Secureworks®

SERVICE DESCRIPTION

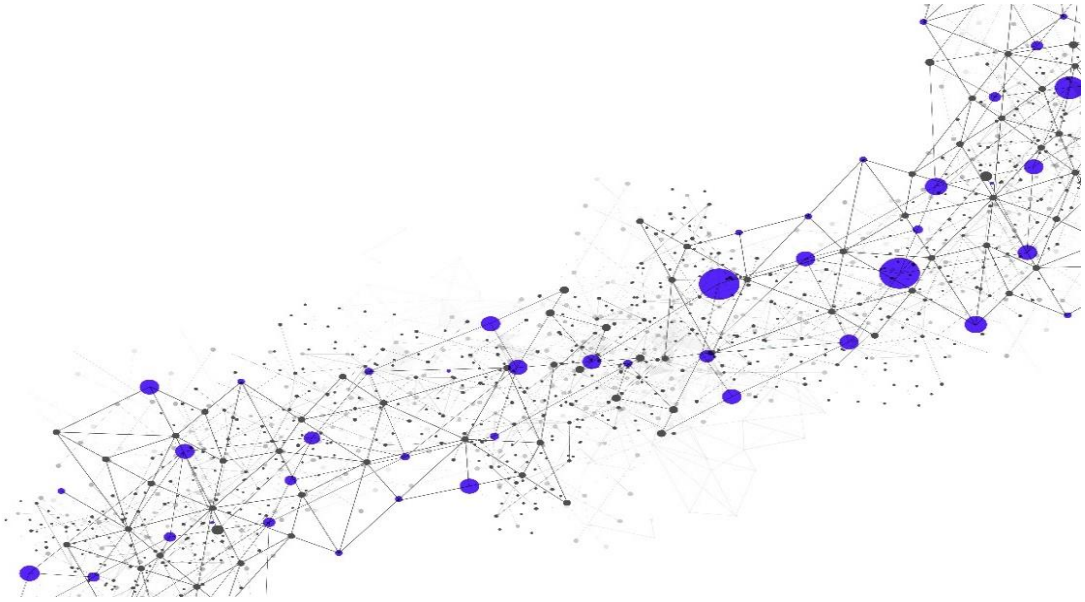
Managed Next Generation Firewall with Policy Auditing (includes monitoring)

Release Date

June 17, 2022

Version

20.3



www.secureworks.com
A Dell Technologies Company

Global Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
Phone: +1 877 838 7947
Email: info@secureworks.com
Additional office locations: https://www.secureworks.com/about/offices

Table of Contents

1 Service Introduction

This Service Description ("**SD**") describes the Managed and Monitored Next Generation Firewall Service ("**Service**"). All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement.

This is a ***managed*** Service. As such, Secureworks® performs Device management functions, which can include changes, rule/policy modifications, upgrades, and similar functions, upon Customer request. Secureworks also performs monitoring and alerting of Device health and Security Events (for events generated from one or more Devices).

1.1 Overview

Secureworks will manage Customer's Next Generation Firewall ("**NGFW**" or "**Firewall**" – collectively referred to as "**Devices**") infrastructure 24 hours a day, 7 days a week. Secureworks reserves the right to staff such 24/7 coverage by providing full-time personnel during Business Hours and on-demand support personnel during non-Business Hours, as needed. In addition, Secureworks will monitor the Devices on an ongoing basis to detect signs of advanced threats and threat actors, search for specific indicators of compromise, maintain updated threat intelligence, analyze event data, and send alerts to Customer with recommendations on how to proceed should threat activity be detected. To perform these activities, the Devices will send logs to the management console(s), and then the logs will be sent to the Secureworks Counter Threat Appliance ("**CTA**") for processing through the Secureworks Counter Threat Platform® ("**CTP**"). This Service enables detection of threats and threat actor activity that some technologies (e.g., common anti-virus software) are unable to detect. Section 2.2.5, Security Event Monitoring and Alerting, contains more information about how events are processed.

The Service allows for maintaining/storing key forensic data necessary to make threat detection and response faster and more efficient, and reducing effort required to investigate and respond to threats.

Secureworks will provide Customer with Device Management support of up to 20 Enterprise Changes per standalone NGFW per Services Term year, and 40 Enterprise Changes per high-availability NGFW pair per Services Term year, combined as an aggregate allowance to be used across any combination of Devices throughout the Term. An "**Enterprise Change**" includes moves, adds, and changes ("**MAC**"). Incident resolution, IP Blocks, and platform upgrades do not count as Enterprise Changes and are therefore supported in an unlimited capacity. See Section 4.1.1, Exceeding Enterprise Change Ticket Volume, for more information.

Managed support for Customer's NGFW is limited to the features approved by Secureworks for support as described herein and is also limited to NGFW components for which Customer has a valid license and vendor support contract.

The Service includes the following components:

- Policy Management
- Secureworks Best Practices Firewall Policy Auditing
- Secureworks Best Practices Intrusion Detection System ("**IDS**") / Intrusion Prevention System ("**IPS**") Policy Management
- Device and Policy Troubleshooting
- Security Event Monitoring and Alerting
- Device Availability and Event Flow Monitoring and Alerting
- Software Maintenance for Devices

- Return Materials Authorization ("**RMA**") Assistance
  Note: *The RMA process for third-party vendor Devices is out of scope in Japan.*
- Device Management Using the Management Console

See Section 2, Service Details, for more information about the Service, including further explanation of the components listed above. Also, see the **Secureworks MSS Services – Service Description Addendum** for information about the following, as applicable to the Service: Device responsibilities, Maintenance Program, and Subscription Program.

Note: Secureworks will not install third-party software on any appliance or system, unless explicitly indicated in Section 2 as being part of the Service.

1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder, including meeting the Service Level Agreements ("**SLAs**") listed further below, are dependent on Customer's compliance with these obligations. Noncompliance with Customer obligations relative to this Service may result in suspension of managed components of the Service and/or SLAs, or a transition to monitor-only components of the Service.

1.2.1 Support Contracts and Licensing

Customer is responsible for maintaining current vendor licensing, vendor support and vendor maintenance contracts for Customer-owned NGFW equipment. Customer is also responsible for associating Secureworks with the existing vendor support and maintenance contracts for Secureworks to work with the vendor on Customer's behalf. If this agreement is not in place, then Secureworks will not be able to engage the vendor directly to resolve support issues.

In some geographic locations, platform vendors such as Cisco, Palo Alto, McAfee, Fortinet and others ("**vendors**") are not allowed to sell their support contracts ("**contracts**") directly to customers. In these locations, a fourth party ("**reseller**") is required to sell the contract(s) on behalf of the vendor. In other locations, vendors are allowed sell their support contracts directly to customers; however, it may still be commonplace in these areas for resellers to perform this function on behalf of the vendor. When support contracts are sold by a reseller, customers will (in most cases) not be allowed to associate Secureworks with the contract(s). This will prevent Secureworks from working directly with the vendor on Customer's behalf. In these situations, Secureworks will communicate only with the reseller and Customer.

For deployments where support is obtained through a reseller, Secureworks will submit support requests (hardware/software support, troubleshooting, RMA) to the reseller and will work with the reseller as if they were the vendor. In any scenario where Secureworks does not have direct access to the vendor and a fourth-party reseller is involved, Secureworks' ability to provide vendor-level support will be best-effort and Secureworks will not be obligated to adhere to any SLA regarding issue resolution. Secureworks' ability to work with fourth-party resellers requires that the reseller communicates in English (both written, web/portal and spoken communication). For deployments in Japan, Secureworks will not interact directly with fourth-party resellers; instead, Secureworks will escalate issues, through the Secureworks SOC in Japan, directly to Customer. Customer will be expected to work solely with their respective fourth party, and Secureworks will be consultative for these situations.

1.2.2 Connectivity

Customer shall provide and maintain remote network connectivity to the Device(s) necessary for Secureworks to manage and/or monitor the Devices that are in scope. SLAs will not apply to the Device(s) that is experiencing connectivity issues that are beyond the control of Secureworks.

1.2.3 Application Program Interface ("API") Integration

Some vendors provide APIs to interact with their systems. Any script or code creation for, usage of, maintenance of, or integration with other third-party tools are not included in this Service; Customer shall be responsible for all API integration, and related activities and licenses. Secureworks will not install any third-party software applications that use the API directly on the appliance.

1.2.4 Communications

Customer will communicate with the Secureworks Security Operations Center ("**SOC**") through telephone (Customer-authorized representative will be authenticated) or the Secureworks Client Portal ("**Portal**") using either the ticketing interface or Chat. Customer should submit all Service-related issues or requests as tickets in the Portal or as requests through the Chat in the Portal. It is Customer's responsibility to ensure that its list of authorized users is up to date with the Secureworks SOC. Customer is responsible for timely responses to tickets that Secureworks escalates to Customer through the Portal.

1.2.5 Maintenance

Customer will notify the Secureworks SOC by submitting a ticket in the Portal or through the Chat in the Portal at least 24 hours in advance of planned Customer-side network maintenance to enable Secureworks to avoid unnecessary escalations to Customer.

1.2.6 Usage Overage

If, for any Services identified in Customer's Transaction Document, Customer's actual usage exceeds the subscription limit of such services ("**Overage**"), then Secureworks may invoice Customer for Overage(s) at the end of the Services Term, and Customer will pay for the Overage(s) as applicable to Customer's actual usage, from the date Secureworks identified the Overage until the end of the Services Term.

1.2.7 Provisioning in a Public Cloud or Private Virtual Environment

When provisioning in a Public Cloud or Private Virtual Environment, Customer will provide to Secureworks information about the environment, and may be required to make configuration changes as applicable to the Service. Customer will provide access and appropriate privileges within the environment to enable Secureworks to deploy and configure the Service.

1.2.8 Hardware and Software Procurement

Customer will purchase or lease the hardware and license the software necessary for Secureworks to deliver the Service. Customer will ensure that its hardware and software are at versions that are supported by Secureworks prior to provisioning of the Service and remains at versions that are Secureworks supported during the Services Term. Secureworks SLAs will not apply to platforms or versions that are End-of-Life ("**EOL**"), end of support, or are otherwise not receiving updates by the vendor or supported by Secureworks.

1.2.9 General

- Customer will ensure that Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- Customer will provide to Secureworks all required information (key personnel contact information, credentials, and related information) prior to work being started.

- Customer will promptly reply to all requests from Secureworks.
- Customer-scheduled downtime and maintenance intervals will allow adequate time for Secureworks to perform the Service.
- Customer will promptly inform Customer personnel and third parties of Secureworks testing activities as needed, to prevent any disruption to Secureworks business and performance of the Service (e.g., takedown requests, ISP blacklisting).

1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Transaction Document to schedule the first meeting during which Service Implementation will be discussed.

Customer and Secureworks will designate respective points of contact ("**POC**") to facilitate communication and support ongoing activities related to implementation of the Service.

2 Service Details

The subsections below contain details about the Service and how it will be implemented.

2.1 Service Implementation

The standard service implementation period begins after Secureworks reviews and approves Customer's signed Transaction Document, and ends when the Service is activated (made available to Customer for Customer's use), any Devices supporting the Service are activated, and management or monitoring of Devices is transferred to the Secureworks SOC. The subsections below explain the Secureworks implementation methodology for Managed Security Services (known as MSS Services) that is used to provision, install (if applicable), and activate the Service.

Note: *Secureworks does not provide SLAs for completing implementation within a specified period of time; the duration of the implementation is dependent on several factors, such as the number of Counter Threat Appliances ("**CTAs**") required (if applicable to the Service), the number of physical locations where managed or monitored Devices will be activated for the Service (if applicable to the Service), complexity of Customer requirements, and the ability of Customer to provide Secureworks with requested information within a mutually agreed-upon time period.*

A typical implementation with one (1) physical location, two (2) CTAs, and between one and four (4) managed or monitored Devices can generally be completed within six (6) weeks. This does not include any policy migrations or the time required for Customer activities or other external dependencies.

*Any effort that is required to upgrade software or replace hardware in support of Service implementation requirements can be performed by Secureworks through a separate Statement of Work ("**SOW**").*

2.1.1 Implementation Methodology

Secureworks will follow the Secureworks standard implementation methodology to implement the Service. The implementation methodology can be reasonably adjusted to meet Customer needs at the sole discretion of Secureworks. As part of implementation, Secureworks will help ensure Customer understands how to use the Service through collaborative meetings and training. Below is a high-level overview of the MSS implementation methodology.

- **Organize:** Start the project, document success criteria, enable Portal access, and finalize technical design of the Service
  - Secureworks will work jointly with Customer to validate accuracy of the information used to create the original Transaction Document against the actual Customer environment where services will be performed ("**Due Diligence**"). As a result of Due Diligence, changes in the types (e.g., hardware make and/or model and software package or version) of equipment, the number of locations, or the quantities of equipment to be provisioned may be identified ("**Identified Changes**"). Customer acknowledges that (i) in order for Secureworks to provide intended Service coverage across such

Identified Changes, an amended or additional Transaction Document may be required, which may include changes to scope and fees, and (ii) without such an amended or additional Transaction Document, Secureworks may only be able to provide services as scoped, defined, and charged per the original Transaction Document. In some cases, an amended or additional Transaction Document may be required to provide the services in the original Transaction Document. For example, an additional CTA may be required at a location that was not originally determined to be in scope.

- **Prepare:** Baseline the project schedule, identify required training, and send CTA(s) to Customer for installation; Customer provides information necessary to execute implementation for MSS Services
  - **CTA Deployment Guidelines:** For most Secureworks MSS Services, one or more CTAs will need to be installed, and will be included in the Transaction Document. The CTA is a Secureworks-proprietary Device that is used in the secure delivery of the Service for Device health and Security Event collection and transport.
    - If one or more **physical CTAs** are to be deployed, then Secureworks sends them directly to Customer for installation. Customer is responsible for ensuring that the implementation site complies with the Secureworks physical/environmental specification, which will be provided to Customer prior to commencement of CTA deployment.
    - Alternatively, if one or more **virtual CTAs** ("**vCTAs**") will be deployed in a Public Cloud or Private Virtual Environment, then Customer is responsible for providing information to Secureworks about the Public Cloud or Private Virtual Environment, and Customer will make configuration changes as applicable to the Service. Customer must provide access and appropriate privileges to the Public Cloud or Private Virtual Environment to enable Secureworks to manage the vCTA and configure it as applicable to the Service. See Section 2.1.2.1, Provisioning a vCTA into a Virtual Environment for information about provisioning in virtual environments.
  - Secureworks reserves the right, in its reasonable discretion, to use one or more **CTAs deployed in a Secureworks data center (a Hosted CTA or "HCTA")** to communicate with Devices that Secureworks is monitoring, in lieu of deploying physical or virtual CTAs for use directly in Customer's environment. In such cases, the guidelines above pertaining to CTA deployment do not apply. A service deployment using a Secureworks HCTA design will be discussed and agreed upon during the solution scoping engagement within the Sales cycle. Service interruptions or failure to achieve the SLAs (as defined herein) will not be subject to penalty in the event of Customer's non-compliance with the above-listed CTA deployment guidelines.
- **Execute:** Complete configuration of CTA(s) and related service-enabling technology, validate ingestion of identified log source(s) if applicable, schedule and deliver foundational training, and activate services

  Notes:

  - New managed Equipment to be deployed can be sent directly to Secureworks (Customer incurs shipping charge) for configuration and subsequent shipment to Customer location for installation with on-site support from Customer.
  - Existing Customer Devices that Secureworks will manage for Customer per an Transaction Document (i.e., the equipment is already installed on Customer premises) will be provisioned remotely with on-site support from Customer.
  - Secureworks provides telephone support to Customer for installing Equipment (i.e., Devices Customer purchases or leases from Secureworks).
  - After Equipment that Secureworks will be managing is installed, Secureworks will access Equipment (whether physical or virtual) remotely and perform the remaining configuration and implementation tasks, which may require a mutually agreed-upon maintenance interval for downtime.

- **Rationalize:** Confirm Customer's ability to access and participate in management of the Service within the Portal; ensure ticket data quality and tuning of the Service and processes to Customer's environment
- **Accept:** Validate successful deployment of the Service and transition of Customer to steady-state operations

2.1.2 Service Provisioning, Installation, and Activation

Service provisioning consists of the initial actions that are completed in advance of implementing the Service for Customer, such as configuring and sending Devices to Customer and configuring Devices. **Service installation** consists of physically putting in place a piece of equipment, connecting it to Customer's environment, and testing the ability of Secureworks to connect to the equipment. **Service activation** consists of Customer and Secureworks validating all Devices and components of the Service are available to Customer for Customer's use, and the Secureworks implementation team transferring Customer to the Secureworks SOC.

If provisioning Equipment is part of the Service, then installation activities are also part of provisioning.

Secureworks performs the following provisioning, installation, and activation activities:

- Create implementation ticket in Portal (for ongoing tracked communication between Customer and Secureworks during implementation)
- Schedule initial meeting (remote) with Customer and review Transaction Document (or on-site meeting for Customers in Japan, if needed) *(**Note:** Receipt of a Customer-executed Transaction Document is required prior to scheduling initial meeting.)*
- Provide Customer with access to the Portal
- Collect Customer information that is necessary for implementation
- Complete provisioning and installation activities (e.g., sending Devices to Customer, configuring Devices within CTP, and performing connectivity testing, if applicable)
    - ***Activity for physical CTAs Only:*** Send CTAs to Customer through ground shipping method *(**Note:** Installation and completion of minimal configuration by Customer for CTAs is required.)* Customer is responsible for physical installation and completion of minimal configuration of the CTA(s).
- Provide any new Secureworks Customer with opportunity to participate in foundational training (see Section 2.4)
- Notify Customer (e.g., through email, telephone, or scheduled meeting) to activate the Service *(**Note:** Customer and Secureworks will work together to ensure that Service is activated for in-scope Devices.)*
    - Secureworks can schedule Service activation in accordance with change management procedures communicated by Customer. Standard activations are performed during Business Hours on Business Days in the following regions: US, EMEA, APJ, and ANZ; however, activation can be performed at other times when scheduled in advance with Secureworks.
- Notify Customer (e.g., through email, telephone, or scheduled meeting) that the Service activation is complete, and Customer is transitioned to Secureworks SOC

2.1.2.1 Provisioning a vCTA into a Virtual Environment

Virtualization includes various methods by which hardware resources are abstracted to allow multiple virtual machines ("**VMs**") to share a common hardware platform. This subsection explains provisioning a vCTA into a virtual environment (i.e., a Public Cloud or Private Virtual Environment), which enables delivery of Secureworks security services in Customer's environment. See the Glossary for definitions of terms related to virtualization that are used in this SD.

If Customer has a Private Virtual Environment, then Secureworks will provide Customer with an image to install on the Hypervisor in Customer's Private Virtual Environment, which is used to create the vCTA on a Guest VM. If Customer has a Public Cloud Environment, then Customer will access the Portal and complete steps to obtain the vCTA for use in the Public Cloud Environment. Depending on Customer's environment, the specific steps for installing and provisioning the vCTA may vary, and Secureworks will provide applicable information to Customer.

When provisioning the vCTA into a virtual environment, Customer is responsible for creating and supporting the underlying Guest VM. This includes all management and maintenance of the Guest VM (i.e., the Host), Hypervisor, and related hardware. See Section 2.5, Support for Private Virtual Environments, for more information about Virtual Environments including additional Customer responsibilities.

Provisioning Requirements: Customer must perform the provisioning activities when provisioning the vCTA into Customer's virtual environment (including private or public cloud). Customer must also provide all required virtual hardware needed to operate the vCTA on the Guest VM. This includes vCPU(s), RAM, vHDD capacity, network interface card/adapter, and storage IOPS. Customer must also provide a virtual environment that supports the required network connectivity, which will enable Secureworks to manage the vCTA remotely.

2.2 Service Components

The subsections below contain information about the components of the Service.

2.2.1 Policy Management

Secureworks will manage policies associated with NGFW Devices. After the initial tuning period is completed, Customer will submit change requests to Secureworks through the Portal for all policy changes. Customer must call the SOC for emergency changes (defined in the table below). All change requests must be made by an authorized Customer contact. Secureworks will contact Customer to clarify requests as needed. Change requests will only be implemented for NGFW components that Secureworks supports. The detailed Secureworks-supported product matrix is available upon request. The table below explains Secureworks responsibilities associated with managing policies for NGFW components that Secureworks supports.

Policy Management Component Descriptions	
Firewall	Secureworks will manage the NGFW Device and policy configuration for the managed NGFW on behalf of Customer. Secureworks will follow a standardized change process, which will include a peer review (unless it is an emergency change as defined below), and implement Customer-requested changes. Secureworks does not design or validate rule sets. It is the responsibility of Customer to provide necessary information for each request for Secureworks to implement the request successfully. Customer must use the Secureworks change request form. Change request information must include the following: • NGFW target Devices • Source and destination IP addresses • Routing information • Port or protocol information Emergency change requests must be submitted through telephone to the Secureworks SOC by an authorized Customer contact. Emergency requests are defined as business-impacting change(s)

Policy Management Component Descriptions	
	required to resolve a malfunction of the NGFW, to return Customer to an operational state, or to remediate an active security threat. Additional access through the NGFW is not defined as an emergency change. The SOC will accommodate the change at a best level effort based on preexisting requests. For platforms where Secureworks supports dynamic routing protocol(s), support for these protocol(s) is limited to basic configuration which includes configuring the protocol in passive mode where it participates in peering with other peers and advertises local routes only. Architecture and design advice, advanced configurations at the firewall level, and assistance with any other device Customer owns (i.e., peer devices) involved in the dynamic routing protocol relationship are outside of the scope of support.
IDS/IPS	Secureworks will ensure vendor supported signature set is applied to the managed Device where applicable. Signature sets are deployed regularly to managed Devices. These signatures are enabled during the specified update interval set on the Device. It is Customer's responsibility to ensure that the managed Device has a valid Intrusion IDS/IPS license to receive signature updates from the vendor.
Anti-Virus ("**AV**")/Anti-Malware Protection	Secureworks can enable AV and anti-malware functionality on managed NGFW Devices per Customer's request. As a component of this service, Secureworks will update AV policies regularly as updates are released by vendor. Security-relevant AV events are logged in the Portal. These events will not result in ticket creation or viewing by a Secureworks analyst. Content blocked by AV will not be recoverable.
Web URL Filtering	Secureworks will deploy the default categorization policy for Web URL filtering as specified by Customer in the information-gathering documentation that Customer completes during implementation. Access to websites within a block category will be denied. Customers can request a change of category in the Portal. Requests for whitelisting or blacklisting of domains are permitted under a change request.
Content Filtering	Secureworks can enable content filtering functionality on managed NGFW Devices as specified by in the information-gathering documentation that Customer completes during implementation. Changes after implementation will need to be requested through a change request in the Portal. Security-relevant content filtering events are logged to the Portal. These events will not result in ticket creation or be reviewed by a Secureworks analyst. Content blocked will not be recoverable.
VPN Configuration	Secureworks configures VPN connections and troubleshoots the NGFW managed Device in the event of an outage. At least one (1) NGFW Device must be managed by Secureworks to provide this Service.

Policy Management Component Descriptions	
Multi-Wide Area Network ("**WAN**") Support	At implementation time, Customer can specify single-WAN or multi-WAN (primary and backup) configuration. It is Customer's responsibility to provide and maintain the data circuits. Secureworks shall set-up and test multi-WAN functionality in conjunction with Customer. Secureworks is not responsible for advising Customers about network priority changes.
Self-Signed Certificates	Most security devices use a self-signed certificate for https access to manage device policies. The self-signed certificates are generic and are provided free of charge with the devices. The self-signed certificates allow for "man-in-the-middle" attacks vectors because the self-signed certifications are too generic and predicable across each platform. Secureworks recommends Customer purchases and provides Secureworks with a third-party SSL certificate to ensure security best practices are followed. If Customer does not purchase a third-party SSL then Customer assumes all risk and responsibility and Secureworks shall not be liable for any breach or disclosure of Customer data or confidential information.

2.2.2 Secureworks Best Practices Firewall Policy Auditing

Secureworks will use Best Practices Firewall Policy Auditing to improve Customer's infrastructure security through reviewing and refining firewall policies. Secureworks will use a combination of technology and security analysts to facilitate a thorough best practices analysis of firewall policies currently under management and will work with Customer to identify firewall rules which are a security concern. The intent of this audit is to enhance the security posture of the NGFW Device at start of service and provide the option for additional audits to be performed at a one-time service fee.

2.2.2.1 Initial Firewall Policy Security Review

Upon service activation, Secureworks will assess the firewall policy and create a Secureworks Best Practices audit report for each NGFW Device following service commencement of the firewall being managed. Secureworks will contact Customer to review the audit report(s) and work with Customer to discuss security concerns and define a remediation plan as it pertains to firewall policies and Customer's environment. This discussion will occur with Customer in an optional working session (maximum of two hours) to provide recommendations on securing the firewall policies pertaining to the Secureworks Best Practices reports. Customer can purchase additional working sessions on a time and materials basis pursuant to a separate SOW. Secureworks will work with Customer to update the policies based on the findings during the working session. The Best Practices Policy Audit report will be attached to a ticket within the Portal for Customer's consumption regardless of whether the optional working session occurs.

Customer will need to approve all firewall policy changes resulting from each Secureworks Best Practice auditing review. Policy remediation creates the risk of potential disruption to Customer's business. Secureworks is not responsible for negative impacts to Customer resulting from any remediation efforts applied to the firewall policies.

2.2.2.2 Audit Reporting

The Secureworks Best Practices audit report will be provided with optional discussion working sessions following the initial security audit review. Customer may request additional

audits at any time for an additional fee through Customer's Secureworks Sales Representative.

The table below indicates the reports that are available.

Report Type	Description
Secureworks Best Practices Report	This report leverages Secureworks recommended policy best practices to analyze and evaluate the security integrity of the policy. Additionally, this report analyzes the current policy and provides a list of security rules that are considered complex based on the number of objects within the source, destination, or services.
Firewall Policy Report	This report provides a visual representation of the current policy implemented on the NGFW Device.
Firewall Policy History Report	This report provides a record of changes to each rule in an NGFW policy at the end of the audit.

2.2.2.3 Security Audit Report Optional Working Session

Secureworks will review the current policy implemented on the NGFW Device and offer security recommendations to Customer based on the Secureworks Best Practices report. Recommendations may include:

- Discussion on how firewall policies should handle inbound and outbound network traffic; Examples of policy requirements include permitting only necessary Internet Protocol (IP) protocols to pass, appropriate source and destination IP addresses to be used, particular ports such as Transmission Control Protocol ("**TCP**") and User Datagram Protocol ("**UDP**") ports to be accessed, and certain Internet Control Message Protocol ("**ICMP**") types and codes to be used.
- Discussion on how firewall policies should securely handle management access and traffic; Firewall rulesets should be as specific as possible with regards to the network traffic they control. Secureworks consultation involves discussing what types of traffic are required, including protocols the firewall may need to use for management purposes. These discussions can vary widely by type of firewall, specific product type, and Customer's organizational needs.

2.2.2.4 Policy Rule Implementation

Secureworks will work with Customer to construct security policy adjustments based on the Secureworks Best Practices audit review. Customer will need to approve any changes before they can be applied to the policy. Secureworks will create the change tickets related to the modifications agreed upon with Customer and Secureworks will schedule the change tickets according to the change intervals provided by Customer. All tickets can be viewed and tracked via the Portal.

2.2.3 Secureworks Best Practices IDS/IPS Policy Management

See Section 5 for information on Secureworks Threat Intelligence ("**TI**") add-on content that is applicable to this subsection.

2.2.3.1 Baseline Policy

Many NGFWs also support IDS/IPS functionality. If the Device supports IDS/IPS and Customer elects to use it, then Secureworks can apply one baseline policy to each Device when the Service is activated. Signatures are applied based on the vendor's recommendations and Secureworks best practices.

2.2.3.2 IDS/IPS Policy Maintenance

IDS/IPS policies are updated on a predetermined automatic update with the latest signatures from the vendor. Vendor signatures are applied based on the vendor's recommendations. These signatures can be suppressed, enabled, or disabled on an as needed basis by submitting a ticket via the Portal or calling the Secureworks SOC.

2.2.4 Device and Policy Troubleshooting

Secureworks will work with Customer to troubleshoot issues with the managed NGFW Device. If necessary, Secureworks will engage the vendor on Customer's behalf.

- If the root cause of the issue is specific to the NGFW Device that Secureworks is managing, then Secureworks will work with Customer's designated point of contact through telephone to resolve the issue.
- If the root cause of the issue is not related to the NGFW Device that Secureworks is managing (such as a network change, outage, or Customer-managed device), then Secureworks will provide Customer with troubleshooting information, but Secureworks is not responsible for troubleshooting issues that do not directly relate to the managed Device, any Secureworks Equipment, or Secureworks network.

Note: For Customers in Japan, it is Customer's responsibility to submit tickets with the fourth-party vendor (i.e., Reseller, Distributer, Sier who has the support contract with vendor) for issues requiring vendor assistance. Secureworks will work with Customer and provide best-effort support to resolve the issue.

2.2.5 Security Event Monitoring and Alerting

To provide Customer with Security Event monitoring and alerting of potential threat actors and threat activity, Secureworks will use a combination of the following:

- Secureworks Threat Intelligence ("**TI**")
- Machine learning
- Signature-based detections
- Human-based pattern identification – through ongoing research conducted by the Secureworks Counter Threat Unit™ ("**CTU™**") and SOC analysts
- Long-term correlation
- Big data analytics

Secureworks aggregates and analyzes data from the above-listed sources and uses the data to conduct security activities that help Customer prevent and defend against attacks. The data from these sources enables faster detection of malicious activity, and action against the activity. As new threat activity is identified, new detectors are developed and deployed to the CTP, providing customers with protection from threat actors and threat activity.

Secureworks only monitors and alerts Customer of threat actors and threat activity using the above-listed sources (includes data from Devices or Security Events that are provisioned and maintained as part of the Service); no other sources such as Customer-created custom alerts and custom watch lists, or TI from other sources will be used. Secureworks reserves the right to change how monitoring and alerting is conducted, and conduct maintenance at any time to ensure the best quality of TI is applied promptly. Customer-created custom alerts can be configured for monitoring and alerting. Customer can submit a Service Request to Secureworks, and Secureworks will work with Customer to evaluate the request and determine how to proceed. Secureworks does not monitor the availability of the threat intelligence sources that are used for these Customer-created custom alerts and will not be subject to penalties associated with the Security Monitoring SLA if the sources become unavailable.

2.2.5.1 Security Incident Identification Methods

Secureworks will use two methods to identify and act upon Security Incidents, as explained in the table below.

Identification	Description
Real-Time Security Incidents	Upon receiving alerts that are triggered by Devices, Secureworks will process all Security Events in real-time using its proprietary Multi-Purpose Logic Engine ("**MPLE**") in order to identify patterns that may indicate malicious activity. This process includes analyzing Security Events to add additional context to activity and help reduce the number of false-positive Incidents. During processing, Security Events may be held for 10 to 40 minutes for correlation and context gathering (actual time depends on the use cases that may be matched within the CTP). Security Events that are malicious will be logged as Security Incidents, and further action will be taken, as applicable to the Security Incident.
Retroactive Security Incidents	Secureworks will use a combination of machine learning, look-back alerting for newly discovered threat indicators, and the Secureworks proprietary Long-Term Correlation Engine ("**LTCE**") in order to identify patterns of malicious activity over extended periods of time to generate and analyze Security Incidents. Security Incidents generated from this retroactive analysis are not subject to the Security Monitoring SLA.

2.2.5.2 Security Event Prioritization and Security Incidents

When a Security Event is detected, initial correlation, de-duplication and false positive reduction is performed by the CTP correlation logic. Usually, if the Security Event is prioritized as Medium or High severity, then a Security Incident ticket is either automatically generated by the CTP or manually generated by a security analyst. Secureworks prioritizes all Security Events based on the severity levels described in the table below. Secureworks uses a default event handling policy and can provide this to Customer upon request. This default event handling policy can be reasonably customized during service implementation or during ongoing Service delivery, at the sole discretion of Secureworks.

All Security Events in normalized format are available to Customer in the Portal. Depending on the prioritization of a Security Event and analysis by a security analyst, Security Events become Security Incident tickets, and Secureworks will notify Customer through electronic notification to enable Customer to act on the Security Incident.

Ticket Severity	Description
High*	Security Events that require immediate attention and/or represent potential business impact to Customer environment (e.g., targeted threats, opportunistic malware infection)
Medium	Security Events that do not require immediate attention and typically represent pre-compromise, compliance, audit, reconnaissance, or other types of activity that is unlikely to indicate a significant threat to Customer environment
Low	Security Events that may represent a misconfigured security control, false positive-prone countermeasures, and other activity that has little to no impact to Customer environment

* ***Note:*** The Secureworks ticket severity of “High” includes Security Events that are commonly referred to as “Critical.”

2.2.5.3 Security Incident Analysis and Information

Upon determination of a Security Incident, Secureworks will conduct analysis to provide Customer with as much information as possible through the Security Incident ticket in the Portal. Not all Security Incidents will have the same information available (depends on one or more detection methods) and as such, the information provided can vary between Security Incidents. The following are examples of information that will be provided:

- A description of the Security Event(s) and the activity that was identified
- A copy of the Security Event(s) including packet captures when provided by identifying Device
- Technical details on the threat or activity that was identified, including references
- Source and destination information including hostnames when available
- Additional content and context will be added, but can vary based on detection methods and the activity that is occurring
- Impact of the event on the affected asset
- Corroborating event data that correlates with the original event and is related to the affected asset
- Other assets in Customer’s environment that were overtly interacted with by the threat actor that is related to the event
- Relevant CTU or third-party TI
- Additional contextual information related to the threat
- Recommended next steps based on the identified activity

In-depth analysis, incident response, forensics, and countermeasure implementation beyond policy changes to Devices are not included in this Service. Customer can purchase these services through a separate, signed Transaction Document.

2.2.5.4 Retroactive Security Incident Investigations

Security Incidents that are considered retroactive (i.e., “Retroactive Security Incidents” in the above table) are escalations developed from applying newly identified indicators to historical logs, researchers manually reviewing alerts from countermeasures still under active development (i.e., research for developing new countermeasures), and other similar processes. Researchers investigate threats and relevant details to determine Customer impact, and to develop new countermeasures.

Retroactive escalations may be related to threats still being actively researched and/or ongoing Security Incidents. As such, details related to Retroactive Security Incidents may be limited or privileged.

There is no limit on the number of Secureworks-initiated Retroactive Security Incident investigations that will be conducted for Security Incidents that are created based on Secureworks TI and external resources such as Secureworks trusted partners and OSINT.

Details that can be provided to Customer are added to the Security Incident ticket in the Portal.

2.2.5.5 Security Event Reporting

Customer can use the Portal to create, customize, and access executive and technical level reports, and view and report on detailed, historical Security Event data. Customer will be able to create both standard and customized reports that can be named, scheduled (one time or regular intervals), automatically emailed, or forwarded for review and sign-off for audit/approval purposes.

2.2.6 Device Availability and Event Flow Monitoring and Alerting

Secureworks must be able to connect to the Device(s) using Internet Control Message Protocol ("**ICMP**") or Secure Shell ("**SSH**") depending on the platform type. Secureworks conducts a Host Status validation (approximately every 1-5 minutes; timing is subject to change) on the Device(s) to confirm availability. If a failed or negative response is received from a Host Status validation, then an alert is automatically triggered, which sends an auto-generated ticket to the SOC.

Upon detection of loss of device availability and Host Status ticket generation, Secureworks will notify the Customer through electronic notification within the time specified in the SLA. Secureworks will then perform additional troubleshooting to resolve any availability issue. If such troubleshooting is unsuccessful, then Secureworks will notify the Customer through telephone, ticket, or electronic notification based on Customer's configured notification preferences. After such Customer notification, Secureworks will work with Customer to perform further troubleshooting steps until the issue is resolved and worked to identify root cause.

In addition, Secureworks will use Event Flow Disruption ("**EFD**") to detect data flow issues that result in logs not being sent to Secureworks, improperly formatted logs, or when all logs received do not generate Security Events. When event flow issues are detected, an alert is automatically triggered, which sends an auto-generated ticket to the SOC. Secureworks will perform troubleshooting and then notify Customer about the event flow issue through a ticket in the Portal.

For both Host Status and EFD tickets:

- Secureworks will attempt to restore event flow if the root cause is determined to be related to the Device(s). Secureworks will work with Customer's designated POC(s) to address any Device-related issues.
- If the root cause of the EFD is not related to the Device (e.g., a Customer-side network change, outage, or misconfiguration), then Secureworks will provide Customer with troubleshooting information, but Secureworks is not responsible for troubleshooting issues that do not directly relate to the managed Device(s), Equipment, or Secureworks networks and environments.

2.2.7 Software Maintenance for Devices

Secureworks monitors all vendors represented on the Secureworks approved platforms list for release activities related to software patches and updates for managed Devices. As software patches and updates are released, Secureworks will assess their criticality, security, and applicability as part of the Secureworks certification process to maintain Service delivery. Secureworks will install software patches and updates as part of the Service, when the following conditions apply:

- Software patch or update can be performed remotely, with limited or no on-site assistance from Customer
- Software patch or update does not require a change to underlying hardware on which Customer equipment (i.e., equipment not purchased from Secureworks) is deployed
- Customer provides a maintenance interval with notice of at least 48 hours for Secureworks to schedule a resource to perform the work

When vulnerabilities are disclosed, Secureworks assesses the applicability of each disclosure (and related patch or patches, if available) to Customer's managed Devices. Secureworks will notify Customer about critical vulnerabilities that apply to managed Devices.

2.2.8 Return Materials Authorization ("RMA") Assistance

If the NGFW hardware/software (Device) being managed by Secureworks is determined to be in a failed or faulty state and requires replacement, then Secureworks can initiate and fulfill the RMA process with the Device's vendor on Customer's behalf. Customer is responsible for maintaining

a valid support contract and licensing. Customer is also responsible for associating Secureworks with the vendor support contract.

Note: The RMA process for third-party vendors is out of scope in Japan.

2.2.9 Device Management Using the Management Console

Some vendors may require management of the NGFW through the Management Console. In this case, it is Secureworks policy to also accept some management tasks executed within the Management Console along with the NGFW Device(s). The specific management tasks supported by Secureworks are detailed in the "Management Console" description in Section 5.

2.3 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.3.1 Security Operations Centers ("SOCs")

Secureworks maintains SOCs in the United States and internationally. To provide Service to Customers around the world, Secureworks administers security services and support from these SOCs, such as monitoring Security Events, aggregating and correlating data, conducting analysis, escalating Security Events, and performing other security-related activities. Contact information for SOCs will be provided to Customer.

The Secureworks SOC is available 24 hours a day, 7 days a week, for questions and support. During non-Business Days and Hours, some SOC inquires may be sent to other support groups to address during Business Days and Hours.

2.3.2 Business Days and Business Hours

Business Days for Secureworks global headquarters are Monday – Friday and Business Hours are 8 a.m. – 5 p.m. US Eastern Time, excluding US holidays. Business Days and Business Hours for all other Secureworks locations vary according to local time zone and country.

2.3.3 Service Location(s) and Languages

The Service will be delivered remotely from a Secureworks location(s). Voice and email support are provided in English only, except in Japan where support is provided in both English and Japanese. Other components of the Service that are visible to Customer (such as reports, documentation, and the Portal) are provided in English only. Additionally, Secureworks requires that inputs and interfaces to the Service, including but not limited to logs, Application Programming Interfaces ("**APIs**"), and Command Line Interfaces ("**CLIs**"), be provided in English. Service options and availability may vary by country; contact Secureworks sales representative for details.

2.3.4 Service-Enabling Technology

Customer will be provided with access to the Secureworks Client Portal and the Secureworks Mobile Application ("**Mobile Application**"). Customer's use of the Mobile Application shall be subject to the terms and conditions set forth in the Mobile Application. In addition, one or more CTAs will be provisioned. Below are explanations of these items.

2.3.4.1 Secureworks Client Portal

The Portal is the online site for all Managed Security Services Customers, and provides the following:

- Visibility to Customer's Secureworks Services
- Ability to submit tickets to Secureworks with concerns or issues relating to Managed Security Services
- Monitor events and escalations generated

- Access the Secureworks Learning Center (training and self-education – webinars, documentation, SDs, Portal-specific features, and related content)

Access to the Portal is enabled for Customer-specified authorized users during the Organize phase of service implementation (see Section 2.1.1 for more information), and training regarding Portal use is conducted during the Execute phase of service implementation. It is Customer's responsibility to ensure that access for authorized users of the Portal remains current.

All information received by Customer through the Portal is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

2.3.4.2 Secureworks Mobile Application

The Service is integrated into the Mobile Application. As part of Consultation, Customer and Secureworks will review Customer roles and access to Service features in the Mobile Application. All information received by Customer through the Mobile Application is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

2.3.4.3 Counter Threat Appliance

The Service requires a physical and/or virtual CTA(s) to communicate with Customer-Side Technology (e.g., for data collection and transfer for monitored Devices). CTAs should be provisioned in advance of Service Commencement Date and meet minimum hardware and version requirements.

2.3.5 Customer and Secureworks Responsibilities

The following responsibility assignment matrix describes the participation required by both Customer and Secureworks in completing tasks or deliverables for a project or business process to facilitate successful service delivery. Secureworks uses the standard RACI role criteria for managing Customer projects and deliverables. These roles are defined as follows:

- R – Responsible: Role(s) assigned to do the work. For any individual task, there could be multiple roles responsible.
- A – Accountable: Role(s) that make the final decision and has ultimate ownership.
- C – Consulted: Role(s) consulted as the subject matter expert ("**SME**") before a decision or action is taken.
- I – Informed: Role(s) updated with status of work being done, status of ongoing work, and results of work completed.

Note: The SOC provides Quick Start guides to Customer, which contains more detail about SOC-specific roles and responsibilities.

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
Service Preparation	Provide contact information for authorized contacts regarding Customer's account	R, A	I
	Provide information for authorized users who need access to the Portal (Customer will modify as needed at any time through the Portal, and add / remove users as needed)	R, A	I

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
	Provide shipping information for Secureworks to send physical Devices required to implement Service	R, A	I
	Create and provide to Secureworks the escalation procedures to follow for tickets (Customer will modify as needed at any time through the Portal)	R, A	I
	Enter Customer's initial escalation procedures into Portal	A, C, I	R
	Provide information on support requirements, sizing recommendations and sample deployment scripts (applicable to Public Cloud Environments only)	I	R, A
	Provide to Customer the implementation guidelines for service implementation	I	R, A
	Ensure managed Device(s) meets Secureworks-provided hardware and software specifications prior to the start of implementation	R, A	C, I
	Ensure managed Device(s) meets minimum third-party vendor hardware and software specifications prior to the start of implementation	R, A	C, I
	Prepare the environment as required to implement Service, which may include rack space, power, cooling, network connectivity, public cloud access, or other modifications	R, A	I
	Send CTA(s) to Customer-provided location(s) (if using physical CTAs)	I	R, A
Service Implementation	Provide information (e.g., host name, IP address) that Secureworks will use for Devices	R, A	I
	Provide Secureworks with access (e.g., login credentials, access to Customer network) to Devices	R, A	I
	Implement all requirements per guidelines provided to Customer by Secureworks	R, A	I

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
	Install the CTA(s), and use cables to appropriately connect the CTA(s) to the network ***Note:*** In Japan, Customer and Secureworks can agree to on-site installation and device provisioning per a SOW as applicable.	R, A	I
	Finish configuration of CTA(s) (remotely)	I	R, A
	Configure implementation rules on Customer side based on guidelines provided by Secureworks, vendor, or both, as applicable	R, A	I
	Configure implementation rules in the Secureworks environment	I	R, A
	Configure Devices for Security Event logging	I	R, A
	Configure Portal access for Customer's authorized users	C, I	R, A
	Provide training (remotely) to Customer for Portal	I	R, A
	Provide Customer-side post-install validation steps to Customer	I	R, A
	Complete Customer-side post-install validation steps	R, A	I
	Complete Secureworks-side post-install validation steps	I	R, A
Security Monitoring	Conduct daily monitoring activities to include review, triage, and forwarding of Customer-related validated alerts/Security Events/Security Incidents for next steps	I	R, A
	Conduct incident response activities for alerts, Security Events or Security Incidents identified by Secureworks	R, A	I
	Monitor Service-specific logs and create Security Events or Security Incidents for security concerns	C, I	R, A
	Conduct real-time analysis of Security Events that are created (manually create Security Incident tickets if needed); escalate Security	C, I	R, A

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
	Incidents as applicable, using Customer's escalation procedures		
	Conduct log correlation to identify internal sources/destinations of traffic related to escalated Security Incidents (if applicable)	I	R, A
	Submit ticket through Portal to request Security Event tuning calls (include sample of events or incidents) at least five (5) days in advance; Secureworks will provide Customer with guidance	R, A	I
	Adjust filters, MPLE rules, and escalation criteria to meet Customer's incident alerting requirements as a result of Security Event tuning calls	I	R, A
	Submit through Portal (or otherwise contact SOC to submit) request to create custom IP watch lists and related alerting procedures (submit changes to watch lists and alerting procedures through Portal as needed)	R, A	C, I
	Implement Customer-provided custom IP watch lists and related alerting procedures (update as needed, upon request from Customer)	C, I	R, A
	Remediate all malware and threat actor activity	R, A	I
Initial Policy Tuning ***(only with purchase of CTU TI or separate IDS/IPS Tuning Service)***	Provide schedule and teleconference information within Portal ticket for initial policy tuning meetings	C, I	R, A
	Provide information about network assets and configuration to reduce false positives	R, A	I
	Answer security questions from Secureworks (answers may result in policy updates; requires developers and application subject matter experts)	R, A	I
	Recommend policy changes based on information that Customer provides	C, I	R, A
	Approve recommended policy changes for implementation during a Customer-approved change management interval	R, A	I

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
	Implement approved policy tuning recommendations	I	R, A
	Conduct closing activities for tuning (e.g., IDS/IPS blocking and malware blocking)	C, I	R, A
Change Management	Investigate and confirm validity and potential business impacts of changes (i.e., conduct due diligence) prior to submitting a change request in Portal for implementation	R, A	I
	Submit through Portal (or otherwise contact SOC to submit) all change requests for Devices; ensure requests are internally vetted and approved within Customer's organization, and include all information necessary to implement each request	R, A	I
	Advise Secureworks of appropriate timing for maintenance interval to perform changes (e.g., Customer-submitted change requests) and maintenance (e.g., in-scope software upgrades) for Devices	R, A	C, I
	Perform maintenance that is specific to Customer's environment and implement Customer-submitted change requests during Customer-designated maintenance interval	C, I	R, A
	Perform validation on completed changes to Devices in Customer's environment	R, A	C
	Notify Customer (through Portal or email) that requested change was completed	I	R, A
	Provide explicit approval for Secureworks to implement emergency IP blocks without first obtaining Customer approval (optional)	R, A	C, I
	Implement emergency blocking-rule changes as necessary (e.g., to address real-time malicious traffic)	C, I	R, A
	Advise Customer of emergency blocking-rule changes after implementation	C, I	R, A
	Notify Secureworks through Portal or telephone of issues that occur after changes have been implemented	R, A	I

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
	Investigate Customer-reported issue(s) with changes made, and revert to previous state if Secureworks-implemented changes caused issue(s)	A, C	R
	Submit ticket through Portal or otherwise engage SOC for any unplanned changes	R, A	I
	Conduct ad-hoc changes and troubleshooting that is out of scope for the Service	R, A	I
	Complete Secureworks Best Practices report from FW audit and send to Customer POC through email	I	R, A
	Track all changes made to co-managed environment	R, A	I
	Approve changes resulting from Secureworks Best Practices report from FW audit	R, A	I
Support	Investigate Secureworks-identified health-related issues (e.g., a system event such as a memory threshold being exceeded) on Devices	R, A	C, I
	Conduct troubleshooting related to the Service to determine root cause of an issue	C, I	R, A
	Support validation (including validation for health-related issue) for upgrades and updates implemented on Devices	I	R, A
	Work directly with Device vendor on Customer's behalf to support RMA activity ***Note:*** The RMA process for third-party vendors is out of scope in Japan.	C, I	R, A
	Initiate RMA process to send replacement Device(s) to Customer as needed and according to Customer eligibility	C, I	R, A
	Install Secureworks-provided RMA replacement Device(s) for Secureworks remote access (includes minor network configuration and account creation)	R, A	C, I

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
	Notify Secureworks after RMA Device is installed and connected to Customer's network	R, A	I
	Conduct software upgrades and configuration changes that are in scope for the Service (software must be Secureworks supported)	C, I	R, A
	Provide on-site personnel to assist Secureworks while conducting Device software upgrades, hardware changes, Device power cycling, and any activity that must be physically performed on-site	R, A	C, I
	Send electronic notification to Customer about critical Device vulnerabilities and requests for authorization to apply a patch or patches (if applicable to one or more Devices)	C, I	R, A
	Provide support to Customer for issues relating to the Portal (including mobile access)	C, I	R, A
	Ensure Secureworks has current contact information for authorized contacts regarding Customer's account	R, A	I
	Create and maintain scripts for health-specific events to monitor status of Devices	I	R, A
	Send electronic notification to Customer about Secureworks-identified health event issues or concerns ***Note:*** Auto-SMS is out of scope in Japan.	I	R, A
	Notify Customer through electronic notification of connectivity loss for managed Devices within the time specified in the Health Monitoring SLA	I	R, A
General	Submit through Portal (or otherwise contact SOC to submit) any tickets for in-scope work	R, A	I
	Monitor MACs (Enterprise Change Tickets) to ensure subscription limit(s) is not exceeded (see Section 4.1.1 for details)	R, A	C
	Provide Secureworks with advance notice of Customer-authorized scans or Customer network maintenance periods (to avoid	R, A	I

Managed and Monitored Next Generation Firewall with Policy Auditing			
Activity	**Task**	**Customer**	**Secureworks**
	unnecessary Secureworks escalations resulting from these activities)		
	Provide Customer network design and specification for integration with Secureworks services (includes auditing and providing updated designs and specifications when changes are made)	R, A	I
	Download and register mobile application (named "Secureworks Mobile") to mobile device from an application store	R, A	C
	Maintain network ranges (e.g., public, DMZ, and private) and network translation devices (e.g., NAT pools, proxies, and load balancers)	R, A	C, I
	Notify Secureworks of any changes to network ranges (e.g., public, DMZ, and private) and changes to network translation devices (e.g., NAT pools, proxies, and load balancers)	R, A	C, I
	Conduct policy audits (e.g., firewall, IDS/IPS)	R, A	I
	Conduct Secureworks Best Practices policy audit; work with Customer to identify policies that are a security concern	I	R, A
	Maintain valid vendor support contracts for all managed Devices	R, A	I

2.4 Training and Documentation

Each new Secureworks Customer can participate in foundational training for Secureworks Managed Security Services Integration. Foundational training (primarily webinar-based) is offered to align and mature Customer's Secureworks Managed Security Services Integration and compliment the service implementation process. The training is scheduled during the service implementation process, and is delivered through live, interactive training sessions. Other Service-specific training may be provided. Foundational training includes the following topics, as applicable to the Service:

- Portal Training
- Portal User Roles and Audit
- Escalation Procedures
- MPLE Rules Review
- Ticket Review and Baseline Portal Reports
- Managed Device Alignment (e.g., ensuring understanding of expectations between Customer and Secureworks for Devices being managed by Secureworks)

Customer is responsible for its own training and documentation for any third-party products used as part of the Service.

Secureworks will provide Service-related documentation to Customer. Documentation is generally provided through the Portal.

2.5 Support for Private Virtual Environments

Depending on Device types, Customer's environment, Customer's requirements, and other criteria, Secureworks will provide support as described herein, for a single-tenant Private Virtual Environment that is located on Customer's premises as part of a service that Customer purchases from Secureworks. The information in this section is part of Customer agreement with Secureworks, and takes precedence over any conflicting information elsewhere in this SD. The subsections below contain information about Customer responsibilities, Secureworks responsibilities, and out-of-scope services with regard to a Customer's Private Virtual Environment. See the Glossary for definitions of terms related to virtualization that are used in this SD.

Note: The Secureworks managed security services and SLAs are the same for both non-virtualized (physical) environments and virtual environments.

2.5.1 Customer Responsibilities

Customer agrees to the responsibilities explained in the subsections below and acknowledges and agrees that Secureworks' ability to perform its obligations and responsibilities, and its liability under the SLAs, are dependent upon Customer's compliance with these responsibilities.

2.5.1.1 Provisioning and Maintenance

Customer is responsible for all aspects of provisioning (installation, configuration, and setup) of supported Hypervisor technology, such as VMware, including but not limited to the following:

- Virtual switches
- Virtual network interfaces
- Virtual networks
- VMs

Customer must perform all maintenance for the Guest VM, which includes the items listed below.

- Guest VM snapshot backup
- Restoration of the image on the Guest VM
- Underlying Hypervisor that provides in-band management access (e.g., access to Customer's network through Simple Network Management Protocol/SNMP) for Secureworks (*Customer must resolve in-band access issues in case of loss of network connectivity for Secureworks to manage the vCTA and if applicable, Virtual Security Appliance*)
- Troubleshooting (Hypervisor, hardware, and Host/Guest VM)

2.5.1.2 VMs

Customer is responsible for providing the Guest VM(s) on which the Secureworks-provided image (the vCTA) and, if applicable, Virtual Security Appliance ("**VSA**") will be installed. Customer must provision the VM with the required central processing unit ("**CPU**"), memory, storage capacity, and network resources needed for proper functionality and delivery of the Service. Customer shall provide Secureworks with a privileged account with access to the Guest VM(s). This account may also be used for automation purposes. The OS on the Guest

VM must have a valid license for support. Secureworks will not provide any assistance without in-band access to the Guest VM and without a valid license.

2.5.2 Secureworks Responsibilities

Secureworks is responsible for providing the vCTA and, if applicable, VSA, providing support to Customer during provisioning of the vCTA and VSA, and managing and monitoring the vCTA and VSA that are operating on the Guest VM(s). Customer must maintain a suitable environment in which to operate the Guest VM(s) that is being used for the vCTA and VSA. This includes using a Secureworks-supported Hypervisor version.

2.5.3 Shared Responsibilities

2.5.3.1 VSA and vCTA Upgrades

Secureworks will implement upgrades only for the VSA and vCTA on the Guest VM, as applicable to the Service; Customer is responsible for any other upgrades (e.g., Host/Guest VM, Hypervisor).

2.5.3.2 VSA and vCTA Backups

Secureworks will back up the configuration for the VSA and vCTA only. It is Customer's responsibility to back up (and otherwise maintain) the image or virtual hard disk for the Guest VM. If a Guest VM requires a rebuild, then Secureworks will restore the prior vCTA configuration after Customer restores the Guest VM and its connectivity. Secureworks recommends that any virtual infrastructure be deployed on redundant systems.

2.5.4 VSA and vCTA Health, and Adding Capacity

Secureworks will perform health-related validations on the VSA. Secureworks must be able to connect to the VSA through the Internet using ICMP and SSH. Each VSA is always assumed to be powered on, and any disappearance of a VSA from the network is considered a failure.

Secureworks will monitor the vCTA. If it is determined that a health-related issue caused by performance of the Host/Guest VM hardware, or insufficient capacity for the Guest VM, is negatively affecting the vCTA, then it is Customer's responsibility to resolve the performance issue or add sufficient capacity to the Guest VM.

Secureworks will perform availability monitoring of the VSA and vCTA using periodic polling (approximately every 1-5 minutes; timing is subject to change) of each Device. If a failed or negative response is received through polling, then an automatic alert is sent to Secureworks, which then generates a ticket. Secureworks will conduct troubleshooting and contact Customer as applicable to the Service.

Health monitoring is limited to VSAs, CTAs, and other Devices. Secureworks does not perform health monitoring for Hypervisors or underlying hardware.

2.5.5 Virtual Firewall Instances

Secureworks will not automatically detect and add Virtual Firewall Instances when they are implemented within a physical firewall or standalone instances. For the Service to be provisioned correctly, Customer must inform Secureworks that the Virtual Firewall Instance has been implemented. A firewall is defined as ***any*** firewall platform whether physical, cloud, virtual machine (VM), or instance. Since each Virtual Firewall Instance acts as its own device, invoicing is based on the number of Virtual Firewall Instances instead of the number of firewall Devices. For example, if a firewall device has five (5) Virtual Firewall Instances, then Customer will be billed for five (5) Virtual Firewall Instances and the host firewall Device, for a total of six (6) firewalls in this example.

2.5.5.1 Requirements for Implementing or Decommissioning a Virtual Firewall Instance

After a new Virtual Firewall Instance is implemented, Customer must submit a ticket in the Portal so that a corresponding Device record can be provisioned within CTP. When Customer decommissions a Virtual Firewall Instance, Customer must also submit a ticket in the Portal so that the corresponding Device record can be removed, and Customer will no longer be billed. This process ensures that appropriate monitoring and management functionality will be applied, and that Customer will be billed correctly.

Customer shall submit a ticket through the Portal to inform Secureworks that Customer has implemented a new Virtual Firewall Instance or decommissioned a firewall instance. Access the Portal, click the "Service" option in the top navigation bar, and click the "Create Service Request" link to create the ticket.

2.5.5.2 Self-Service Provisioning Requirements

Virtual Firewall Instances that are within the scope of support for Self-Service Provisioning ("**SSP**") will be automatically discovered and entered in the Portal for review and activation.

If monitoring needs to be added to a Virtual Firewall Instance, then Customer will first need to enable monitoring through the "Activate Monitoring" function within the Portal.

If the Virtual Firewall Instance is decommissioned through SSP, then Customer will also need to remove it from monitoring from within the Portal.

2.5.6 Out-of-Scope Services in a Virtual Environment

The following are considered out of scope for this Service:

- Restoring the VM image backups
- Troubleshooting issues at the Hypervisor level
- Troubleshooting performance issues not directly related to the VSA or the vCTA (i.e., the image on the Guest VM) such as hardware, Hypervisor, or Host-level issues
- Anything not specifically described herein as part of the standard offering for the Service

2.6 Out of Scope

The information in Section 2 comprises the Secureworks standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Items listed below are examples of services and activities that are out of scope. Upon request, Secureworks may provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document.

- Incident management services
- On-site installation and provisioning of Device
  Note: *In Japan, Customer and Secureworks can agree to on-site installation and device provisioning per a SOW as applicable*.
- Analysis of minor events
- Integration of complementary products that are not managed by Secureworks (e.g., anti-virus software, web reporting software)
- Custom analysis or reports
- Forensics
- Configuration of any tunnel endpoint that is not terminated on a Secureworks-managed Device
- Vendor API Integration
- Rule set design and validation
- NGFW policy or rule utilization

- Development of customized IDS/IPS signatures
- Tuning of IDS/IPS signatures without purchase of CTU TI or a separate tuning service
- Any change requests and NGFW policy auditing not specified in this SD
- Product training and any security best practices consulting not specified in this SD
- Policy migration

3 Feature Support for Managed Devices

Below are capabilities that Secureworks can enable and support for Customer when Secureworks is managing Devices for Customer.

3.1 Application Intelligence and Control

Some platforms offer application intelligence and control. At the time of initial deployment, by default, these capabilities are disabled, but they can be enabled upon Customer's request. For example, there could be thousands of applications supported within the Device(s) that Secureworks is managing. Therefore, it is Customer's responsibility to specify all application control and application rule settings required for application intelligence. Secureworks will configure the Device(s) in accordance with Customer's specifications. Only pre-defined, vendor-provided application controls are supported.

4 Service Fees and Related Information

Service Fees are based on the Devices being managed. See Customer's MSA or CRA (as applicable), and Transaction Document for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

If during the course of activation, the monitoring component of this Service is activated prior to the management component, Customer acknowledges that Secureworks reserves the right to commence invoicing Customer, and Customer agrees to pay for the monitored component provided by Secureworks, in accordance with billing terms in the MSA or CRA and based on the then-current Secureworks list price for the monitoring component(s) activated, until such time as the management component is activated, at which time invoicing for the full service fee will commence.

4.1 Invoice Commencement and Related Information

See the Service-specific Addendum or Transaction Document for information about invoice commencement.

4.1.1 Exceeding Enterprise Change Ticket Volume

Customer will be provided with limited Device Management ticket-based support for Enterprise Changes ("**Enterprise Change Tickets**"). If Customer exceeds the total number of allowed Enterprise Change Tickets (which includes MAC and incident troubleshooting) as determined in accordance with the number of NGFWs being managed (see the examples below), then Secureworks reserves the right to assess an overage charge to Customer at the end of the Services Term. The charge will be based on total number of Enterprise Change Tickets exceeding the per Services Term year allowance of 20 Enterprise Change Tickets per NGFW or 40 per high availability ("**HA**") NGFW pair at the rate indicated in Customer's Transaction Document.

Customer is entitled to 20 Enterprise Change Tickets per NGFW or 40 per HA NGFW pair	
Example 1	**Example 2**
Secureworks manages three NGFWs for Customer; Customer can use 60 tickets equally across the NGFWs or for any combination, such as the following: NGFW 1: 20 Enterprise Change Tickets NGFW 2: 20 Enterprise Change Tickets NGFW 3: 20 Enterprise Change Tickets OR NGFW 1: 3 Enterprise Change Tickets NGFW 2: 10 Enterprise Change Tickets NGFW 3: 47 Enterprise Change Tickets	Secureworks manages two HA NGFW pairs for Customer; Customer can use 80 tickets equally for each pair or for any combination, such as the following: NGFW HA Pair 1: 40 Enterprise Change Tickets NGFW HA Pair 2: 40 Enterprise Change Tickets OR NGFW HA Pair 1: 15 Enterprise Change Tickets NGFW HA Pair 2: 65 Enterprise Change Tickets

5 Recommended Add-on Services

The Secureworks offerings listed below are optional and are sold independent of this Service or bundled with this Service. In addition, output from the Service can be used in delivering these add-on services for an additional charge.

- **High Availability:** As an optional service upgrade, Secureworks offers a high availability solution for NGFWs that support redundancy. This solution involves a NGFW pair deployed in an active/standby or active/active configuration. The information in this SD is applicable to the NGFW pair.
- **Management Console:** Secureworks will manage a management console located at a Secureworks site ("**Hosted Management Console**") or at a Customer site ("**Customer On-Premises Management Console**") if the vendor management console is supported by Secureworks. Some vendors may require management of the NGFW through the management console. The specific management tasks supported by Secureworks are detailed below; any other service requests associated with managing a management console are out-of-scope.
  - **Secureworks Hosted Management Console** – In this scenario, management consoles are located within a Secureworks data center. Secureworks shall maintain exclusive administrative privileges to the management console and will manage all Devices contained within the management console. Upon Customer's request, read-only access to the management console may be provided to Customer. Customers who have read-only access to the Hosted Management Console will be notified in advance of work being performed on the management console. Secureworks will perform the following:
    - ***Console backup and restore:*** Secureworks will maintain Hosted Management Console backups at a Secureworks site to rebuild the management console, in the event of a hosted managed management console failure.
    - ***Application updates:*** Secureworks will perform application updates from time to time to maintain vendor support, and to resolve existing application issues. Customers will be notified in advance of any maintenance that needs to be performed on the Hosted Management Console as well as any mandatory software updates that the NGFW managed Devices may require to maintain connectivity to the Hosted Management Console.
    - ***License costs:*** Customer is responsible for any license costs associated with the hosted console management.

- **Customer On-Premises Management Console** – In this scenario, management consoles are located at a Customer site. Two delivery models are associated with On-Premises Hosted Management Console: Co-Managed and Customer Managed. Both are explained in the subsections below.
    - ***Co-Managed:*** Customer provides Secureworks with a privileged application account and a privileged operating system account to the management console if applicable. Customer retains administrative operating system access and application access to the management console. Customer must maintain a valid vendor maintenance support contact and licensing.
        - ***Console backup and restore*** – Secureworks requires that the management console backups be stored and maintained by Customer on a remote device at Customer site. If a remotely-managed management console failure requires a rebuild, then Secureworks will work with Customer to transfer a copy of the latest backup to Customer's On-Premises Management Console.
        - ***Application upgrades*** – Application upgrades will be required from time to time to maintain vendor support and resolve existing application issues. Secureworks can perform the update to the management console on behalf of Customer. If Secureworks deems the upgrade is of significant risk, Secureworks may request that a technically skilled representative be available during the update and will work with Customer to establish a mutually acceptable maintenance interval. If Customer performs an application update, Secureworks must be notified at least one (1) business day prior to a console software update to ensure that service continuity is maintained.
    - ***Customer Managed:*** Limited Secureworks Access – Customer will provide Secureworks with an application user account with the necessary privileges to perform policy modifications, deletions, additions, and installation of policies and objects for the Secureworks managed Devices. Customer is solely responsible for ongoing maintenance, updates, and backups of Customer-Managed management console. To ensure that the proper support is maintained, Customer must notify Secureworks at least five (5) days prior to a console software or hardware update. This option may not be available for some deployments due to functionality of the NGFW platform or network architecture.

- **Advanced Endpoint Threat Detection:** A managed security service that monitors Endpoints running on compatible operating systems for signs of advanced threat actor activity. The service includes searching for specific indicators of compromise, maintaining TI, analyzing telemetry, and sending alerts to Customer with recommendations on how to proceed should threat activity be detected.
- **Secureworks Threat Intelligence ("TI"):** This optional addition to the service includes the application of Secureworks TI content developed by the CTU that is applied regularly to enhance its protective capabilities. The TI content can only be applied to Secureworks-supported platforms; a list of these platforms can be provided upon request.
    - **Attacker Database** – The Secureworks Attacker Database ("AttackerDB") can be provided as a part of an add-on to the managed NGFW Service on selected Secureworks-supported platforms. The Secureworks AttackerDB contains a list of domain names and IP addresses used to conduct malicious activity. AttackerDB includes a TI data feed that can be applied to each managed NGFW. Integration of AttackerDB with the NGFW Devices facilitates cyberattack prevention through proactively blocking traffic to known malicious domain names and IP addresses, with block-lists being automatically updated using the AttackerDB TI feed.

      A subset of the AttackerDB (Coal Black lists of malicious IP and domain names) is available at no charge to Customers with the following appliances that Secureworks is managing: Palo Alto Networks, Juniper with Sky ATP, Firepower, and Firepower Threat Defense.
    - **CTU Countermeasures** – CTU Countermeasures are derived from analysis of malware samples and comprehensive vulnerability analysis. The CTU countermeasures for NGFW platforms consist of select rules to complement the existing coverage provided the vendor's

own threat research team. Deploying these countermeasures increases the effectiveness of Customer's managed NGFW to alert or block communications to known command and control centers. Customers subscribed to this service are offered expert installation and configuration support of CTU countermeasures from Secureworks SOC. Secureworks SOC may initiate additional signature updates to address critical vulnerabilities as and when required.

- ***Initial IPS Policy Tuning:*** If Customer purchases the Secureworks-supported NGFW Device, and purchases CTU Countermeasures for the Device as part of the Service, then Secureworks will contact Customer to tune the IDS/IPS policy to Customer's environment during the thirty (30) day tuning period that begins on the Service Commencement Date. During this tuning period, Secureworks will work with Customer to suppress, enable, and disable signatures and rules. Blocking traffic creates the risk of potential disruption to Customer's business. Secureworks is not responsible for negative impacts to Customer as a result of network traffic blocked by a Device.
- ***IDS/IPS Signature Maintenance:*** IDS/IPS policies are updated once a week with the latest signatures from CTU. These signatures can be suppressed, enabled, or disabled on an as needed basis by submitting a ticket via the Portal or calling the Secureworks SOC.

Secureworks can also update the managed Device with Customer-provided signatures depending on the NGFW platform. Customer will be required to provide signatures in a relevant format that is specific to, and supported by, the managed Device. Signature removal may occur if the format required is not followed. Secureworks will address Management Console errors as a result of importing signatures. Secureworks will upload and apply signatures on a per ticket request basis that is not auto-reoccurring.

Custom signatures are supported when:

- Customer provides text file with signatures
- Custom signature is provided from the vendor, with the stipulation that if there is an error with a non-standard ruleset signature, the vendor would need to either adjust the rule or the rule would be removed

Custom signatures are not supported when:

- Custom signature causes performance issues – Secureworks will remove the signature causing the performance issue
- Custom signature has syntax errors – Secureworks will report any errors regarding the custom signature(s) and Customer will be responsible for rewriting the signature
- Customer signature numbers or signature keys conflict with vendor or Secureworks authored signatures
- Other restrictions may apply

6 Service Level Agreements ("SLAs")

The table below contains the SLAs that are applicable to the Service.

SLA	Definition	Credit
Firewall Standard Change Request	Standard change requests will be acknowledged within one (1) hour from the creation time stamp on the ticket.	1/30th of monthly fee for Service for the affected Device
Service Request	A service request (applies to all non-change and non-incident tickets) submitted through telephone or the Secureworks Client Portal will be acknowledged through human or electronic notification (e.g., Portal,	1/30th of monthly fee for Service for each calendar day the service request was not

SLA	Definition	Credit
	mobile app) within one (1) hour from the creation time stamp on the ticket. Customer must contact SOC through telephone or the Chat in the Portal for immediate engagement with urgent service request tickets.	acknowledged within the specified timeframe
Security Monitoring *(Security Incident analysis)*	Customer shall receive electronic notification of a Security Incident (in accordance with Customer's defined escalation procedures) within fifteen (15) minutes of the determination by Secureworks that the given activity constitutes a Security Incident. This is measured by the difference between the time stamp on the incident ticket created by Secureworks SOC personnel or technology and the time stamp of the correspondence documenting the initial escalation Security incidents generated from long-term correlation logic and retroactive analyses based on newly identified threat indicators are not subject to this SLA. Event(s) deemed low severity may be sent to Customer for review, and will be available through the Portal for reporting	1/30th of monthly fee for Service for the affected Device
Health Monitoring	Health incident validation identifying unreachable Devices: 30-minute response time through telephone, ticket in Portal, or other electronic notification; measured as the difference between the creation time stamp on the Device unreachable ticket to the time stamp of the first correspondence documenting the initial escalation to Customer.	1/30th of monthly fee for Service for each calendar day on which Device unreachable event(s) were not communicated to Customer in the specified timeframe, up to, but not exceeding, 100% of the monthly fee for Service
Availability	Communications availability to the Internet and Customer access to the Secureworks Client Portal shall equal no less than 99.9% of the time during any calendar month. "Communications availability" is defined as the ability of a Secureworks SOC to successfully send and receive TCP/IP packets between the CTP and its upstream Internet service provider. "Customer access to the Secureworks Client Portal" is defined as the ability of the Secureworks monitoring service to successfully log in to the Portal. Secureworks does not provide a guarantee with regard to availability or performance of the Internet. Measurement of 99.9% is executed from multiple sites connecting to a Secureworks SOC.	1/30th of monthly fee for Service

Warranty Exclusion: While the Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Secureworks makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer's network.

The SLAs set forth above are subject to the following limitations:

- Secureworks schedules maintenance outages for Secureworks-owned equipment that is being used to provide the Service and will provide Customer-designated contact(s) with 24 hours of notice of an outage. The SLAs shall not apply during scheduled maintenance outages, and no SLA credit shall apply during a maintenance outage.
- Secureworks shall not be responsible for any Service impact related to any product configuration on a managed Device that is not supported by Secureworks.
- The SLAs shall not apply if any act or omission by Customer prohibits or otherwise limits Secureworks from providing the Service or meeting the SLAs, including but not limited to misconduct, negligence, provision of inaccurate or incomplete information, modifications to the Service, or any unauthorized modifications made to any managed hardware or software Devices, by Customer or its employees, or third parties acting on behalf of Customer.
- The SLAs shall not apply to the extent Customer does not fulfill and comply with the obligations and responsibilities set forth within this SD. The obligations of Secureworks to comply with the SLAs with respect to any Security Incident response or Service Request are also dependent on Secureworks' ability to connect directly to Customer-Side Technology on Customer's network.
- The SLAs shall not apply if Customer-Side Technology is unreachable due to network connectivity issues, authentication issues, configuration issues, or public cloud downtimes that are outside the direct control of Secureworks.

For Customer to receive an SLA credit, subject to the limitations above, the notification of the SLA failure must be submitted to Secureworks within thirty (30) days of the date of such SLA failure. Secureworks will research the notification and respond to Customer within thirty (30) days from the date such notification is received. The total amount credited to Customer in connection with any of the above SLAs in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. The foregoing SLA credit(s) shall be Customer's sole and exclusive remedy for failure to meet or exceed the foregoing SLAs.

7 Additional Considerations and Information

7.1 Secureworks Lifecycle Policy and Related Information

Secureworks provides its Lifecycle Policy through this link: https://www.secureworks.com/client-support/lifecycle-policy. This policy includes information for customers purchasing service bundles and products. Use the following link for direct access to the Policy ***in PDF format***: Secureworks Lifecycle Policy. Customer can also access the Secureworks Hardware and Software Support Status matrix, End-of-Sale ("**EOS**") and End-of-Life ("**EOL**") notifications, and other information through the aforementioned link. Secureworks reserves the right to alter the General Availability ("**GA**"), EOS, and EOL dates at any time for any reason. Secureworks is not responsible for errors within the Hardware and Software Support Status matrix.

7.2 Cisco End User License Agreement (EULA)

If Customer is a service bundle customer or product customer (see the information in the aforementioned Secureworks Lifecycle Policy) or Customer's use of the Service includes hardware and/or software from

Cisco, then Customer agrees to Cisco's end user terms, which are available through this link: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

8 Glossary

Term	Description
Attacker Database ("**AttackerDB**")	A database of known malicious attackers determined by analyzing Secureworks security device data.
Counter Threat Appliance ("**CTA**")	Equipment that specifically allows Secureworks to collect data while performing a Secureworks-defined service for Customer, such as monitoring Customer's network and environment for security threats.
Counter Threat Platform ("**CTP**")	A Secureworks proprietary MSS Services platform that ingests log data to produce events within the platform, which are then correlated and analyzed to protect customers from emerging and existing threats.
Counter Threat Unit ("**CTU**")	Internal team of security experts that research and analyze threat data across Secureworks global Customer base and actively monitors the threat landscape. Provides threat intelligence that extends visibility into cyber threats beyond the edges of the networks of Secureworks Customers. The threat intelligence, applied to technology and the Secureworks suite of services, enables Customers to expand visibility and reduce the time it takes to see and respond to them, thereby resisting and avoiding cyberattacks.
Customer Device(s)	One or more devices that are owned by Customer and were not purchased from Secureworks.
Device(s)	Equipment that is in scope for the Service.
Due Diligence	Validating the accuracy of information used to create Customer's original Transaction Document against the actual environment in which services will be performed.
End of Life ("**EOL**")	The date on which all support for a product ends, which includes any software upgrades, hardware upgrades, maintenance, warranties, or technical support.
End of Sale ("**EOS**")	The date on which a product is no longer available for purchase.
Event Flow Disruption ("**EFD**")	A proactive method that detects differences with logs being sent to Secureworks from individual Devices – e.g., complete loss of log flow, incorrect log format, or an overall lack of logs to trigger Security Event generation within the CTP.
General Availability ("**GA**")	The date on which hardware or software is made available to the public for purchase.
Identified Changes	Differences (e.g., Device quantity, make, model, software package, or software version) that are discovered while conducting due diligence for the Service.
Security Event	Identified occurrence of a system or network state that may be malicious, anomalous, or informational, which is ingested into the Secureworks technology infrastructure.

Term	Description
Security Incident	One or more related and identified Security Events that can potentially impact the confidentiality, integrity, or availability of a Customer's information or systems, and requires further analysis and disposition.
Service Level Agreement ("**SLA**")	A legally-binding arrangement to meet defined standards for the Service.
Definitions for Virtual Environments	
Guest	Separate and independent instance of operating system and application software that operates on a Host.
Host	Virtual Machine host server that provides the physical computing resources, such as processing power, memory, disk, and network I/O.
Hypervisor	Virtual machine monitor that isolates each Guest, enabling multiple Guests to reside and operate on the Host simultaneously.
Virtual Contexts	A form of virtualization where one physical firewall is divided into two (2) or more virtual firewalls.
Virtual Firewall Instance	A logical instance or “slice” of resources within a firewall device. Multiple firewall instances may exist within a single firewall device and each needs to be represented by its own device record within CTP.
Virtual Machine (“**VM**”)	A logical instance of the physical Host that houses the operating system of the Guest.
Virtual Security Appliance (“**VSA**”)	Software implementation of a security device—e.g., a log retention appliance, scanner appliance (VMS), intrusion detection system—that executes programs in the same manner as a physical machine.