Check Point
Collaborative Enterprise Support

Service Level Agreement

Worldwide Technical Services
Check Point Software Technologies Ltd.

Updated: 01-Jan-2025

COLLABORATIVE ENTERPRISE SUPPORT (CES)
SERVICE LEVEL AGREEMENT

This Collaborative Enterprise Support Service Level Agreement (the "SLA") is an agreement between you, the Certified Collaborative Support Provider (hereinafter "CCSP") and Check Point Software Technologies Ltd. (hereinafter "Check Point"). This SLA is intended to identify the features and define the processes involved with the delivery of various support functions to CCSP for the Software and Hardware products purchased and licensed from Check Point under this collaborative relationship.

1. DEFINITIONS:

"Advance Hardware Replacement" means a Hardware replacement service for Customers who have purchased Hardware Support, whereby after Check Point TAC approves an RMA, Check Point delivers a replacement to Customer's Site before Customer returns the faulty hardware to Check Point.

"ACE Partner" means an authorized Check Point partner who is staffed with Check Point Certified Professionals and Appliance Certified Experts (ACE) in accordance with Check Point ACE Partner requirements. A CCSP is not necessarily an ACE partner, as ACE requires obtaining a specialization to provide to Check Point appliance customers with special maintenance for hardware issues involving the replacement of an appliance within 4 hours or Next Business Day of notification of a problem.

"Activation Date" means the date a License Key is registered for activation of Software within the Check Point User Center.

"Appliance" shall have the meaning set forth in this SLA for the term "Hardware".

"Business Day" means normal working day in the time zone where the Customer is located.

"CCSE" stands for Check Point Certified Security Expert, which means a level of certification by Check Point which is recognized as the industry standard for Internet security certifications.

"CCSM" stands for "Check Point Certified Security Master" (CCSM), which is the most advanced Check Point technical credential, which validates the ability to use advanced commands to troubleshoot, configure and optimize Check Point Security Systems. To earn the CCSM, one needs to possess an active CCSE (R80 or higher) certification and achieve 2 infinity Specialist accreditations. With an active CCSE certification as well as two Infinity Specializations, the CCSM will be automatically awarded. There is a top certification "Check Point Certified Security Master Elite" (CCSM Elite), which will also be automatically awarded with an active CCSE and four Infinity Specializations.

"CCSP" shall mean the party identified as the Certified Collaborative Support Provider, who is the Certified Professional having the expertise and knowledge of customer needs to provide first-line support to customers having access to Collaborative Enterprise Support, and who will work directly with Check Point hereunder for backline support in order to address the customer's problems.

"CCTE" means a Check Point Certified Troubleshooting Expert (CCTE) who provides advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing a Check Point security environment.

"Certified Professional" means an individual who has passed the appropriate current Check Point Certification Test(s) to demonstrate technical competency. The current minimum requirement of a Certified Professional is a Check Point Certified Security Expert (CCSE™) for the current Major Release of Network Software and Check Point Certified Troubleshooting Expert (CCTE).

"Check Point" means Check Point Software Technologies Ltd., the party to this SLA with CCSP.

"Check Point CES Support Plan Descriptions" shall mean the document attached hereto as <u>Exhibit A</u>, which outlines the level of support to be provided to end users of the Software and Appliance products as part of the Collaborative Enterprise Support (defined below).

"Collaborative Enterprise Support (CES)" shall mean the currently marketed Check Point Software and Appliance support solution available to customers to keep their businesses secure, which combines the capabilities of first-line support of the CCSP, with the backline expertise and resources of Check Point. Information on the program, its support levels, as well as other details, is contained in Exhibit A (Check Point CES Support Plan Descriptions), and/or may be obtained directly from Check Point.

"Customer" means the party identified as the organization that has purchased a Check Point Support offering in connection with this SLA and initially identified a problem or issue with the Software or Appliance. Such customer interfaces directly with CCSP on first-line support issues with respect to Problem Resolution (defined below).

"Dead On Arrival (DOA)" means that a purchased Hardware product fails to operate substantially in accordance with published specifications due to defects in design, materials and workmanship during the first thirty (30) days from activation or no more than one hundred and twenty (120) days from the date of Check Point's shipment of the Hardware product, whichever is less.

"Designated Contacts" shall mean the CCSP engineering resources that are Check Point Certified Professionals and are established in the User Center account associated with the Customer support contract.

"Device Number" means a unique identifier of a hardware device, which can be located in a label on a Hardware Product. Check Point uses Media Access Control (MAC) Address, Serial Number (SN), or Service Tag Number (STN) as a Device Number, depending on the type of Hardware.

"Documentation" means user and technical manuals provided by Check Point for use with the Software and Hardware.

"Endpoint Security Product(s)" means Check Point product(s) with an Endpoint device security focus.

"Enhancement" means all Software changes, including new releases, new versions, product improvements, system modifications, updates, upgrades, Service Packs, Feature Packs, field modifications, and all Hardware changes, including official Check Point Hardware product enhancements and accessories.

"Error" means an Error in the product, which degrades the product as defined by the Severity definitions, as compared to Check Point published functionality and performance specifications.

"Hardware" means a computing device and/or its component with a specific function and limited configuration ability. The Hardware is sold by Check Point for the purpose of executing the specific Check Point Software supplied with it.

"Information" means any idea, data, program, technical, business, or other intangible information, however conveyed.

"Intellectual Property" means Patents, copyrights, trademarks, and/or trade secrets whose owners have rights at law or in equity to exclude others from exploiting such property.

"Level 1 Support" means the ability to provide general pre and post-sales product information; hardware and software configuration; questions on upgrade Support; collect relevant technical problem identification information; perform base problem determination; provide basic Support on the standard products, protocols and features; replace Field Replaceable Units (FRUs) or whole Hardware units.

"Level 2 Support" means the ability to provide Level 1 Support plus the ability to resolve the majority of misconfigurations, troubleshoot and simulate complex configuration, hardware, and software problems; perform Hardware diagnostics to determine Hardware malfunction; support problem isolation and determination of product specification defects; provide lab simulation and interoperability and compatibility testing for new software and hardware releases prior to being deployed into a Customer production network; define an action plan; provide advanced Support on all products, protocols and features; have the ability to analyze traces, diagnose problems remotely, and provide Customer with complete steps to reproduce a problem.

"Level 3 Support" means the ability to provide Level 1 and Level 2 Support plus the ability to provide software enhancements such as patches and Hotfixes, fixing or generating workarounds that address software bugs; troubleshoot bugs that were not diagnosed during Level 2 Support; work with Customers to resolve critical situations, and building action plans with Customers to address complex issues.

"License Key" means code provided by Check Point, which activates the Software and enables the Software to operate.

"Major Release" means the current issuance of Software and/or Hardware that is designated by Check Point, as a change in the number or name, signifying a new product level. Hot Fix Accumulators (HFAs), Hotfixes, and/or Feature Packs do not constitute a Major Release change.

"Network Security Product(s)" means Check Point product(s) with network security focus.

"Previous Sequential Release" means Release of Software or Hardware, which has been replaced by a subsequent version of the product.

"Release" means Major Release of the same product.

"Problem Resolution" means the use of reasonable commercial efforts to resolve the reported problem. These methods may include (but are not limited to): configuration changes, patches that fix an issue, replacing a failed hardware, reinstalling the software, etc.

"Respond" means addressing the initial request and taking ownership of the issue.

"Response Time" means the amount of time elapsed between the initial contact by Customer to CCSP (indirect) or Check Point TAC (direct) (for co-Premium/co-Elite support level only) and the returned response to Customer by CCSP or Check Point support staff.

"RMA" means Return Material Authorization (RMA), the process of replacing a faulty Hardware or a component of a Hardware product. The process must be authorized by Check Point TAC.

"Service Level Agreement (SLA)" means the Service Level Agreement (SLA) that identifies the features and defines the processes involved with the delivery by Check Point of various support functions to the CCSP (and through the CCSP to the customer), as presented by this document's: (1) CES Support Term and Conditions; and (2) Exhibit A – Check Point CES Support Plan Descriptions.

"Service Request (SR)" means a single issue opened with Check Point TAC. The SR number identifies the Service Request. The format for the unique SR number can be as follows: 1-nnnnnnnnnn or 11-nnnnnnnn ("n" is a digit).

"Severity" Definitions for Network Security product(s):

"Severity 1" means
(a) an Error with a direct security impact on the product;
(b) an Error isolated to Software or Appliance in a production environment that renders the product inoperative or causes the product to fail catastrophically; e.g., critical system impact, system down;

(c) a reported defect in the licensed product in a production environment, which cannot be reasonably circumvented, in which there is an emergency condition that significantly restricts the use of the licensed product to perform necessary business functions; or

(d) inability to use the licensed product or a critical impact on operation requiring an immediate solution.

"Severity 2" means

(a) an Error isolated to Software or the Appliance that substantially degrades the performance of the product or materially restricts business; e.g., major system impact, temporary system hanging;

(b) a reported defect in the licensed product, which restricts the use of one or more features of the licensed product to perform necessary business functions but does not completely restrict use of the licensed product; or

(c) ability to use the licensed product, but an important function is not available, and operations are severely impacted.

"Severity 3" means

(a) an Error isolated to the Software or Appliance that causes only a moderate impact on the use of the product; e.g., moderate system impact, performance/operational impact;

(b) a reported defect in the licensed product that restricts the use of one or more features of the licensed product to perform necessary business functions, while the defect can be easily circumvented; or

(c) an Error that can cause some functional restrictions but it does not have a critical or severe impact on operations.

"Severity 4" means

(a) a reported anomaly in the licensed product that does not substantially restrict the use of one or more features of the licensed product to perform necessary business functions; this is a minor problem and is not significant to operation; or

(b) an anomaly that may be easily circumvented or may need to be submitted to Check Point Research and Development as a request for enhancement.

"Severity" Definitions for Endpoint Security product(s):

"Severity 1" means

(a) an Error with a direct security impact on the product; or

(b) an Error isolated to Software, for which there is no reasonable Workaround, which renders the product inoperative, causing the end-point devices to fail catastrophically, affecting more than 1000 end point devices or 35% of deployed client base (in any case more than 100 affected end-point devices) within a production environment (not pre-deployment or staging) where end-point devices have been interrupted and not recovered; e.g., severe and general deployment wide system impact, systems are down, making end-point devices unable to perform (even with reduced performance) necessary business operations even after a change of, and/or addition of procedures, configurations, applications, tools and/or data.

"Severity 2" means

(a) an Error isolated to Software, for which there is no reasonable workaround, which substantially degrades the usability of the end-point devices, restricting the usage of and/or access to one or more necessary business functions without completely restricting the use of the licensed product, affecting more than 500 end-point devices or 25% of deployed client base (in any case more than 50 affected end-point devices) within a production environment (not pre-deployment or staging) where the end-point devices and/or Software may have been interrupted but recovered, in part or completely; e.g., end-point devices are operative but with limited capacity, substantially impacting the end-point devices' ability to perform one or more necessary business functions; end-point devices and/or Software are operative, but an important product function is unavailable or not operating; end-point devices and/or Software may have been interrupted but recovered, in part or completely; inability to connect to the Internet /Intranet; or

(b) an Error causing severe Software deployment/upgrade problems without prohibiting necessary business operations, affecting more than 500 end-point devices or 25% or more of the actual/intended client base (at least 50 devices affected); it may, or may not, be possible to circumvent the error, e.g., inability to

install and/or upgrade product, without prohibiting the end-point devices ability to perform necessary business operations; or business operations are not prohibited but may run with reduced performance.

"Severity 3" means

(a) an Error isolated to Software, for which there is a reasonable Workaround, or an Error that causes only a minor impact on the end-point client. Restriction in usage of one or more features of the licensed product with minor impact of necessary business functions. The Error can cause some functional restrictions but it does not have a critical or severe impact on operations, e.g., the end-point device is operational but may experience performance or operational limitations; or

(b) an Error isolated to Software only affecting one or a limited number of individual end-point devices, that is not common for the installed end-point device population; it may, or may not, be possible to circumvent the error, e.g., an individual end-point device(s) is encountering issues not common for deployed end-point device client base.

"Severity 4" means a reported anomaly in the licensed product that does not substantially affect end-point ability to perform normal business operations. This is a minor problem and does not constitute any significant limitation to products ability to allow normal business operation. An anomaly may be easily circumvented, e.g., a product cosmetic anomaly or documentation flaw; end-point devices and/or Software may have been interrupted but recovered.

"Shelf Spare Unit(s)" means Check Point Hardware unit(s) that is stored at Customer's Site and which is reserved for Hardware replacement usage only in case of failure of Customer's Hardware which is covered under Check Point On-Site Hardware Support Plan.

"Site" means the physical location where System(s) are installed as specified by Customer in Customer's User Center account.

"Software" means the object code version of the intangible information constituting one or more computer or apparatus programs and the informational content of such programs, together with any Documentation supplied in conjunction with, and supplementing such programs, the foregoing being provided to Customer by way of electronic transmission or by being fixed in media furnished to Customer.

"Software Subscription" means registered access to modifications, corrections, and/or updates to Software; including Hot Fix Accumulators (HFAs), security fixes, Feature Packs, and/ or major upgrades, provided to Customer by unlimited web download access or by mail upon Customer's request. Software Subscription is a deliverable for all Support Contracts.

"Support" means the technical telephone, web and e-mail assistance provided by Check Point to help the CCSP Designated Contact with Problem Resolution with respect to a Customer covered by a Support Plan and Hardware replacement services as set forth in this SLA.

"Support Plan" means the CES Support program offering options and benefits set forth on Exhibit A.

"System(s)" means the Hardware, Software and Documentation that have been provided to Customer by Check Point or Check Point's authorized resellers/partners.

"TAC" means Check Point Technical Assistance Center, which is staffed by Check Point Support personnel providing assistance with diagnosis and resolution of defects and/or failures in Check Point products.

"Workaround" means a change in the followed procedures or data to avoid error without substantially impairing use of the product.

2. SUPPORT:

A description of Check Point's CES Support offerings is set forth on Exhibit A, attached hereto. Upon Check Point's acceptance of a valid purchase order, and corresponding payment for that Support offering selected,

Customer will be entitled to receive Support through the CCSP, according to the features and benefits provided under that offering, subject to the terms and conditions of this SLA.

2.1 <u>Technical Support:</u>
For Customers covered under a Check Point CES Support offering, technical Support will be provided via the CCSP pursuant to the terms of Section 5 TECHNICAL SUPPORT. Check Point agrees to provide Support, where appropriate, to CCSP, which may include but is not limited to, the following actions:

(a) Provide CCSP with access to product update releases, related Documentation and knowledge articles, upon general commercial release;

(b) Provide CCSP with access to TAC Technical Representatives who will work with CCSP to diagnose customer issues, and provide Problem Resolutions, including escalating the issue through TAC management as needed.

2.2 <u>Hardware Replacement</u>. For Customers covered under Hardware Support, Check Point will use commercially reasonable efforts to provide Hardware replacement via the CCSP in accordance with the terms set forth in Section 4 HARDWARE REPLACEMENT.

2.3 <u>On-site Hardware Support</u>. For those Customers whose Hardware Support level includes an on-site service feature, the Customer will approach their CCSP for 1st level diagnosis. If the CCSP determines that the issue requires RMA replacement, the CCSP will open a Service Request on behalf of the Customer with Check Point TAC. For Appliance with Co-Premium or Co-Elite support, after a repair action plan has been defined by TAC, an RMA process will be initiated by TAC immediately. For Appliance with Co-Standard support, after TAC determines with the CCSP that the hardware issue is related to a malfunction of one of the Hardware components, and after a repair action plan has been defined, an RMA process will be initiated by Check Point TAC. For Customers whose Hardware Support levels includes an on-site service feature, Check Point will use commercially reasonable efforts to dispatch a Check Point Certified On-site Technician or ACE Partner to the Site in accordance with the terms and timeframes of such plan as set forth on <u>Exhibit A</u>. On-site Hardware Support is effective one (1) month from the day it was purchased. Provision of on-site support is subject to the following limitations:

(a) On-site Hardware Support is limited to Advance Hardware Replacement only, and does not include on-site service for Software troubleshooting or any Software related issues.

(b) On-site Hardware Support may not be available for some Check Point Hardware products or in some geographic regions, and may require a set-up period before it can be made available to Customers. During such set-up period, Check Point will use commercially reasonable efforts to provide to Customer the closest available service then available, with respect to such product line or in such geographic region. Changes may apply outside of Check Point's normal service area.

(c) On-site service response times may be dependent upon the Customer's Site address for the Hardware, the timely arrival of replacement parts at Customer's Site, and accessibility to the Site.

Note: For full unit replacement, a technician will verify that the current base software image and hotfix level are installed and will restore a backup of the machine only if the prerequisite software image dependencies are preinstalled and the backup files are available onsite and handy.

2.4 <u>On-site Software Support for Critical Severity 1 Issues</u>. For those Customers covered under Co-Elite Support, the Customer, or CCSP partner on behalf of the Customer, shall contact Check Point TAC directly by telephone or live chat. After TAC confirms that the matter is a Severity 1 issue, TAC and the Customer will work diligently, with highly skilled, experienced engineers to resolve the critical situation and to restore operation. In the case the criticality of the issue remains or no progress is made, after four (4) hours, Check Point will use commercially reasonable efforts to dispatch a local engineer to Customer's Site. If no local resources are available, travel arrangements will be made for the next available flight to the Customer's Site. The engineer will remain on site until the issue is no longer defined as critical (an acceptable resolution or workaround was achieved) or up to three (3) days, with travel and expense included. Provision of on-site critical Severity 1 case support under Co-Elite Support is subject to the following limitations:

(a) A Co-Elite Customer is entitled up to three (3) visits on-site a year as required to resolve critical Severity 1 cases.

(b) For any additional days on site that is required after the first 3 days, will be charged at a discounted rate of $2,000 per day.

(c) On-site critical case Support is limited to Software Support only, and does not include on-site service for Hardware issues and Hardware replacement. For On-site Hardware Support, please refer to Section 2.3 Onsite Hardware Support and Appliance Support SLA options as set forth on Exhibit A.

(d) On-site critial case Support may not be available for some Check Point Software products or in some geographic regions, and may require a set-up period before it can be made available to Customers.

(e) For Co-Elite support service for critical issues which requires fast arrival to the site, Check Point will cover all locations which are accessible within 12 hour elapsed commercial travel time from G7 countries hubs (US (mainland), UK, Germany, Italy, France, Japan, and Canada). In some remote locations, entry certifications requirements might add additional time to the engineer arrival on site.

(a) Co-Elite support is account based and requires that the entire User Center install base be covered by the Co-Elite SLA. Co-Elite may not be applied to cover only portions of the User Center's products.

(b) It is necessary that the Co-Elite Customer and the CCSP commit the necessary resources around the clock (24x7) in working with Check Point towards Problem Resolution of Severity 1 Errors.

For Severity definitions for Network Security Product(s) or Endpoint Security Product(s), refer to Section 1 DEFINITIONS, "Severity" Definitions for Network Security Product(s) and "Severity" Definitions for Endpoint Security product(s).

2.5 Support Lifecycle.

(a) Check Point provides a comprehensive support lifecycle for its Software and Hardware. Support lifecycle policy is available at URL: http://www.checkpoint.com/services/lifecycle/.

(b) Check Point will provide End of Support notification for discontinued Software to CCSP and Customer through an announcement posted on the Check Point Software Support Timeline website at URL: https://www.checkpoint.com/support-services/support-life-cycle-policy/.

(c) Check Point will provide the date of Check Point's new appliance availability announcement and End of Support notification for discontinued Hardware to CCSP and Customer through an announcement posted on the Check Point Appliance Support Timeline website at URL: https://www.checkpoint.com/support-services/support-life-cycle-policy/.

(d) Check Point reserves the right to modify Support Lifecycle policy at any time; notifications regarding changes in policy will be posted on the websites in Section 2.5 (b) and 2.5 (c).

2.6   Nonconformance. If Check Point determines the problem is due to nonconformance to published specifications of a Software version, or another substantial Check Point related problem, then under Check Point's Support plan, Check Point will provide any Software fix for the reported nonconformance that may be available at the time the problem is reported. If there no such fix is available, Check Point will use commercially reasonable efforts to remedy such nonconformance, which may include a Workaround or other temporary fix to the Software. If a Workaround or other temporary fix to the Software is provided, Check Point shall make reasonable commercial efforts to include it in a subsequent Software updates.

2.7 Exclusions.

Support does not include the following items or actions:

(a) Step-by-step installation of Software or Service Packs;

(b) Onsite services (unless Customer's level of Support, as purchased, includes this feature), Professional Services, or Educational Services;

(c) Modification of software code, security-policy configuration, audits, or security design.

Check Point shall have no obligation to Support:

(a) An altered, damaged, or modified product or any portion of the product incorporated with or into other software, hardware, or products not specifically approved by Check Point;

(b) Product problems caused by Customer negligence, misuse, or misapplication, or use of the product other than as specified in the Check Point user manual, or any other causes beyond the control of Check Point;

(c) Product installed on any computer hardware that is not supported by Check Point;

(d) Product not purchased from the Check Point Price List.

(e) Products subjected to unusual physical or electrical stress, misuse, negligence or accident, or used in ultra-hazardous activities;

(f) Products that are past their End-of-Support date, as provided in Section 2.5 above.

Check Point shall have no obligation to provide Support if:

(a) Appropriate payment for Support has not been made; or

(b) Customer annual Support term has expired without renewal.

2.8 <u>Reporting Non-Check Point Errors to Partner</u>. Upon working the Service Request under normal processes, and with appropriate management review, if at that point Check Point believes that a problem reported by the CCSP may not be due to an error in the Check Point product, Check Point will notify the CCSP. At that time, the CCSP may: (a) instruct Check Point to proceed with problem determination at CCSP's possible expense as set forth herein; or (b) instruct Check Point that CCSP does not wish the problem to be pursued at CCSP's possible expense.

If CCSP requests that Check Point proceed with problem determination at CCSP's possible expense and Check Point determines that the error was not due to the error in the product, CCSP shall pay Check Point, at the Check Point then-current standard consulting rates, for all work performed in connection with such determination, plus reasonable related expenses incurred therewith. CCSP shall not be liable for:

(a) problem determination or repair to the extent the problems are due to anomalies in the Check Point product; or

(b) work performed after the CCSP has notified Check Point that it no longer wishes problem determination to be continued at CCSP's possible expense (such notice shall be deemed given when actually received by Check Point).

If CCSP instructs Check Point that it does not wish the problem pursued at CCSP's possible expense or such determination requires effort in excess of CCSP instructions, Check Point may, at its sole discretion, investigate the anomaly with no liability thereof.

3. CCSP AND CUSTOMER OBLIGATIONS:

3.1. <u>CCSP Requirements</u>. It is required that CCSP provide 24x7 Service and Support operation, and allow Customer to open unlimited Service Requests for Service and Support. CCSP shall commit to the following: (i) 30 minute response time to Customer for Severity 1 issues (note that in the case of a Co-Elite Customer, both Severity 1 and Severity 2 issues shall require a 30 minute response time); and (ii) a minimum 4-hour response time for all other issues. CCSP shall have the ability to provide Level 1 & Level 2 Support Services, and for those Customers having an onsite Support feature, the ability to provide fast arrival on site.

3.2. <u>Support Level Alignment.</u> CCSP shall maintain alignment between the Customer, CCSP and Check Point support levels, so that CCSP will only sell to Customer the same level of support purchased from Check Point. Thus, if CCSP sells a 24x7 Customer SLA, a Co-Premium/Co-Elite level support must be purchased by CCSP from Check Point (CCSP may not buy from Check Point a Co-Standard level support and resell it to Customer as a higher (7x24) support level).

3.3. <u>CCSP shall be the point of contact for support issues</u>. CCSP will perform Level 1 Support and Level 2 Support for Customers in connection with any Software and Appliance failure reported to CCSP by Customer as set forth below. When issues are escalated to Check Point (i) the Service Request will be submitted by a CCSE, CCSM or CCTE only, and (ii) the test and debug files will be according to Check Point's guidelines for diagnostics and troubleshooting.

3.4. <u>Level 1 Support.</u> requires CCSP to act as the initial and primary interface to the Customer and thereafter requires CCSP to perform various responsibilities such as:

- Collection of relevant information.

- Problem identification and analysis.

- Initial diagnosis.

- Troubleshooting.

- Problem Resolution, where possible.

- Request approval from Check Point TAC to authorize the RMA for Co-standard Customer, to be provided at Check Point's sole discretion, in case of hardware failure in an appliance.

3.5. <u>Level 2 Support.</u> requires CCSP to perform greater troubleshooting and diagnosis, and thereafter requires CCSP to perform various responsibilities, such as:

- Perform greater troubleshooting and diagnosis.

- Potentially replicating the issue in a test lab environment.

- Provide Workaround solutions to Customer issues.

- Diagnose a Hardware issue, and determine if is related to a malfunction of one of the Appliance components, and authorize the RMA in case of hardware failure in a Check Point appliance. (Not applicable to old Nokia IP Appliances with legacy Essential /Access Appliance Support).

3.6. <u>Direct Contact</u>. In some limited cases, Check Point may provide Support directly to Customers in order to resolve Service Requests. CCSP and Customer are expected to provide standard support information in accordance with Section 3.9 (Support Information) in order to bring resolution to an issue in a timely fashion.

3.7. Certification and Staffing. All CCSP personnel contacting Check Point for Support must be fully trained Check Point Certified Professionals with respect to both the Major Release of the Check Point Software and the current issue with which CCSP requires assistance. The CCSP certification process requires that CCSP: (i) pass annual review and audit processing guidelines, (ii) submit performance metrics to Check Point annually or upon request, and (iii) meet customer satisfaction survey criteria at least 4 out of 5.

    3.7.1.   Staffing CCSE /CCSM /CCSM Elite. The number of Active CCSEs/CCSMs is set forth in the table below. The term 'Active' refers to a CCSE/CCSM (or CCSM Elite) that obtains updated certification every two (2) years. CCSEs must be trained on current Major Release and supported versions. The minimum percentage of Service Requests out of the total solved by CCSP is 75%.

    3.7.2   Staffing CCTE: The number of Active CCTEs is set forth in the table below. The term 'Active' refers to CCTE which obtains an updated certification every two (2) years.

    3.7.3.   RMA Approval Certification for Co-Elite and Co-Premium SLAs. Annual RMA rate lower than 7.5% and False Positive Rate lower than 25%.

        The Collaborative Enterprise Support level that the CCSP offers for sale to customers requires that the CCSP have a minimum number of Check Point Certified Security Experts (CCSE) and Check Point Certified Troubleshooting Experts (CCTE) on staff entitled to call for technical support:

Partner Level	Check Point Certified Security Expert/Master (CCSE/CCSM)	Check Point Certified Troubleshooting Expert (CCTE)
Distributor	2	2
2 Stars	1	1
3 Stars	1	1
4 Stars	2	2
5 Stars	2	2
Elite	2	2

For example:

A 2 Stars partner with CCSP needs to complete 1 CCSE/CCSM + 1 CCTE to meet the minimum requirements for CCSP partner.

An Elite partner with CCSP needs to complete 2 CCSE/CCSM + 2 CCTE to meet the minimum requirements for CCSP partner.

3.8. Designated Contacts: CCSP agrees that contact with Check Point will be through the specified number of Designated Contacts. Designated Contacts are named contact specified as Support Contacts within the CSP User Center Account containing the CSP Support ID, and specified as named user within the associated CSP PartnerMap account. Refer to the number of approved Designated Contracts listed in Section 3.7 Certification and Staffing. The ability to add additional contact(s) may be purchased according to prevailing program guidelines.

3.9. Support Information: The following information is requested to open an issue with Check Point TAC:

- CCSP must provide Check Point's Technical Representatives with Customer details when they open Service Requests (SR), including, but not limited to, the company name, UC number, Customer name, e-mail, and phone, and the date that the Customer opened the SR with the CCSP.

- Execute debug information, divert the output to a file, and attach the file to a web request.

- Describe the hardware platform(s) involved in this issue, including the amount of memory, disk space, and NIC card types (manufacturer and model).

- Describe the operating system(s) involved in this issue, including the version number and patch level information.

- Provide a detailed description of the problem or issue, including any symptoms noted, any patterns seen and any specific error messages received.

- Log file contains relevant log errors.

- Any kind of technical information and network environment information that Check Point's TAC engineer defines as necessary to solve the issue.

- Check Point may ask for remote access to the Customer's environment where the issue occurred.

CCSP will be asked to provide or verify the information needed for the understanding and resolution of the problem. Check Point understands that due to unusual circumstances, it may not always be feasible to include all of this information. In order to provide better service to the CCSP, Check Point requests that this information and additional information (as needed), be provided as soon as possible, as access to the appropriate data and information facilitates Problem Resolution. If it is not possible to provide this information, Check Point may be hindered in the ability to bring timely resolution to an issue.

3.10.   Network Access. To the extent possible, and as requested by Check Point, CCSP and Customer understand that it may be necessary to provide Check Point or its authorized Technical Representative access to the affect network environment for any Severity 1 issue, or when Check Point determines that its Technical Representative need to access Customer's network in order to remotely diagnose an issue. CCSP and Customer understand that if access is not provided as requested by Check Point, problem determination will be slower or impaired.

3.11.   System Information. CCSP and Customer must provide to Check Point information for each System under a Support Plan by registering all products in the Customer's User Center Account with accurate details:

(a)   Product License Key or Device Number;

(b)   Physical Site location of the Hardware product; and

(c)   Site contact person.

If Customer physically moves any Hardware from the original Site to an other location, CCSP or Customer must inform Check Point of such change immediately with updated Site location and contact. It is Customer's responsibility to update such change in the Customer's User Center Account. Prior to Check Point's receipt of such notification from Customer, Check Point shall not be liable for any lapses in service coverage or Hardware delivery delays with respect to such Hardware.

3.12.   Backup and Removal of Data.

To reconstruct lost or altered Customer files, data, or programs, Customer must maintain a separate backup system or procedure that is not dependent on the Software or Hardware products under Support.

Where applicable, before receiving Hardware Replacement Services or before disposal or return of Hardware to Check Point, CCSP and Customer agree to:

(a) backup and secure all programs and data contained in the Hardware;

(b) securely erase all programs and data not provided by Check Point with the Hardware product. CCSP and Customer acknowledge that, to perform its responsibilities under this Replacement Service, Check

Point may ship all or part of the Hardware product or its Software to third party locations around the world, and CCSP and Customer authorize Check Point to do so; and

(c) remove all features, parts, options, alterations, and attachments not provided by Check Point with the Hardware product, and ensure that the Hardware is free of any legal obligations or restrictions that prevent its exchange.

3.13. <u>On-site Access</u>. Where applicable, CCSP and Customer agree to provide Check Point or its authorized partner with sufficient and safe access to Customer's facilities in order to permit Check Point to fulfill its obligations.

3.14. <u>Customer Survey</u>. Upon request by Check Point, CCSP shall provide Check Point with a list of its customers under support for the purpose of customer satisfaction survey. Check Point reserves the right to directly contact Customer for the purpose of soliciting Customer feedback about the CCSP in order to ensure the quality and consistent delivery of Support services by CCSP.

4. HARDWARE REPLACEMENT:

4.1 <u>Hardware Return Procedure</u>. If a Hardware product or one of its component parts does not function during the Hardware Support period, and such nonconformance can be verified by Check Point, Check Point, at its election, will provide Advance Hardware Replacement service with a refurbished part /unit for the Hardware under the type of Hardware Support Plan Check Point designates for that Hardware. A defective Hardware product or one of its component parts may only be returned to Check Point upon Check Point's prior written approval. Any such approval shall reference a Returned Material Authorization ("RMA") number issued by an authorized Check Point service representative. To request an RMA number, CCSP must contact Check Point TAC and open a Service Request. Customer should always register the Hardware Product in Customer's Check Point User Center account. If Customer does not register the Hardware Product with Check Point, Customer may be required to present proof of purchase as evidence of entitlement to Hardware Support service. The Hardware Product's Device Number will be required for all RMA cases.

Transportation costs, if any, incurred in connection with the return of a defective item to Check Point shall be borne by Customer. If such RMA Service orders are covered by Standard On-site, Premium On-Site or Elite On-Site SLA, then for the return of the defective item, Check Point will provide prep-paid shipment labels and customer will arrange pick-up of the defective item with the respective shipment service provider. Any transportation costs incurred in connection with the redelivery of a repaired or replacement item to Customer by Check Point shall be borne by Check Point.

4.2 <u>Hardware Replacement Procedure</u>. For Customers who have purchased Support for their Hardware, upon a suspicion of a Hardware related issue, the Customer will approach their CCSP for 1st level diagnosis. If the CCSP determines that the issue requires RMA replacement – the CCSP will open a Service Request on behalf of the Customer with Check Point TAC. For Appliance with Co-Premium or Co-Elite support, Check Point TAC will process RMA immediately. For Appliance with Co-Standard support, Check Point will attempt to diagnose and resolve problem over the phone or web. Upon determination that the Hardware issue is related to a malfunction of one of the Hardware components, an RMA process will be initiated by Check Point TAC. Check Point TAC will either issue a replacement of the faulty part (like Power Supply, Fan, Hard Disk, etc.) or a full Unit Replacement. Check Point will send the required hardware to the Site location, as it appears in Customer's User Center and as verified with CCSP when opening the Support Service Request, in accordance with the Hardware Support Plan Check Point designates for that Hardware.

Customer must ship back the faulty Hardware product (or replaceable unit) suitably packaged according to the guidelines, as specified by Check Point in the RMA letter shipped with the replacement, to a location that Check Point designates. Return shipment of the faulty Hardware should be made within five (5) business

days of the arrival of the replacement or approval of the RMA for Shelf Spare Unit usage, or pay standard Check Point list price of replacement for any Hardware.

4.3 <u>Dead on Approval (DOA).</u> If a defective Hardware product covered under warranty fails to operate within thirty (30) days from its activation, or no more than one hundred and twenty (120) days from the date of Check Point's shipment of the Hardware product, whichever is less, Check Point will provide expedited replacement of a new unit within two (2) business days from Check Point fulfillment hub, following confirmation of any such failure. Customers outside of the fulfillment hub region should allow for additional transit time due to international customs clearance.

5. TECHNICAL SUPPORT:

5.1 <u>Web-based Support</u>. Check Point web-based Support available at URL: <u>https://support.checkpoint.com</u> provides the CCSP and Customer access to:

(a) **Documentation**, containing product documentation, release notes, troubleshooting guides and technical white papers about Check Point Software and Hardware products, as releases become generally commercially available.

(b) **SecureKnowledge^{SM}**, a self-service knowledge base, restricted repository of thousands of technical documents as well as tools covering everything from planning installation and upgrades, to understanding error messages and fixing specific known issues. Technical solutions, how-to's, and troubleshooting documents written by Check Point engineers and technical staff are added daily. CCSPs have Expert Access in accordance with the specifications of this SLA. Customers have Advanced or Expert Access in accordance with their support plan and the specifications on this SLA. When a solution is identified to solve an issue, Check Point TAC may share this solution with CCSPs via email or verbal communication.

(c) **Software Subscription Downloads**, restricted download site for the use of the CCSP and the Supported Customers; includes latest product upgrades, Hot Fix Accumulators (HFAs), Feature Packs, security fixes, tools, and utilities for the contract term. Software Subscription guarantees that Check Point solutions are kept as current as possible through the latest product enhancements and capabilities. For Major Product releases, CCSPs and Customers may request Check Point to ship a Media Kit that includes Software upgrade package.

(d) **Product Forums**, containing shared knowledge of Check Point products and solutions within an online community of customers, partners and employees, as well as news on Check Point products and technologies. Support Partners can view and post on the discussion threads in all Forums.

5.2 Contact TAC. CCSP's access to TAC should be either by telephone, by web request, or by live chat. CCSP's engineer's email address must be provided as well as the account details of the Customer on which behalf this ticket is opened. Once TAC verified CCSP's engineer is a CCSP Partner's Certified and Designated Contact and Customer's account has a valid Support contract, TAC representitive or system will inquire information about the issue and create a Service Request in the Check Point database.

(a) **By Telephone**: Contact the nearest TAC (refer to URL: https://www.checkpoint.com/support-services/contact-support/). An Automatic Call Distribution System (ACD) will prompt CSP to select a product group. Once CSP chooses the support option, CSP will be directed to appropriate TAC Technical Representative.

(b) **By Web Request**: Log into User Center, under the "Support" Tab, select the "Create Service Request" link. Complete the request form with all of the appropriate information about the issue and submit the request. A Service Request will be generated in the Check Point database.

   PLEASE NOTE: DO NOT submit a Service Request for a Severity 1 issue via the Web request form. For a Severity 1 case, please contact Check Point by telephone and select the appropriate options for your support.

(c) **By Live Chat**: Log into User Center, under the "Support" Tab, select "Live Chat" icon. Live Chat is for quick and simple questions about Check Point products and services. Any issue requires troubleshooting must be submitted by telephone or by web request.

(d) **By Email**: Check Point does not allow opening a Service Request via email. All requests should be opened by Telephone or by web request. Correspondence on an open Service Request may be made via email, as long as the Customer Designated Contact writes a reply to emails received from Check Point TAC.

TAC access is intended to supplement the CCSP senior technical staff in accordance with Section 3 (CCSP and Customer Obligations).

Availability and accessibility of TAC is in accordance with the specifications of this SLA, subject to the situations set forth in Section 8.1 Force Majeure.

	Co-Standard	Co-Premium	Co-Elite
TAC Availability	5x9 Business Day	7x24 Every Day	7x24 Every Day
Unlimited Service Requests	Yes	Yes	Yes

5.3 Technical Support Procedures. Under Check Point's CES Support plan, Check Point TAC utilizes a multi-tier support model for Problem Resolution. When initial contact with TAC is made, a Technical Representative or Web Service Request Tool will validate CCSP and Customer information, contract information, Device Number, and gather details relevant to the question or issue. A unique Service Request (SR) number will be assigned and delivered to the Partner Certified Professional Contact, either verbally, via Web request, or via email. This SR number will be used to track any given issue from initial contact to final Problem Resolution. If appropriate, an issue will be reproduced in the Check Point Test Lab. Additional testing and problem duplication may take place in a network laboratory environment. Further investigation, including additional troubleshooting or debugging activity may be required. Based on the results of the Test Lab investigation, an issue may be resolved, or, if an anomaly is identified, elevated to the appropriate Check Point Team for final Problem Resolution.

Check Point agrees to use commercially reasonable efforts to work with the CCSP for Problem Resolution for an issue in accordance with the specifications of this SLA. Timely efforts must be made by all parties

involved. If communication from Partner ceases without notice, after five (5) business days, Check Point may, upon notice, close a Service Request due to inactivity on the part of the Partner. A Service Request may be reopened within sixty (60) consecutive days of closure. Once a Service Request is closed for sixty (60) consecutive days, this issue will be considered permanently closed, and it cannot be reopened. If further work is necessary, a new Service Request will be opened, and all pertinent materials may need to be resubmitted before work can continue.

5.4   Severity Level Response Time and Resource Commitment. Check Point agrees to use commercially reasonable efforts to respond to Partner requests based on the Severity of the issue as follows:

Severity Level	Response Time (in accordance with Support Plan)			Commitment
	Co-Standard	Co-Premium	Co-Elite	
Severity 1	30 Minutes (Indirect – 30 minute response to the CCSP)	30 Minutes (direct – Customer can contact TAC directly)	30 Minutes (direct – Customer can contact TAC directly)	Check Point and CCSP (and Customer when needed) will commit the necessary resources around the clock for Problem Resolution to obtain workaround or reduce the severity of the Error.
Severity 2	4 Hours	2 Hours	30 Minutes (direct – Customer can contact TAC directly)	Check Point and CCSP (and Customer when needed) will commit full-time resources during normal business hours for Problem Resolution to obtain workaround or reduce the severity of the Error and alternative resources during non-Standard Business Hours.
Severity 3	4 Hours	4 Hours	4 Hours	Check Point and CCSP will commit full-time resources during normal business hours for Problem Resolution, to obtain workaround or reduce the severity of the Error.
Severity 4	4 Hours	4 Hours	4 Hours	Check Point and CCSP will provide resources during normal business hours for Problem Resolution.

Note: Check Point does not guarantee the resolution of a problem within the times specified.

For Severity definitions for Network Security Product(s) or Endpoint Security Product(s), refer to Section 1 DEFINITIONS, "Severity" Definitions for Network Security Product(s) and "Severity" Definitions for Endpoint Security product(s).

The response times set forth in this Section 5.4 constitute targeted goals of the Technical Support to be provided by Check Point to CCSP, and it is understood that Check Point shall use commercially reasonable efforts to respond to CCSP requests within the target times set for the relevant Severity level. The parties acknowledge the potentially idiosyncratic nature of any issue, and agree that any sporadic failure to meet targeted times shall not constitute a breach of Check Point Support obligations under this SLA.

5.5   Escalation Process and Procedure.

(a) Co-Premium and Co-Elite ticket handling: Support Tickets opened for Co-Premium and Co-Elite customers will be handled by Check Point TAC's Escalation group. After initial analysis of the issue and verification that information is sufficient and that there is no known solution to the problem at hand, the ticket will be automatically escalated to the handling of an Escalation Engineer.

(b) CCSP-initiated Escalation: Under Check Point's Support plan, some work items (especially those associated with critical situations) may need to be expedited. When this becomes the case, CCSP shall notify Check Point TAC of the critical situation. If TAC determines that sufficient information has been provided by CCSP and the escalation is accepted, Check Point will work with CCSP on providing the appropriate solution. The escalation begins in accordance to Check Point standard business practices. Upon request, Check Point may provide an action plan to CCSP that may include (but is not limited by) problem statement, next action items to resolve the issue and time estimates on these action items.

(c) Check Point Internal Escalation Process: When TAC determines an issue needs internal escalation, the issue receives a combination of increasing levels of engineering expertise and managerial attentions in accordance with Check Point standard business practice. Except for the case of a CCSP-initiated Escalation in accordance with Section 5.5 (d) below, that issue need not be escalated to a higher managerial level until the Severity of the issue increases or progress toward resolution ceases or is unduly delayed.

(d) Management Escalation: If CCSP feels that the issue is not moving forward in an appropriate timeframe to closure, and/or an issue requires managerial attention, for immediate escalation, CCSP can either request Technical Representative to connect the CCSP to a Team Leader or contact the Team Leader of the Technical Representative handling the case directly. Team Leader's contact details are located at the bottom of the Service Request email. Regardless of the total elapsed time of an outstanding Service Request, the point of escalation shall be initiated at the Technical Representative level, escalated to the Team Leader(s), followed by TAC Manager(s), the TAC Director(s), and then the TAC Vice President. For the most current list of Check Point TAC Escalation Management contacts, refer to Escalation Management link in Service Request Web tool in the User Center.

6. LIMITATION OF LIABILITY:

NOTWITHSTANDING ANYTHING ELSE IN THIS SLA OR OTHERWISE, NEITHER CHECK POINT NOR ITS SUPPLIERS WILL BE LIABLE WITH RESPECT TO ANY SUBJECT MATTER OF THIS SLA UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR OTHER LEGAL OR EQUITABLE THEORY, REGARDLESS OF WHETHER CHECK POINT OR ITS SUPPLIERS WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, FOR: (i) ANY PUNITIVE, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOST DATA OR LOST PROFITS; OR (ii) FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, TECHNOLOGY OR SERVICES; OR (iii) FOR ANY CLAIMS BASED ON ANY ERROR, DEFECT OR NONCONFORMITY IN THE PRODUCTS OR SERVICE, FOR ANY AMOUNT IN EXCESS OF THE PRICE PAID TO CHECK POINT FOR SUCH DEFECTIVE PRODUCT(S) OR SERVICE; OR (IV) FOR ALL OTHER CLAIMS NOT RELATED TO AN ERROR, DEFECT OR NONCONFORMITY IN THE PRODUCTS, ANY AMOUNTS IN EXCESS IN THE AGGREGATE OF THE AMOUNT PAID TO CHECK POINT HEREUNDER DURING THE THREE (3) MONTHS PRECEDING THE DATE THE CAUSE OF ACTION AROSE.

7. TERM and TERMINATION:

7.1 <u>Term</u>. Support shall be provided in annual terms and shall be renewable to the then-current Support Plan when Check Point is notified of Customer's intent to renew the existing contract, or Check Point is notified of Customer's intent to change Support Plan level. The availability of Support contract renewal is limited for products that are subject to End-of-Support notices in accordance with Section 2.5.

In order to prevent a lapse in Support, Check Point, through a reseller or CCSP support partner, must receive purchase order for renewal prior to the expiration date of a Support contract. In the event renewal made after the expiration date, Support payment terms will be back-dated to the day following the expiration date of Customer's prior contract and invoiced according to Check Point's then-current list price.

7.2 <u>Termination</u>. Check Point may terminate this SLA in the event Customer has not made the applicable payments to the reseller or CCSP for the designated Support Plan. Check Point shall provide a period of up to thirty (30) days to cure prior to termination.

Check Point may terminate this SLA, without liability, in the event CCSP:

- Is adjudged as bankrupt, or makes a general assignment for the benefit of its creditors, or if a receiver is appointed on account of its insolvency;

- Fails to maintain the designated number of Certified Professionals;

- Fails to solve most of the Severity 3 and 4 issues. If Support is not performed for any reason by CCSP, CCSP will work continuously to remedy the problem to the satisfaction of Check Point. Should CCSP fail to proceed with appropriate corrections to its work in an expedient manner within the timeframe set forth below, Check Point reserves the right to have the support service completed by Check Point staff or another qualified vendor, and all reasonable cost of such work shall be paid by CCSP. Check Point may elect to terminate of this SLA in accordance with this Section.

- CCSP fails to begin Problem Resolution toward a reported problem in a timely manner, fails to meet any CCSP responsibilities or obligations hereunder (and such failure or breach is not excused by Force Majeure event in Section 8.1 below) or completely cured within 5 days of the receipt of notice thereof from Check Point (or by a shorter period of time if urgent circumstances require such shorter notice), then Check Point may terminate this SLA upon the delivery of a written notice of termination to CCSP and pursue any and all remedies available at law or equity. In the event that Check Point terminates this SLA in accordance with this Section, CCSP shall be responsible for the commercially reasonable costs of having Check Point or another qualified vendor complete performance hereunder. In the event of an uncured breach by CCSP, Check Point reserves the right to assume or award the entire CCSP support service under this SLA to a third party certified professional, and until such time as such qualified vendor can be located by Check Point, Check Point may request that CCSP continue to perform its support under this SLA until its expiration or any earlier termination date as specified by Check Point in its notice to CCSP, and CCSP will work continuously with Check Point or its third party agents to carry out its work hereunder until such time period; or

- Delays under Section 20 and such delay may be prolonged.

  After receipt of notice of termination hereunder, CCSP shall: (a) comply with any instructions by Check Point with respect to stopping immediately or continuing its support until the termination date designated by Check Point; (b) make no further arrangements under this SLA, except as otherwise directed by Check Point; and (c) return to Check Point all Information belonging to Check Point.

7.3 <u>SLA Update</u>. This SLA and related Check Point Support Plans are operational in nature and may be modified at any time by Check Point. Check Point will take appropriate measures to inform CCSP and Customer of modifications and will provide CCSP and Customer the right and window of time to review any proposed change, discuss it with Check Point, and terminate the Customer relationship without penalty if all parties cannot abide by the revisions. This SLA supersedes any previous service level agreements.

7.4 <u>Support Plan Upgrades</u>. Check Point permits upgrades of annual Support at any time during the term of the Support agreement. In the event a Support contract is terminated, Check Point shall not issue prorated refunds. Notwithstanding the aforementioned, in the event Check Point modifies this SLA in accordance with Section 7.3, and such modification has or will have the substantially impact on the Check Point Support Plan offered under this SLA, then the Customer may terminate said Support forthwith upon Check Point implementing any such modification and Customer may obtain a prorated refund for the remainder of the effective period.

8. Miscellaneous:

8.1 <u>Force Majeure</u>. Except for the obligation to pay monies due and owing, neither party shall be liable for any delay or failure in performance due to event outside the defaulting party's reasonable control, including without limitation, acts of God, earthquakes, labor disputes, shortages of supplies, actions of governmental entities, riots, war, fire, epidemics, or other circumstances beyond its reasonable control. The obligations and rights of the excused party shall be extended on a day-to-day basis for the period equal to the period of the excusable delay.

8.2 <u>Non-solicitation</u>. CCSP agrees not to solicit any employee of Check Point for employment, or encourage any employee of Check Point to leave his or her employment with Check Point, without the expressed written consent of Check Point. The above limitation shall be effective for the term of this Agreement and for a period of one (1) year following the termination of this SLA or any extension hereto. Solicitation does not include advertisements in the general media and, except to the extent an individual was specifically encouraged to respond to such advertisements, there shall be no restriction on the hiring of individuals so responding.

8.3 <u>Assignment</u>. CCSP may not assign this SLA without the prior written consent of Check Point. Check Point may transfer its rights to any wholly owned Check Point subsidiary.

8.4 <u>Entire Agreement.</u> This SLA, outlining the terms and conditions of Software technical support and/or Hardware replacement services for Check Point products, constitutes the entire agreement between Check Point and the CCSP and supersedes all previous written or oral agreement between the parties with respect to the subject matter of this SLA. The terms in this SLA override any contrary terms contained in any purchase order or other CCSP documentation.

9. **Office Locations:**

Worldwide Headquarters:	**Check Point Software Technologies Ltd.** 5 Ha'Solelim Street, Tel Aviv 67897, Israel Main Tel: +1 972-3-753-4555 Main Fax: +1 972-3-575-9256
U.S. Headquarters:	**Check Point Software Technologies, Inc.** 959 Skyway Road, Suite 300 San Carlos, California 94070 Main Tel: +1 650-628-2000 Main Fax: +1 650-654-4233
Worldwide Technical Services:	**Check Point Software Technologies, Inc.** 6330 Commerce Drive, Suite 120 Irving, Texas, 75063 Main Tel: +1 972-444-6625 Main Fax: +1 972-444-6552
Check Point Web Site:	http://www.checkpoint.com
Check Point Support Site:	http://support.checkpoint.com
Check Point User Center:	http://usercenter.checkpoint.com
Support Programs:	http://www.checkpoint.com/techsupport/
Support Services:	http://www.checkpoint.com/services/
Support Secure FTP site:	US TAC: sftp.ts.checkpoint.com Ottawa TAC: sftp.ott.checkpoint.com International TAC: ftp.checkpoint.com

EXHIBIT A

Check Point CES Support Plan Descriptions

Support offerings and services listed herein are subject to availability by product family and by service geographic area. Customer is advised to contact a Check Point authorized Certified Collaborative Support Partner (CCSP), or Check Point will confirm the support programs that are available for purchase at its discretion.

To contact Check Point Technical Support, please refer to URL:
http://www.checkpoint.com/services/contact/index.html.

1. CHECK POINT SUPPORT OFFERINGS

In order to meet the needs of its enterprise Customers, Check Point offers its Collaborative Enterprise Support program for the support of Check Point Software and Hardware products. This provides a total support service solution to enterprise/business customers through a CCSP. Below, are the program levels available under Check Point's Collaborative Enterprise Support program:

Collaborative Enterprise Support	Collaborative Enterprise Support on Appliance
- Co-Standard - Co-Standard PRO* - Co-Premium - Co-Premium PRO* - Co-Elite - Co-Elite PRO*	- Co-Standard - Co-Standard PRO* - Co-Standard Onsite** - Co-Standard Onsite PRO* ** - Co-Premium - Co-Premium PRO* - Co-Premium Onsite** - Co-Premium Onsite PRO* ** - Co-Elite - Co-Elite PRO* - Co-Elite Onsite** - Co-Elite Onsite PRO* **

*PRO support refers to enhancements to the Collaborative Enterprise Support programs which enable proactive ticket creation for severe issues, comprehensive reporting and daily monitoring of the Check Point environment.

**Onsite services refer to enhancements to the Collaborative Enterprise Support programs that deliver on-site Hardware Replacement service in case of a hardware issue is found and determined to require an RMA.

2. SUPPORT PLAN DESCRIPTION

For the most updated feature list of the Check Point Support plan, please visit the following online URL:
http://www.checkpoint.com/services/techsupport/programs/ces/compare_enterprise_support.html

2.1 TAC Access.

With Check Point Software and/or Hardware Support, CCSP has access to TAC engineers per the Support plan, in accordance with the terms of this SLA, 7 x 24 - seven (7) days a week, twenty-four (24) hours a day, every day.

2.2 Support Web Access.

Access to restricted websites and resources for the sole use of the Customer and CCSP at Check Point User Center: http://usercenter.checkpoint.com; Check Point Support Center: http://support.checkpoint.com.

2.3 SecureKnowledge.

Check Point provides CCSPs with access to restricted portions of its knowledgebase per the Support plan, in addition to the general installation and upgrade knowledge articles given to users with General Access. Expert Access – in addition to knowledge articles available to Customer with Advanced Access, Expert Access contains solutions regarding issues with high fix complexity, known issues with Workarounds or Hotfixes, in-depth complex troubleshooting, and RFEs. Expert Access is given to CCSPs.

2.4 Software Subscription.
Access to restricted download site for the sole use of the CCSP and Customers; includes latest product upgrades, enhancement, Hot Fix Accumulators (HFAs), Feature Packs, security fixes, tools, and utilities.

2.5 Severity Level Response Time.
Check Point agrees to use commercially reasonable efforts to respond to CCSPs requests based on the Severity of the issue within specified time target(s) per the Support plan, in accordance with the terms of this SLA.

2.6 Support Focal Point.
Check Point Technical Assistance Centers are staffed by Support engineers who have extensive experience in supporting large-scale networks and providing assistance with diagnosis and resolution of defects and/or failures in Check Point products. As a single point of contact for all of CCSP's support needs, TAC Support engineers are grouped by expertise and experience, to ensure that TAC responds as quickly as possible by priority in accordance with the terms of the Support plan and this SLA.

- Desks Support Engineer
- Premium Support Engineer
- Escalation Support Engineer

2.7 Advance Replacement.

With Check Point Hardware Support, Customer is entitled to Advance Replacement service on the Hardware in accordance with the terms of the Support plan and this Agreement. Replacement delivery targets are listed per the Support plan.

Appliance Standard; Appliance Premium; Appliance Elite
After TAC determines that the Hardware issue is related to a malfunction of one of the Appliance components, Check Point will provide Advance Hardware Replacement of the faulty Hardware Product. Check Point shall use commerically reasonable efforts to ship the replacement hardware on the same busines day, however, shipment my occur on the next business day if required for operational reasons.

Appliance Standard Onsite
After TAC determines that the Hardware issue is related to a malfunction of one of the Appliance components, and after a repair action plan has been defined, Check Point will provide Onsite Hardware Replacement next business day (NBD), which includes delivery of replacement hardware to the Site and basic installation by a Check Point Certified Onsite Technician or ACE Partner. (For RMA determination completed by 5 pm local time).

Appliance Premium Onsite; Appliance Elite Onsite
After TAC determines that the Hardware issue is related to a malfunction of one of the Appliance components, and after a repair action plan has been defined, Check Point will provide Onsite Hardware Replacement within four (4) hours (4Hr), which includes delivery of replacement hardware to the Site and basic installation by a Check Point Certified Onsite Technician or ACE Partner.