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.

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 Cognitive Threat Analytics solution for deep visibility into both web and network traffic. Rather than decrypting the traffic, this integration with Cognitive Threat Analytics will 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, and Table 2 lists its specifications.

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.

Table 2. Flow Collector Specifications, by Model

	FC4200	FC 5200
Description	Full hardware redundancy and flow-processing horsepower for extremely large NetFlow, sFlow, or IPFIX environments.	High-capacity flow-ingestion solution created for enterprise customers needing superior performance capabilities. Built on the Cisco UCS® platform.
Hardware platform	UCSC-C220-M4S	**Engine:** UCSC-C220-M4S **Database node:** UCSC-C240-M4S2 (2 RU)
Maximum flows per second*	120,000 fps*	Up to 240,000
Maximum exporters or routers	2000	
Network	• Reserved ports: 2; 10 GB SFP+ • CIMC management port: 1; 100/1000 copper • Stealthwatch management port: 1; 100/1000 copper • Monitoring port: 1; 100/1000 copper **Note:** You can configure a monitoring port to be a dedicated interface (ingress only) for receiving NetFlow traffic.	**Engine:** • Engine to database cross connect port: 1; 10 GB SFP+ fiber DA Cross Connect • CIMC management port:1; 100/1000 copper • Stealthwatch management port:1; 100/1000 copper • Monitoring port: 1; 100/1000 copper **Database:** • Engine to database cross connect port: 1; 10 GB SFP+ fiber DA Cross Connect • CIMC management port: 1; 100/1000 copper

	FC4200	FC 5200
		• Stealthwatch management port:1; 100/1000 copper
Flow storage	4 TB, RAID6, Redundant	Engine: 300 GB HDD (8x) - 1.2TB total RAID6 Database: 1.2 TB HDD (16x) - 9.6 TB total RAID10
Addressable Storage	7.2TB	
Memory	32 GB DDR4 (16x) - 512GB total	
Rack units (mountable)	1U	• **Engine: 1U** • **Database: 2U**
Power	• Redundant 750W AC 50/60 • Auto Ranging (100v to 240V)	**Engine:** • Redundant 770W • **AC input voltage: Nominal range 100-127 VAC, 200-240 VAC** • **AC input frequency: Nominal range 50 to 60 Hz** • **Max AC input current: 9.5 A at 100 VAC, 4.5 A at 208 VAC** **Database:** • Redundant 1200W • AC input voltage: Nominal range 100-120 VAC, 200-240 VAC • AC input frequency: Nominal range 50 to 60 Hz Max • AC input current: 11A at 100 VAC, 7A at 200 VAC
Heat dissipation	1741.13 BTU per hour maximum (estimated)	**Engine:** 1816.63 BTU per hour maximum (estimated) **Database:** 2492.78 BTU per hour maximum (estimated)
Dimensions	• Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm)	**Engine:** • Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm) **Database:** • Height: 3.43 inches (8.7 cm) • Width: 18.96 inches (44.8 cm) with rack latches; 17.65 in. (44.8 cm) without rack latches • Depth: 30.18 inches (76.6 cm) with handles; 29.0 in. (73.8 cm) without handle
Weight	37.9 pounds (17.2 kg)	• Engine: 37.9 pounds (17.2 kg) • Database: 58.9 pounds (27.7 kg)
Virtual Appliance	L-ST-FC-VE-K9	

* The maximum number of flows per second can change, depending on network conditions.

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. Tables 3 and 4, list the benefits, and specifications of the consoles, respectively.

Table 3. 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	Rapidly detects and prioritizes security threats, pinpoints network misuse and suboptimal performance, and

Benefit	Description
prioritize security threats	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.

Table 4. Management Console Specifications, by Model

	SMC 2200
Hardware platform	UCSC-C220-M4S
Network	• Reserved ports: 2; fiber - 10 GB SFP+ • CIMC management port: 1; 100/1000 copper • Stealthwatch management port: 1; 100/1000 copper
Processor	2.40 GHz E5-2680 v4
Memory	32G DDR4 (16x) - 512GB total
Rack unit (mountable)	**1U**
Power	• Redundant 750W AC 50/60 • Auto Ranging (100v to 240V)
Heat dissipation	741.13 BTU per hour maximum (estimated)
Dimensions	• Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm)
Unit weight	37.9 pounds (17.2 kg)
Virtual Appliance	L-ST-FC-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 produces NetFlow data for segments of the switching and routing infrastructure that do not support NetFlow. The Flow Sensor can provide Layer 7 application information for environments where Cisco Network-Based Application Recognition (NBAR) is not enabled. It also works in environments where an overlay monitoring solution better fits the operations model of the IT organization. The Flow Sensor delivers comprehensive visibility of network and server performance metrics. It combines Deep Packet Inspection (DPI) and behavior analysis to identify applications and protocols. The result is optimized security, network operations, and application performance.

The volume of NetFlow data 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 software to monitor virtual machine environments. Tables 5 and 6 list the major benefits and specifications of the Flow Sensor.

Table 5. Major Benefits of the Flow Sensor

Benefit	Description
Layer 7 application visibility	Provides true Layer 7 application visibility by gathering application information along with packet-level performance statistics.
Packet-level performance and analysis	Provides true Layer 7 application visibility by gathering application information along with packet-level performance statistics.
Alerts on network anomalies	Pinpoints any unusual network behavior and immediately sends an alarm 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 environment.

Table 6. Flow Sensor Specifications

	FS 1200	FS 2200	FS 3200	FS 4200
Platform	UCSC-C220-M4S	UCSC-C220-M4S	UCSC-C220-M4S	UCSC-C220-M4S
Network	• Monitoring ports: 5; 100/1000 copper • **Note:** All monitoring ports are used to receive raw network traffic. • CIMC management port: 1; 100/1000 copper • SW management port: 1; 100/1000 copper	• Monitoring ports: 5; 100/1000 copper • Monitoring ports: 2; 1 GB Base-SX LC • **Note:** All monitoring ports are used to receive raw network traffic. • CIMC management port: 1; 100/1000 copper • Stealthwatch management port: 1; 100/1000 copper	• Monitoring ports: 2; SFP-10G-SR-S 10GBASE-SR SFP Module, Enterprise-Class or SFP-10G-LR-S 10GBASE-LR SFP Module, Enterprise-Class • **Note:** All monitoring ports are used to receive raw network traffic. • CIMC management port: 1; 100/1000 copper • SW management port: 1; 100/1000 copper	• Monitoring ports: 4; 10 GB SFP+ • **Note:** All monitoring ports are used to receive raw network traffic. • CIMC management port: 1; 100/1000 copper • Stealthwatch management port1: 1; 100/1000 copper
Rated to Monitor	1 Gbps*	2.5 Gbps*	5 Gbps*	20 Gbps*
Processor	1.7 GHz E5-2609 v4	2.2 GHz E5-2650 v4	2.2 GHz E5-2650 v4	2.2 GHz E5-2650 v4
Memory	8 GB DDR4 (2x) - 16 GB total	16 GB DDR4 (16x) - 256 GB total	16 GB DDR4 (16x) - 256 GB total	16 GB DDR4 (16x) - 256 GB total
Storage	300 GB HDD (2x) - 600 GB total RAID1	300 GB HDD (6x) - 1.2 TB total RAID6	300 GB HDD (6x) - 1.2 TB total RAID6	300 GB HDD (6x) - 1.2 TB total RAID6

	FS 1200	FS 2200	FS 3200	FS 4200
Throughput	1 Gbps	2.5 Gbps	5 Gbps	20 Gbps
Power	• Redundant 750W AC 50/60 • Auto Ranging (100v to 240V)	• Redundant 750W AC 50/60 • Auto Ranging (100v to 240V)	• Redundant 750W AC 50/60 • Auto Ranging (100v to 240V)	• Redundant 750W AC 50/60 • Auto Ranging (100v to 240V)
Heat dissipation	664.86 BTU per hour maximum (estimated)	1164.77 BTU per hour maximum (estimated)	1149.71 BTU per hour maximum (estimated)	1282.64 BTU per hour maximum (estimated)
Dimensions	• Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm)	• Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm)	• Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm)	• Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm)
Unit Weight	37.9 pounds (17.2 kg)	37.9 pounds (17.2 kg)	37.9 pounds (17.2 kg)	37.9 pounds (17.2 kg)
Temperature	• Operating: 41° F to 95° F (5° C to 35° C) • Derate the maximum temperature by 1°C for every 305 meters of altitude above sea level. • Storage: -40° F to 149° F (-40° C to 65° C)	• Operating: 41° F to 95° F (5° C to 35° C) • Derate the maximum temperature by 1°C for every 305 meters of altitude above sea level. • Storage: -40° F to 149° F (-40° C to 65° C)	• Operating: 41° F to 95° F (5° C to 35° C) • Derate the maximum temperature by 1°C for every 305 meters of altitude above sea level. • Storage: -40° F to 149° F (-40° C to 65° C)	• Operating: 41° F to 95° F (5° C to 35° C) • Derate the maximum temperature by 1°C for every 305 meters of altitude above sea level. • Storage: -40° F to 149° F (-40° C to 65° C)
Virtual Appliance	L-ST-FS-VE-K9			

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

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. Tables 7 and 8 list the major benefits and specifications of the UDP Director.

Table 7. 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.

Table 8. UDP Director Specifications

	UDP Director 2200
Hardware Platform	UCSC-C220-M4S
Network	• Monitoring ports: 3; 100/1000 copper **Note:** All monitoring ports are enabled in promisc mode by default. If desired, you can use them to receive all packets on those interfaces (ingress only) and forward only those matched in any forwarding rules.

	UDP Director 2200
	• Reserved ports: 2; 1 GB Base-SX LC • CIMC management port: 1; 100/1000 copper • Stealthwatch management port: 1; 100/1000 copper • HA Cross Connect ports: 2 **Note:** HA ports are used only in an HA environment where two UDPD2000 series appliances are cross-connected and HA configurations have been provisioned. (Refer to the Stealthwatch System Hardware Configuration Guide for details.
Processor	2.2 GHz E5-2650 v4
Memory	16 GB DDR4 (16x) - 256 GB total
Storage	300 GB HDD (6x) - 1.2 TB total RAID6
Power	• Redundant 750W AC 50/60 • Auto Ranging (100v to 240V)
Heat dissipation	1164.77 BTU per hour maximum (estimated)
Dimensions	• Height: 1.7 inches (4.3 cm) • Width: 16.9 inches (42.9 cm) • Depth: 29.8 inches (75.8 cm)
Unit Weight	37.9 pounds (17.2 kg)
Temperature	• Operating: 41° F to 95° F (5° C to 35° C) Derate the maximum temperature by 1°C for every 305 meters of altitude above sea level. • Storage: -40° F to 149° F (-40° C to 65° C)
Virtual Appliance	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 C78-739398-02 10/17