Service Description for Cisco Secure Endpoint Professional (Pro)

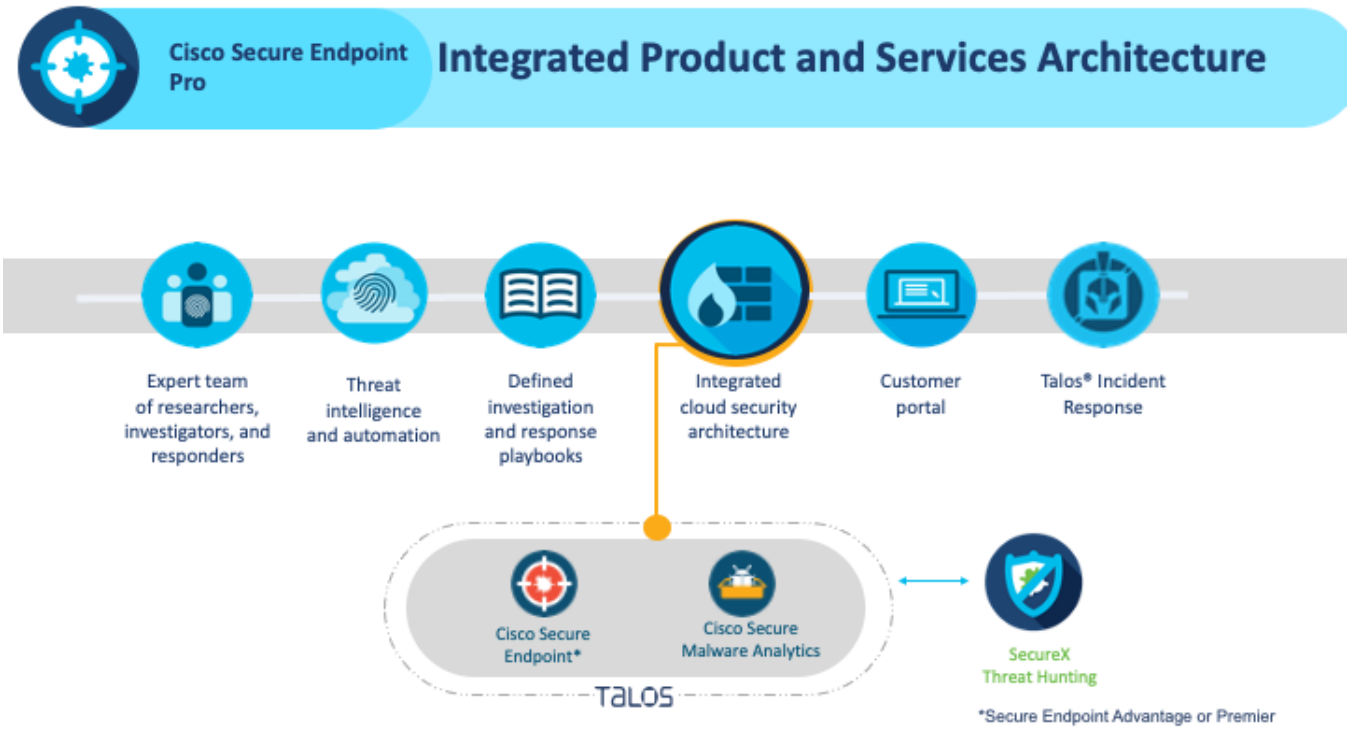
This document (this "**Service Description**") describes the service features, components, and terms of the Cisco Secure Endpoint Pro (the **"Services"**) that Cisco will provide to the designated customer listed in the order **(**"**Customer**"). The specific quantity and type of the Services purchased by Customer (directly or via an Authorized Reseller) will be documented in a service order, quote, or web order that is signed or click accepted, or other means of assent (e.g., issuing a purchase order) ("**Order**") between the parties. This Service Description should be read in conjunction with How Cisco Provides Services located at: How Cisco Provides Services. Appendix A to this Service Description has additional terms and conditions governing the Services.

1. Offer Description

1.1. Offer Overview

the Services provide an integrated Cisco security solution by combining the capabilities of Cisco Secure Endpoint with:

a) the ability to monitor for additional indicators of compromise or alert,
b) a security operations center ("SOC") that monitors for indicators of compromise 24/7, and
c) a team of Cisco researchers, investigators and responders with threat intelligence, and defined investigation and response playbooks supported by Talos threat research. The team's responses may include information, recommendations, or changes based on the type of threat or indication of compromise. the Services are based on the following Cisco technologies:



1.2. Services Features Summary

Service Element	Description	Cisco Secure Endpoint Subscription Type	
		Advantage	Premier
Validated Secure endpoint policy	Cisco Secure Endpoint/AMP configuration in Customer environment is validated and aligned to Cisco recommended Configuration during Customer Activation phase.	✓	✓
24x7x365 Security incident and alert monitoring	Correlation, threat analysis, investigation, and response by an experienced team of researchers, analysts, investigators responders, and customer support, with specialists for various industry verticals and geographies	✓	✓
Automation and orchestrated investigation and response playbooks	Issue detection, investigation, and response action recommendation based on response playbook managed by threat analysts	✓	✓
Integrated Threat intelligence (TALOS and Third-party)	Detect, analyze, investigate, and correlate against our threat intelligence research by leveraging TALOS, allowing faster response to threats before they progress.	✓	✓
Guided response actions to contain, mitigate, remediate, or eradicate a threat	Create a Security Incident ticket, notify, and update Customer of the status of the Security Incident, recommend responses to help contain, mitigate, remediate, or eradicate the threat.	✓	✓
Automation and active response (pro-active mitigation of detected threat)	Pro-actively mitigate, stop, or prevent a detected threats based on the intelligence and advisories, as relevant to the threat and customer's environment.	✓	✓
Quarterly Threat Briefing	Cisco Talos Incident Response will host a remote service review meeting on a quarterly basis open to all Customers (not private). This quarterly briefing will provide updates on current threat patterns, detection volumes, and trending events.	✓	✓
Automated Response Action against Threat Hunting alerts	Pro-actively mitigate, stop, or prevent threats generated from Threat Hunting alerts based on the intelligence and security advisories, as relevant to customer's environment.		✓
Optional integrated Cisco Talos Incident Response Service*	Cisco Talos Incident Response Services provides emergency support and proactive services to assess, strengthen, and evolve a Customer's incident readiness program. A description of those Services can be found here: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/cisco-talos-incident-response-retainer-service.pdf	✓	✓

* Optional Service – subject to additional terms and fees

1.3 **Cisco Secure Endpoint (formerly, Advanced Malware Protection (AMP).** Cisco Secure Endpoint is a cloud-based advanced malware analysis and protection solution that allows Customer to conduct metadata File analysis to detect malware and cyber threats. Cryptographic hashes of files are collected and transmitted to a Cisco-managed cloud server where file reputation analysis is performed, and a disposition is made as to whether the file is good, bad, or unknown. If a disposition is unable to be made after analysis of the hash of a file, then Customer has the option (depending on the license(s) purchased) to submit the file to Cisco Secure Malware Analytics (described in Section 1.4 below) for further sandboxing analysis up to Customer's licensed daily submission limit. After the file analysis is completed, AMP will act on the disposition (e.g., by deleting the File and putting it into quarantine if it is determined to be malicious). The Services are available with Cisco Secure Endpoint Advantage and Premier.

1.4 **Cisco Secure Malware Analytics (formerly, Threat Grid).** Threat Grid is a cloud-based malware analysis and threat intelligence sandbox solution to which Customer can submit malware samples for additional analysis. Threat Grid analyzes each File to record its behavior and determine whether it is malicious. Threat Grid will search and correlate data elements of a single malware sample against millions of samples collected and sourced from around the world to help give Customer a global view of malware attacks and its association.

1.5 **SecureX Threat Hunting.** SecureX Threat Hunting is a proactive analyst-centric approach to detecting hidden advanced threats and is used as a part of the Service's Automated Response Action against Threat Hunting alerts and is offered exclusively as part of the new Premier license tier for Secure Endpoint. It helps tell the incident responders a narrative of how an attack was spotted or how it evolved and suggests what to do next in terms of response. The purpose is to discover and thwart attacks before they cause any damage. SecureX Threat Hunting leverages the expertise of both Talos and the Cisco Research and Efficacy Team to help identify threats found within the customer environment. Cisco delivers highly automated human-driven hunts based on playbooks producing high-fidelity alerts. The process uniquely combines the Orbital Advanced Search technology with expertise from elite threat hunters, with extensive industry experience, to proactively find more sophisticated threats. (Note: The Secure Endpoint Premier license is available to order globally in all regions. However, the SecureX Threat Hunting infrastructure that processes the customer telemetry and executes hunts is currently available only in North America.)

1.6 **Covered Endpoints.** The Services are dependent on Customer having specific cloud services, endpoint software and configuring these items as defined in documentation provided by Cisco ("**Covered Endpoints**"). Customer is also required to obtain and maintain all applicable Cisco support and maintenance agreements and any required infrastructure (i.e. compatible device types) to support typical Customer needs. The charges and the Services do not include the Covered Endpoints, their support, maintenance, implementation, or configuration, and these must be purchased separately.

2 **Service Activation.** Cisco will define the requirements to activate the Services. Those requirements include changing the configurations of the Covered Endpoints, programming APIs, opening network connections to allow Cisco to receive telemetry data to Cisco's SOCs and testing to confirm the Services are activated. Finally, Cisco will recommend an initial configuration policy for the Covered Endpoints

Cisco Responsibilities

- Provide documentation to Customer to help Customer define the necessary steps to configure the Covered Endpoints, including the API interface requirements needed to connect the Covered Endpoints to the SOC and other systems needed to provide the Services;
- Implement its Cisco Managed Services Platform (CMSP) and conduct tests to confirm that the Services are ready; and
- Recommend initial configuration policies for Covered Endpoints

Customer Responsibilities

- Program/configure the APIs to create and maintain connectivity to of the Covered Endpoints to the Cisco SOC;
- Customer will assist Cisco in establishing and validating connectivity between the Covered Endpoints and Managed Secure Endpoint Platform; and
- Performing necessary configuration changes to the Covered Endpoints to activate the Services and (if desired) implement recommended Covered Endpoint policies.

3 Services Procedure

Cisco uses the following procedure to provide the Services (when combined with the Covered Endpoints) and help prevent and mitigate threats:

3.1 **Monitor and Detect**. Cisco will monitor the security alerts from the Covered Endpoints for potential Security Incidents. Cisco will correlate the Alerts with common threats, Talos Threat Intelligence and certain third-party threat intelligence using analytics, security orchestration, and automation response systems to help determine whether observed events are a Security Incident or a likely Security Incident.

Cisco Responsibilities

- Monitor Covered Endpoints and provide escalated Security Incident alerting systems for known and emerging attacks with a focus on using early detection to support accelerating security operations to help stop, prevent, or contain the threat or attack:
    - Deploy adaptive defenses to help detect non-standard attacks;
    - Detect suspicious and anomalous activities using cloud native security analytics;
    - Utilize Cisco Talos to help identify threats, indicators of attack or compromise and mitigation; and
    - Utilize threat research and tools to collect data on new attack Tactics, Techniques, and Procedures (TTPs) to help identify Security Incidents.

Customer Responsibilities

- Notify Cisco of planned activities or outages (e.g., software updates) or if it detects a possible Security Incident.

3.2 Analyze. Cisco will analyze anomalous events and traffic to help identify threats.

Cisco Responsibilities

- Track and analyze tagged suspicious files on Covered Endpoints, as they traverse the network, and across email and web content; and
- Investigate certain categories of anomalous events and traffic where there is not a known cause, where these events and/or this traffic may pose a material threat.

Customer Responsibilities

- When requested, provide requested context data (e.g., systems running, any maintenance activities, etc.)

3.3 Investigate. Cisco will Investigate threats on Covered Endpoints, user behaviors, applications, and the network elements protected by the Covered Endpoints.

Cisco Responsibilities

- Use threat intelligence to research indicators of compromise (IOCs) and attack (IOAs) to confirm threats, attacks, compromises, or exploitation;
- Create an Incident ticket and notify Customer if a Security Incident is identified by Cisco or reported by Customer and verified by Cisco;
- Use established investigation methodology to add context from integrated Cisco security products and help identify impact, severity, and scope of Security Incident to the endpoint; and
- Investigate the Security Incident for impact, the attacker's level of success and their Tactics, Techniques & Procedures.

3.4 Respond. Cisco will notify and update Customer of the status of the Security Incident and, based on the nature of the Security Incident: perform approved changes to the Covered Endpoints, provide guided recommendations, and/or provide general recommendation responses to help contain, mitigate, remediate, or eradicate the Security Incident.

Cisco Responsibilities

- Provide guidance (see sub-bullets below for details) on how to mitigate, stop, or prevent a Security Incident based on the intelligence and advisories provided, as relevant to customer's environment. Cisco's recommended response to Incident, may be one or more of the following:
  - With Customer's permission, make Changes to the Covered Endpoints to help mitigate or stop the Security Incident (Note: automated responses are limited to those in the Response Playbook);
  - Where Incident is a known attack, recommend response(s) to mitigate or stop attack and provide guidance on how to implement the mitigation(s) on the Covered Endpoints;
  - Where the threat is not fully discovered or understood, recommend Customer perform further analysis with focus on key areas; and
  - Where the threat or attack occurs outside of Covered Endpoints coverage, make general recommendations for Customer to investigate or resolve the Incident.
- Create and modify the detection and response playbooks based on new information and threats from security events detected from the Covered Endpoints and processes described above;
- Cisco will release advisories as new information is obtained about new or novel threats (these advisories are not specific to Customer); and
- If Customer has purchased the optional Cisco Talos Incident Response (CTIR) service, Cisco will notify the CTIR team and route Customer to them.

Customer Responsibilities

- Participate in diagnostic testing to help identify the source of the Security Incident;
- Perform Cisco recommended changes to Covered Endpoints and be responsible for acting on recommendations from Cisco, including determining any dependencies resulting from the recommended actions.

Appendix A – Terms

1. Services Terms

1.1 **Scope of Services and Exclusions.** Unless the Services are expressly provided for above, all other Cisco services are out of scope for this Service Description. For clarity, the following are out of scope:

a) Change Management or implementation of changes not listed in the Services Catalog.
b) Connectivity, such as (for example) a local circuit.

1.2 **Reporting.** Cisco will provide, or make available via the Portal, the reports listed in the reporting documentation for the Services. Cisco reserves the right to add, change, or remove reports in its reasonable discretion.

1.3 **Logging.** The Covered Endpoints contain their own logging capabilities. Please see the product/service description and logging data for the Covered Endpoints Components. The Services retain Security Incident ticket data for one year and then are deleted or overwritten on a rolling basis (oldest data first).

1.4 **Data Exchange.** Except where expressly provided as in scope, security operations center, incident response, etc. services are not included in the Services. Therefore, if Customer wishes for a Partner or a third party to receive Incident data (e.g., Security Incident tickets) to provide complementary services on Customer's behalf, Customer will provide Cisco with a Letter of Authorization, allowing this sharing of data and coordination of Services.

1.5 **Detection and Response Capabilities.** While Cisco has implemented commercially reasonable technologies and processes as a part of the Service, Cisco cannot guarantee it will prevent, detect, stop, or mitigate all Security Incidents.

1.6 **Covered Endpoint Technical Support.** The Services do not include technical support for the Covered Endpoints. If Customer's issue requires technical support Covered Endpoints, Cisco Managed Services may perform initial triage and then direct Customer to Cisco's technical support services or direct Customer to contact Cisco technical support directly.

2. Commercial Terms

2.1 **Pricing Summary.** The Charges consist of a monthly fee based on the number and type of endpoints covered by the Services.

2.2 **Charges.** The charges for the Services ("**Charges**") and payment terms will be detailed in the applicable Order or the Agreement. Except as provided in the Orders or Cisco's material breach which gives Customer a right to terminate, all Charges paid are non-refundable. Cisco's rights to invoice for the Charges for the Services and Customer's obligation to pay will not be affected by (i) any delays caused by Partner or Customer (or anyone acting on their behalf), (ii) Customer's failure to perform or delay in performing its obligations under this Service Description or any Supplement, or (iii) Customer's failure to issue a purchase order or Customer's delay or failure to pay an authorized reseller.

2.3 **Service Activation.** The Order will contain the requested Service Activation Date. The parties will activate the Services within 10 business days of the requested Service Activation date, or the Services will be deemed

activated. If Cisco is the primary cause of the delay in Service Activation, the Service Activation date will be delayed on a "day for day" basis.

2.4 Term, Termination, and Renewal

2.4.1 **Term.** The term of the Services will be provided in the Orders. Unless provided in the Orders, the Term will begin upon the Effective Date of the Order.

2.4.2 **Termination.** Where an Order contains a minimum commitment or contract value, if Customer terminates the Services for convenience, Cisco will invoice the remainder of contract value or minimum commitment due under the Order. If the Order does not contain a minimum commitment, Customer may not terminate the Services for convenience, even if the Agreement allows it, unless expressly provided in the Order. Rights to terminate for material breach are provided in the Agreement.

2.4.3 **Renewal.** If automatic renewal for the Covered Endpoints is enabled, the Services will also automatically renew on the same basis, unless the parties are notified that they do not wish renew the Services as follows:

- **a)** Cisco must notify Customer in writing at least ninety (90) days in advance of the renewal date that it will not renew.
- **b)** Customer must notify Cisco in writing at least thirty (30) days in advance of the renewal date that it will not renew.

3. Legal Terms

3.1 License. Upon expiration or termination of the Services, the license to the Portal, Services, and any associated software will automatically terminate. Note, this license is separate from the licensing and rights associated with the Covered Endpoints, which are covered by their applicable licenses.

3.2 Data Protection. Privacy Data Sheet(s) (available here) describe the Personal Data that Cisco collects and processes as part of the delivery of the Services and the data process by the Covered Endpoints. The Privacy Data Sheets for the Covered Endpoints are separate but found at the same location.

Appendix B – Priority Levels

This Appendix describes the methodology and associated terminology used in determining the priority level of a Security Incident.

1. Priority Definition

The Priority of a Security Incident is based on the Impact and Urgency of an Incident.

Impact: A Security Incident is classified according to the breadth of its impact on Customer's business (the size, scope, and complexity of the Incident).	**Urgency:** The Urgency of a Security Incident is classified according to its impact on the monitored endpoints and impact to Customer's business.
There are four impact levels: **Widespread:** Entire Service is affected. **Large:** Multiple locations are affected. **Localized:** A single location or an individual user at multiple locations are affected. **Individualized:** A single user is affected.	There are four urgency levels: **Critical:** Significant Security Incident causing primary function to be stopped, or significant loss, corruption, or unauthorized encryption of sensitive data. There may be a significant, immediate financial impact to Customer's business. **Major:** Primary function is severely degraded due to loss in functionality or data loss, corruption, or unauthorized encryption. There is a probable significant financial impact to Customer's business. **Minor:** Non-critical function is stopped or severely degraded. There is a possible financial impact to Customer's business. **Low/Notice**: Non-critical business function is degraded. There is no material impact. Customer perceives the issue as low.

3.3 Priority Definitions

Priority defines the level of effort that will be expended by Cisco and Customer to resolve the Security Incident. The Priority level is determined by applying the Impact and Urgency definitions to the chart below.

		IMPACT			
URGENCY		Widespread	Large	Localized	Individualized
	Critical	P1	P1	P2	P2
	Major	P1	P2	P2	P3
	Minor	P2	P3	P3	P3
	Low/Notice	P4	P4	P4	P4

- P1: Cisco and Customer will commit all reasonable resources 24x7 to assist in resolving the Incident (as provided above).
- P2-P4: Cisco and Customer will commit reasonable full-time resources during standard business hours to resolve the Security Incident, provide information, or provide assistance (as applicable).

Cisco will adjust the case priority in accordance with updated priority of impact or incident resolution. In addition, the ticket may be left open after containment or restoration for a prescribed period while remediation efforts are being assessed.

Appendix C- Service Level Agreement ("SLA") for Cisco Managed Secure Endpoint

1. Overview

This SLA describes the parties' responsibilities and sets Cisco's performance targets for the Services ("Service Level(s)") and amounts Cisco will provide to Customer as a credit if Cisco fails to meet the performance objectives for the Service Levels set forth in this SLA ("Service Credits"). This SLA only applies to the Services.

2. Incident Priority Levels

Cisco will categorize and respond to Incidents according to the Priority level methodology described in Appendix B of the Service Description for Services.

3. Service Levels, Service Credits, Service Level Objectives, Key Performance Indicators.

Subject to the terms of this SLA, Cisco will perform the Services so that they will meet or exceed the performance targets Service Levels and Customer will be entitled to claim Service Credits for Cisco's unexcused failure to achieve the Service Levels.

4. Performance Measurement

a) Cisco will use its standard processes and tools for measuring its performance and determining whether the Service Levels were achieved.

b) The window to measure performance against the Service Levels is the Measurement Period. The first Measurement Period will begin 60 days after Service Activation.

c) Within thirty (30) days of the end of each Measurement Period, Cisco will make available to Customer data on the Service Level Performance for the relevant Measurement Period ("Performance Report").

d) If Customer disputes the Performance Report, the parties will review the matter, including providing underlying information to support or dispute the contents of the Performance Report.

5. Confidential Information

The Performance Reports and any underlying data provided to Customer to support the Performance Report is Confidential Information and may not be publicized.

6. Entitlement and Payment of Service Credits

Customer must submit a written claim to Cisco to receive Service Credits within sixty (60) days of receiving the Performance Report, or the right to receive them will be waived. Service Credits will be provided in the form of a Letter of Credit, which must be used during the term of the Services.

7. Limitations

a) Customer may not claim multiple Service Level breaches (and associated credits) where a single Incident has resulted in Cisco failing to achieve multiple Service Levels. If this happens, Customer will have a right to claim (1) Service Credit of its choosing.

b) Customer may not apply a Service Credit unless Customer has first paid remainder of the Charges (i.e., Charges minus the Service Credit Amount).

c) Customer may not sell, transfer, or assign any Service Credits or convert the Service Credit to cash.

d) The maximum and aggregate Service Credits will be (5%) of the recurring Charges paid by Customer for the Service for the relevant Measurement Period.

8. Exclusive Remedy

Cisco's issuance of Service Credits represents Cisco's sole liability to Customer, and Customer's sole and exclusive remedy against Cisco, for Cisco's failure to meet the Service Levels. Any Service Credits paid by Cisco under this SLA will count toward the limitation of Cisco's liability under the Agreement.

9. Customer Responsibilities

Customer will provide Cisco a point of contact to cooperate with Cisco and provide reasonably requested information to help verify Service Level Performance

10. Exceptions

Any failure by Cisco to achieve the Service Levels will be excused if caused by:

a) A material act or omission by Customer in breach of the terms and conditions of the Agreement, the Service Description, and/or the Order;

b) Customer's failure to comply with its responsibilities under the Service Description or this SLA or failure to implement Cisco's reasonable recommendations that would prevent the SLA failure;

c) Any delays or faults caused by Customer, third party equipment, software, services, support, or vendors not under the control of Cisco (e.g., Carrier cycle time);

d) Periods of maintenance where updates, patches, etc. are installed and configured (i.e., Maintenance Windows);

e) A Force Majeure Event;

f) The Covered Endpoints being past the End of Support (EOS) date or not covered by support and maintenance.

g) Software defects that require installation of major software updates or reinstallation of the software on the Cisco equipment;

h) Changes in the Covered Endpoints or network that were not validated or approved by Cisco or delays by Customer in implementing Changes requested by Cisco or otherwise agreed between Customer and Cisco;

i) Failure by Customer to provide a required response necessary for Cisco to meet the Service Levels (Please note: Incident Tickets will be on "hold" during the time Cisco is delayed in receiving required information from the Customer, the End User, or applicable third-party service providers);

j) Changes to the Covered Endpoints that were not approved by Cisco.

11. Security Audit

If there are repeated Security Incidents that Cisco reasonably believes can be prevented through the proper use of the Covered Endpoints and Services, Cisco may conduct, at its own expense and discretion, a review of Customer's security environment. Customer will reasonably cooperate with this review. Following any such review, Customer will make commercially reasonable efforts to implement any reasonable Cisco recommendations. If Customer fails to do so, this SLA will not apply.

12. Governance and Escalation

Cisco and Customer will hold regular meetings to review and assess Service Level Performance, address any Customer concerns, and work in good faith to resolve any disputes between the Parties with respect to Service Level Performance.

Appendix D – Service Levels, Service Level Objectives, and Key Performance Indicators

Portal Availability

Definitions

"**Availability**" means the following, converted to a percentage:

Calculation: (Number of minutes in the month – Outage Time) / Number of minutes in the month.

Portal Availability - is the availability of the web accessible portal made available to Customer to view reports and submit tickets.

Outage Time shall commence upon the earlier of: (1) Cisco's detecting the outage and logging an Incident ticket or (2) Cisco's logging an Incident ticket upon Customer's notice to Cisco of the outage, which notice contains sufficient information to confirm that the outage is occurring in the System. The Outage Time ends when the System is returned to a usable level of service. The duration of Outage time shall be rounded to the nearest minute. Cisco will log an Incident ticket promptly following notification from Customer or its own detection of an outage.

Service Level

Platform Availability: 100%

Portal Availability: 99%

Service Credit

Platform Availability	Service Credit (% of the fixed monthly services charges for the Measurement Period)	Portal Availability	Service Credit (% of the Fixed Monthly Service Charges for the Measurement Period)
> 100% and < 99.9%	1%	<99% and ≥ 98.5%	1%
> 99.9% and < 99%	2%	<98.5% and ≥ 98%	2%
> 99% and < 98.5%	3%	<98% and ≥ 97.5	3%
>98.5%	5%	<97.5%	5%

Measurement Period: Monthly (one calendar month)

Time to Engage

Definition

Cisco will contact Customer's designated contact by phone or MSS Chat within 30 minutes of prioritizing a P1 Security Incident (45 minutes for a P2) if a recommendation to mitigate, stop, research, etc. has already not been provided by this time.

Calculation: Cisco contacts customer in timeframes above for unresolved P1 and P2 Incidents / Total number of P1 and P2 Security Incidents in the month that require engagement after prioritization (i.e., no automatic recommendation provided).

Service Level: On time engagement 95%

Service Credit

Time to Engage	Service Credit (% of the Fixed Monthly Service Charges for the Measurement Period)
<95% and ≥ 90%	1%
<90% and ≥ 80%	2%
<80% and ³ 75%	3%
<75%	5%

Measurement Period: Monthly (one calendar month)