

## Managed IDS/IPS (includes monitoring)

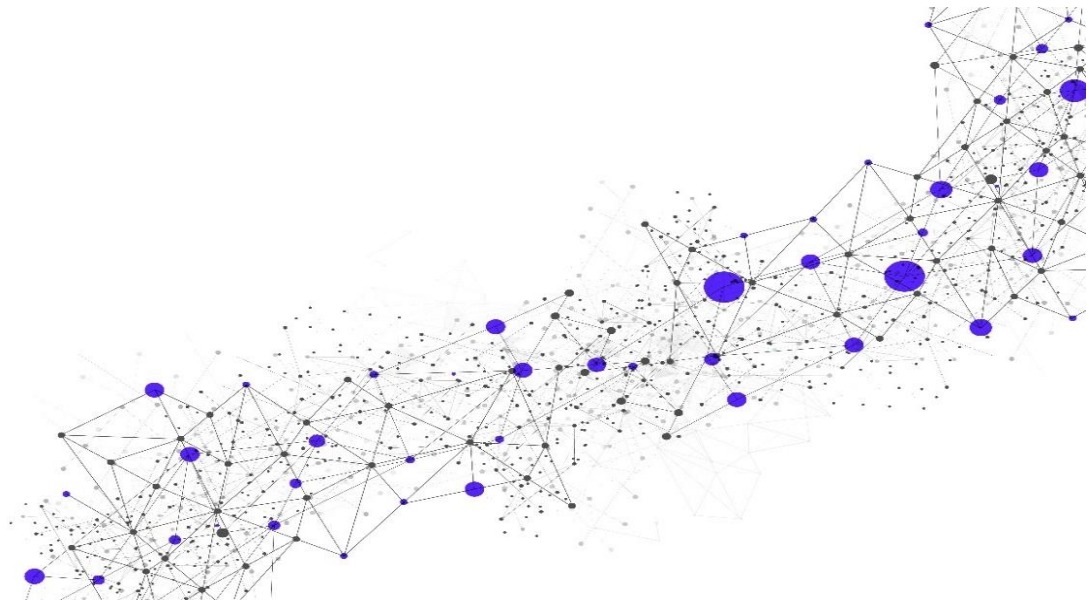
---

Release Date

**July 13, 2021**

Version

**18.2**



[www.secureworks.com](http://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](mailto:info@secureworks.com)

Additional office locations: <https://www.secureworks.com/about/offices>

---

## Table of Contents

<b>1</b>	<b>Service Introduction .....</b>	<b>4</b>
1.1	Overview .....	4
1.2	Customer Obligations .....	5
1.2.1	Licensing and Support Contracts .....	5
1.2.2	Connectivity .....	5
1.2.3	Application Program Interface ("API") Integration .....	5
1.2.4	Communications .....	5
1.2.5	Maintenance .....	6
1.2.6	Usage Overage.....	6
1.2.7	Provisioning in a Public Cloud or Private Virtual Environment .....	6
1.2.8	Hardware and Software Procurement .....	6
1.2.9	General .....	6
1.3	Initial Implementation Scheduling and Points of Contact .....	6
<b>2</b>	<b>Service Details .....</b>	<b>7</b>
2.1	Service Implementation .....	7
2.1.1	Implementation Methodology .....	7
2.1.2	Service Provisioning, Installation, and Activation .....	8
2.2	Service Components .....	10
2.2.1	Policy Management .....	10
2.2.2	Device and Policy Troubleshooting .....	10
2.2.3	Management Console(s) .....	11
2.2.4	Security Event Monitoring and Alerting.....	12
2.2.5	Device Availability and Event Flow Monitoring and Alerting.....	14
2.2.6	Software Maintenance for Devices.....	15
2.2.7	Return Materials Authorization ("RMA") Assistance .....	15
2.3	Service Delivery .....	15
2.3.1	Security Operations Centers ("SOCs") .....	15
2.3.2	Business Days and Business Hours .....	15
2.3.3	Service Location(s) and Languages .....	15
2.3.4	Service-Enabling Technology .....	16
2.3.5	Customer and Secureworks Responsibilities .....	16
2.3.6	Secureworks Platform Maintenance .....	23
2.4	Training and Documentation .....	23
2.5	Support for Private Virtual Environments .....	24
2.5.1	Customer Responsibilities .....	24
2.5.2	Secureworks Responsibilities .....	25
2.5.3	Shared Responsibilities .....	25
2.5.4	VSA and vCTA Health, and Adding Capacity.....	25
2.5.5	Out-of-Scope Services in a Virtual Environment .....	25
2.6	Out of Scope .....	26
<b>3</b>	<b>Feature Support for Managed Devices .....</b>	<b>26</b>
3.1	Application Intelligence and Control .....	26
3.2	User Control .....	26
<b>4</b>	<b>Service Fees and Related Information .....</b>	<b>27</b>
<b>5</b>	<b>Recommended Add-on Services.....</b>	<b>27</b>

<b>6</b>	<b>Service Level Agreements (“SLAs”)</b> .....	<b>28</b>
<b>7</b>	<b>Additional Considerations and Information</b> .....	<b>30</b>
7.1	Secureworks Lifecycle Policy and Related Information .....	30
<b>8</b>	<b>Glossary</b> .....	<b>30</b>

## Copyright

© Copyright 2007-2021. SecureWorks, Inc. or its affiliates. All Rights Reserved.

This publication contains information that is confidential and proprietary to Secureworks® and is subject to your confidentiality obligations set forth in your contract with Secureworks or its affiliates. This publication and related hardware and software are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Copying and/or reverse engineering of any Secureworks hardware, software, documentation, or training materials is strictly prohibited.

This publication and related Secureworks software remain the exclusive property of Secureworks. No part of this publication or related software may be reproduced, stored in a retrieval system, or transmitted in any form or any means, electronic or mechanical, photocopying, recording, or otherwise without the prior written permission from Secureworks.

Due to continued service development, the information in this publication and related software may change without notice. Please refer to your contract with Secureworks for any provided warranty information.

Secureworks® is a trademark or registered trademark of SecureWorks, Inc. or its affiliates. All other trademarks not owned by Secureworks that appear on this publication are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Secureworks.

## 1 Service Introduction

This Service Description (“SD”) describes the Managed Intrusion Detection System / Intrusion Prevention System 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 on-premises physical or virtual Intrusion Detection System (“IDS”) and/or Intrusion Prevention System (“IPS”) (also collectively referred to as “IDS/IPS Devices” or “Devices” in this SD) 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. Secureworks will provide policy management, troubleshooting, software maintenance for Devices, and management of one or more management consoles associated with the Devices. Secureworks will only manage Devices for which Customer has a valid license(s), vendor support contract, and Secureworks-supported features (see Section 3, [Feature Support for Managed Devices](#)). For a list of IDS/IPS Devices that Secureworks will manage, see the [Hardware and Software Support Status](#) matrix that is accessible from the [Secureworks Lifecycle Policy](#) page on the Secureworks company website.

Secureworks will also 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 event data 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 2.2.4, [Security Event Monitoring and Alerting](#), contains more information about how events are processed.

Customer will purchase and install the Devices in Customer’s environment and ensure connectivity to the applicable management console(s). Secureworks, or Secureworks and Customer, will use the management console(s) to manage the Devices. See Section 2.2.3, [Management Console\(s\)](#), for details.

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.

The Service includes the following components:

- Policy Management
- Device and Policy Troubleshooting
- Management Console(s) – *managing the console(s) and using it to manage the Devices*
- Security Event Monitoring and Alerting
- Device Availability and Event Flow Monitoring and Alerting
- Device Maintenance
- Return Materials Authorization (“RMA”) Assistance

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 Licensing and Support Contracts

Customer will obtain and maintain current vendor licensing, vendor support, and vendor maintenance contracts for the IDS/IPS Devices. Customer is also responsible for associating Secureworks with the existing vendor support and vendor maintenance contracts to enable 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.

**Note:** For Customers in Japan, it is Customer’s responsibility to submit support tickets with its fourth-party vendor (i.e., Reseller, Distributer, or Sier who has the support contract with vendor) for issues requiring vendor assistance. Secureworks will provide best effort to Customer for resolving issues with the IDS/IPS Devices.

### 1.2.2 Connectivity

Customer will provide and maintain remote network connectivity to Customer’s environment, including ensuring sufficient network bandwidth, and the in-scope Device(s) that are necessary for Secureworks to perform the Service. Customer will also allow connectivity from Secureworks IP range to Customer location(s) as applicable to the Service. 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 will 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 representatives 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, and Customer will pay for the Overage 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 may need to purchase additional network equipment – e.g., cables and redundant power supplies. 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 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 terms and conditions 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.

**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 the 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. 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/adaptor, 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

#### 2.2.1.1 Initial Device Policy Tuning

Upon service activation, Secureworks applies one baseline policy of signatures and rules to each Device. Secureworks then tunes this policy to Customer's environment during the thirty (30) day tuning period which begins on the Service Commencement Date. During this tuning period, Secureworks will work with Customer to suppress, enable, and disable signatures and rules as they pertain to the Device policy and Customer's environment. Blocking traffic creates the risk of potential disruption to Customer's business. Secureworks is not responsible for negative impacts to Customer resulting from network traffic blocked by a Device.

#### 2.2.1.2 Policy Maintenance

Device policies will be updated manually or automatically (depending on Device type and vendor's update procedures), provided the Device has the necessary connectivity to obtain the updates. Manual updating of policies occurs within one to seven calendar days of updates being released by each IDS/IPS 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 Customer submitting a ticket through the Portal or otherwise contacting the SOC.

Secureworks can update a managed Device with custom signatures. Customer shall provide the signatures in a relevant format that is specific to the managed Device, and submit a ticket in the Portal for Secureworks to upload and apply signatures. Secureworks will address management console errors that result from uploading and applying signatures. An incorrectly formatted signature may not upload properly to the Device or it may cause issues that lead to removal of the signature. Secureworks will upload and apply signatures on a per-ticket basis that is not auto-recurring.

Custom signatures are supported for the following:

- Customer provides text file with signatures
- Customer provides custom signature that vendor creates, with the stipulation that if there is an issue with the signature, the vendor will need to either adjust the signature or the signature can be removed per Customer decision

Custom signatures are not supported for the following:

- Custom signature causes performance issues – Secureworks can remove the signature causing the performance issue per Customer decision; no further troubleshooting support will be provided
- Custom signature has syntax errors – Secureworks can report on errors but will not assist with rewriting the signature

### 2.2.2 Device and Policy Troubleshooting

Secureworks will work with Customer to troubleshoot issues with Customer's managed Device(s) and associated policies. If necessary, Secureworks will engage the vendor on Customer's behalf.

- If the root cause of the issue is with the managed Device, then Secureworks will work with Customer's designated point of contact through telephone to address any Device-related issues.

- If the root cause of the issue is not related to the managed Device (e.g., a network change, outage, or issue with a 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(s), Equipment, or Secureworks networks and environments.

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

### 2.2.3 Management Console(s)

Secureworks will manage one or more management consoles located at a Customer site, which are also used to manage Customer's on-premises Devices. The subsections below contain information (including responsibilities) about the Co-Managed and Customer Managed options for management consoles. Upon request, Secureworks can provide out-of-scope technical support for management consoles on a time and materials basis pursuant to a separate SOW.

If Customer has more than one management console, then Customer will determine which option will be used for **each** management console; any combination of the two options can be used.

#### 2.2.3.1 Co-Managed

Customer and Secureworks will share responsibility for managing one or more management consoles (as well as sharing responsibility for managing the Devices), and Customer will provide Secureworks with administrative privileges for both the operating system and application for the management console and the Devices. Customer will retain its own administrative privileges to the management consoles. Customer must maintain valid vendor maintenance support contracts and licensing for the management consoles.

- **Backups and restores:** Secureworks requires that Customer store and maintain backups of the management consoles on a separate (secondary) device at any Customer site. If a management console fails, then Secureworks will work with Customer (remotely through teleconference) to use the latest backup to restore the management console.
- **Updates and Upgrades:** On behalf of Customer, Secureworks can implement updates and upgrades as needed to maintain vendor support for the management consoles, and to resolve issues that arise. Secureworks will notify Customer of available updates or upgrades that are necessary and recommended, and Customer will indicate which updates and upgrades will be implemented. If Secureworks deems the update or upgrade is of significant risk, then Secureworks may request that a technically-competent Customer representative be available during the update or upgrade, and Secureworks will work with Customer (remotely through teleconference) to establish a mutually acceptable maintenance interval for implementation. If Customer implements updates or upgrades, then Customer will notify Secureworks at least one (1) business day in advance to ensure that Service continuity is maintained.

#### 2.2.3.2 Customer Managed - Limited Secureworks Access

Customer will provide Secureworks with administrative privileges for both the operating system and application for one or more management consoles to perform the following activities for the Devices that Secureworks will manage: policy modifications, deletions, and additions; and installation of policies and objects. Customer will be solely responsible for ongoing maintenance, updates and upgrades, and backups of the management consoles. To ensure support from Secureworks is maintained, Customer must notify Secureworks at least one (1) business day in advance of implementing updates or upgrades to the management consoles.

**Note:** The Customer Managed – Limited Secureworks Access option may not be available for some Customer environments due to functionality of the IDS/IPS or Customer's network architecture.

## 2.2.4 Security Event Monitoring and Alerting

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

- Secureworks Threat Intelligence (“TI”)
- Machine learning
- Signature-based detections
- Human-based pattern identification (through ongoing research that CTU™ and SOC analysts conduct)
- 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.

### 2.2.4.1 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 are 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.

#### 2.2.4.2 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 at time of 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.”

#### 2.2.4.3 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.

#### 2.2.4.4 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.

#### 2.2.4.5 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.

### 2.2.5 **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.

### 2.2.6 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 Customer to upgrade/replace the managed Device(s)
- 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.

### 2.2.7 Return Materials Authorization ("RMA") Assistance

If a Device that Secureworks is managing for Customer is determined to be in a failed or faulty state and requires replacement, then Secureworks can initiate and fulfill the RMA process with the managed Device's vendor on Customer's behalf. Customer is responsible for maintaining a valid support contract and licensing for the Device. 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.

## 2.3 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.

### 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. 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 inquiries may be sent to other support groups to address during Business Days and Hours.

### 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 IDS/IPS			
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
	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 (if applicable)	R, A	C, I
	Prepare the environment as required to implement Service, which may include rack space, power, cooling, network connectivity,	R, A	I

Managed IDS/IPS			
Activity	Task	Customer	Secureworks
	public cloud access, or other modifications		
	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
	Install the CTA(s), and use cables to appropriately connect the CTA(s) to the network  <b>Note:</b> 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 initial 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

Managed IDS/IPS			
Activity	Task	Customer	Secureworks
	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 Incidents as applicable, using Customer's escalation procedures	C, I	R, A
	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

Managed IDS/IPS			
Activity	Task	Customer	Secureworks
<b>Initial Policy Tuning</b>	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
	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
<b>Change Management</b>	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 the Customer-designated maintenance interval	C, I	R, A
	Perform validation on completed changes to	R, A	C



Managed IDS/IPS			
Activity	Task	Customer	Secureworks
	Devices in Customer's environment		
	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
	Investigate Customer-reported issue(s) with changes made, and revert to previous state if Secureworks-implemented changes caused issue(s)	A, C	R
	Conduct ad-hoc changes and troubleshooting that is out of scope for the Service	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 execute RMA activities <b>Note:</b> 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

Managed IDS/IPS			
Activity	Task	Customer	Secureworks
	Install RMA replacement Device(s) for Secureworks remote access	R, A	C, I
	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 to 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
	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 <b>Note:</b> 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
	Ensure Secureworks has current contact information for authorized contacts regarding Customer's account	R, A	I
<b>General</b>	Provide Secureworks with advance notice of Customer-authorized scans or Customer network maintenance periods (to avoid unnecessary Secureworks escalations)	R, A	I

Managed IDS/IPS			
Activity	Task	Customer	Secureworks
	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
	Maintain valid vendor support contracts for all managed Devices	R, A	I

### 2.3.6 Secureworks Platform Maintenance

To ensure Customer receives the highest level of Service possible, Secureworks will conduct platform maintenance (updates, upgrades, patching, and other platform-specific work) on a periodic basis, as maintenance changes are validated and approved for release into the Secureworks platform. Secureworks follows internal change control processes to ensure platform stability. Generally, maintenance does not require a network outage. Secureworks will conduct platform maintenance without Customer approval or use a maintenance interval when a network outage is not required. Customer acknowledges and agrees that approval or a maintenance interval is only mandatory when a network outage is required.

## 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 with regard to 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 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 described in the subsection(s) below are examples of services and activities that are out of scope. Upon request, Secureworks can 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 Statement of Work ("SOW") as applicable.*
- Human 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 custom reports
- Forensics
- Vendor API Integration
- Development of customized signatures

---

## 3 Feature Support for Managed Devices

Listed 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 IDS/IPS Device that is being managed by Secureworks. 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.

### 3.2 User Control

The Service enables control and monitoring of user activity in Customer's network. To perform user control, Customer must use Microsoft Active Directory using the LDAP protocol. The system obtains the users and groups that can be used in access control rules from Active Directory, and also ties users to IP addresses with the logins reported by the user agents installed on Active Directory servers. The user agent works in conjunction with the managed IDS/IPS device to gather user data. The user agent is also essential to implementing user access control.

Secureworks will implement the configuration on the management console to enable User Control. Secureworks will also provide appropriate instructions to Customer to configure user agents on Microsoft Active Directory servers. Upon Customer's request, Secureworks can control or monitor appropriate user



activity in the Customer network. The Service does not include installation or continued management or monitoring of user agents installed on non-Secureworks managed Devices.

---

## 4 Service Fees and Related Information

Service Fees are based on the number of 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 billing for the full service fee will commence.

---

## 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.

- **Managed Security Services**
  - **High Availability:** If the vendor of the Device(s) supports High Availability ("HA"), then Secureworks can manage an HA solution for Customer. Customer will design and implement the HA solution in its environment, and then work with Secureworks to ensure proper connectivity for Secureworks to manage the Devices that are part of the HA solution. This SD is applicable to both Devices that are part of the HA solution.
  - **Global Threat Intelligence ("TI"):** Secureworks will make available to Customer through the Secureworks Client Portal a collection of threat intelligence (i.e., reports, data feeds, and related content and information about any technique or software used to exploit vulnerabilities) that will help Customer to understand the threat landscape, protect against cyber threats and vulnerabilities, and mitigate risk in its environment. The TI provides Customer with analysis of emerging threats and vulnerabilities, and deliver early warnings and actionable global TI. A monthly TI webinar that Secureworks hosts will be available to Customer.
  - **CTU Countermeasures:** CTU countermeasures are derived from thorough analysis of malware samples and vulnerabilities. Deploying CTU countermeasures on the IDS/IPS improves the effectiveness of Customer's IDS/IPS to alert or block communications to known command and control centers. Secureworks can install and configure CTU countermeasures, and initiate additional signature updates to address critical vulnerabilities as and when required.
  - **AttackerDB:** AttackerDB contains lists of malicious internet protocol ("IP") addresses and domains identified by Secureworks. Secureworks correlates attacks (any malicious attempts to subvert, gain control, or otherwise cause damage to Customer's environment or equipment) across monitored security devices daily. These attacks are processed into an AttackerDB. A subset of the highest-fidelity indicators will be applied to the managed Devices (as applicable/allowable by the Device).

- **Professional Services**

- **Incident Management Retainer (“IMR”)**: Secureworks will provide Customer with emergency and/or proactive incident response services such as incident response readiness, planning, workshops, and related services; digital forensic analysis; and targeted threat hunting.

## 6 Service Level Agreements (“SLAs”)

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

SLA	Definition	Credit
Service Request	<p>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, mobile app) within one (1) hour from the creation time stamp on the ticket.</p> <p>Customer must contact SOC through telephone or the Chat in the Portal for immediate engagement with urgent service request tickets.</p>	1/30 <sup>th</sup> of monthly fee for Service for each calendar day the service request was not acknowledged within the specified timeframe
Security Monitoring ( <i>Security Incident analysis</i> )	<p>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.</p> <p>Security Incidents generated from long-term correlation logic and retroactive analyses based on newly identified threat indicators are not subject to this SLA.</p> <p>Event(s) deemed low severity may be sent to Customer for review, and will be available through the Portal for reporting.</p>	1/30 <sup>th</sup> of monthly fee for Service for the affected Device
Availability	<p>Communications availability to the Internet and Customer access to the Portal shall equal no less than 99.9% of the time during any calendar month.</p> <p>“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.</p> <p>“Customer access to the Portal” is defined as the ability of the Secureworks monitoring service to successfully log in to the Portal.</p> <p>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.</p>	1/30 <sup>th</sup> of monthly fee for Service each day in which the Service fails to meet this SLA

SLA	Definition	Credit
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.	1/30 <sup>th</sup> 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

**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.

## 8 Glossary

Term	Description
Counter Threat Appliance (“ <b>CTA</b> ”)	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 (“ <b>CTP</b> ”)	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.
Counter Threat Unit (“ <b>CTU</b> ”)	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.
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 (“ <b>EOL</b> ”)	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 (“ <b>EOS</b> ”)	The date on which a product is no longer available for purchase.
Event Flow Disruption (“ <b>EFD</b> ”)	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 (“ <b>GA</b> ”)	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

Term	Description
	version) that are discovered while conducting due diligence for the Service.
In-Band	Activity within a defined telecommunications frequency band.
Multi-Purpose Logic Engine ("MPLE")	Secureworks proprietary tool that uses specific rules to identify, in real time, patterns that may indicate malicious activity.
Private Virtual Environment	Customer's on-premises virtual infrastructure.
Public Cloud Environment	Third-party virtual infrastructure that hosts the Customer's network and security devices.
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.
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.
<b>Definitions for Virtual Environments</b>	
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 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.