

GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE

AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order are available through *GSA Advantage!*, a menu-driven database system. The INTERNET address *GSA Advantage!* is: GSAAdvantage.gov.



SCHEDULE TITLE MULTIPLE AWARD SCHEDULE

FEDERAL SUPPLY GROUP PROFESSIONAL SERVICES

CONTRACT NUMBER: GS-35F-0563X
For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov.

CONTRACT PERIOD: AUGUST 23, 2016 – AUGUST 22, 2021
PRICELIST CURRENT THRU MOD #PS-A824, EFFECTIVE 8/19/2020

CONTRACTOR: SWISH DATA CORPORATION
1420 SPRING HILL ROAD, SUITE 320
MCLEAN, VA 22102-3027
PHONE: 703-635-3324
INFO@SWISHDATA.COM
WWW.SWISHDATA.COM

Point of Contact: Bob Kerr
e-mail: bkerr@swishdata.com
Tel: 201-627-2725
Fax: 703-852-7904

Business Size: Small

CUSTOMER INFORMATION

1a	Awarded SIN(s):	<table border="1"> <tr> <td>33411</td> <td>Purchasing of new electronic equipment</td> </tr> <tr> <td>511210</td> <td>Software Licenses</td> </tr> <tr> <td>54151</td> <td>Software Maintenance Services</td> </tr> <tr> <td>54151HACS</td> <td>Highly Adaptive Cybersecurity Services (HACS)</td> </tr> <tr> <td>54151S</td> <td>Information Technology Professional Services</td> </tr> <tr> <td>611420</td> <td>Information Technology Training</td> </tr> <tr> <td>811212</td> <td>Maintenance of Equipment, Repair Services and/or Repair/Spare Parts</td> </tr> <tr> <td>OLM</td> <td>Order-Level Materials</td> </tr> </table>	33411	Purchasing of new electronic equipment	511210	Software Licenses	54151	Software Maintenance Services	54151HACS	Highly Adaptive Cybersecurity Services (HACS)	54151S	Information Technology Professional Services	611420	Information Technology Training	811212	Maintenance of Equipment, Repair Services and/or Repair/Spare Parts	OLM	Order-Level Materials
33411	Purchasing of new electronic equipment																	
511210	Software Licenses																	
54151	Software Maintenance Services																	
54151HACS	Highly Adaptive Cybersecurity Services (HACS)																	
54151S	Information Technology Professional Services																	
611420	Information Technology Training																	
811212	Maintenance of Equipment, Repair Services and/or Repair/Spare Parts																	
OLM	Order-Level Materials																	
1b	Lowest Priced Item:	See Pricelist																
1c	Hourly Rates & Labor Category Descriptions:	See below																
2	Maximum Order:	SIN 33411, 511210, 54151, 54151HACS, 54151S and 811212 - \$500,000; SIN 611420 and OLM - \$250,000																
3	Minimum Order:	\$100																
4	Geographic Coverage:	Worldwide																
5	Point of Production:	US, Israel, Spain, Norway, Taiwan and Great Britain																
6	Discount:	Prices shown are net of discount.																
7	Quantity Discounts:	None																
8	Prompt Payment Terms:	Net 30 Days Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.																
9a	Government Purchase Cards	Government Purchase Cards are accepted at or below the micro-purchase threshold.																
9b		Contract will accept the Government Commercial Credit Card above the micro-purchase threshold.																
10	Foreign Items:	Some products are manufactured in Israel, Spain and Norway, Taiwan and Great Britain																
11	Time of Delivery:																	
	a. Normal:	As Agreed Upon with Ordering Activity																
	b. Expedited	Contact Contractor																
	c. Overnight & 2-day delivery	Contact Contractor																
	d. Urgent Requirements	Contact Contractor																

- 12 **FOB Point(s):** Destination
- 13a **Ordering Address:** Same as Contractor address
- 13b **Ordering procedures:** For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's), are found in Federal Acquisition Regulation (FAR) 8.405-3.
- 14 **Payment Address:** Same as Contractor address
- 15 **Warranty Provision:** Standard Commercial Warranty
- 16 **Export packing charges, if applicable:** N/A
- 17 **Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level):** Contact Contractor
- 18 **Terms and conditions of rental, maintenance, and repair (if applicable):** N/A
- 19 **Terms and conditions of installation (if applicable):** N/A
- 20 **Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable):** N/A
- 20a **Terms and conditions for any other services (if applicable):** N/A
- 21 **List of service and distribution points (if applicable):** N/A
- 22 **List of participating dealers (if applicable):** N/A
- 23 **Preventive maintenance (if applicable):** N/A
- 24a **Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants):** N/A
- 24b **Section 508 Compliance for EIT:** N/A
- 25 **DUNS Number:** 961526758
- 26 **Notification regarding registration in SAM database:** Contractor has an Active Registration in the SAM database.

54151S Labor Categories

SIN	Part Number	Labor Category	Hourly Rate
54151S	MAD-PROJM-HR	Project Manager	161.25
54151S	MAD-PA-HR	Project Administrator	58.64
54151S	MAD-JSEM-HR	Junior IT Security Engineer	122.16
54151S	MAD-TW-HR	Technical Writer	92.84
54151S	MAD-SSEM-HR	Senior IT Security Engineer	180.79
54151S	MAD-PROJM-HR	Program Manager	161.25
54151S	MAD-SME-HR	IT Subject Matter Expert	317.61
54151S	MAD-TIS-HR	Technical IT Instruction	635.23

54151S Labor Category Descriptions

Project Manager

Minimum/General Experience: 5 years' experience managing information technology projects. Requires thorough knowledge of project planning, risk management, reporting and project management tools. The project manager enforces work standards, assigns schedules, reviews work discrepancies, supervises contractor personnel, and communicates policies, purposes, and goals of the organization to subordinates and is responsible for contract performance. Briefs Company principals on anticipated problems on the contract and makes recommendations towards resolving issues.

Functional Responsibility: Serves as Senior Contract Manager and authorized liaison with the Government Contracting Officer (CO), the Contracting Officer's Representative (COR), government management personnel, and customer agency representatives. Responsible for the timely execution of various tasks. Project planning, team composition, task monitoring and allocation, risk management and disaster recovery, Technical presentations.

Minimum Education: BS / BA Degree or equivalent in Information Systems, Information Technology or Computer Science.

Project Administrator

Minimum/General Experience: 5 Years of administrative experience

Functional Responsibility: Provide administrative support to technical and management personnel. This includes, but is not limited to: documentation, planning and support, project administration and office support

Minimum Education: BS / BA Degree or equivalent in Information Systems, Information Technology, Computer Science or Business Administration.

Junior IT Security Engineer

Minimum/General Experience: Over 5 Years of network security project experience in various IT environments.

Functional Responsibility: Provides specific network security expertise under the direction of the Sr. Security Engineer or Project Manager. Assists in the completion of specific network engineering tasks as directed.

Minimum Education: BS / BA Degree or equivalent in Information Systems, Information Technology or Computer Science.

Technical Writer

Minimum/General Experience: 3 or more years experience in technical writing and preparing technical documentation and technical manuals.

Functional Responsibility: Prepares technical documentation including but not limited to technical training manuals, training documents, operation manuals, and test and validation reports.

Minimum Education: BS / BA Degree or equivalent in Information Systems, Information Technology or Computer Science.

Senior IT Security Engineer

Minimum/General Experience: Over 10 years of network security project experience

Functional Responsibility: Provides in-depth network security expertise in C&A, Forensics, Reverse Engineering, Penetration Testing problems and resolutions.

Minimum Education: BS / BA Degree or equivalent in Information Systems, Information Technology or Computer Science.

IT Subject Matter Expert

Minimum/General Experience: A senior-level security architect with 12-15 Years of experience, in-depth knowledge of strategic and tactical facets of network security, engineering and design.

Functional Responsibility: Provides guidance and recommendations on complex multi-vendor environments, security expert in C&A, Forensics, Reverse Engineering, Penetration Testing, Reporting and multiple project management. Provides advanced theories and concepts that contribute to the technical excellence of the organization. Analyses costs and provides guidance to ensure customer's requirements are met. Establishes proven baseline recommendations.

Minimum Education: Advanced Degree or equivalent in Information Systems, Information

Technology, Computer Science coupled with Industry Certifications and Training

Program Manager

Minimum/General Experience: Over 10 Years' experience leading and providing technical direction of IT projects .Demonstrated experience in managing and directing multiple IT projects. Coordinates all tasks. Ensures adherence to all customer requirements. Briefs Project Manager on anticipated problems on the contract and makes recommendations towards resolving issues.

Functional Responsibility: Assists in the performance of all Project Manager responsibilities. Experienced in both managerial and technical areas. Responsible for individual task orders under the supervision of the Project Manager. Demonstrated experience to work independently or under only general direction. Responsible for project remaining within budgetary expectations.

Minimum Education: BS / BA/ or equivalent in Information Systems, Information Technology or Computer Science.

Technical IT Instruction Specialist

Minimum/General Experience: 7 Years of managing information technology and security training programs including training documentation. Experience with Multimedia added instruction preferred.

Functional Responsibility: Provides training and classroom instruction to users and staff personnel Gathers and assembles relevant materials. Utilize appropriate teaching methods to include individual group or workshop. Ensure students understand the practical aspects of subject material being taught.

Minimum Education: BS / BA Degree or equivalent in Information Systems, Information Technology or Computer Science.

EULA

This License Agreement (the "Agreement") is an agreement between you (both the individual installing the Product and any legal entity on whose behalf such individual is acting) (hereinafter "You" or "Your") and Check Point Software Technologies Ltd. (hereinafter "Check Point").

TAKING ANY STEP TO SET-UP, USE OR INSTALL THE PRODUCT CONSTITUTES YOUR ASSENT TO AND ACCEPTANCE OF THIS AGREEMENT. WRITTEN APPROVAL IS NOT A PREREQUISITE TO THE VALIDITY OR ENFORCEABILITY OF THIS AGREEMENT AND NO SOLICITATION OF ANY SUCH WRITTEN APPROVAL BY OR ON BEHALF OF YOU SHALL BE CONSTRUED AS AN INFERENCE TO THE CONTRARY. IF YOU HAVE ORDERED THIS PRODUCT SUCH ORDER IS CONSIDERED AN OFFER BY YOU, CHECK POINT'S ACCEPTANCE OF YOUR OFFER IS EXPRESSLY CONDITIONAL ON YOUR ASSENT TO THE TERMS OF THIS AGREEMENT, TO THE EXCLUSION OF ALL OTHER TERMS. THIS AGREEMENT

SUPERSEDES ANY PREVIOUS VERSIONS. IF THESE TERMS ARE CONSIDERED AN OFFER BY CHECK POINT, YOUR ACCEPTANCE IS EXPRESSLY LIMITED TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH ALL THE TERMS OF THIS AGREEMENT, YOU MUST RETURN THIS PRODUCT WITH THE ORIGINAL PACKAGE AND THE PROOF OF PAYMENT TO THE PLACE YOU OBTAINED IT FOR A FULL REFUND.

Limited Software Warranty

Check Point warrants to You that the encoding of the software program on the media on which the Product is furnished will be free from defects in material and workmanship, and that the Product shall substantially conform to its user manual, as it exists at the date of delivery, for a period of ninety (90) days. Check Point's entire liability and Your exclusive remedy under this warranty shall be, at Check Point's option, either:

return of the price paid to Check Point for the Product, resulting in the termination of this Agreement, or (ii) repair or replacement of the Product or media that does not meet this limited warranty. EXCEPT FOR THE LIMITED WARRANTIES SET FORTH IN THIS SECTION 7.1, THE PRODUCT AND ANY SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. CHECK POINT DOES NOT WARRANT THAT THE PRODUCT WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. CHECK POINT DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to You. This warranty gives You specific legal rights. You may have other rights that vary from state to state.

Limitation of Liability. You are solely responsible for adequate protection and backup of the data and equipment used in connection with the Product. Check Point does not guarantee that use of the Product will be uninterrupted or error-free. Check Point does not guarantee that the information accessed by the Product will be accurate or complete. You acknowledge that performance of the Product may be affected by any number of factors, including without limitation, technical failure of the Product, the acts or omissions of third parties and other causes reasonably beyond the control of Check Point. Certain features of the Product may not be forward-compatible with future versions of the Product and use of such features with future versions of the Product may require purchase of the applicable future version of the Product.

EXCEPT FOR BODILY INJURY OF A PERSON, IN NO EVENT WILL CHECK POINT BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING OUT OF THE SUBJECT MATTER OF THIS AGREEMENT, THE PRODUCT OR ANY SERVICES UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY, FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS), OR FOR LOSS OF OR CORRUPTION OF DATA, OR FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS OR TECHNOLOGY IRRESPECTIVE OF WHETHER CHECK POINT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. CHECK POINT'S MAXIMUM LIABILITY FOR DAMAGES SHALL BE LIMITED TO THE LICENSE FEES RECEIVED

BY CHECK POINT UNDER THIS LICENSE FOR THE PARTICULAR PRODUCT(S) WHICH CAUSED

THE DAMAGES. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

LIMITED HARDWARE WARRANTY

Check Point warrants that the hardware components of its Hardware Product shall be free from material defects in design, materials, and workmanship and will function, under normal use and circumstances, in accordance with the documentation provided, for a period of one (1) year from the date of activation of the Hardware Product. If the Hardware Product has not been activated, the warranty will be valid for fifteen (15) months from the date of Check Point’s shipment of the Hardware Product (“Warranty Period”).

After the Warranty Period, certain return material authorization (“RMA”) services, as provided by Check Point (which are not covered under this warranty), are available for all Hardware Products pursuant to a purchased and active Check Point support agreement.

Your sole and exclusive remedy, and Check Point’s sole and exclusive liability for defective hardware components, shall be that Check Point, subject to the terms and conditions of this Section 1, and solely upon confirmation of a defect or failure of a hardware component to perform as warranted, shall at its sole option, either repair or replace the nonconforming hardware component or return of the price paid for the Hardware Product. All replacement parts furnished to you under this warranty shall be refurbished and equivalent to new, and shall be warranted as new for the remainder of the original warranty period. If a hardware failure occurs in the first 30 days from the product’s software activation, Check Point will replace it with new part or full unit as may be needed. All defective parts, which have been replaced, shall become the property of Check Point. All defective parts that have been repaired shall remain Your property. This warranty gives You specific legal rights. You may have other rights that vary from state to state.

54151HACS

Labor Category	Hourly GSA RATE W/ IFF
Senior Penetration Tester	\$171.03
Mid-Level Penetration Tester	\$143.58
Senior Incident Response Analyst	\$176.32
Mid-Level Incident Response Analyst	\$143.58
Senior Cyber Hunt	\$181.36
Mid-Level Cyber Hunt	\$139.04

Senior Risk & Vulnerability Analyst Mid-Level Risk & Vulnerability Analyst	\$179.47
Mid-Level Risk & Vulnerability Analyst	\$143.58

54151HACS Labor Category Descriptions

Special Item Number	IT Labor Category	Minimum/General Experience and Years of Experience	Functionality Responsibility (Summary)	Educational Responsibility
54151HACS	Senior Penetration Tester	More than 10 years relevant experience. Must have at least four years of practical experience conducting penetration testing. Serve as the lead Penetration Tester and responsible for management of penetration testing program. Must have a working knowledge of NIST 800 series guidance for cyber security.	Conducts remote and onsite testing of Information Technology Systems (IT) to detect weaknesses, vulnerabilities, and compliance issues. Experienced in Network architectures, operating systems, application software, and cyber security tools and techniques. Expert in the use of penetration testing tools, techniques, and attack vectors to be used in a sanctioned attack or intrusion for the sole purpose of evaluating the security of an IT system and to discover weaknesses, vulnerabilities, or compliance issues that are unknown to the system owner.	Bachelor's Degree in Computer Science, Programming, Software Engineering, or other related discipline from an accredited institution.
54151HACS	Mid-Level Penetration Tester	More than 5 years relevant experience. Must have at least three years of practical experience conducting penetration testing. Must have a working knowledge of NIST 800 series guidance for cyber security.	Conducts remote and onsite testing of Information Technology Systems (IT) to detect weaknesses, vulnerabilities, and compliance issues. Experienced in Network architectures, operating systems, application software, and cyber security tools and techniques. Expert in the use of penetration testing tools, techniques, and attack vectors to be used in a sanctioned attack or intrusion for the sole purpose of evaluating the security of an IT system and to discover weaknesses, vulnerabilities, or compliance issues that are unknown to the system owner.	B.S. Degree from an accredited institution. 6+ years of experience is equivalent to a BS degree.
54151HACS	Senior Incident Response Analyst	More than 8 years of practical experience with incident response. Must have a working knowledge of NIST 800 series guidance for cyber security.	Under general direction, leads security event monitoring and correlation within a tiered Security Operations Center. Proven experience and ability to leverage CND analyst toolsets to detect and respond to IT security incidents. Ability to implement standard procedures for incident response interfacing with Information Security Officer and IT staff. Conducts research and document threats and their behavior to include monitoring external	Bachelor's or Master's Degree in Computer Science or related discipline. 6 years of general experience is considered

Special Item Number	IT Labor Category	Minimum/General Experience and Years of Experience	Functionality Responsibility (Summary)	Educational Responsibility
			CSIRTS/CERTs. Provide recommendations to threat mitigation strategies. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Perform routine event reporting over time including trend reporting and analysis. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on design/Implementation/Administration role. Demonstrates in-depth knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection. Professionally certified, within a CND discipline, as Technical Level III as defined by DODI 8570 is a requirement.	equivalent to a Bachelor's Degree.
54151HACS	Mid-Level Incident Response Analyst	More than four years of practical experience with incident response. Must have a working knowledge of NIST 800 series guidance for cyber security.	Under general supervision, participates in security event monitoring and correlation within a tiered Security Operations Center. Proven experience and ability to leverage CND analyst toolsets to detect and respond to IT security incidents. Conducts research and document threats and their behavior to include monitoring external CSIRTS/CERTs. Assist in providing recommendations to threat mitigation strategies. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Perform routine event reporting over time including trend reporting and analysis. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on Implementation or Administration role. Demonstrates thorough knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection. Professionally certified, within a CND discipline, as Technical Level II as defined by DODI 8570 is a requirement.	Bachelor's Degree in Computer Science or related discipline. 6 years of general experience is considered equivalent to a Bachelor's Degree.
54151HACS	Senior Cyber Hunt Analyst	More than 8 years relevant experience. Experience in	Possess a strong knowledge of security operations concepts to include security incident and event management, cyber	Bachelor's or Master's Degree in

Special Item Number	IT Labor Category	Minimum/General Experience and Years of Experience	Functionality Responsibility (Summary)	Educational Responsibility
		computer network defense and in depth technical knowledge/mastery with intrusion detection systems. Must have a working knowledge of NIST 800 series guidance for cyber security.	intelligence, malware analysis, and tracing network traffic.	Computer Science or related discipline. 6 years of general experience is considered equivalent to a Bachelor's Degree.
54151HACS	Mid-Level Cyber Hunt Analyst	More than 4 years relevant experience. Experience in computer network defense and in depth technical knowledge/mastery with intrusion detection systems. Must have a working knowledge of NIST 800 series guidance for cyber security.	Possess a working knowledge of security operations concepts to include security incident and event management, cyber intelligence, malware analysis, and tracing network traffic.	B.S. Degree from an accredited institution. 6+ years of experience is equivalent to a BS degree.
54151HACS	Senior Risk & Vulnerability Analyst	More than 8 years relevant experience. Experience in computer network defense and in depth technical knowledge/mastery with intrusion detection systems. Must have a working knowledge of NIST 800 series guidance for cyber security.	Possess a working knowledge of network technologies such as: Windows, Linux Operating Systems; Database security, Active Directory, Service Oriented Architectures, vulnerability testing, networking protocols and topologies, security architectures, and incident management. Develops technical solutions including: information operations and analysis related to security intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools, data visualization techniques. Serves as lead analyst in the detection of malicious activity to prevent, detect, contain, and eradicated intrusions and intrusion attempts. Conduct analysis of system logs, forensic results, vulnerability assessment tool results, risk, and investigate instances of security concern throughout the enterprise. Ensure required cyber security policies are adhered to and that required controls are implemented.	Bachelor's Degree in Computer Science, Programming, Software Engineering, or other related discipline from an accredited institution. Experience above 8 years can be used in lieu of education where appropriate.
54151HACS	Mid-Level Risk & Vulnerability Analyst	More than 5 years relevant experience. Experience in computer network	Possess a working knowledge of network technologies such as: Windows, Linux Operating Systems; Database security, Active Directory, Service Oriented	B.S. Degree from an accredited institution. 6+

Special Item Number	IT Labor Category	Minimum/General Experience and Years of Experience	Functionality Responsibility (Summary)	Educational Responsibility
		defense and in depth technical knowledge/mastery with intrusion detection systems. Must have a working knowledge of NIST 800 series guidance for cyber security.	Architectures, vulnerability testing, networking protocols and topologies, security architectures, and incident management. Develops technical solutions including: information operations and analysis related to security intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools, data visualization techniques. Serves as lead analyst in the detection of malicious activity to prevent, detect, contain, and eradicate intrusions and intrusion attempts. Ensure required cyber security policies are adhered to and that required controls are implemented. Experience Conducting Web application, operating system, database & wireless testing and assessments using COTS tools.	years of experience is equivalent to a BS degree.

The Service Contract Labor Standards (SCLS) is applicable to this contract as it applies to the entire Multiple Award Schedule and all services provided. While no specific labor categories have been identified as being subject to SCLS due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CRF 541.300), this contract still maintains the provisions and protections for SCLS eligible labor categories. If and / or when the contractor adds SCLS labor categories / employees to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS matrix identifying the GSA labor category titles, the occupational code, SCLS labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.

Appliance Support Price Calculations:

ALL VALUES ARE BASED ON MSRP PRICES, THE GSA DISCOUNT OFF OF MSRP FOR CHECK POINT SUPPORT IS: 2%, EXCLUSIVE OF IFF

Value of SOFTWARE Products being Purchased or Renewed	CPES-SS	CPES-SS-STANDARD	CPES-SS-PREMIUM	CPES-SS-ELITE
< \$50,000	15	30%	40%	43%
\$50,000 - \$100,000	15	28%	36%	39%
\$100,001 - \$250,000	14	26%	33%	36%
\$250,001 - \$500,000	14	24%	30%	33%
\$500,001 - \$1 million	13	22%	27%	30%
\$1 million and above	13	20%	24%	27%

*Available in North America and other selected geographies

** Emergency engineer dispatch for critical software issues for more info [click here](#)

Please note: For Elite Support there is a minimum fee of \$3,500

Annual Direct APPLIANCE Support (EBS) Product Range	CPES-SS Not Available on HW	CPES-SS-STANDARD	CPES-SS-PREMIUM	CPES-SS-ELITE	CPES-SS-STANDARD-ONSITE	CPES-SS-PREMIUM-ONSITE	CPES-SS-ELITE-ONSITE
High End	N/A	12%	17%	20%	20%	23%	26%
Mid Range	N/A	12%	17%	20%	22%	25%	28%
Low End	N/A	12%	17%	20%	27%	30%	33%
2 Blade appliance xx2 series	N/A	Standard account rate	Premium account rate	Elite account rate	Standard account rate + 10%	Premium account rate + 8%	Elite account rate + 8%

xt Flight Out/Express Delivery is available in the European Union and mainland US. Appliances are shipped during normal business hours and may arrive during off hours or next business day until 9AM.

** Onsite services are provided world wide by Check Point certified technicians. For available locations click [Check Point Onsite services](#).

*** Emergency engineer dispatch for critical software issues for more info [Chat](#) Please note: On site RMA services are not available on all 1100 appliances and 600 appliances. Please note: For Elite Support there is a minimum fee of \$3,500

Note: On site Hardware Support becomes effective one (1) month from the day it was purchased.

Note: All other Check Point appliances that do not appear in the Appliance Classification table receives regular account rate and no onsite service is available.

Note: Customers may upgrade support for specific appliances based on their operational needs regardless to the customer's User Account Service Level Agreement.

Note: Onsite Support for Accessories is calculated at the account rates the same as EBS and CES appliances in the Low, Mid and High end Product range. For example EBS is 17% for Premium-Onsite, 12% for Standard Onsite, CES is 15% for CO-Premium Onsite, 10% for CO-Standard Onsite for accessories.

Training Classes

SIN	Part Number	Description	Daily GSA Rate
611420	CPTS-PRO-21K-NGTX-JS	NGTX Jumpstarting 21000 Appliance Including travel expense, assistance in implementation and basic knowledge transfer	\$34,051.39
611420	CPTS-PRO-4K-JS	Jumpstart for 4000 Appliance including travel expense assistance in implementation and basic knowledge transfer	\$9,591.94

611420	CPTS-PRO-4K-NGTP-JS	NGTP Jumpstarting 4000 Appliance Including travel expense, assistance in implementation and basic knowledge transfer	\$12,949.12
611420	CPTS-PRO-4K-NGTX-JS	NGTX Jumpstarting 4000 Appliance Including travel expense, assistance in implementation and basic knowledge transfer	\$13,908.31
611420	CPTS-PRO-ADD-ATAM 1	Additional on-site TAM days	\$38,367.76
611420	CPTS-PRO-ATAM1	Advanced Technical Account Management	\$71,939.55
611420	CPTS-PRO-ATAM2	Up to two days of dedicated support on the customer site	\$43,163.73
611420	CPTS-PRO-ATAM3	Up to one day of dedicated support on the customer site	\$23,979.85
611420	CPTS-PRO-CON-10D	On-Site Engineering - 10 days package	\$21,581.86
611420	CPTS-PRO-CON-5D	Consulting Services - 5 days bundle	\$11,510.33
611420	CPTS-PRO-CON-DAILY	On-Site Engineering - Daily Consulting	\$2,397.98
611420	CPTS-PRO-CON-MNTH	Professional Service Engineer on monthly basis	\$38,367.76
611420	CPTS-PRO-DDOS-JS	Jumpstart package for DDoS Protector solution deployment	\$14,867.51
611420	CPTS-PRO-EXP-DAILY	Senior Expert Consultant, Consulting services - daily rate (non-business hours/ urgent rate / Senior Expert)	\$3,357.18
611420	CPTS-PRO-OPTIMIZE- GWADD	Analysis of a single GW/Cluster (Add-on to Smart Optimize only)	\$2,397.98
611420	CPTS-PRO-PERF-TRN	Performance and optimization Premium Course, conveyed by Professional Services expert - 2 days	\$2,877.58
611420	CPTS-PRO-PJM	A Project Manager will be engaged and assist with building and monitoring a project plan, tasks, risks, resources, dependencies and progress	\$3,357.18
611420	CPTS-PRO-TE-CUST	Threat Emulation customization: either image is custom built offsite per customer needs or scripts development for TE API	\$11,989.92
611420	CPTS-PRO-TE-JS	Threat Emulation Jumpstart, implementation and basic knowledge transfer. Limited to 3 days on-site and 0.5 day off-site	\$9,591.94
611420	CPTS-PRO-61K-JS	Jumpstart for 61000/41000 Appliance including travel expense, assistance in implementation and basic knowledge transfer	\$24,050.00

