Secureworks®

SERVICE DESCRIPTION

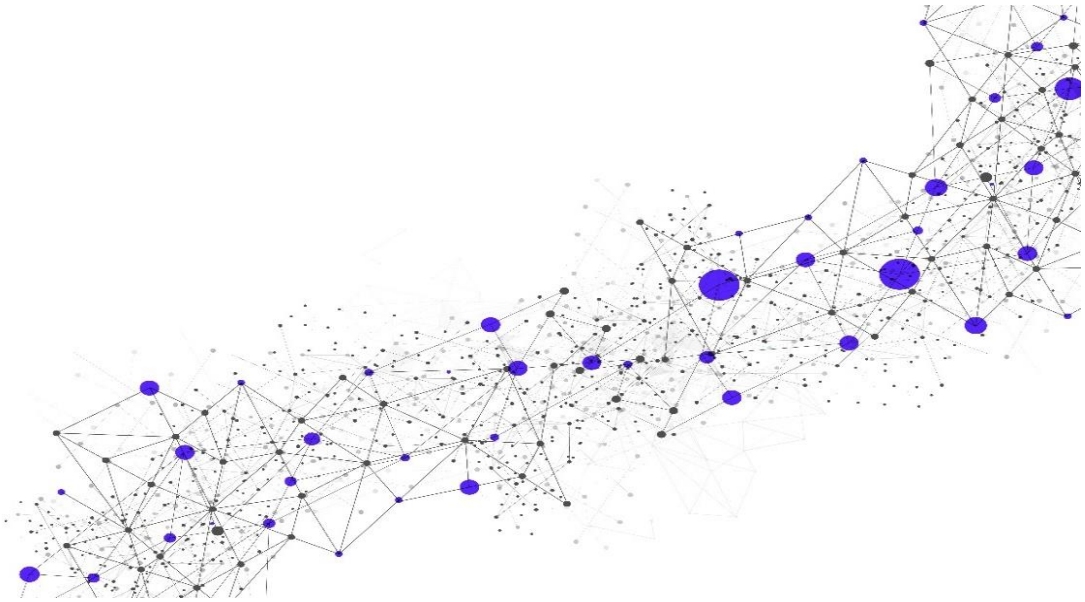
Advanced Endpoint Threat Prevention with Carbon Black Defense

Release Date

June 11, 2021

Version

15.1



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 Advanced Endpoint Threat Prevention with Carbon Black Defense 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 the following:

- Event stream management functions, which can include changes– e.g., Multi-Purpose Logic Engine ("**MPLE**") tuning, Red Cloak™ watchlist and suppression rule modifications), and rule/policy modifications
- Monitoring and alerting to detect event data (log) flow issues for the Service
- Managing the Secureworks Red Cloak hosted infrastructure for analyzing Endpoint telemetry

1.1 Overview

Secureworks will configure, manage, and maintain the cloud-based Advanced Endpoint Threat Prevention ("**AETP**") Carbon Black ("**CB**") Defense Management Console (also referred to as "**Management Console**" or "**Device**" in this SD) that is licensed to Customer. Customer can procure the CB Defense license from Secureworks or from a third party. The license provides access to, and use of, both the Management Console and the Endpoint Sensor Software. Customer will install the Endpoint Sensor Software on the in-scope Endpoints that will be monitored for threats. Customer will be able to access the Management Console to view Endpoint telemetry.

Secureworks will monitor the Management Console, and monitor the Endpoints operating on systems that are compatible with the Endpoint Sensor Software 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 Management Console receives events from Endpoint Sensor Software that is installed on Endpoints, and the events are processed by the AETP system that is integrated with the Management Console. In addition, Endpoint telemetry will be forwarded from the Management Console to Red Cloak for further processing and analytics. This Service enables detection of threats and threat actor activity that some technologies (e.g., common anti-virus software) are unable to detect. Customer will be provided with access to the Red Cloak Portal for additional information and analytics. Section 2.2.1, Security Event Monitoring and Alerting, contains more information about how events are processed.

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

The Service includes the following components:

- Security Event Monitoring and Alerting
- Event Flow Monitoring and Alerting
- AETP Management Activities
- CB Defense Management Console Activities

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.

1.2 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 AETP Application ("CB Defense Management Console")

Customer will do the following for the Management Console:

- Provide a list of authorized users who will be given administrative access to the CB Defense Management Console; list will be provided at the beginning of the implementation process; after these authorized users have access, they can manage and maintain all user accounts (e.g., create more administrative accounts, manage permissions and access for all users) or submit service requests through the Secureworks Client Portal to have Secureworks add user accounts or make changes
- Procure required software that meets Carbon Black's published minimum requirements
- Install and manage the optional anti-virus ("**AV**") signature server
- Perform periodic tuning of the AETP software that resides on the AETP Application per guidance from Secureworks

1.2.2 Endpoint Sensor Software

Customer will do the following:

- Ensure all operating systems ("**OSs**") used with the Endpoint Sensor Software are supported by Carbon Black; a list of supported OSs is located in the Carbon Black Community: https://community.carbonblack.com
- Ensure all Endpoint Sensor Software versions used are currently supported by Carbon Black; a list of supported versions is located in the Carbon Black Community: https://community.carbonblack.com
- Ensure Endpoints have sufficient available resources for installation and operation of the Endpoint Sensor Software as defined by Carbon Black's operating environment requirements
- Install the Endpoint Sensor Software on each Endpoint, and only on Endpoints owned by Customer as Secureworks will deliver the Service only to such Endpoints
- Update/upgrade Endpoint Sensor Software as needed; use a process to deploy updates/upgrades first in a test environment, and assess any impact before deploying updates to production Endpoints and environments
- Manage and troubleshoot the Endpoint Sensor Software that is installed on Endpoints
- Ensure availability of the Endpoint Sensor Software
- Respond to and remediate issues with the Endpoint Sensor Software availability and performance
- Conduct all required ongoing maintenance of the Endpoint Sensor Software
- Reinstall the Endpoint Sensor Software as required

- Remove all Endpoint Sensor Software from all Endpoints and Customer's environment by the contract end or termination date
- Contact SOC to request assistance with Carbon Black host isolation or process disruption (Customer will manage prevention hashes and Endpoint threat prevention policies)

1.2.3 Customer-Provided License

Customer will maintain current AETP licensing, support, and maintenance contracts for the AETP software. Customer will also be responsible for associating Secureworks with Customer's existing Carbon Black support and maintenance contracts to enable Secureworks to work directly with the vendor on Customer's behalf.

1.2.4 Licenses and Support Contract for Carbon Black

Customer can purchase AETP licenses for Carbon Black through Secureworks, and these licenses can be renewed annually. Secureworks will automatically be associated with the support contract to engage with Carbon Black on Customer's behalf. If Customer does not purchase licenses from Secureworks, then Customer will be responsible for maintaining the Carbon Black licenses including the necessary support contract. Customer will also be responsible for associating Secureworks with the support contract if Partner provides the licenses.

1.2.5 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.

1.2.6 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.

1.2.7 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 Secureworks Client Portal.

1.2.8 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 i escalations to Customer.

1.2.9 Usage Overage

If Customer's actual usage exceeds the subscription limit for any services identified in Customer's Service Order(s) ("**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 Subscription Term.

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.

1.2.10 General

Customer will do the following:

- Ensure that Customer personnel are scheduled and available to assist as required for the Service
- Obtain 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
- Provide to Secureworks all required information (key personnel contact information, credentials, and related information) prior to work being started
- Promptly reply to all requests from Secureworks
- Ensure Customer-scheduled downtime and maintenance windows will allow adequate time for Secureworks to perform the Service
- 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)
- Remediate all malware and threat actor activity (unless otherwise contracted with Secureworks under a separate Service Order)
- Implement and maintain password policies for external and internal applications (Secureworks recommends Customer implement and maintain password policies that adhere to Section 5, Authenticator and Verifier Requirements, within NIST Special Publication 800-63B)
- Ensure all Endpoints report into the Management Console at least every 30 days
    - Any Endpoint that has not communicated properly within 30 days will no longer be monitored and will not be included in other analytics or in the total Endpoint count
- Manage file lists for applying process disruption, except when Customer specifically opts-in to global process disruption lists that Secureworks manages
- Before requesting a process ban or disruption, Customer must ensure the process is correctly identified and not required by Customer's business; it is entirely Customer's responsibility to ensure the validity of the request before submitting to Secureworks
- Before requesting host isolation (of an Endpoint), Customer must ensure the Endpoint is correctly identified and the process of isolating that Endpoint will not negatively impact Customer's business; it is entirely Customer's responsibility to ensure the validity of the request before submitting to Secureworks; each request for a ban, disruption, or host isolation must be in an individual ticket in the Secureworks Client Portal
- Monitor Endpoint availability and performance through the Management Console
- Respond to and remediate issues with Endpoint availability and performance
- Ensure the contracted number of Endpoints is not exceeded
    - If the number of Endpoints contracted for is exceeded, the additional charges for the overage of Endpoints will be reflected on the subsequent billing periods remaining for the contract

1.3 Initial Implementation Scheduling and Points of Contact

Secureworks will contact Customer within seven (7) Business Days after execution of the Service Order ("**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), which occurs after the Domain(s) is configured in the Management Console, Customer is configured in the Secureworks Client Portal, and management of the Service 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 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 can be completed within two weeks, not including time required for Customer activities.

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 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 quantities of Endpoints 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 the services in the original SO.
    - Secureworks will provide Customer with one or more forms to be completed. After Customer returns completed form(s), Secureworks will schedule a technical meeting to review the completed form(s) and other relevant information with Customer.
- **Prepare:** Baseline the project schedule and identify required training; Customer provides information necessary to execute implementation for MSS Services
- **Execute:** Complete configuration of service-enabling technology, validate ingestion of identified log source(s), schedule and deliver foundational training, and activate services

- **Rationalize:** Confirm Customer's ability to access and participate in management of the Service within the Secureworks Client Portal and Management Console; 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 and Activation

Service provisioning consists of the initial actions that are completed in advance of implementing the Service for Customer. **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.

Secureworks will provide software packages to support Customer deployment and installation in accordance with Customer's change management procedures. Support is available during Business Hours (see Section 2.3.2).

Secureworks performs the following provisioning and activation activities:

- Create implementation ticket in Secureworks Client 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.)*
- Create Domain(s) for Customer in Management Console
- Provide Customer with access to the Secureworks Client Portal, Red Cloak Portal, and the Management Console
- Collect Customer information that is necessary for implementation
- Complete provisioning activities (e.g., configuration, and verification of network connectivity and event flow from Customer's Endpoint to the Management Console)
- 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

2.2 Service Components

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

2.2.1 Security Event Monitoring and Alerting

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

- Secureworks Threat Intelligence ("**TI**")
- Machine learning

- Signature-based detections
- Human-based pattern identification – through ongoing research 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 Secureworks Counter Threat Platform ("**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. Secureworks does not guarantee that Customer-created alerts will generate events that appear in the Secureworks Client Portal. 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.

2.2.1.1 Security Incident Identification Methods

CB Defense uses a combination of Secureworks and third party-derived threat intelligence, pattern-based detection, big data analytics, file and process artifact analysis, and threat actor behavior modeling to identify malicious activity on Endpoints. Secureworks will use two methods to identify and act upon Security Incidents, as explained in the table below.

Identification	Description
Real-Time Security Incidents	CB Defense collects and processes Endpoint telemetry in near real-time seeking indicators of compromise. If malicious activity is identified, the alert is sent to the Secureworks proprietary Multi-Purpose Logic Engine ("**MPLE**") for additional processing and creation of Security Incident tickets if applicable. Events that are forwarded from CB Defense to CTP 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).
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.

2.2.1.2 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 Secureworks Client 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*	CB Defense Security Events that require immediate attention and/or represent a significant threat to a Customer asset – e.g., host infection(s); successful exploitations; and other known Tactics, Techniques, and Procedures ("**TTPs**") used by threat actors
Medium	CB Defense Security Events that do not require immediate attention and do not represent a significant threat to a Customer asset – e.g., the CB Collective Defense Cloud process-based alerts, which is an aggregation of known malicious activity
Low	CB Defense Security Events that have little to no impact to a Customer asset or have been determined to be a false positive – e.g., instant messaging usage, adware, spyware, remote access software such as TeamViewer; usual recommended action is for Customer to tune security policies if applicable

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

2.2.1.3 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 Secureworks Client 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 Secureworks 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 SO or Statement of work ("**SOW**").

2.2.1.4 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 Secureworks Client Portal.

2.2.1.5 Incident Investigations with Red Cloak

For Security Incident tickets, Secureworks performs Incident Investigation activities for Endpoint telemetry that is processed through Red Cloak Analytics and is defined as a critical threat. A threat must meet the following conditions to be considered critical: Detection of targeted malware, a threat actor operating within a Customer's environment, or the observation of tactics, techniques, and procedures associated with known threat actors. Secureworks will investigate these Security Incidents to provide Customer with the following information:

- Corroborating event data that correlates with the original event and is related to the affected asset
- Additional contextual information related to the threat
- Other assets in Customer’s environment that were overtly interacted with by the threat actor
- Relevant CTU or third-party TI
- Impact of the threat on the affected asset
- Recommended next actions

An investigation is only performed for a Security Incident ticket that is automatically generated based on Secureworks TI and is defined as a critical threat. There is no limit (unmetered) on the number of investigations that will be conducted for these tickets. Details of each additional Incident Investigation are provided to Customer through the existing ticket in the Secureworks Client Portal within 24 hours of automatic ticket generation.

2.2.1.6 Security Event Reporting

Customer can use the Secureworks Client 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.

2.2.2 Event Flow Monitoring and Alerting

Secureworks will use Event Flow Disruption (“**EFD**”) to detect data flow issues for the Service (e.g., connection between Management Console and associated storage resource or collection of telemetry fed into the hosted CTA, not data flow issues with individual Endpoints) 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 Secureworks Client 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 Partner 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 issue), then Secureworks will advise Customer to troubleshoot issues directly with Partner, 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.

2.2.3 AETP Management Activities

Secureworks will perform the following management activities:

- Provide guidance on how to access the Service and product documentation
- Provide Endpoint Sensor Software to be downloaded by Customer
- Assist Customer with troubleshooting issues related to Endpoint Sensor Software
- Apply TI that is produced by the Secureworks Counter Threat Unit™ ("**CTU**") and Secureworks-selected third-party vendor intelligence resources to the telemetry feed that is sent by CB Defense
- Monitor availability of telemetry feed from CB Defense
- When requested by Customer, provide authorized users with access to the portals
- Display valid Security Events to Customer in the portals
- Leverage technology and a team of security analysts to analyze Endpoint Sensor Software output (Security Events) forwarded to the CTP, determine whether an escalation is required and, if so, convert Security Events to Security Incidents and escalate per Customer's established escalation procedures
- Collect Endpoint telemetry in CTP for potential use with other services that Secureworks may be providing for Customer
- For threats classified by Secureworks as medium or low severity, provide alert and automated context information to Customer with available CTU™ TI Data
- For threats classified by Secureworks as high severity, provide alert and automated context information to Customer with available CTU TI Data and conduct an Incident Investigation as described in Section 2.2.1.5, Incident Investigations with Red Cloak
- Provide guidance to Customer on how to quarantine or isolate an Endpoint
- Provide guidance to Customer on how to blacklist an application
- Schedule and host initial tuning orientation meeting with Customer and provide guidance on how to perform ongoing Endpoint Sensor Software tuning

2.2.4 CB Defense Management Console Activities

Secureworks provides Customer with access to the Management Console to access additional capabilities that are not available through the Secureworks Client Portal. The Management Console may only be accessed by Secureworks and personnel authorized by the Customer. All information received by Customer through the Management Console is solely for Customer's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's organization.

Secureworks will monitor events from the Management Console and act as explained in Section 2.2.1.

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 Secureworks Client 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, the Red Cloak 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. Below are explanations of these items.

2.3.4.1 Secureworks Client Portal

The Secureworks Client 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, Secureworks Client Portal-specific features, and related content)

Access to the Secureworks Client 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 Secureworks Client 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 Secureworks Client Portal remains current.

All information received by Customer through the Secureworks Client 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 Red Cloak Portal

The Red Cloak Portal, which contains information about Customer's Endpoint, is the online site for customers with AETD Red Cloak and AETP CB Defense, and provides the following:

- Visibility into AETD Red Cloak functionality and Endpoint-specific information, including events, watchlist results, and other alerts
- Ability to search through retained telemetry from Customer's Endpoints, or visualize the telemetry from CB Defense through custom dashboard widgets
- Ability to create an investigation to organize events related to an incident or attacker activity patterns
- Access to the Secureworks Learning Center (training and self-education – webinars, documentation, SDs, Red Cloak-specific features, and related content)

2.3.5 Customer and Secureworks Responsibilities

The following responsibility assignment matrix describes the participation required of 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.

AETP CB Defense			
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 Secureworks Client Portal, Red Cloak Portal, and Management Console (Customer will modify as needed at any time through the Secureworks Client Portal, and add / remove users as needed)	R, A	I

AETP CB Defense			
Activity	**Task**	**Customer**	**Secureworks**
	Create and provide to Secureworks the escalation procedures to follow for tickets (Customer will modify as needed at any time through the Secureworks Client Portal)	R, A	I
	Enter Customer's initial escalation procedures into Secureworks Client 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
	Verify that the Endpoint or environment in which the Endpoint Sensor Software is being installed meets the specifications of the vendor for the Endpoint Sensor Software prior to the start of implementation	R, A	C, I
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
	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 connectivity of Endpoints to designated IP ranges and ports of the CB Defense cloud	R, A	I
	Configure Endpoints (e.g., hosts, laptops) for Security Event logging	I	R, A
	Test Endpoint Sensor Software before deployment	R, A	C

AETP CB Defense			
Activity	**Task**	**Customer**	**Secureworks**
	Deploy Endpoint Sensor Software	R, A	I
	Conduct Customer orientation call and provide minimal assistance with initial sensor tuning	C, I	R, A
	Configure Secureworks Client Portal and Management Console access for Customer's authorized users	I	R, A
	Provide training (remotely) to Customer for Secureworks Client Portal	I	R, A
	Provide Customer-side post-install validation steps to Customer	I	R, A
	Complete Customer-side post-install validation steps	R, A	I
	Complete Secureworks-side post-install validation steps	I	R, A
Security Monitoring	Conduct daily monitoring activities to include review, triage, and forwarding of Customer-related validated alerts/Security Events/Security Incidents for next steps	I	R, A
	Conduct incident response activities for alerts, Security Events or Security Incidents identified by Secureworks	R, A	I
	Monitor Service-specific logs and create Security Events or Security Incidents for security concerns	C, I	R, A
	Conduct real-time analysis of Security Events that are created (manually create Security Incident tickets if needed); escalate Security 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 Secureworks Client 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

AETP CB Defense			
Activity	**Task**	**Customer**	**Secureworks**
	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 Secureworks Client 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 Secureworks Client 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
Change Management	Investigate and confirm validity and potential business impacts of changes (i.e., conduct due diligence) prior to submitting any change request in Secureworks Client Portal for implementation, such as changes to AETP policies, process disruption, hash banning, or host isolation	R, A	I
	Submit through Secureworks Client Portal (or otherwise contact SOC to submit) all in-scope change requests; 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 window 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 window	C, I	R, A
	Perform validation on completed changes to Devices in Customer's environment	R, A	C

AETP CB Defense			
Activity	**Task**	**Customer**	**Secureworks**
	Notify Customer (through Secureworks Client 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 Secureworks Client 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
	Submit ticket through Secureworks Client Portal or otherwise engage SOC for any unplanned changes	R, A	I
	Conduct ad-hoc changes and troubleshooting that is out of scope for the Service	R, A	I
Support	Investigate Secureworks-identified health-related issues (e.g., a system event such as a memory threshold being exceeded) on Endpoints	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 Endpoints	I	R, A
	Conduct software upgrades and configuration changes that are in scope for the Service (software must be Secureworks supported)	C, I	R, A
	Provide on-site personnel to assist Secureworks while conducting any activity that must be physically performed on-site	R, A	C, I

AETP CB Defense			
Activity	**Task**	**Customer**	**Secureworks**
	Provide support to Customer for issues relating to the Secureworks Client Portal (including mobile access), Red Cloak Portal, and Management Console	C, I	R, A
	Ensure Secureworks has current contact information for authorized contacts regarding Customer's account	R, A	I
	Create and maintain scripts for health-specific events to monitor status of Endpoints	I	R, A
	Perform ongoing tuning of Endpoint Sensor Software	R, A	C
General	Submit through Secureworks Client Portal (or otherwise contact SOC to submit) any tickets for in-scope work	R, A	I
	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 (e.g., NAT pools, proxies, and load balancers)	R, A	C, I
	Notify Secureworks of any changes to network ranges (e.g., public, DMZ, and private) and changes to network translation devices (e.g., NAT pools, proxies, and load balancers)	R, A	C, I
	Conduct policy audits (e.g., firewall, IDS/IPS)	R, A	I
	Conduct Secureworks Best Practices policy audit; work with Customer to identify policies that are a security concern	I	R, A

AETP CB Defense			
Activity	**Task**	**Customer**	**Secureworks**
	Maintain valid vendor support contracts for all managed Devices	R, A	I
	Update Endpoint Sensor Software when notified that updates are available from Endpoint Sensor Software Vendor	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:

- Secureworks Client Portal Training
- Secureworks Client Portal User Roles and Audit
- Escalation Procedures
- MPLE Rules Review
- Ticket Review and Baseline Secureworks Client 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 Secureworks Client Portal. In addition, Training for the Red Cloak Portal will be made available to Customer.

2.5 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.

- Custom reports and customizing AETP-generated reports
- Dedicated incident response services
- On-site installation and provisioning of any device(s)
- Analysis of minor events
- Integration of complementary products that are not managed by Secureworks (e.g., anti-virus software, web reporting software)
- Vendor API Integration
- Remediation of malware and threat actor activity
- Training on the AETP Application / Management Console

3 Service Fees and Related Information

Service Fees are based on the number of Endpoints being monitored through the Management Console. 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

Service commencement will begin once the first Endpoint Sensor Software is deployed and is reporting to the Management Console. It is Customer's responsibility to download the Endpoint Sensor Software and install it on all in-scope Endpoints.

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

4 Recommended Add-on Services

The Secureworks offerings listed below are optional and may be 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**
  - **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 delivers early warnings and actionable global TI. A monthly TI webinar that Secureworks hosts will be available to Customer.
- **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 threat hunting.

5 Service Level Agreements ("SLAs")

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

SLA	Definition	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 Secureworks Client Portal for reporting.	1/30th of monthly fee for Service for the affected Device
Incident Investigations *(AETP and Red Cloak)*	Upon generation of an AETP Security Incident designated by Secureworks as significant, Secureworks will provide an Incident Investigation within twenty-four (24) hours from the timestamp of creation of the Security Incident. Requests for Incident Investigations that Secureworks does not deem significant are performed at the discretion of Secureworks and with no associated SLAs. Some requests may be referred to professional services through a separately signed Statement of Work.	1/30th of monthly fee for Service for the affected Device
Service Request	A service request (applies to all non-change and non-incident tickets) submitted through telephone or the Secureworks Client Portal will be acknowledged through human or electronic notification (e.g., Secureworks Client 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 Secureworks Client Portal, Red Cloak Portal, and CB Defense Management Console shall equal no less than 99.9% of the time during any calendar month. "Communications availability" is defined as the ability of a Secureworks SOC to successfully send and	1/30th of monthly fee for Service each day in which the Service fails to meet this SLA

SLA	Definition	Credit
	receive TCP/IP packets between the CTP and its upstream Internet service provider. "Customer access to the Secureworks Client Portal, Red Cloak Portal, and CB Defense Management Console" is defined as the ability of the Secureworks monitoring service to successfully log in to the Secureworks Client Portal, Red Cloak Portal, and the Management Console. 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.	

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.
- 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.

6 Additional Considerations and Information

6.1 Service Features and Limitations

The table below contains additional information about the Service.

Additional Managed AETP CB Defense Service Features and Limitations	
Data Retention	Secureworks will provide up to thirty (30) days of data in the Management Console.
Non-standard Configurations	Secureworks will not support any non-standard configurations. This includes any configuration that is not a default setting of the Endpoint Sensor Software or a Secureworks-defined and tested configuration. Customer must ensure all connectivity requirements are met, including all web proxies and outbound controls, which includes allowing connectivity to Secureworks-designated IP ranges and ports.
Training Support	Management Console online training is provided free of charge by Carbon Black in conjunction with the CB Defense service.

6.2 CB Defense Endpoint Sensor Software Installation, Management, Maintenance, and Limitation of Liability

1) The installation, ongoing management, and maintenance of Endpoint Sensor Software are the sole responsibility of Customer.
2) Customer can install and perform ongoing management of the Endpoint Sensor Software by utilizing both the CB Defense Management Console and the CB Defense user guide in combination with Customer's software distribution process.
3) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY LOSSES, COSTS, OR DAMAGES RELATING TO THE INSTALLATION OF THE ENDPOINT USER SOFTWARE. SECUREWORKS STRONGLY RECOMMENDS THAT THE CUSTOMER INSTALL AND EVALUATE ENDPOINT SENSOR SOFTWARE IN A TEST ENVIRONMENT AND DEPLOY IT IN SMALL BATCHES IN ACCORDANCE WITH CUSTOMER'S CHANGE MANAGEMENT POLICIES TO ENSURE THERE ARE NO ISSUES BEFORE IMPLEMENTING IT AS TO ITS ENTIRE INFRASTRUCTURE.
4) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY IMPACT THAT MAY BE INCURRED FROM INSTALLING ENDPOINT SENSOR SOFTWARE ON AN UNSUPPORTED OPERATING SYSTEM OR CUSTOM BUILT IMAGE.
5) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY IMPACT FROM CUSTOMER'S FAILURE TO COMPLY WITH THE ENDPOINT SENSOR SOFTWARE UPDATING PROCESS.
6) SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY LOSSES, COSTS, OR DAMAGES RELATING TO THE INSTALLATION OF THE END POINT USER SOFTWARE ON ANY ENDPOINTS NOT OWNED BY CUSTOMER.
7) THE SOFTWARE MAY COME BUNDLED OR OTHERWISE BE DISTRIBUTED WITH OPEN SOURCE OR OTHER THIRD PARTY SOFTWARE, WHICH IS SUBJECT TO THE TERMS AND CONDITIONS OF THE SPECIFIC LICENSE UNDER WHICH IT IS DISTRIBUTED. OPEN SOURCE SOFTWARE IS PROVIDED BY SECUREWORKS "AS IS" WITHOUT ANY WARRANTY, EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. SECUREWORKS SHALL HAVE NO RESPONSIBILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF OPEN SOURCE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. UNDER CERTAIN OPEN SOURCE SOFTWARE LICENSES, YOU ARE ENTITLED

TO OBTAIN THE CORRESPONDING SOURCE FILES. YOU MAY FIND CORRESPONDING SOURCE FILES FOR THE SOFTWARE IN THE CB DEFENSE MANAGEMENT CONSOLE.

6.2.1 Endpoint Count and Contract Alignment

1) It is Customer's responsibility to ensure the contracted amount of Endpoints is not exceeded.

2) If at any time throughout the course of the Agreement, Secureworks determines that Customer's total number of Endpoints exceeds the number of Endpoints contracted for, a change order will be required. The change order will reflect both the change in number of Endpoints, and the corresponding increase in charges. Customer hereby agrees to a change order and pays for any corresponding increase in charges (when applicable).

6.2.2 Contract Termination and Endpoint Sensor Software Removal

Secureworks will decommission all Customer domain(s) immediately upon the termination date or end date of the Agreement. Once a contract is terminated it is Customer's responsibility to remove all Endpoint Sensor Software from its environment by the termination date. SECUREWORKS WILL NOT BE RESPONSIBLE FOR ANY LOSSES, DAMAGES, OR COSTS RELATING TO CUSTOMER'S FAILURE TO REMOVE ALL ENDPOINT SENSOR SOFTWARE FROM ITS ENVIRONMENT AS OF THE TERMINATION DATE.

6.3 Secureworks Lifecycle Policy and Related Information

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

7 Glossary

Term	Description
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.
CTU TI Data	All data provided to Customers as part of the Secureworks Counter Threat Unit Threat Intelligence Service, including but not limited to, vulnerabilities, advisories, and threat analysis.
Device(s)	Equipment that is in scope for the Service.

Term	Description
Domain	Customer account(s) that is created in the CB Defense Management Console.
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.
Endpoint Sensor Software	Software that is installed on an Endpoint, which sends telemetry to the Endpoint's management application that is enabling the Service to be delivered.
Identified Changes	Differences (e.g., Device quantity, make, model, software package, or software version) that are discovered while conducting due diligence for the Service.
Multi-Purpose Logic Engine ("**MPLE**")	Secureworks proprietary tool that uses specific rules to identify, in real time, patterns that may indicate malicious activity.
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.