Cisco Stealthwatch Enterprise

Contents

Solution overview

Cisco Stealthwatch® Enterprise provides enterprise-wide network visibility and applies advanced security analytics to detect and respond to threats in real time. Using a combination of behavioral modeling, machine learning, and global threat intelligence, Stealthwatch Enterprise can quickly, and with high confidence, detect threats such as command-and-control (C&C) attacks, ransomware, distributed-denial-of-service (DDoS) attacks, illicit cryptomining, unknown malware, and insider threats. With a single, agentless solution, you get comprehensive threat monitoring across the entire network traffic, even if it's encrypted.

Organizations have already invested a lot into their IT infrastructure and security. Yet, threats are finding ways to get through. Moreover, it takes them months or even years to detect threats. This lack of visibility is a function of the growing network complexity as well as the constantly evolving threats. And security teams with their limited resources and disjointed tools can only do so much. We all have security solutions, such as firewalls, but how do we know those are working, managed, and configured properly? How do we know these tools are doing the job that we need them to do?

We decided to turn the problem on its head—why not enlist your existing investment, the network, to secure your organization? The network telemetry is a rich data source that can provide useful insights about who is connecting to the organization and what they are up to. Everything touches the network, so this visibility extends from the HQ to the branch, data center, roaming users, and smart devices. And also, from the private to the public cloud. Analyzing this data can help detect threats that may have found a way to bypass your existing controls, **before** they are able to have a major impact.

The solution is Cisco Stealthwatch, which enlists the network to provide end-to-end visibility of traffic. This visibility includes knowing every host—seeing who is accessing which information at any given point. From there, it's important to know what is normal behavior for a particular user or "host" and establish a baseline from which you can be alerted to any change in the user's behavior the instant it happens.

Stealthwatch offers different deployment models—on-premises as a hardware appliance or a virtual machine called Stealthwatch Enterprise—or cloud-delivered as a software-as-a-service (SaaS) solution called Stealthwatch Cloud.

Primary use cases

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

- Real-time threat detection
  - Unknown threat—Identify suspicious behavior and communications to malicious domains
  - Insider threat—Get alarmed on data hoarding or exfiltration, suspicious lateral movement
  - Encrypted malware—Use multilayered machine learning to analyze traffic without decryption
  - Policy violation—Ensure security and compliance policies set in other tools are enforced
- Incident response and forensics
- Network segmentation
- Ability to satisfy regulatory requirements
- Network performance and capacity planning

Key benefits

- **No more blind spots**—Stealthwatch is the only security analytics solution that can provide comprehensive visibility in the private network as well as the public cloud, and without deploying sensors everywhere. It is also the first solution to detect malware in encrypted traffic, without any decryption.
- **Focus on incidents, not noise**—Using the power of behavioral modeling, multilayered machine learning, and global threat intelligence, Stealthwatch reduces false positives and alarms on critical threats affecting your environment.
- **Catch them in the act**—Stealthwatch is constantly monitoring the network in order to detect advanced threats in real time. Attacks are usually preceded by activities such as port scanning, constant pinging, etc. Stealthwatch can recognize these early signs to prevent high impact. Once a threat is identified, you can also conduct forensic investigations to pinpoint the source of the threat and determine where else it might have propagated.
- **Make the most of your investment**—With a single, agentless solution, you are using the rich telemetry generated by your existing network infrastructure to improve your security posture.
- **Scale security with business growth**—Now there's no need to compromise on security as the business needs change. Whether you are adding a new branch or a data center, moving workloads to the cloud, or simply adding more devices, Stealthwatch deployment can be expanded easily to provide coverage. It can be deployed on-premises or on the cloud, can be consumed as a SaaS-based or license-based solution, and has the automatic role classification capability to automatically classify new devices being added to the network.

Encrypted Traffic Analytics

The rapid rise in encrypted traffic is changing the threat landscape. As more businesses become digital, a significant number of services and applications are using encryption as the primary method of securing information. Encryption technology has enabled much greater privacy and security for enterprises that use the Internet to communicate and transact business online. However, threat actors have leveraged these same benefits to evade detection and to secure their malicious activities.

Traditional threat inspection with bulk decryption, analysis, and re-encryption is not always practical or feasible, for performance and resource reasons. Also, it compromises privacy and data integrity.

Cisco, with its expertise in the network infrastructure market, conducted extensive research and has introduced an innovative and revolutionary technology, Encrypted Traffic Analytics (ETA). It helps illuminate the dark corners in encrypted traffic without any decryption by using new types of data elements or telemetry that are independent of protocol details. This enhanced ETA telemetry is generated by the next-generation Cisco® routers, switches, and wireless controllers, as well as the Stealthwatch Flow Sensor. Stealthwatch analyses this ETA telemetry to detect threats in encrypted traffic as well as to ensure cryptographic compliance.

Solution components

At the core of Stealthwatch Enterprise are the required components: the Flow Rate License, Flow Collector, and Management Console. In addition, optional components like the Flow Sensor and the UDP (User Datagram Protocol) Director are also available. Following are other optional licenses available for added functionality:

- Cisco Stealthwatch Endpoint License: Available as a license add-on to extend visibility to end user devices. (Requires Cisco AnyConnect® Network Visibility Module to be purchased separately.)
- Cisco Stealthwatch Cloud: Available as an SaaS product offer to provide visibility and threat detection within public cloud infrastructures such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
- Cisco Stealthwatch 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.

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 (Internet Protocol Flow Information Export), 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 cloud-based, multilayered machine learning engine, Cognitive Intelligence, for deep visibility into both web and network traffic. Please note that the Cognitive Intelligence feature is built into the system at no extra cost, but 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.

Benefit	Description
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 or KVM Hypervisor environment. This solution scales dynamically according to the resources allocated to it.

Flow Collector specifications

- Stealthwatch Flow Collector 4210—Part number: ST-FC4210-K9
- Stealthwatch Flow Collector 5210—Part number: ST-FC5210-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

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, 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.

Benefit	Description
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 or KVM Hypervisor environment.

Management Console specifications

- Stealthwatch Management Console 2210–Part number: ST-SMC2210-K9
- Stealthwatch Management Console Virtual Edition can be configured as either SMC VE or SMC VE 2000–Part number: L-ST-SMC-VE-K9

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. And starting with Stealthwatch Software Release 7.1, Flow Sensor is also able to generate enhanced ETA telemetry to be able to analyze encrypted traffic. 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. This includes data features like RTT (Round trip time), SRT (Server Response Time), and Retransmissions.
Packet-level performance and analysis	Provides true Layer 7 application visibility by gathering application information. This includes data features like RTT, SRT, and 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.

Benefit	Description
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.

Flow Sensor specifications

- Stealthwatch Flow Sensor 1210—Part number: ST-FS1210-K9
- Stealthwatch Flow Sensor 3210—Part number: ST-FS3210-K9
- Stealthwatch Flow Sensor 4210—Part number: ST-FS4210-K9
- Stealthwatch Flow Sensor Virtual Edition—Part number: L-ST-FS-VE-K9

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 applies to the UDP Director 2210 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 2210—Part number: ST-UDP2210-K9
- Cisco Stealthwatch UDP Director Virtual Edition—Part number: L-ST-UDP-VE-K9

Ordering information

Stealthwatch is available as a one-, three-, and five-year term subscription. The Cisco Stealthwatch ordering guide provides more details about 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

Flexible payment solutions to help you achieve your objectives

Cisco Capital® makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about Cisco Stealthwatch, visit 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 C78-739398-07 06/20