Secureworks®

SERVICE DESCRIPTION

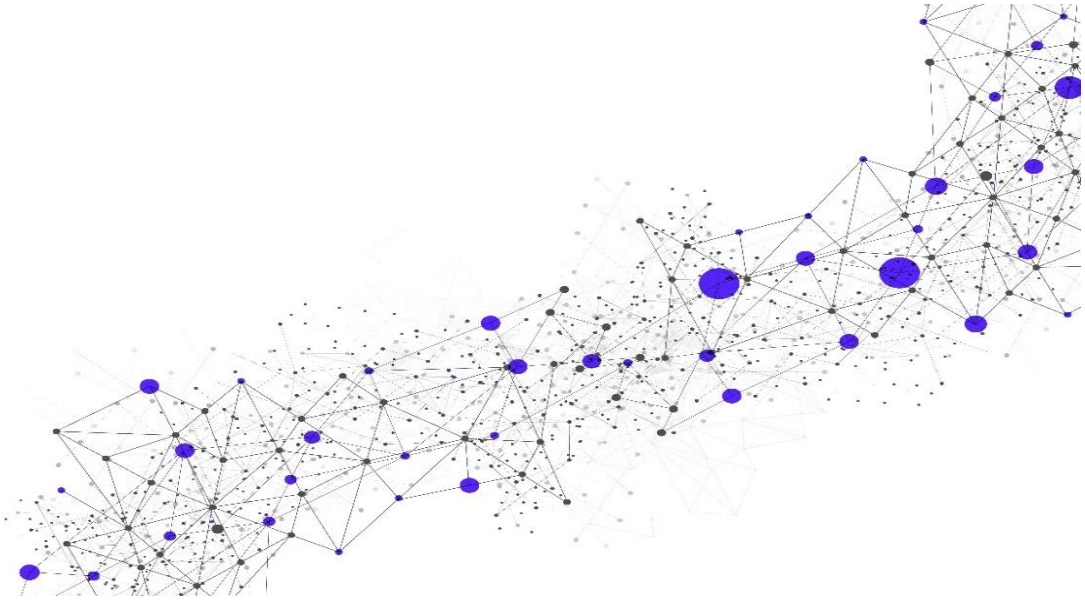
Detect and Prevent Package

Release Date

June 11, 2021

Version

9.1



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 Detect and Prevent Package 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 bundled Service that contains both management and monitoring as described below and in the Overview.

- **Management:** Secureworks performs Device management functions for ***Secureworks-provided Devices only*** (i.e., the Counter Threat Appliance ("**CTA**") and iSensor™), 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).
- **Monitoring:** Secureworks receives logs from the Devices specified in Customer's Service Order ("**SO**") and performs only monitoring and alerting of Security Events (for events generated from one or more of Customer's specified Devices), and monitoring and alerting for event flow disruption (see Sections 2.2.2 and 2.2.3 for details).

1.1 Overview

Secureworks will monitor multiple types of Customer's Devices that are specified in the Service Order ("**SO**") and provide Customer with Security Event analysis. Secureworks will monitor the Devices to detect signs of advanced threats and threat actors, search for specific indicators of compromise, maintain updated threat intelligence ("**TI**"), analyze telemetry, and send alerts to Customer with recommendations on how to proceed should threat activity be detected.

The Service is comprised of multiple Secureworks services to provide Customer with advanced malware protection and detection, advanced analytics, and event monitoring and alerting for multiple types of Devices. Further, the Service enables detection of threats and threat actor activity that some technologies (e.g., common anti-virus software) are unable to detect, allows for maintaining/storing key forensic data necessary to make threat detection and response faster and more efficient, and reduces effort required to investigate and respond to threats.

The Service includes the following components:

- iSensor – Customer installs iSensor on Devices for security event monitoring and alerting
  *(see the **iSensor SD** in addition to the information provided herein)*
- Security Event Monitoring with Advanced Analytics – Customer installs CTA(s) and/or Red Cloak™ Agents on Customer's Devices or in Customer's environments for Secureworks to conduct security event monitoring and alerting
  *(see the **Security Event Monitoring with Advanced Analytics SD** and the **AETD or AETD Elite with Red Cloak SD** in addition to the information provided herein)*
- Event Flow Monitoring and Alerting – Secureworks monitors event flow to ensure logs/events are being received from Customer's Devices for security event monitoring and alerting
- Return Materials Authorization ("**RMA**") Assistance (***for Secureworks-provided Devices only***) – Device replacement for Devices that Secureworks manages

The Service includes a subscription for one (1) physical CTA or one (1) virtual CTA to facilitate data collection and transfer from monitored Devices to the Secureworks Counter Threat Platform™ ("**CTP**"). The Service also includes provisioning of Snare agents for log collection from Windows servers.

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: Responsibilities for Devices (Customer and Secureworks), 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.

1.1.1 Quantities for Security Event Monitoring

Customer selects an appropriate package size for the Service, which includes onboarding for a specified number of Devices, and Secureworks monitors the Devices to detect and prevent threats and threat actor activity. Listed in the table below are the allowable quantities of devices and security devices for each package size. For purposes of defining the package sizes, security devices are defined as firewalls, next-generation firewalls, and IDS and IPS systems; server and network infrastructure devices comprise the remaining devices that are included in the value located in the "Total Allowable Device Quantity" column.

Detect and Prevent Package Size	Total Allowable Device Quantity	Allowable Security Device Quantity
Small	10	3
Medium	20	5
Large	50	10
Extra Large	100	20

To further clarify with an example, the Small package includes monitoring of 10 total devices, and three (3) of these can be security devices.

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 Maintenance of Monitored Device(s)

Customer will maintain the Device(s) being monitored and any intermediate systems that convey monitoring data. If a Device(s) fails or is misconfigured, then Customer will be responsible for executing the actions necessary to replace or reconfigure the Device(s) and return it to a state in which Secureworks can continue to monitor the Device(s). SLAs will not apply to the Device(s) while it is inoperative.

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 Service Order(s), 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 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.
- 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 windows will allow adequate time for Secureworks to perform the Service(s).
- 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 SO 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 SO, 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 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 SO 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 SO may be required, which may include changes to scope and fees, and (ii) without such an amended or additional SO, Secureworks may only be able to provide services as scoped, defined, and charged per the original SO. In some cases, an amended or additional SO may be required to provide services in the original SO. 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 SO. 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 cost of shipping) 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 SO (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 window 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 SO (or on-site meeting for Customers in Japan, if needed) *(**Note:** Receipt of a Customer-executed SO 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 a 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. Some components of the Service are governed and defined by other Secureworks SDs as indicated below. In case of conflict, this SD supersedes the SDs indicated below.

2.2.1 iSensor

Secureworks will manage Customer's iSensor Device(s) on an ongoing basis. Customer will lease or purchase this Device(s) from Secureworks and install it in Customer's environment to enable delivery of the Service.

Secureworks will work with Customer to ensure proper connectivity of the Devices, and will monitor the Devices on an ongoing basis to detect and prevent threats and threat actor activity. The Devices send logs to the 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.

See the **iSensor SD** for more information.

2.2.2 Security Event Monitoring with Advanced Analytics

Secureworks will monitor Customer's Device(s) as specified in Customer's SO on an ongoing basis. Secureworks can also provide Customer with advanced analytics (advanced security event analysis and response capabilities) through use of Red Cloak if Customer installs Red Cloak Agents on one or more servers that are specified in Customer's SO.

The Devices will be monitored to detect and prevent threats and threat actor activity. Log data (events) from the Devices will be processed through the CTP, which enables detection of threats and threat actor activity that some technologies (e.g., common anti-virus software) are unable to detect.

In addition, Customer will have access to Red Cloak Analytics as part of this Service. Customer can install the Red Cloak Agent on servers that are in scope for this Service. The Red Cloak Agent collects relevant events, and sends them to Red Cloak Analytics and to CTP for analysis to detect threats and threat actor activity. Customer will procure the appropriate number of licenses for Red Cloak Agents from Secureworks.

See the **Security Event Monitoring with Advanced Analytics SD** for more information about security event monitoring with advanced analytics. See the **AETD or AETD Elite with Red Cloak SD** for more information about the Red Cloak Agent, advanced analytics, and Incident Investigations. (***Note:*** The AETD Elite information that is in the Appendix of the **AETD or AETD**

Elite with Red Cloak SD is not applicable to the Security Event Monitoring with Advanced Analytics service.)

2.2.3 Event Flow Monitoring and Alerting

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 EFD tickets:

- Secureworks will attempt to restore event flow if the root cause is determined to be related to the Service. Secureworks will work with the third-party vendor to address backend connectivity log forwarding as related to the Service.
- If the root cause of the EFD is not related to the Service (e.g., a Customer-side network change or Agent misconfiguration), then Secureworks will advise Customer to troubleshoot issues directly with the vendor, or Customer will need to troubleshoot and resolve the event flow issue. Secureworks shall not be responsible for troubleshooting issues that do not directly relate to the Service, or Secureworks networks and environments.

2.2.4 Return Materials Authorization ("RMA") Assistance

If a Device that Secureworks is managing for Customer (i.e., the CTA and iSensor) is determined to be in a failed or faulty state and requires replacement, then Secureworks will initiate and fulfill the RMA process. Customer is responsible for maintaining a valid support contract and licensing for the Device.

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 inquires 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 Client-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 responsibility assignment matrix below 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. Some components of the Service are governed and defined by other Secureworks SDs as indicated in Section 2.2, Service Components. In case of conflict, the RACI below supercedes the RACIs in the other SDs.

Secureworks uses 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.

Detect and Prevent Service			
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, public cloud access, or other modifications	R, A	I

Detect and Prevent Service			
Activity	**Task**	**Customer**	**Secureworks**
	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 ***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	Conduct daily monitoring activities to include review, triage, and forwarding of Customer-	I	R, A

Detect and Prevent Service			
Activity	**Task**	**Customer**	**Secureworks**
Monitoring	related validated alerts/Security Events/Security Incidents for next steps		
	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
Support	Conduct troubleshooting related to the Service to determine root cause of an issue	C, I	R, A
	Conduct ad-hoc changes and troubleshooting	R, A	I

Detect and Prevent Service			
Activity	**Task**	**Customer**	**Secureworks**
	that is out of scope for the Service		
	Work directly with vendor for replacement of Device(s) not provided by Secureworks as needed	R, A	C, I
	Initiate RMA process for Secureworks-provided Device(s) 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
	Notify Secureworks after RMA Device is installed and connected to Customer's network	R, A	I
	Provide support to Customer for issues relating to the Portal (including mobile access)	C, I	R, A
	Send electronic notification (e.g., auto-E-mail or auto-SMS) to Customer about Secureworks-identified event flow issues ***Note:*** Auto-SMS is out of scope in Japan.	I	R, A
	Ensure Secureworks has current contact information for authorized contacts regarding Customer's account	R, A	I
General	Provide Secureworks with advance notice of Customer-authorized scans or Customer network maintenance periods (to avoid unnecessary Secureworks escalations resulting from these activities)	R, A	I
	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	R, A	C, I

Detect and Prevent Service			
Activity	**Task**	**Customer**	**Secureworks**
	(e.g., NAT pools, proxies, and load balancers)		
	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
	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 a maintenance window when a network outage is not required. Customer acknowledges and agrees that approval or a maintenance window 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 regarding 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 the 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 listed 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 SO or SOW.

- Incident management services
- On-site installation and provisioning of device

- Analysis of events deemed Low severity (see the "Security Event Monitoring and Alerting" section in the **Security Event Monitoring with Advanced Analytics SD** for information about ticket severities for security events)
- Integration of complementary products that are not managed by Secureworks (e.g., anti-virus software, web reporting software)
- Custom analysis
- Custom reports
- Forensics
- Health monitoring beyond EFD as described in this SD
- Any activity associated with direct management of any monitored device (e.g., upgrades, configurations, network solution design)

3 Service Fees and Related Information

Service Fees are based on package size that Customer selects. See Customer's MSA or CRA (as applicable), and SO or SOW (as applicable) for details, including the following:

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

3.1 Invoice Commencement and Related Information

Invoicing will commence upon installation of the CTA. Customer agrees to pay the full value as specified and agreed per the SO and in the agreed installments. Customer may onboard devices for the service, up to the device quantity limits as specified by device type on the SO and in the table in Section 1.1.1, Quantities for Security Event Monitoring.

4 Service Level Agreements ("SLAs")

The table below contains the SLAs that are applicable to the Service. Some components of the Service are governed and defined by other Secureworks SDs. The SLAs in this SD supersede the SLAs in the other SDs that are identified in Section 2.2, Service Components.

SLA	Description	Credit
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.	1/60th of monthly fee for Service for the affected Device

SLA	Description	Credit
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, 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.	1/30th of monthly fee for Service for each calendar day the service request was not acknowledged within the specified timeframe
Availability	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. "Communications availability" is defined as the ability of a Secureworks SOC to send and receive TCP/IP packets between the CTP and its upstream Internet service provider. Customer access to the Portal and Red Cloak Portal" is defined as the ability of the Secureworks monitoring service to successfully log in to these portals. 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.	1/60th of monthly fee for Service
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

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.

5 Additional Considerations and Information

5.1 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.

6 Glossary

Term	Description
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 CTP system, which are then correlated and analyzed to protect Customer's organization 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.

Term	Description
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 Service Order 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.
Endpoint	An Internet-capable computing machine or end unit such as a desktop computer, laptop, smart phone, tablet, thin client, or another similar device.
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.
Identified Changes	Differences (e.g., Device quantity, make, model, software package, or software 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 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.
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

Term	Description
	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.