Cisco Stealthwatch Enterprise

For UCS Hardware

Stealthwatch™ Enterprise is the industry-leading visibility and security analytics solution that leverages enterprise telemetry from the existing network infrastructure. It provides advanced threat detection, accelerated threat response and simplified network segmentation using multi-layer machine learning and advanced behavioral modeling, all across the extended network.

With Stealthwatch Enterprise, you get real-time visibility that helps you gain better insight into activities occurring within your network. You can scale this visibility into the cloud, across the network, at branch locations, in the data center, and down to endpoints.

At the core of Stealthwatch Enterprise are the Flow Rate License, the Flow Collector, Management Console and Flow Sensor. For added functionality, please refer the individual datasheets below:

- Cisco Stealthwatch Endpoint License: Available as a license add-on to extend visibility to end user devices.
- Cisco Stealthwatch Cloud – Available as a product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.
- **Threat Intelligence License** - A global threat intelligence feed powered by the industry-leading threat intelligence group, Cisco Talos, provides an additional layer of protection against botnets and other sophisticated attacks. It correlates suspicious activity in the local network environment with data on thousands of known command-and-control servers and campaigns, to provide high fidelity detection and faster threat response. Cisco Talos sees 1.5 million unique malware samples and blocks 20 billion threats per day.

System Benefits

Through its unique view and analysis of network traffic, Stealthwatch Enterprise dramatically improves:

- Real-time threat detection
- Incident response and forensics
- Network segmentation
- Network performance and capacity planning
- Ability to satisfy regulatory requirements

Required Components of the System

Flow Rate License

The Flow Rate License is required for the collection, management, and analysis of flow telemetry and aggregates flows at the Management Console. The Flow Rate License also defines the volume of flows that may be collected and is licensed on the basis of flows per second (fps). Licenses may be combined in any permutation to achieve the desired level of flow capacity.

Flow Collector

The Flow Collector leverages enterprise telemetry such as NetFlow, IPFIX and other types of flow data from existing infrastructure such as routers, switches, firewalls, endpoints and other network infrastructure devices. The Flow Collector can also receive and collect telemetry from proxy data sources, which can be analyzed by the Global Threat Analytics (formerly Cognitive Threat Analytics), the multilayered machine learning engine, for deep visibility into both web and network traffic. Also, Stealthwatch Enterprise, using Encrypted Traffic Analytics, can use analytics to pinpoint malicious patterns in encrypted traffic to identify threats and accelerate response. Though this feature is built in to the system at no extra cost, it will need to be enabled upon deployment.

The telemetry data is analyzed to provide a complete picture of network activity. Months or even years of data can be stored creating an audit trail that can be used to improve forensic investigations and compliance initiatives. The volume of 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. Table 1 outlines Flow Collector's benefits.

Table 1. Major Benefits of the Flow Collector

Benefit	Description
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).
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.
Extended data retention	Allows organizations and agencies to retain large amounts of data for long periods.
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.
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 maximum number of flows per second can change, depending on network conditions.

Flow Collector Specifications

- Stealthwatch Flow Collector 4200 - Part number: ST-FC4200-K9
- Stealthwatch Flow Collector 5200 - Part number: ST-FC5200-K9
- Stealthwatch Flow Collector Virtual Edition can be configured as either FCVE-1000, FCVE-2000, or FCVE-4000 - Part number: L-ST-FC-VE-K9

Note: These specifications apply to the Stealthwatch system version 6.9.1 and newer

Management Console

The Stealthwatch Management Console aggregates, organizes, and presents analysis from up to 25 Flow Collectors, the Cisco Identity Services Engine, and other sources. It uses graphical representations of network traffic, identity information, customized summary reports, and integrated security and network intelligence for comprehensive analysis.

The capacity of the console determines the volume of telemetry data that can be analyzed and presented, as well as the number of Flow Collectors that are deployed. The console is available as a hardware appliance or a virtual machine. Table 2 list the benefits of the consoles.

Table 2. 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.
Management of appliances	Configures, coordinates, and manages Cisco Stealthwatch appliances, including the Flow Collector, Flow Sensor, and UDP Director.
Use of multiple types of flow data	Consumes multiple types of flow data, including NetFlow, Internet Protocol Flow Information Export (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.
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.
Flexible delivery options	You can order the Physical Appliance, 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.

Management Console Specifications

- Stealthwatch Management Console 2200 - Part number: ST-SMC2200-K9
- Stealthwatch Management Console Virtual Edition can be configured as either SMC VE or SMC VE 2000 - Part number: L-ST-SMC-VE-K9

Note: These specifications apply to the Stealthwatch system version 6.9.1 and newer

Optional Components of the System

Flow Sensor

The Flow Sensor is an optional component of Stealthwatch Enterprise and produces telemetry for segments of the switching and routing infrastructure that can't generate NetFlow natively. It also provides visibility into the application layer data. In addition to all the telemetry collected by Stealthwatch, the Flow Sensor provides additional security context to enhance the Stealthwatch security analytics. Advanced behavioral modeling and cloud-based multilayered machine learning is applied to this dataset to detect advanced threats and perform faster investigations.

The Flow Sensor is installed on a mirroring port or network tap and generates telemetry based on the observed traffic. The volume of telemetry generated from the network is determined by the capacity of the deployed Flow Sensors. Multiple Flow Sensors may be installed. Flow Sensors are available as hardware appliances or as virtual appliances to monitor virtual machine environments. It also works in environments where an overlay monitoring solution requiring additional security context better fits the operations model of the IT organization.

Table 3 lists the major benefits of the Flow Sensor.

Table 3. Major Benefits of the Flow Sensor

Benefit	Description
Layer 7 application visibility	Provides true Layer 7 application visibility by gathering application information along with ad-hoc on-demand packet capture (PCAP). This includes data features like RTT (Round trip time), SRT (Server Response Time), Retransmissions.
Packet-level performance and analysis	Provides true Layer 7 application visibility by gathering application information along with ad-hoc on-demand packet capture (PCAP). This includes data features like RTT (Round trip time), SRT (Server Response Time), Retransmissions.
Alerts on network anomalies	Additional telemetry from the Flow Sensor, such as URL information for web traffic and TCP flag detail, helps generate alarms with contextual intelligence so that security personnel can take quick action and mitigate damage.
Lower costs	Enhances operational efficiency and reduces costs by identifying and isolating the root cause of an issue or incident within seconds.
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 function as the appliance edition, but in a VMware or KVM Hypervisor environment.

* These numbers are generated in our test environments using average customer data.

Flow Sensor Specifications

- Stealthwatch Flow Sensor 1200 - Part number: ST-FS1200-K9
- Stealthwatch Flow Sensor 2200 - Part number: ST-FS2200-K9
- Stealthwatch Flow Sensor 3200 - Part number: ST-FS3200-K9
- Stealthwatch Flow Sensor 4200 - Part number: ST-FS4200-K9
- Stealthwatch Flow Sensor Virtual Edition - Part number: L-ST-FS-VE-K9

Note: These specifications apply to Cisco Stealthwatch 6.9.1 and newer

UDP Director

The UDP Director simplifies the collection and distribution of network and security data across the enterprise. It helps reduce the processing power on network routers and switches by receiving essential network and security information from multiple locations and then forwarding it to a single data stream to one or more destinations. Table 4 list the major benefits of the UDP Director.

Table 4. Major Benefits of the UDP Director

Benefit	Description
Reduces unplanned downtime and service disruption	UDP Director high availability is available on the UDP Director 2200 appliance.
Simplifies network security and monitoring	UDP Director aggregates and provides a single standardized destination for NetFlow, sFlow, syslog, and Simple Network Management Protocol (SNMP) information. UDP Director appliances can receive data from any connectionless UDP application, and then retransmit it to multiple destinations, duplicating the data if required.
Can direct UDP data from any source to any destination	Receives data from any connectionless UDP application, and then retransmits it to multiple destinations, duplicating the data if required.
Removes the need to reconfigure infrastructure	Directs point log data (NetFlow, sFlow, syslog, SNMP) to a single destination without the need to reconfigure the infrastructure when new tools are added or removed.

UDP Director Specifications

- Stealthwatch UDP Director 2200 - Part number: ST-UDP2200-K9
- Cisco Stealthwatch UDP Director Virtual Edition - Part number: L-ST-UDP-VE-K9

Ordering Information

The Cisco Stealthwatch System ordering guide will help you understand the system's models, components, and licensing types. To place an order, contact your account representative.

Service and Support

A number of service programs are available for the Cisco Stealthwatch system. 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 homepage.

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 https://www.cisco.com/go/stealthwatch or contact your Cisco Security account representative to learn how your organization can gain visibility across your extended network by participating in a complimentary Stealthwatch Visibility Assessment.

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 **https://www.cisco.com/go/offices**.

Printed in USA C78-739398-03 04/18