



Offer Description

Cisco Security Analytics and Logging

This Offer Description is part of the [General Terms](#) or similar terms existing between You and Cisco (e.g., the End User License Agreement) (the “**Agreement**”). Capitalized terms, unless defined in this document, have the meaning in the Agreement. Any references to the Supplemental End User License Agreement or SEULA mean Offer Description.

1. Summary

This Offer Description applies to Cisco Security Analytics and Logging SaaS (“**SAL SaaS**”) and Cisco Security Analytics and Logging On-Premise (“**SAL On-Prem**”) and any Cisco Offers that reference this Offer Description (collectively, the “**Cisco Offer**”). The Cisco Offer provides Central Log Management (CLM) for streamlining IT operations, with added ability to analyze logs for enhanced visibility and advanced threat detection. The Product debuted with Cisco Firewall logs (FTD and ASA), with Network Flow Logs and other log sources being included progressively. Disparate log types are covered by the same offer structure, which adopts a nested licensing model (i.e., with lower licenses nested in higher license capabilities). The licenses are:

- **Essentials** (formerly Logging and Troubleshooting or LT): Scalable central logging service with long-term retention options, with drill-down enabled through advanced viewer controls such as search, filter, download, etc.
- **Advantage** (formerly Log Analytics or LA): An optional capability to analyze logs for advanced threats using behavioral modelling techniques. These threat detection algorithms leverage existing Cisco Secure Cloud Analytics (“SCA”) or Secure Network Analytics (“SNA”) analytics, as well as trigger new alerts customized for Product logs.
- **Premier** (formerly Total Network Analytics or TA): Aggregates log analysis with native Cisco SCA or SNA logs, for end-to-end analysis.

2. Support and Other Services

2.1 **Cisco SecureX.** Your Cisco Offer subscription includes access to Cisco SecureX, Cisco’s integrated security platform that aggregates threat intelligence (through SecureX threat response, also known as Cisco Threat Response), unifies visibility across various Cisco and third-party security products, enables automated workflows, and more. Since SAL data triggers alerts in SCA and/or SNA, such alerts will be visualized in SecureX leveraging SCA’s or SNA’s native integration with SecureX. For more information on SecureX, please see the [SecureX Offer Description](#).

2.2 **Other Services.** SAL SaaS subscriptions include the right to use the Cisco Defense Orchestrator (“**CDO**”) for firewall log viewing. In addition, Advantage (Log Analytics) and Premier (Total Network Analytics) licenses include the right to use SCA for advanced threat detection. Please note that a SAL SaaS subscription does not require a separate subscription for either CDO or SCA, and neither is it mandatory for Cisco Offer logging firewall devices to be managed by CDO.

Similarly, SAL On-Prem subscriptions leverage the SNA virtual and physical appliances, without the need for separate SNA flow rate licenses for Cisco Offer OP purposes. Flow rate licenses continue to be required for purposes of SNA.

2.3 Support

(A) [SAL SaaS subscriptions](#). SAL SaaS subscriptions include Embedded [Cisco Software Support Services](#).

(B) [SAL On-Prem subscriptions](#). SAL On-Prem subscriptions include Basic [Cisco Software Support Services](#).

3. Data Handling

The [Disclosure Documents](#) for Cisco Security Analytics and Logging provide information about data handling practices, security controls, and other features specific to this Cisco Offer.

4. Special Terms

4.1 **Overage Billing.** The Cisco Offer is priced on log volume in gigabytes (GB) per day. For the SAL SaaS offer only, Cisco may bill for overages monthly in arrears. At the end of each calendar month, Cisco calculates the actual

average daily firewall event log volume for the month and automatically invoices customers for any overage. For example, if a customer purchases a subscription for 10 GB/day, the customer is entitled to 300 GB of firewall event log volume for a 30-day calendar month. If at the end of such calendar month the customer used 330 GB, the average daily usage is $330/30 = 11$, and Cisco shall have the right to bill the customer for an overage subscription 1 GB/day for that month.

- 4.2 Disclaimers. Cisco does not represent or warrant that the product software will guarantee absolute security due to the continual development of new techniques for intruding upon and attacking files, networks, and endpoints. Cisco does not represent or warrant that the product will protect all your files, network, or endpoints from all malware, viruses or third-party malicious attacks. Cisco does not make any representations or warranties regarding any third-party system or service to which a product integrates or to any ongoing integration support. Integrations made accessible to you that are not a generally available product included on your order are provided on an “as is” basis.**