

Sophos Taegis™ ManagedXDR Enhanced—Service Description

This Service Description describes Sophos Taegis ManagedXDR Enhanced (“**Service**”). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below) or in the Glossary section below.

This Service Description is part of and incorporated into, as applicable: (i) Customer’s manually or digitally-signed agreement with Sophos covering the purchase of a Service subscription; (ii) if no such signed agreement exists, then this Service Description will be governed by the terms of the Sophos End User Terms of Use posted at <https://www.sophos.com/en-us/legal> (collectively referred to as the “Agreement”). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence.

Notwithstanding anything to the contrary in the Agreement, Customer acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to <https://www.sophos.com/en-us/legal>.

- **New customers of Taegis MDR or Taegis MDR Elite:** For Customers purchasing Taegis MDR Enhanced simultaneously with Taegis MDR or Taegis MDR Elite, prior to onboarding, Sophos will activate Customer’s Service by provisioning access to Customer’s instance of Taegis™ XDR, which will also provide Customer with access to: 1) online documentation; and 2) instructions to access and deploy the Taegis™ XDR Endpoint Agent/Red Cloak™ Endpoint Agent.
- **Existing customers of Taegis MDR or ManagedXDR Elite:** For customers adding ManagedXDR Enhanced to an existing ManagedXDR or ManagedXDR Elite subscription, Sophos will activate Customer’s Service on the effective date of the Agreement for ManagedXDR Enhanced.

The Service provides Customer with a designated team of security professionals (the “**Enhanced Team**”) to conduct in-depth analysis for investigations as well as orchestrated response and remediation 24 hours a day, 7 days a week (“**24x7**”).

Customer **must** purchase the Taegis MaDR service (“**MDR**”) in conjunction with this Service. (Please see the MDR service description (<https://www.sophos.com/en-us/legal>) for information about that service.) As part of MDR, the MDR Security Analysts will review and investigate Threats detected within Customer’s Taegis XDR (“**XDR**”) tenant(s). Threats requiring further analysis as determined by Sophos will result in creation of an Investigation within XDR. The Enhanced Team will conduct additional analyses of investigations identified in XDR. The Enhanced Team will also conduct an analysis of suspicious emails (phishing). After analysis is completed for each Investigation, the Enhanced Team will take appropriate action based on the documentation developed during Onboarding.

All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the applicable Sophos Agreement.

Service Components

24x7 Access to Designated Enhanced Team

Customer will have access to the Enhanced Team 24x7. From a remote location, the Enhanced Team will conduct work on Customer's behalf and support Customer as defined herein. The Enhanced Team will be available to Customer through email and Ticketing System for support related to the activities described herein. The Enhanced Team will also be available to Customer through telephone solely for investigations deemed by Sophos to be High or Critical.

Threat and Phishing Investigations

The Enhanced Team will conduct analyses for Threat Investigations in Customer's XDR tenant(s) as well as for phishing emails. Three sources that can trigger an Investigation are as follows: Taegis XDR, Customer's ITSM system, and Customer's phishing mailbox. While the MDR Security Analysts will monitor Alerts in XDR and create Investigations as needed, it is the Enhanced Team that will conduct further analyses for these Investigations and add the findings to these Investigations. The Enhanced Team will also review and conduct analyses for Investigations that are automatically created through orchestration playbooks within XDR and add the findings to these Investigations. In addition, the Enhanced Team will analyze suspicious emails that are sent to Customer's phishing mailbox.

For all Investigations, upon confirmation of a threat by the Enhanced Team, the Enhanced Team will help orchestrate responses and remediation with Customer, which includes communicating with responsible stakeholders and advising Customer about appropriate executing actions.

Security Management

The Enhanced Team will provide Security Management through working within Customer's environment to provide a comprehensive approach for delivering the Service. The Enhanced Team will follow the documentation that will be developed by Customer and Sophos during Onboarding. This Service includes usage of Customer's systems and tools within Customer's environment as well as using defined security workflows, and monitoring and responding to custom rules. The Customer's environment is defined as the following:

- Taegis Tenant(s)
- One (1) common set of Customer platforms, which is:
 - One (1) Ticketing System
 - One (1) Phishing/Email security tool (**Note:** This tool refers to both the email phishing mailbox and the tool used for conducting investigations for phishing)
- One (1) common set of Customer processes
- One (1) point of contact for operational governance
- One (1) network accessible through a single point of presence

The sub-sections below explain the elements of Security Management.

Systems and Tools

The Enhanced Team will use up to ten (10) Customer-specified systems and tools, to be identified and documented during onboarding for this Service. The systems and tools will be used to conduct analyses, identify additional business context, and consolidate findings within the appropriate Customer tool. The Enhanced Team will apply their experience, expertise, and knowledge gained from Customer's systems and tools to do the following:

- Conduct an analysis for each investigation
- Determine appropriate next steps
- Collaborate with Customer to orchestrate response and remediation

Note: The Enhanced Team does not conduct any activities related to managing Customer's systems and tools (e.g., no software license or platform/configuration management).

Security Workflows

The Enhanced Team will provide support for up to four (4) documented workflows, to be identified and documented during onboarding for this Service. Supported workflows are as follows:

- Credential-based threats
- Network-based threats
- Host-based threats
- Phishing and Social Engineering

Custom Rules

The Enhanced Team will monitor and respond to Customer's custom rules (as created and used within Taegis XDR) using Taegis XDR detection and orchestration capabilities and other documented Customer-deployed security platforms and tools). The Enhanced Team will not create new custom rules or manage any existing custom rules.

Customer is responsible for creating custom rules unless Customer has purchased the Rule Creation service. Notwithstanding the foregoing, Sophos will create up to five (5) total custom and/or suppression rules for Customer. Maintenance of all rules and any additional rule creation will be the responsibility of Customer.

Security Governance and Advisory

The Enhanced Team will provide support to Customer for security governance strategies and processes. In addition, the team will provide security advisory reviews and recommendations based on knowledge of Customer's environment. Reviews and recommendations include participation in root cause analysis of threats as well as tuning and compliance, remediation guidance.

Service Phases

There are two primary phases for delivering the Service: Onboarding and Steady State.

Onboarding

This phase will be managed by an assigned Program Manager ("PM"). The PM will coordinate the activities that must be completed during this phase. Sophos will guide Customer through multiple activities to help ensure that the Enhanced Team has the access, training, and guidance needed to deliver the Service to Customer. Onboarding is expected to be completed within 8-12 weeks;

timeline will be based on dependencies and the project plan that will be agreed-upon during Onboarding.

Steady State

Steady State commences when the Onboarding Checklist is completed and Customer has satisfied all Steady State requirements for the standard MDR service, which must accompany this Service (see <https://docs.ctpx.secureworks.com/mxdr/onboarding/>). During Steady State, the Enhanced Team will conduct investigations and apply Customer’s business context based on their knowledge of and access to Customer’s environment. When the Enhanced Team confirms a threat, they will help coordinate the response and remediation for Customer and will collaborate with Customer-designated personnel as appropriate.

The table below indicates timing and activities conducted by Sophos during the Service Phases. Please note that timing is approximate and predicated on Customer performing its responsibilities described herein.

Phase	Activities
Onboarding	<p>Timing: Upon start of Services Term</p> <ul style="list-style-type: none"> • Ensure that the Enhanced Team can access and use Customer’s existing in-scope systems and tools in Customer’s environment • Agree upon and document the processes, procedures, and related work instructions that will be used to deliver the Service as well as agree upon the Service goals, project plan, and dependencies • Interview Customer-designated personnel to obtain information necessary to deliver the Service • Collect relevant materials and information about Customer’s environment • Work with Customer to develop and customize documentation for the Enhanced Team to deliver the Service, which will include the following: <ul style="list-style-type: none"> ○ RACI ○ Workflows ○ Escalation procedures ○ Playbooks (Note: These are separate and different from the automated playbooks in Taegis XDR.) • Introduce the Steady State governance function • Complete Onboarding Checklist to verify readiness for transitioning to Steady State
Steady State	<p>Timing: 8-12 weeks after Onboarding begins</p> <ul style="list-style-type: none"> • Weekly Operations Review • Conduct analysis for investigations from the specified Ticket sources • Engage Customer as needed for orchestrated response and remediation activities
<i>Monthly Service Review</i>	<p>Timing: Monthly after Steady State is reached</p> <ul style="list-style-type: none"> • Recommendations related to the Service based on processes and technology • Ticket reporting (e.g., proposed tuning metrics, # of Tickets used) • Issues/Risks

Customer Obligations

Customer is required to perform the obligations listed below and acknowledges and agrees that the ability of Sophos to perform its obligations hereunder are dependent on Customer’s compliance with these obligations. Noncompliance with Customer obligations relative to this Service may result

in limitations and reduced service capabilities or suspension of managed components of the Service.

Customer will do the following:

- Ensure that all MDR obligations are met (see https://docs.ctpx.secureworks.com/legal/mxdr_service_description/#customer-obligations)
- Document and provide access to one (1) Customer environment (see the “System Management” section for details)
- Work with Sophos to create RACI, workflows, and escalation procedures
- Perform Customer Obligations in accordance with the RACI agreed upon by the Parties
- Document and provide access to Customer’s environment as required to conduct analyses in addition to XDR
- Provide the Enhanced Team with credentials for accessing Customer’s network and the tools within Customer’s environment
- Provide and maintain VDI for the Enhanced Team to access Customer’s on-prem tools, if needed
- Ensure list of Customer’s authorized contacts remains current, including permissions and associated information
- Obtain consent and authorization from the applicable third party, in form and substance satisfactory to Sophos, to permit Sophos to provide the Service if Customer does not own network resources such as IP addresses, tools, systems, hosts, facilities or web applications

Additional Information

Billing for the Service begins at the same time as billing for Taegis XDR. Contact account manager or refer to the official terms as stated on Customer’s Agreement from purchase for the most up-to-date details.

See the documentation within Taegis XDR (<https://docs.ctpx.secureworks.com/>) for information about compatible browsers, Integrations, detectors, dashboards, and training.

Tickets (for Conducting Investigations)

The Service provides Customer with a specified number of Tickets for each calendar month in Customer’s Services Term. A Ticket corresponds to the performance of a Threat or Phishing investigation as described in the Threats and Phishing Investigations section of this service description. Tickets for any given calendar month of Customer’s Services Term cannot be used before the start of said calendar month, and any unused tickets expire at the end of the calendar month during Customer’s Services Term. The standard Service includes 300 Tickets per calendar month. Additional Tickets can be purchased in groups of 150 Tickets. For example, if Customer requires 600 Tickets per calendar month, then two additional groups of Tickets are required (300 as part of the Service + one (1) group of 150 + one (1) group of 150 = 600 Tickets per calendar month).

For any given calendar month of Service, should Customer exceed their purchased volume of Tickets, then Customer will be required to pay for Ticket overages. Customer shall be charged overages on a per-Ticket basis, calculated at the then-current per-Ticket list price.

During a Services Term, Customer cannot reduce the initially purchased per-month Ticket volume.

Warranty Exclusion

While the Service is intended to reduce risk, it is impossible to completely eliminate risk, and therefore Sophos makes no guarantee that intrusion, compromises, or any other unauthorized activity will not occur on Customer’s systems.

Glossary

Term	Definition
Alert	Prioritized occurrences of suspicious or malicious behavior detected by a detector in XDR.
Investigation	A central location within XDR that is used to collect evidence, analysis, and recommendations related to a Threat that may be targeting an asset in a Customer’s IT environment. Investigations are categorized into types, such as Security and Incident Response.
Parties	Customer and Sophos are referenced jointly using this term.
Security Analyst	A Sophos security expert who analyzes alerts deemed High and Critical for customers, and creates and escalates Investigations. Note: A Security Analyst may also be referred to as a MDR analyst or an MDR analyst across other Sophos documentation.
Services Term	Period of time identified in the Agreement during which Services will be delivered to Customer.
Threat	Any activity identified by XDR that may cause harm to an asset in a Customer’s IT environment.
Ticket	A support request object in the Taegis platform, the Customer’s Ticketing System, or Phishing tool – used to track a Service Request to closure as it is handled by stakeholders across an organization
Ticketing System	ITIL-compliant help desk software that collects Customer’s support requests from various stakeholders into a single location. The support requests are referred to as Tickets and the Tickets are managed and updated within the single location.