinet is a channel-centric company that has created a large, global network of trusted advisors that customers can rely on to secure their digital transformation and strategically drive their business growth.

ENGAGE FORTINET PARTNER PROGRAM **60,000+** ACTIVE PARTNERS

The Engage Partner Program is designed to help partners built a valuable, highly-differentiated security practice that leverages the industry's best solutions to drive customer success. Fortinet's global partner program is driven by three basic concepts:

Growth Through Technology Differentiation

Fortinet's breadth of products are tightly integrated into one highly-automated, high-performing platform that spans endpoint, network, and cloud, and includes tools to easily connect with adjacent technologies.

Business Success with Proven Credibility

Fortinet's superior technology innovation and industry leading threat intelligence, alongside our customer ratings and independent analyst reports leadership validates and differentiates our partners' offerings.

Long-term, Sustained Growth

The Engage Partner Program offers sustained sales, marketing, and executive support so you can grow productive, predictable, and successful relationships. With drivers of growth built into the program, like our Specializations, we provide paths to expertise for solutions that are driving demand in the market — ensuring you are positioned for success.

- SPECIALIZATION: SD-WAN
- SPECIALIZATION: Zero Trust Access
- SPECIALIZATION: Security Operations
- SPECIALIZATION: Data Center
- SPECIALIZATION: Operational Technology
- SPECIALIZATION: Adaptive Cloud Security
- SPECIALIZATION: LAN Edge and SD-Branch

Analyst Recognition

Gartner — Magic Quadrants: 7
- Network Firewall
- SD-WAN
- WLAN/LAN
- Endpoint
- SIEM
- WAAP
- Indoor Location Services

Gartner — Market Guides: 8
- DEM
- VPN
- NAC
- EMAIL
- IRM
- XDR
- SOAR
- Indoor Location Services

Gartner — #1 in Critical Capabilities: 5

Network Firewall
- Data-Center Edge
- Distributed Edge

SD-WAN
- Security w/ SD-WAN
- Small Branch WAN
- Remote Workforce

Gartner — Peer Insights Customers' Choice: 4
- Network Firewall
- WLAN/LAN Access Infrastructure
- Email Security
- WAN Edge Infrastructure

Forrester — Waves: 4
- Enterprise Email Security
- ICS
- Endpoint Detection and Response
- Enterprise Firewalls

Forrester — Nowtechs: 5
- WAF
- All-In-One ZeroTrust Edge
- Software-Defined WAN
- Endpoint Detection and Response
- Enterprise EmailSecurity

Frost & Sullivan — Top Vendor & Leadership Awards: 6
- SD-WAN
- Critical Infrastructure
- SWG
- NAC
- WAN Edge Infrastructure
- North America Healthcare

IDG — Marketscape Leader & Major Player: 2
- Worldwide SD-WAN Infrastructure
- Modern Endpoint

Westlands Advisory — Platform Navigator: 1
- IT/OT Security Platform

Kuppingercole — Leadership Compass: 2
- SIEM
- ICS

GIGAOM — GIGAOM Radar: 2
- Security Service Access (SSA) - Forward Mover
- Zero-Trust Network Access (ZTNA) - Fast Mover

Gartner

Fortinet is recognized as a LEADER in 2 Gartner® 2021 Magic Quadrant™ Reports:

- **Network Firewalls**
- **WAN Edge Infrastructure**

Fortinet is also recognized in 4 additional Gartner 2021 Magic Quadrant Reports, including a wide range of technologies:

- **Web Application and API Protection**
- **SIEM**
- **Wired and WLAN**
- **Endpoint Protection Platforms**

And Fortinet is an 'Honorable Mention' in 2 additional Gartner 2020/2021 Magic Quadrant Reports:

- **Secure Web Gateway**
- **Indoor Location Services**

Learn more at **Fortinet.com/solutions/gartner-magic-quadrants**

Third Party Testing and Certifications

Fortinet submits its products for impartial, third party performance and effectiveness testing with the most prominent organizations in the industry, with consistent positive results.

Virus Bulletin

- Only vendor with all three VB100, VBSpam, and VBWeb certifications
- Highest "VBSpam+" rating

ICSA Labs

Certified in 5 technology areas:

- Anti-Malware Network
- Network Firewall
- IPsec VPN
- Web Application Firewall
- Advanced Threat Defense

AV Comparatives

- Antiphishing Approved

MITRE

100% Protection, 2 Years in a Row

- All Test Cases
- All Signature-Independent
- Top Analytical Detection

CUSTOMER RECOGNITION

Gartner Peer Insights Customers' Choice distinctions are based on the ratings of vendors by verified end-user professionals across a variety of industries and from locations around the world. These distinctions take into account both the number of end-user reviews a vendor receives, along with the overall ratings score a vendor receives from those end users.

Fortinet is proud to be named a Gartner Peer Insights Customers' Choice in several critical areas:

- **Network Firewalls**
- **Wired and Wireless LAN Access Infrastructure**
- **Email Security**
- **WAN Edge Infrastructure**

See our Gartner Peer Insights reviews and distinctions at ***www.gartner.com/reviews***

Gartner, Gartner Peer Insights 'Voice of the Customer': Network Firewalls, Peer Contributors, 9 April 2021

Gartner, Gartner Peer Insights 'Voice of the Customer': Wired and Wireless LAN Access Infrastructure, Peer Contributors, 12 May 2021

Gartner, Gartner Peer Insights 'Voice of the Customer': Email Security, Peer Contributors, 5 February 2021

Gartner, Gartner Peer Insights 'Voice of the Customer': WAN Edge Infrastructure, Peer Contributors, 5 February 2021

Fortinet secures over half a million enterprises, service providers, and government organizations around the world.

Alaska Airlines

5th largest airline in the United States.

HQ: United States

Region Stockholm

Sweden's largest regional health provider.

HQ: Sweden

SoftBank

SoftBank is a multinational conglomerate that aspires to drive towards digital transformation.

HQ: Japan

Checkers

A chain of double drive-thru restaurants in the United States. The company operates Checkers and Rally's restaurants in 28 states, and the District of Columbia.

HQ: United States

University of Birmingham

One of the UK's largest universities, the University of Birmingham is over 100 years old with over 30,000 students across the world.

HQ: United Kingdom

WeLab

Provider of online financial services to more than 42 million individual users and more than 300 corporate users in Hong Kong, Mainland China, and Indonesia.

HQ: Hong Kong

HUGHES

A global leader in managed services providing end-to-end fully managed cybersecurity, networking, and digital signage solutions tailored to the unique business requirements of today's enterprise.

HQ: United States

orange Business Services

Orange is one of the world's leading telecommunications operators and global provider of IT and telecommunication services.

HQ: France

macquarie CLOUD SERVICES

Provider of flexible hybrid IT solutions for business and government.

HQ: Austrailia

Visit Fortinet.com/Customers to see how many of our customers benefit from Fortinet solutions and the Fortinet Security Fabric.

FTNT Nasdaq Listed

Revision: Q2 / 2022 v2 07.06.22

FortiCare Services

Technical Support, Advanced Services, and Professional Services

Hit the ground running with new capabilities

Fast-track return on investment with streamlined migration and deployment

Get expert help when you need it

Accelerate incident resolution and maximize efficacy with 24×7 assistance from technical experts

Enhance your security with tailored guidance

Increase productivity and avoid incidents with operational reviews, account planning, and upgrade assistance

Confidence in Your Investment

Businesses are making huge investments in security and Fortinet Security Fabric technologies to provide essential services critical to securing their most valuable assets. Organizations often lack the in-house expertise or resources for initial deployment, product support, and ongoing operations. At Fortinet, we understand these challenges and provide FortiCare Services to thousands of organizations every year to address them.

We want organizations to feel confident that they are maximizing the value of their investments quickly and realizing efficiency and efficacy gains over time. Whether migrating to a Fortinet Next-Generation Firewall (NGFW), implementing software-defined wide-area networking (SD-WAN) to protect your branch locations, or automating security operations functions, we will work with you to match the proper services with your unique business needs. We are dedicated to your success and provide the expertise you need when you need it.

Services

FortiCare Support Services is per-device support services, and it provides customers access to over 1,400 experts to ensure efficient and effective operations and maintenance of their Fortinet capabilities. Global technical support is offered 24×7 with flexible add-ons, including enhanced service level agreements (SLAs) and premium hardware replacement through 200+ in-country depots.

Advanced Services is account-based services, and provides high-touch account management and business guidance through designated resources to meet the needs of enterprises and service providers. Additionally, Enterprise Support Agreements (ESAs) are available to simplify consumption of the services.

Expertise at Your Service

- 24×7 Global Support
- 1,400+ NSE and Industry Certified Global Resources
- 3 Regional Centers of Expertise
- 23 Support Centers
- 40 Regional Depots
- 200+ In-country Depots
- 4-hour Expedited Hardware Replacement Availability

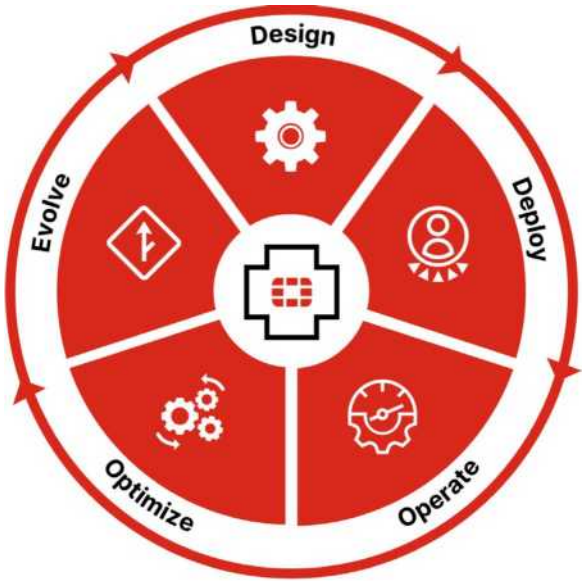
FortiCare Worldwide 24×7 Support

support.fortinet.com

Professional Services provides accelerated implementation and configuration optimization through QuickStart or custom engagements leveraging the services of highly skilled experts to promote first-time accuracy and avoid costly post-deployment issues.

The Journey

Adopting new technologies is not a project with a start and a finish. Instead, it is a journey from design and implementation to operations, optimization, and ongoing management of the solution. Fortinet has you covered every step of the way, freeing up your resources to focus on your business.



Feature Highlights: Technical Support

Organizations depend on Fortinet solutions to provide critical services. If any issues arise, they need to be addressed quickly to help ensure security and business continuity. Flexible support options help organizations maximize uptime, security, and performance according to the individual needs of each business.

Fortinet offers three different per-device support options to meet the needs of different devices, i.e., FortiCare Essential, FortiCare Premium, and FortiCare Elite. Organizations have the flexibility to buy different levels of service for different devices based on their needs.

FortiCare Essential

FortiCare Essential is the base-level service, and it is targeted toward devices that require a limited amount of support and can tolerate next-business-day, web-only response for critical as well as non-critical issues. This service is only offered to FortiGate models 8x and below and to low-end FortiWifi devices.

FortiCare Premium

FortiCare Premium is targeted toward devices that require 24×7×365 with one-hour response for critical issues and the next business-day response for non-critical issues.

FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

FortiCare Service Offerings

FortiCare Included Features	Per-device Service Options		
	FortiCare ESSENTIAL	FortiCare PREMIUM	FortiCare ELITE
RMA	Return and replace only	Advanced replacement (PRMA available)	Advanced replacement (PRMA available)
Web Support	✓	✓	✓
Telephone Support	—	✓	✓
Firmware Updates	✓	✓	✓
Asset Management Portal	✓	✓	✓
Response Time (Critical Issue)	Next business day	1 hour	15 mins
Response Time (Non-critical Issue)	Next business day	Next business day	2 business hours
Extended End-of-Engineering-Support (E-EoES) for Long Term Supported Firmware (LTS) of 18 months*	—	—	✓
Device Insights and Monitoring Portal (FortiCare Elite Portal)	—	—	✓

* Currently available for FortiGate only

FortiCare Services is provided by the support teams located in the three regional Technical Assistance Centers (TACs) and three regional Centers of Excellence (COE).

Fortinet Technical Assistance Centers

Regional COE:
- Vancouver
- Sophia Antipolis
- Kuala Lumpur

AMER Regional TAC:
- Ottawa
- Chicago
- Sunnyvale
- Plano
- Sunrise
- Mexico City
- Bogota
- Uberlandia

EMEA Regional TAC:
- Bangalore
- Dubai
- Frankfurt
- Prague
- Lisbon
- Tel Aviv

APAC Regional TAC:
- Beijing
- Sydney
- Seoul
- Tokyo
- Manila
- Singapore

Self-service Resources

For expedited answers, Fortinet maintains ample self-service resources to get you the answers you need, fast. All the answers to your questions are now in one place. The Fortinet community is a knowledge-sharing hub for customers, partners, Fortinet experts, and colleagues. The community is a place to collaborate, share insights and experiences, and get answers to questions.

community.fortinet.com

Feature Highlights: Advanced Services

For enhanced security and tailored guidance, FortiCare Advanced Services gives you direct assistance from technical experts who know your business and can help accelerate issue resolution. With designated account management and service delivery, you can focus on your business while we focus on your success.

Entitlements vary by level but can include:

Designated Advanced Technical Support	for focused resolution of incoming technical support issues.
Service Relationship Management	annual service and performance review. Quarterly operational review to cover technical ticket statistics, quality issues, overall ongoing ticket analysis, product life cycle, ongoing activity, and 90-day project planning.
Root Cause Analysis	of critital incidents (Priority-1 and Priority-2) related to Fortinet appliances.
Upgrade Assistance	which may include software recommendation, upgrade testing, and planning assistance.
Advanced Service Points	for remote after-hours assistance, product upgrade assistance, and software recommendations.
Annual Training Package	including NSE 4 and NSE 5 training and certification vouchers.

Enterprise Services offerings come in four levels: Premium, Business, First, and Global First..

FortiCare Included Features	Account-level Advanced Services			
	Premium	Business	First	Global First
Technical Support	24×7×365	24×7×365	24×7×365	24×7×365
Direct Access to ASE Team	✓	Designated ASE	Lead TAM	3 Regional TAMs
Enhanced Reponse SLA	✓	✓	✓	✓
Business Review	—	Biannual	Quarterly	Quarterly
Account Planning	✓	✓	✓	✓
Device Performance Advice	—	—	✓	✓
Device Configuration Advice	—	—	✓	✓
Root Cause Analysis	—	P1	P1/P2	P1/P2
NSE 4 Training & Certification	3	3	5	15
NSE 5 Training & Certification	—	3	5	15
Advanced Services Points	—	6	16	48

Service Provider offerings come in two levels: Select and Elite. Benefits vary by level.

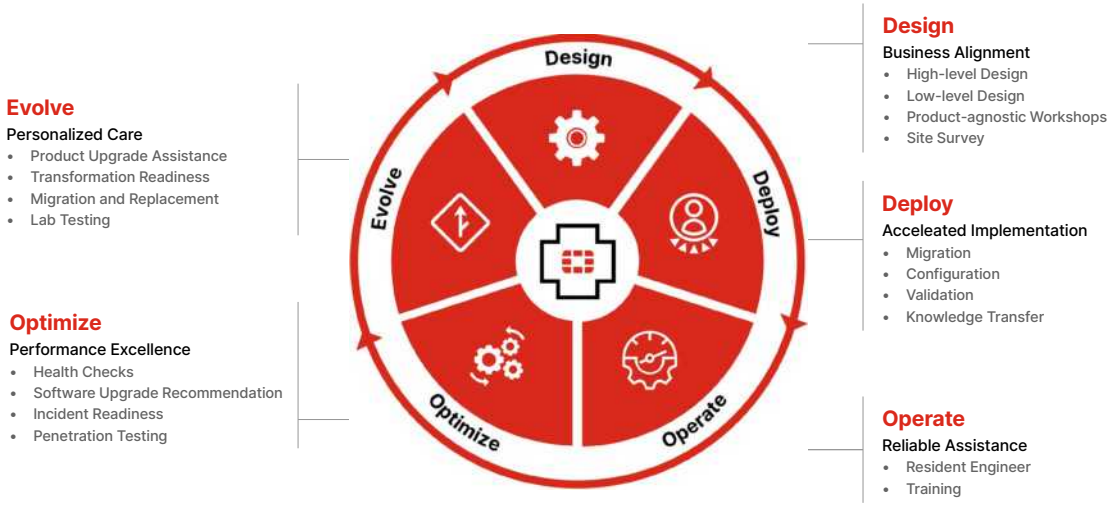
FortiCare Included Features	Account-level Advanced Services		
	Select	Elite	Global Elite
Technical Support	24×7×365	24×7×365	24×7×365
Direct Access to ASE Team	✓	Lead TAM	Lead TAM
Enhanced Reponse SLA	✓	✓	✓
Business Review	—	Quarterly	Quarterly
Account Planning	✓	✓	✓
Performance/Configuration Advice	—	✓	✓
Designated Relationship Manager	✓	✓	✓
18-month Extended Firmware	—	✓	✓
Lab Testing	5 Days	5 Days	15 Days
Upgrade Assistance	—	2 Products	6 Products
Root Cause Analysis	P1/P2	P1/P2	P1/P2
NSE 4 Training & Certification	3	5	15
NSE 5 Training & Certification	3	5	15
Advanced Services Points	6	12	36

In addition, Global First for Enterprises and Global Elite for Service Providers are available to extend the geographical coverage of the service. These service levels provide a designated lead engineer per region covering EMEA, Americas, and Asia Pacific. The service features, as described in the First service, are provided within each region with global coordination.

Feature Highlights: Professional Services

As networks and threats rapidly evolve, it's critical to make sure security capabilities can keep up. Given the global cybersecurity skills shortage, today's organizations often lack the in-house expertise or enough staff to deploy, operate, and maintain the new technologies required to close security gaps. FortiCare Professional Services delivers expert help to ensure Fortinet deployments are optimized for each customer's unique needs.

Professional Services provides Design, Deploy, Operate, Optimize, and Evolve services. In addition, Professional Services also offers product-agnostic consulting services.



Key benefits to engaging Fortinet Professional Services:

Faster Time-to-Value	Hit the ground running with new capabilities, achieve faster time-to-value with streamlined expert deployment of Fortinet products and solutions.
Increased Service Uptime	Achieve increased uptime by leveraging subject matter experts who can proactively review changes, performance, and policies for reliability and sustained security.
Access to Industry Expertise	Supplement in-house teams with dedicated resources that can bring industry expertise to perform upgrades or handle technical incidents.
Increased Productivity	Increase staff productivity by offloading redundant operational tasks including configurations to Fortinet domain experts who know your business

Cybersecurity Advisory and Consulting Services allow our experts to partner with business leaders, helping organizations be at their best through this ever-changing environment. Fortinet experts discover existing security posture elements through a vendor-agnostic approach; align findings to business goals, strategic objectives, and compliance requirements; and guide existing projects and future planning toward framework maturity.

Discover

Business Goals
Security Posture
Systems/Objectives

Align

Security Framework
Compliance Requirements
Strategic Objectives

Guide

Architectural Design
Operational Practices
Maturity Roadmap

FortiGuard Labs Consulting

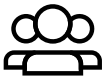
Consulting services are designed to help your organization address your specific threat landscapes and improve your organization's ability to use threat intelligence to meet that challenge. These services leverage the expertise and experience of the FortiGuard Labs team and provide the answers to the questions organizations are asking most:

Threats

What are the most important threats on which I should focus?

Environment

Is my environment as secure as it needs to be?



Operations

Are my people properly trained to defend us against the threats we face?

www.fortinet.com

April 29, 2022 12:09 PM

FIDDLE LEAF:Graphic Design:Fortinet:Projects:fa-forticare-services-brochure:fa-forticare-services-brochure-042922 Folder:fa-forticare-services-brochure-042922

1563571-0-0-EN

BROCHURE

Fortinet Product Certifications

Fortinet Product Certifications

Organizations looking to expand, upgrade, or replace their security solutions often find themselves struggling to compare solutions from different vendors. In addition to consistent information about features and functions, they also need information about the compliance and certification level of individual solutions and whether they will enable them to meet regulatory requirements.

To help companies navigate this process, third-party labs and auditors conduct independent testing to enable a fair comparison between products for things like performance, compliance, and functionality. Using industry standards and advanced benchmarking technologies, such as independent validation of products and services, is essential for businesses to evaluate whether a solution will meet their unique business requirements.

Certifications At-a-Glance

- Fortinet's commitment to innovation and excellence has earned the respect of independent test labs around the world
- 25+ years of consistent testing and compliance
- A wide range of global certifications across verticals

Third-party Testing

Fortinet has actively participated in third-party testing since we first opened our doors. We are committed to the testing and certification process and believe that it provides three key benefits:

- It validates our design and development process. Third-party labs set standards for functionality, performance, and real-world use cases that help drive the development of key features.
- It helps improve our technology. Direct feedback from standardized benchmark testing helps us in our effort to continually improve our technologies.
- It allows our customers to easily compare our technologies against solutions from other vendors. Annual testing helps us set the bar higher every year, with the objective of achieving a leadership position in every test in which we participate.

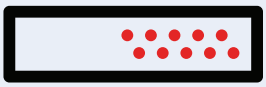
Certifications and Regulatory Compliance

Public and private sector organizations alike require solutions that meet regulatory and compliance requirements. Fortinet is committed to meeting a wide range of national, regional, and international requirements, and we subject our solutions and services to independent third-party audits and testing to guarantee compliance.

The Fortinet Certifications Resource Center (CRC)

Fortinet's CRC is the repository for product compliance reports, certifications, and independent validation results from unbiased agencies. The scope of Fortinet's product certifications includes the following categories:

Product Certifications



Independent lab testing of Fortinet products using industry standards, best practices, and real-world testing environments

Information Security

Certifications and examinations of Fortinet's infrastructure security and networking solutions

Compliance

Certifications attesting to Fortinet products' compliance with public sector regulatory frameworks and standards

Product Certifications Overview

Category	Certification	Description	Latest Publication Date	
Product Certifications	ICSA Labs	ICSA Labs is an independent division of Verizon. They provide third-party testing and certification of security and health-related IT products and network-connected devices to measure product compliance, reliability, and performance.	IPsec VPN	08/10/2021
			Firewall	08/25/2021
			WAF	09/27/2021
	AV-Comparatives	AV-Comparatives is an independent lab offering systematic testing to determine whether security software—such as PC/Mac-based antivirus products and mobile security solutions—lives up to its claims. Using one of the largest sample collections in the world, they create a real-world environment for truly accurate testing. Certification by AV-Comparatives provides a globally recognized seal of approval for software performance.	Business Security Test: Mar-Jun 2021	
	SE Labs	SE Labs tests a range of solutions, including endpoint software, network appliances, and cloud services, on their ability to detect attacks, protect against intrusions, or both.	Email Security Services Protection: Jan-Mar 2020	
	MEF 3.0	MEF 3.0 is an SD-WAN Certification Program that uses Spirent as their SD-WAN Authorized Certification and Test Partner (ACTP). Certification involves rigorous tests of the service attributes and requirements defined in MEF 70 and described in detail in the upcoming MEF SD-WAN Certification Test Requirements (MEF W90) standard.	MEF 3.0 SD-WAN: Jun 2020	
	Virus Bulletin	VB is a world leader in security software testing. Their publicly available test reports cover anti-malware protections of all types as well as enterprise-level email and web security solutions.	VBSpam	Sept 2021
			VB100	Sept 2021
	MITRE Engenuity	MITRE Engenuity's ATT&CK™ evaluations assess the ability of a vendor's solutions to defend against specific adversary tactics and techniques. They openly publish these results to provide end-users with the information needed to make good purchasing decisions. These evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, they show how each vendor approaches threat detection in the context of the MITRE ATT&CK knowledge base to provide an unbiased assessment of detection and protection capabilities and highlight potential gaps to drive the industry forward.	Round 3: Fin7/Carbanak: Apr 2021	
Information Security	SOC2	SOC2 is an auditing procedure that ensures that service providers securely manage their customers' data. It covers their security, availability, processing integrity, confidentiality, and/or privacy controls. Compliance is based on the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria).	SOC2 Type 2: Apr-Sept 2021	
	ISO	ISO/IEC 27001 is an international standard for managing information security. It defines requirements and controls for establishing, implementing, maintaining, and continually improving an organization's Information Security Management System (ISMS).	ISO/IEC 27001: Jun 2021-Jun 2024	
Government Regulations	FIPS Validated	The Federal Information Processing Standard 140-2 (FIPS 140-2) is an information technology security accreditation program for validating cryptographic modules developed by vendors that meet well-defined security standards.	FIPS 140-2 Level 1	Aug 2021
			FIPS 140-2 Level 2	Sept 2021
	Common Criteria	Common Criteria is an international standard (ISO/IEC 15408) operated by 17 certificate-authorizing nations. 31 countries have accepted it for their respective government acquisition requirements for their IT/networking infrastructures.	CC EAL4+	Oct 2021
			FWcPP+IPS +VPN	Jan 2021

Summary

Fortinet is committed to the independent testing and certification of its products and services. ICSA, AV-Comparatives, Virus Bulletin, and other independent testing organizations have consistently validated the effectiveness of Fortinet solutions. Fortinet earned ICSA's prestigious Excellence in Information Security Testing (EIST) award for 15 years of participation in 2017 and has been recognized by ICSA for outstanding achievement in information security certification testing 10 years in a row.

"Real-world third-party validation is an essential resource for enterprises considering security products, helping to cut through the confusion that can be caused by vendor marketing. Fortinet relies on a variety of third-party testing and compliance labs to provide reliable information to organizations making critical security purchasing decisions. They also demonstrate Fortinet's commitment to meeting high industry standards for security detection, performance, reliability, management, and value."

- Fortinet CEO Ken Xie

December 17, 2021 9:47 AM

1380665-0-0-EN

Product License Agreement / EULA and Warranty Terms

Product License Agreement

The parties to this agreement are you (the end-customer) and Fortinet, Inc. ("Fortinet"). CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OR INSTALLATION OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE TERMS IN THIS AGREEMENT, AS AMENDED OR UPDATED FROM TIME TO TIME IN FORTINET'S DISCRETION BY FORTINET PUBLISHING AN AMENDED OR UPDATED VERSION. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY AGREED TO IN A WRITING SIGNED BY THE GENERAL COUNSEL OF FORTINET. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT START THE INSTALLATION PROCESS OR USE THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU SHOULD IMMEDIATELY, AND IN NO EVENT LATER THAN FIVE (5) CALENDAR DAYS AFTER YOUR RECEIPT OF THE PRODUCT, IMMEDIATELY NOTIFY FORTINET LEGAL LEGAL@FORTINET.COM OF REQUESTED EULA CHANGES.

1. License Grant.

This is a license agreement between you and Fortinet, not a sales agreement. The term "Software", as used throughout this Agreement, includes all Fortinet and third party firmware and software provided to you with, or incorporated into, Fortinet appliances and any stand-alone software provided to you by Fortinet, with the exception of any open source software contained in Fortinet's Products which is discussed in detail in section 15 below, and the term "Software" includes any accompanying documentation, any updates and enhancements of the software or firmware provided to you by Fortinet, at its option. Fortinet grants to you a non-transferable (except as provided in section 5 ("Transfer") and section 15 ("Open Source Software") below), non-exclusive, revocable (in the event of your failure to comply with these terms, in the event of termination, or in the event Fortinet is not properly paid for the applicable Product) license to use the Software solely for your internal business purposes (provided, if (a) agreed by Fortinet in writing, (b) you are authorized by Fortinet in writing to provide managed service provider services ("MSSP") to your end-customers, and (c) you pay for an MSSP license, then you may use the Software and/or Software embedded in Fortinet Hardware to provide those services, subject to the other restrictions in this Agreement), in accordance with the terms set forth in this Agreement and subject to any further restrictions in Fortinet documentation (including license term restrictions), and solely on the Fortinet appliance, or, in the case of blades, CPUs, platform, devices or databases, on the single blade, CPU, platform, device or database on which Fortinet installed the Software, or, for stand-alone Software, solely on a single computer running a validly-licensed copy of the operating system for which the Software was designed unless and except set forth in the published documentation otherwise. For clarity, notwithstanding anything to the contrary, all licenses of Software to be installed on blades, CPUs, platforms, devices or databases are licensed per blade, solely for one blade and not for multiple blades that may be installed in a chassis, per CPU, per platform, per device, or per database basis, up to the blade, CPU, platform, device, database number defined in the license and as applicable and in accordance with the documentation. The Software is "in use" on any appliances, blades, CPUs, platforms, devices, or databases when it is loaded into temporary memory (i.e. RAM), accessed, downloaded, installed, or used on an appliance, blade, CPU, platform, device, or database. You agree that, except for the limited, specific license rights granted in this section 1, you receive no license rights to the Software.

2. Limitation on Use.

You are prohibited from and may not attempt to, and, if you are a corporation, you are responsible to prevent your employees and contractors from attempting to: (a) modify, translate, reverse engineer, decompile, disassemble, create derivative works based on, sublicense, or distribute the Software; (b) rent or lease any rights in the Software in any form to any third party or make the Software available or accessible to third parties in any other manner (except as expressly permitted for MSSP partners); (c) transfer assign or sublicense right to any other person or entity (except as provided in section 5): (d) remove any proprietary notice, labels, or marks on the Software, Products, and containers; (e) use the Software to determine, or disclose the results of, any benchmarking or performance measurements; (f) interfere with a platform for use of the Software; (g) use the Software on a device not owned and controlled by you; (h) use automated means to access online portions of the platform for the Software; (i) use the Software for third-party training, commercial time-sharing or service bureau use or (except as expressly set forth in this Agreement) use the Software to provide services to third parties, (j) share non-public features or content of the software with any third party; (k) access the software in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the software, or to copy any ideas, features, functions or graphics of the software; or, (l) engage in web scraping or data scraping on or related to the software, including without limitation, collection of information through any software that simulates human activity or any bot or web crawler.

3. Proprietary Rights.

All rights (including copyrights, trade secret, patent and other intellectual property rights), title, interest in and to the Software and any Product, and any copy thereof remain with Fortinet. You acknowledge that no title or other intellectual property rights in the Software or other Products is transferred to you and you will not acquire any rights to the Software or other Products except for the specific limited license as expressly set forth in section 1 ("License Grant") above. You expressly agree and acknowledge that Fortinet owns, retains, and shall retain all intellectual property rights in and to, and you have no intellectual property rights in and to, the Products and the Software other than the License Grant. You agree to keep confidential all Fortinet confidential information and only to use such information for the purposes for which Fortinet disclosed it.

4. Term and Termination.

The term of the license is the shorter of (a) the term as set forth in the ordering documents, other Fortinet documentation, or per Fortinet practices or policies (such as with evaluation or beta licenses or subscription or other term licenses) and (b) for the duration of Fortinet's copyright in the Software. Fortinet may terminate this Agreement, and the licenses and other rights herein, immediately without notice if you breach or fail to comply with any of the terms and conditions of this Agreement or for other reasons as stated in Fortinet's other documentation. You agree that, upon such termination, you will cease using the Software and any Product and either destroy all copies of the Fortinet documentation or return all materials to Fortinet.

5. Transfer.

If you are a Fortinet contracted and authorized reseller or distributor of Products, you may transfer (not rent or lease unless specifically agreed to in writing by Fortinet) the Software to one end user on a permanent basis, provided that: (i) you ensure that your customer and the end user receives a copy of this Agreement, is bound by its terms and conditions, and, by selling the Product or Software, you hereby agree to enforce the terms in this Agreement against such end user, (ii) you at all times comply with all applicable United States export control laws and regulations, and (iii) you agree to refund any fees paid to you by an end user who purchased Product(s) from you but does not agree to the terms contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Further, if you are a non-authorized reseller of Products and Services, you are not authorized to sell Product(s), Software or Services, but, regardless, by selling Product(s), Software or Services, you hereby agree you are bound by the restrictions and obligations herein and are bound to: (i) ensure that your customer and the end user receive a copy of this Agreement and are bound in full by all restrictions and obligations herein (ii) enforce the restrictions and obligations in this Agreement against such customer and/or end user, (iii) comply with all applicable United States export control laws and regulations and all other applicable laws, and (iv) refund any fees paid to you by a customer and/or end user who purchased Product(s) from you but does not agree to the restrictions and obligations contained in this Agreement and therefore wishes to return the Product(s) as provided for in this Agreement. Notwithstanding anything to the contrary, distributors, resellers and other Fortinet partners (a) are not agents of Fortinet and (b) are not authorized to bind Fortinet in any way. Fortinet's license, warranty, and support is only available for Products that you purchased directly from an authorized Fortinet channel partner. Products not purchased from an authorized Fortinet channel partner are not eligible, will not be supported, and may be blocked from registration.

6. Limited Warranty.

Fortinet provides this limited warranty for its product only to the single end-user person or entity that originally purchased the Product from Fortinet or its authorized reseller or distributor and paid for such Product. The warranty is only valid for Products which are properly registered on Fortinet's Support Website, https://support.fortinet.com, or such other website as provided by Fortinet, or for which the warranty otherwise starts according to Fortinet's policies, and any support is only valid for products properly purchased through authorized distributors and resellers. The warranty periods discussed below will start according to Fortinet's policies posted at http://www.fortinet.com/aboutus/legal.html or such other website as provided by Fortinet. It is the Fortinet distributor's and reseller's responsibility to make clear to the end user the date the product was originally shipped from Fortinet, and it is the end user's responsibility to understand the original ship date from the party from which the end user purchased the product. All warranty claims must be submitted in writing to Fortinet before the expiration of the warranty term or such claims are waived in full. Fortinet provides no warranty for any beta, donation or evaluation Products. Fortinet warrants that the hardware portion of the Products ("Hardware") will be free from material defects in workmanship as compared to the functional specifications for the period set forth as follows and applicable to the Product type ("Hardware Warranty Period"): (a) a three hundred sixty-five (365) day limited warranty for the Hardware products; (b) for FortiAP, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware; (c) for FortiSwitch Hardware appliance products other than the FortiSwitch-5000 series, the warranty herein shall last from the start of the warranty period as discussed above until five (5) years following the product announced end-of-life date Hardware. Fortinet's sole obligation shall be to repair or offer replacement Hardware for the defective Hardware at no charge to the original owner. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Such repair or replacement will be rendered by Fortinet at an authorized Fortinet service facility as determined by Fortinet. The replacement Hardware need not be new or of an identical make, model, or part; Fortinet may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned Product that Fortinet reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Hardware Warranty Period for the repaired or replacement Hardware shall be for the greater of the remaining Hardware Warranty Period or ninety days from the delivery of the repaired or replacement Hardware. If Fortinet determines in its reasonable discretion that a material defect is incapable of correction or that it is not practical to repair or replace defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by Fortinet upon return to Fortinet of the defective Hardware. All Hardware (or part thereof) that is replaced by Fortinet, or for which the purchase price is refunded, shall become the property of Fortinet upon replacement or refund. Fortinet warrants that Software as initially shipped by Fortinet will substantially conform to Fortinet's then-current functional specifications for the Software, as set forth in the applicable documentation for a period of ninety (90) days ("Software Warranty Period"), if the Software is properly installed on approved Hardware and operated as contemplated in its documentation. Fortinet's sole obligation shall be to repair or offer replacement Software for the non-conforming Software with software that substantially conforms to Fortinet's functional specifications. This obligation is exclusive of transport fees, labor, de-installation, installation, reconfiguration, or return shipment and handling fees and costs, and Fortinet shall have no obligation related thereto. Except as otherwise agreed by Fortinet in writing, the warranty replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by Fortinet for the Software. The Software Warranty Period shall extend for an additional ninety (90) days after any warranty replacement software is delivered. If Fortinet determines in its reasonable discretion that a material non-conformance is incapable of correction or that it is not practical to repair or replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by Fortinet; provided that the non-conforming Software (and all copies thereof) is first returned to Fortinet. The license granted respecting any Software for which a refund is given automatically terminates immediately upon refund. For purpose of the above hardware and software warranties, the term "functional specifications" means solely those specifications authorized and published by Fortinet that expressly state in such specifications that they are the functional specifications referred to in this section 6 of this Agreement, and, in the event no such specifications are provided to you with the Software or Hardware, there shall be no warranty on such Software.

7. Disclaimer of Other Warranties and Restrictions.

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED IN SECTION 6 ABOVE, THE PRODUCT AND SOFTWARE ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY, IMPLIED OR EXPRESS WARRANTY OF MERCHANTABILITY, OR WARRANTY FOR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS FROM THE DATE OF ORIGINAL SHIPMENT FROM FORTINET. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT. NOTWITHSTANDING ANYTHING TO THE CONTRARY, THE HARDWARE WARRANTY PERIOD DISCUSSED ABOVE DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS, INCLUDING FORTITOKEN WHICH HAS A 365 DAY WARRANTY FROM THE DATE OF SHIPMENT FROM FORTINET'S FACILITIES, AND THE SOFTWARE WARRANTY DOES NOT APPLY TO CERTAIN FORTINET PRODUCTS. YOU HEREBY ACKNOWLEDGE AND AGREE THAT NO VENDOR CAN ASSURE COMPLETE SECURITY AND NOTHING HEREIN OR ELSEWHERE SHALL BE DEEMED TO IMPLY A SECURITY GUARANTEE OR ASSURANCE, AND FORTINET DISCLAIMS LIABILITY REGARDING YOUR WEB BROWSER'S REQUIREMENTS OR ANY THIRD PARTY DEVICE OR APPLIANCE USED TO OPERATE THE SOFTWARE.

The warranty in Section 6 above does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Fortinet or its authorized representative, (b) has not been installed, operated, repaired, updated to the latest version, or maintained in accordance with instructions supplied by Fortinet, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident; (d) is licensed for beta, evaluation, donation, testing or demonstration purposes or for which Fortinet does not charge a purchase price or license fee; or (e) is procured from a non-authorized reseller or non-authorized distributor. In the case of beta, testing, evaluation, donation or free Software or Product, the end user acknowledges and agrees that such Software or Product may contain bugs or errors and could cause system failures, data loss and other issues, and the end user agrees that such Software or Product is provided "as-is" without any warranty whatsoever, and Fortinet disclaims any warranty or liability whatsoever. An end user's use of evaluation or beta Software or Product is limited to thirty (30) days from original shipment unless otherwise agreed in writing by Fortinet. For clarity, notwithstanding anything to the contrary, all sales are final and no provision in this EULA entitles you to return Products, other than as expressly set forth herein.

8. Governing Law.

Any disputes arising out of this Agreement or Fortinet's limited warranty shall be governed by the laws of the state of California, without regard to the conflict of laws principles. In the event of any disputes arising out of this Agreement or Fortinet's limited warranty, the parties submit to the jurisdiction of the federal and state courts located in Santa Clara County, California, as applicable, and agree that any controversy or claim arising out of or relating to this Agreement shall be determined in the federal and state courts located in Santa Clara County, California, as applicable.

9. Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND NOTWITHSTANDING ANYTHING TO THE CONTRARY, FORTINET IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY, INFRINGEMENT OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT OR SERVICE OR ANY DAMAGES OF ANY KIND WHATSOEVER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF PROFIT, LOSS OF OPPORTUNITY, LOSS OR DAMAGE RELATED TO USE OF THE PRODUCT OR SERVICE IN CONNECTION WITH HIGH RISK ACTIVITIES, DE-INSTALLATION AND INSTALLATION FEES AND COSTS, DAMAGE TO PERSONAL OR REAL PROPERTY, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, COMPUTER SECURITY BREACH, COMPUTER VIRUS INFECTION, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT INCLUDING ANY PRODUCT RETURNED TO FORTINET FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THE LIMITED WARRANTY IN SECTION 6 ABOVE, EVEN IF FORTINET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE LIMITED WARRANTY IS, AT FORTINET'S SOLE AND ABSOLUTE DISCRETION: REPAIR, REPLACEMENT, OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT AS SPECIFICALLY STATED IN SECTION 6 ABOVE; PROVIDED, HOWEVER, IN NO EVENT SHALL ANY END-CUSTOMER REMEDIES UNDER THIS EULA AND ANY SUPPORT AGREEMENT EXCEED THE AMOUNT PAID TO FORTINET FOR THE SPECIFIC APPLICABLE DEFECTIVE OR NON-CONFORMING PRODUCT AT ISSUE.

10. Compliance with Laws, including Import/Export Laws and FCPA.

You are advised that the Products may be subject to the United States Export Administration Regulations and other import and export laws; diversion contrary to United States law and regulation is prohibited. You agree to comply with all applicable international and national laws that apply to the Products as well as end user, end-use, and destination restrictions issued by U.S. and other governments. For additional information on U.S. export controls see https://www.bis.doc.gov. Fortinet assumes no responsibility or liability for your failure to obtain any necessary import and export approvals and licenses, and Fortinet reserves the right to terminate or suspend shipments, services and support in the event Fortinet has a reasonable basis to suspect any import or export violation. You represent that neither the United States Bureau of Industry and Security nor any other governmental agency has issued sanctions against you or otherwise suspended, revoked or denied your export privileges. You agree not to use or transfer the Products for any use relating to nuclear, chemical or biological weapons, or missile technology, unless authorized by the United States Government by regulation or specific written license. Additionally, you agree not to directly or indirectly export, import or transmit the Products contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or use. Furthermore, you hereby agree that, for any orders that you place with Fortinet whereby any legal or regulatory requirements may apply to Fortinet such as requirements related to the International Traffic in Arms Regulations, or Buy American Act, or the Trade Agreements Act: you are responsible to ensure the Purchase Order submitted to Fortinet by you and/or any partners clearly states the specific requirement in writing, or otherwise Fortinet is not bound by any such requirements. You represent that you understand, and you hereby agree to comply with, all applicable laws including but not limited to the U.S. Foreign Corrupt Practices Act . You represent that you hereby agree that you and your employees have not accepted, and will not accept, anything of value, including money, meals, entertainment, paid-for travel, beta, testing, evaluation, donation or free Products and/or related services, or anything else of value, in exchange for Fortinet maintaining current business or for new business opportunities. You represent and warrant to Fortinet that you and your employees, consultants, agents and representatives will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force. You agree you and your employees will be responsible to comply in full with all laws and policies applicable to any and all dealings with Fortinet in general and its distributors, resellers and partners.

11. U.S. Government End Users.

The Software and accompanying documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement and its successors.

12. Tax Liability.

You agree to be responsible for payment of any sales or use taxes imposed at any time on this transaction.

13. General Provisions.

Except as specifically permitted and required in section 5 ("Transfer") above, you agree not to assign this Agreement or transfer any of the rights or obligations under this Agreement without the prior written consent of Fortinet. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties. The United Nations Convention on Contracts for the International Sales of Goods is expressly excluded. This Agreement and other Fortinet agreements may be amended or supplemented only by a writing that refers explicitly to the agreement signed on behalf of both parties, or, for this Agreement, as otherwise expressly provided in the lead-in above Section 1 above, provided, notwithstanding anything to the contrary and except for this Agreement which may be amended or updated as expressly provided in the lead-in above Section 1 above, for any amendment or other agreement to be binding on Fortinet, such amendment or other agreement must be signed by Fortinet's General Counsel. No waiver will be implied from conduct or failure to enforce rights nor effective unless in a writing signed on behalf of the party against whom the waiver is asserted. If any part of this Agreement is found unenforceable, that part will be enforced to the maximum extent permitted and the remainder shall continue in full force and effect. You acknowledge that you have read this Agreement, understand it, and agree to be bound by its terms and conditions. Notwithstanding anything to the contrary, this EULA constitutes the entire agreement between Fortinet and its end-customers and supersedes any and all prior representations or conflicting provisions, such as limitations of liability, warranties, or otherwise in any and all purported end customer agreements, whether entered into now or in the future. In the event of a conflict between this EULA and another agreement, this EULA shall prevail unless the conflicting agreement expressly states that it replaces this EULA, expressly referring to this EULA, and is agreed to in writing by authorized representatives of the parties (which, in the case of Fortinet, is Fortinet's General Counsel).

14. Privacy.

You agree to Fortinet's collection, use, disclosure, protection and transfer of your information, as set forth in the Fortinet privacy policy on the Fortinet web site (http://www.fortinet.com/about-us/privacy.html), including (a) Fortinet's use of the Customer information to send information regarding Fortinet products and services; and (b) Fortinet's disclosure of your information to provide assistance to law enforcement, governmental agencies and other authorities or to allow Fortinet to protect its Customers' and/or end users' rights.

15. Open Source Software.

Fortinet's products may include software modules that are licensed (or sublicensed) to the user under the GNU General Public License, Version 2, of June 1991 ("GPL") or GNU Lesser General Public License, Version 2.1, of February 1999 ("LGPL") or other open source software licenses which, among other rights, permit the user to use, copy, modify and redistribute modules, or portions thereof, and may also require attribution disclosures and access to the source code ("Open Source Software"). The GPL requires that for any Open Source Software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any Open Source Software covered under the GPL, the source code is made available on this CD or download package. If any Open Source Software licenses require that Fortinet provide rights to use, copy or modify any Open Source Software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. Fortinet will provide, for a charge reflecting our standard distribution costs, the complete machine-readable copy of the modified software modules. To obtain a complete machine-readable copy, please send your written request, along with a check in the amount of US $25.00, to General Public License Source Code Request, Fortinet, Inc., 899 Kifer Rd, Sunnyvale, CA 94086 USA. To receive the modified software modules, you must also include the following information: (a) Name, (b) Address, (c) Telephone number, (d) E-mail Address, (e) Product purchased (if applicable), (f) Product Serial Number (if applicable). All open source software modules are licensed free of charge. There is no warranty for these modules, to the extent permitted by applicable law. The copyright holders provide these software modules "AS-IS" without warranty of any kind, either expressed or implied. In no event will the copyright holder for the open source software be liable to you for damages, including any special, incidental or consequential damages arising out of the use or inability to use the software modules, even if such holder has been advised of the possibility of such damages. A full copy of this license, including additional open source software license disclosures and third party license disclosures applicable to certain Fortinet products, may obtained by contacting Fortinet's Legal Department at legal@fortinet.com.

GNU GENERAL PUBLIC LICENSE GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

Source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999
Copyright (C) 1991, 1999 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2 instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for your own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

15. The warranty disclaimer contained in Sections 11 and 12 of the preceding GPL License is incorporated herein.