Data Sheet

Cisco Stealthwatch Endpoint License

With the Cisco Stealthwatch™ Endpoint License you can conduct in-depth, context-rich investigations into endpoints that exhibit suspicious behavior.

In our connected world, mobility is king. More users are connecting to corporate networks with more devices, from more places than ever before. The average worker uses three personal devices for work purposes. That's more than 15 billion mobile devices worldwide with access to enterprise networks. And the reality is that many of those devices could already be compromised.

Security professionals need to see into the applications and processes that occur at the network edge, down to remote devices. The Cisco Stealthwatch endpoint solution permits security professionals to conduct more efficient, context-rich investigations into user machines that are exhibiting suspicious behavior. Tightly integrated with the Cisco AnyConnect® Network Visibility Module, the Stealthwatch Endpoint solution provides greater network visibility while enhancing the investigation of endpoints. It offers easy access to endpoint applications and information that security analysts need to speed incident response and remediate policy violations.

How It Works

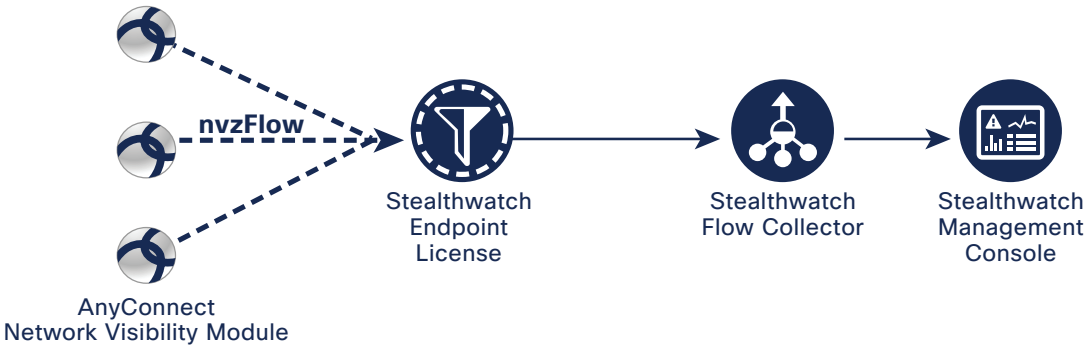
The Endpoint License delivers support for the Cisco® Network Visibility Flow (nvzFlow) protocol introduced with the Cisco AnyConnect 4.2 Network Visibility Module (NVM). The AnyConnect NVM collects high-value endpoint contextual data. It exports that telemetry using the nvzFlow protocol, an extension of the standards-based IP Flow Information Export (IPFIX) protocol, to the Endpoint Concentrator. The Endpoint Concentrator collects this telemetry from multiple endpoints and forwards it to the Flow Collector. There, through a process of stitching and deduplication, the endpoint-specific fields are inserted into the conversational flow records maintained in the Flow Collector database. The endpoint data is then analyzed and displayed in the Stealthwatch console for a single view into activity across the network.

Generating telemetry from the endpoint provides context and awareness. It is a critical step in gaining the visibility needed to secure the endpoint.

Components & Architecture

Figure 1 illustrates the components and architecture of this solution. Table 1 lists its major benefits. Table 2 provides ordering information, and Table 3 gives specifications for the virtual edition.

Figure 1. Cisco Stealthwatch Endpoints Architecture



Components

Endpoint License: The Endpoint License allows telemetry data to be captured from endpoint devices that connect to your network, such as desktop computers, laptops, smartphones, and tablets. The license permits the high-value endpoint contextual data collected by the AnyConnect NVM to be exported to the Endpoint Concentrator for further analysis in the Management Console.

Endpoint Concentrator: The Endpoint Concentrator collects IPFIX data from the Cisco AnyConnect Network Visibility Module. Data is collected from all endpoint devices and is passed through the Endpoint Concentrator to the Flow Collector. A Flow Collector is required for an Endpoint solution deployment.

Table 1. Major Benefits of the Endpoint License

Benefit	Description
Increased visibility	Extends your network as a sensor to personal devices such as laptops, tablets, and smart phones.
Enhanced security	Delivers enhanced security with real-time threat detection on suspicious activity and potential attacks
Accelerated response	Provides superior forensic investigations with sophisticated security analytics
Improve compliance	Offers real-time situational awareness and network visibility to help you meet compliance regulations across your entire network.

Table 2. Endpoint License Ordering Information

Product Part Number*	Tiering
L-SW-EL-XY-S1	Cisco Stealthwatch Endpoint License XYR, 1 – 99 Users
L-SW-EL-XY-S2	Cisco Stealthwatch Endpoint License XYR, 100 – 249 Users
L-SW-EL-XY-S3	Cisco Stealthwatch Endpoint License XYR, 250 – 499 Users
L-SW-EL-XY-S4	Cisco Stealthwatch Endpoint License XYR, 500 – 999 Users
L-SW-EL-XY-S5	Cisco Stealthwatch Endpoint License XYR, 1000 – 2499 Users

Table 2. Endpoint License Ordering Information (continued)

Product Part Number*	Tiering
L-SW-EL-XY-S6	Cisco Stealthwatch Endpoint License XYR, 2500 – 4999 Users
L-SW-EL-XY-S7	Cisco Stealthwatch Endpoint License XYR, 5000 –9999 Users
L-SW-EL-XY-S8	Cisco Stealthwatch Endpoint License XYR, 10000 – 24999 Users
L-SW-EL-XY-S9	Cisco Stealthwatch Endpoint License XYR, 25000– 49999 Users
L-SW-EL-XY-S10	Cisco Stealthwatch Endpoint License XYR, 50000– 9999 Users
L-SW-EL-XY-S11	Cisco Stealthwatch Endpoint License XYR, 100000– 249999 Users

*X = 1 year, 3 years or 5 years

Table 3. Endpoint License Specification for Virtual Edition

Reserved CPU	Reserved Memory	Maximum FPS Rate	Maximum Exporters
2	8 GB	20,000	13,333

Stealthwatch Flow Collector: The Flow Collector provides network visibility and security intelligence across physical and virtual environments to help improve incident response. The volume of NetFlow telemetry collected from the network is determined by the capacity of the deployed Flow Collectors. Multiple Flow Collectors may be installed. Flow Collectors are available as hardware appliances or as virtual machines. The capacity of the Flow Collector must be taken into consideration for the deployment of the Endpoint solution. Table 4 outlines the Flow Collector's benefits.

Table 4. Major Benefits of the Stealthwatch Flow Collector

Benefit	Description
Increased flow context	Ingests URL and proxy user data from proxy servers and associates it with the corresponding network flow data.
Better traffic visibility	Improves visibility for the Cisco Stealthwatch system, given network conversations that pass through web proxies.
Threat Intelligence monitoring	Automatically compares URL data from proxy records with the Threat Intelligence feed.
Investigation enablement	Manually investigates data within the console.
Greater accuracy	Provides context data to the Cisco Stealthwatch system to increase the accuracy of security events.
Correlation of proxy and flow data	Ingests URL and proxy user data from proxy servers and associates it with the corresponding network flow data. This information is automatically compared with the Threat Intelligence feed. It is also used to support manual investigation within the console.
Visibility	Eliminates blind spots on the network by allowing organizations to see the translated address associated with the other side of a proxy conversation
Threat detection	Ingests proxy records and associates them with flow records, delivering the user application and URL information for each flow, to increase contextual awareness. This process enhances your organization's ability to pinpoint threats and shortens your mean time to know (MTTK).
Incident response	Provides additional context around web traffic traversing through a proxy server for more accurate troubleshooting, incident response, and forensics.
Real-time traffic analysis	Delivers real-time traffic analysis for billing, bandwidth accounting, and network performance troubleshooting.
Flow-traffic monitoring	Monitors flow traffic across hundreds of network segments simultaneously, so you can spot suspicious network behavior. This capability is especially valuable at the enterprise level.
Identification of security root cause	Isolates the root cause in seconds for faster security incident response.

Table 4. Major Benefits of the Stealthwatch Flow Collector (continued)

Benefit	Description
Actionable insight	Provides actionable insight into performance without using expensive probes.
Extended data retention	Allows organizations and agencies to retain large amounts of data for long periods.
Multiple types of flow data	Uses multiple types of flow data (Netflow, IPFIX, and sFlow) to provide cost- effective, behavior-based network protection.
Scalability	Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
Deduplication and stitching	Performs deduplication so that any flows that might have traversed more than one router are counted only once. It then stitches the flow information together for full visibility of a network transaction.
End-to-end visibility	Aggregates high-speed network behavior data from multiple networks or network segments to deliver end-to-end protection and improve performance across geographically dispersed networks.
Choice of delivery methods	You can order the Appliance Edition, a scalable device suitable for any size organization. Or you can order the Virtual Edition, designed to perform the same functions as the appliance edition, but in a VMware environment. This solution scales dynamically according to the resources allocated to it.

The Flow Collector should be used as a guide when determining the number of supported hosts for the Endpoint License, because the Flow Collector will experience degradation before the Endpoint Concentrator. The maximum endpoint traffic impact on Flow Collectors is 50,000 fps; standard performance considerations for flows per second (fps) still apply.

Management Console: The Management Console manages, coordinates, and configures Cisco Stealthwatch appliances deployed at critical segments throughout the enterprise. With the Management Console, administrators can easily view, understand, and act upon a plethora of network and security data, all through a single interface. Snapshot views and sophisticated drill-down capabilities provide the exact level of information you need exactly when you need it. Advanced graphics and customizable views of network activity deliver unique insight to help network and security teams understand traffic patterns and identify deviations from normal network behavior. Administrators can view high-level details, or choose to drill down into alarms, security event details, host-level views, and more for fast, efficient troubleshooting and root cause analysis. Dynamic querying, customized reports, and intuitive visualizations of network data help to decrease the time between problem onset and resolution. Major benefits of the Management Console are shown in Table 5. Specifications of the various models are given in Tables 6 and 7.

Table 5. Major Benefits of the Management Console

Benefit	Description
Real-time up-to-the-minute data	Delivers data flow for monitoring traffic across hundreds of network segments simultaneously, so you can spot suspicious network behavior. This capability is especially valuable at the enterprise level.
Capability to detect and prioritize security threats	Rapidly detects and prioritizes security threats, pinpoints network misuse and suboptimal performance, and manages event response across the enterprise – all from a single control center.
Network groupings	Creates network groupings and relationship maps for an easy view of the state of your organization's traffic. Within seconds, operation and security teams can see exactly where to focus their attention.
Graphical representation	Provides a representation of the state of the network in a clean, easy-to-understand format.
Quick assessments of the security posture	Displays multiple alarm categories on the home dashboard, so operators can quickly assess the security posture of the organization.
Management of Cisco Stealthwatch appliances	Configures, coordinates and manages appliances, including the Flow Collector and Flow Sensor appliances.
Use of multiple types of flow data	Consumes multiple types of flow data, including Netflow, IPFIX, and sFlow. The result: Cost-effective, behavior-based network protection.
Scalability	Supports even the largest of network demands. Performs well in extremely high-speed environments and can protect every part of the network that is IP reachable, regardless of size.
Choice of delivery methods	You can order the Appliance Edition, a scalable device suitable for any size organization. Or you can order the Virtual Edition, designed to perform the same functions as the appliance edition, but in a VMware environment.
Enhanced network management	Enhances network management through trend analysis, firewall and capacity planning, and performance monitoring.
Handling of APTs, malware, and insider threats	Provides the in-depth visibility and context needed to thwart evolving threats. This includes everything from worms, viruses, and other malware to targeted attacks, DDoS attempts, insider threats, and APTs. Provides alerts with the contextual information necessary for security personnel to take quick, decisive action to mitigate potential damage.
Audit trails for network transactions	Provides a full audit trail of all network transactions for more effective forensic investigations.
Real-time, customizable relational flow maps	Provides graphical views of the current state of the organization's traffic. Administrators can easily construct maps of their network based on any criteria, such as location, function, or virtual environment. By creating a connection between two groups of hosts, operators can quickly analyze the traffic traveling between them. Then, simply by selecting a data point in question, they can gain even deeper insight into what is happening at any point in time.

Table 6. Management Console Models

Model	Maximum Number of Flow Collectors Supported	Flow Storage Capacity
Management Console VE	Up to 5	1 TB
Management Console 1000	5	1 TB
Management Console 2000	25	2 TB

Table 7. Management Console Specifications, by Model

	Management Console 500 and 1010	Management Console 2010
Network	1 management port: 10/100/1000BASE-TX, copper	
Database capacity	1 TB (RAID 6 redundant)	2 TB (RAID 6 redundant)
Hardware platform	R630	
Hardware generation	13G	
Rack unit (mountable)	1RU	
Power	Redundant 750W AC, 50/60 Hz, auto-ranging (100V to 240V)	
Heat dissipation	2891 Btus per hour maximum	
Dimensions	Height: 1.68 in. (4.3 cm) Width: 17.08 in. (43.4 cm) Depth: 27.25 in. (69.2 cm)	
Unit weight	41 lb (18.6 kg)	
Rails	Sliding Ready Rails with cable management arm	
Regulatory	FCC (U.S. only) Class A DOC (Canada) Class A CE Mark (EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3, EN60950) VCCI Class A UL 1950 CSA 950	

Service and Support

A number of service programs are available for Cisco Stealthwatch. These innovative programs are delivered through a combination of people, processes, tools, and partners to provide high levels of customer satisfaction. These services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Professional Services, see the Technical Support home page.

Cisco Capital

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

For more information about Cisco Stealthwatch visit www.cisco.com/go/stealthwatch. To place an order, contact your account representative or email stealthwatch-interest@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**