Cisco Stealthwatch System

Benefits

- **Gain visibility** across all network conversations, including east-west and north-south traffic, to detect both internal and external threats
- **Conduct advanced security analytics** and obtain in-depth context to detect a wide range of anomalous behaviors that may signify an attack
- **Accelerate and improve threat detection**, incident response, and forensics across the entire network
- **Enable deeper forensic investigations** with audit histories of network activity
- **Simplify compliance**, network segmentation, performance monitoring, and capacity planning

Extend Visibility Across the Network for Enhanced Security Analytics and Threat Detection

Today's enterprise network is more complex and distributed than ever before. New security challenges arise weekly, if not daily. The ever-evolving threat landscape, along with trends such as cloud computing and the Internet of Things, further complicates the situation. Unfortunately, as more and more users and devices are added to the network, gaining visibility into what's going on is harder to achieve. And you can't protect what you can't see.

Seeing into all traffic flows, applications, users, and devices that are known and unknown is critical to determine whether there may be anomalous behavior occurring on your network. Using sophisticated behavioral analytics, the Cisco Stealthwatch system transforms data from your existing infrastructure into actionable intelligence. You get better network visibility and security analytics for faster incident response.

Continuous Network Traffic Analysis for Faster Incident Response and Forensics

The Cisco Stealthwatch system provides real-time, continuous monitoring and pervasive views into all network traffic. It dramatically improves visibility, security, and response times to questionable incidents across the entire network.

Your security operations teams gain real-time situational awareness of all users, devices, and traffic, so they can quickly and effectively respond to threats before, during, and after a security incident.

The Cisco Stealthwatch system applies context-aware analysis to automatically detect anomalous behaviors. It can identify a wide range of attacks, including malware, zero-day attacks, distributed denial-of-service (DDoS) attempts, advanced persistent threats (APTs), and insider threats.

Extending Visibility Into the Cloud

Workloads are increasingly moving off premises and into cloud environments. This gives your organization more flexibility, but it also hinders your ability to view traffic flows within these virtual instances. However, with the Stealthwatch Cloud License, you have all the network visibility, threat detection, and analytics capabilities of Cisco Stealthwatch in public, private, and hybrid cloud environments. Stealthwatch Cloud License is a virtual license add-on to Cisco Stealthwatch that extends your network as a sensor into the cloud. You gain real-time situational awareness and enhanced security across your entire infrastructure.

The license supports installation in Amazon Web Services (AWS) Cloud Computing Services. It currently supports the following host operating systems:

- Linux
- CentOS 5, 6, and 7 (x64 only)
- Red Hat Enterprise Linux 5, 6, and 7 (x64 only)

Extending Visibility to the Endpoint

In our connected world, mobility is king. But to truly monitor all network activity, security professionals need to see into the applications and processes that occur at the network edge, down to remote devices. With the Cisco Stealthwatch endpoint solution, security professionals can conduct more efficient, context-rich investigations into user machines that exhibit suspicious behavior.

Tightly integrated with the Cisco AnyConnect® Network Visibility Module, the Stealthwatch Endpoint License provides network visibility while enhancing the investigation of endpoints. Security analysts gain easy access to endpoint applications and the information they need to speed incident response and remediate policy violations quickly.

Endpoint Solution Components

- **StealthwatchEndpoint License:** Provides visibility to analyzed endpoint data in the Stealthwatch console.
- **Stealthwatch Endpoint Concentrator:** Collects IPFIX data from the Cisco AnyConnect Visibility Module. Data is collected from all endpoint devices and is passed through the Endpoint Concentrator to the StealthwatchFlow Collector.

Extending Visibility Across Proxy Servers

Many organizations rely on proxy servers to boost their security posture and enforce web policies. This is helpful to the organization, but it can disrupt visibility and create a place for attackers to hide. The Cisco Stealthwatch solution aims to close that gap by consuming proxy logs and integrating them into the flow record. The Proxy License obtains additional context around the conversations from the other side of the proxy. Turns proxy servers into a security boon instead of a hindrance by integrating proxy logs and correlating them with the appropriate flows User, application, and URL data is preserved. Not only is traffic monitoring maintained across the proxy, thus reducing investigation times, but it also further informs the Stealthwatch analytics engine, so security operators can identify threat activity more quickly and accurately.

The Proxy License feature supports the following web proxies:

- Cisco® Web Security Appliance
- Blue Coat
- McAfee
- Squid

Extending Visibility to Branch Locations

Gaining visibility across branch traffic, as well as traffic between branches, is critical to securing your network. Cisco Stealthwatch Learning Network License uses the Cisco Integrated Services Router (ISR) as a security sensor to gain deep visibility into a specific branch router's traffic flow. It also uses behavioral analytics with machine learning, packet capture, and immediate local detection of threats at the branch level. Learning Network License is an algorithmic based anomaly detector. The Cisco Stealthwatch solution is a historical and statistical anomaly detector. Together, the solutions deliver broad and deep branch-level visibility.

Cisco Stealthwatch provides:

- Deep visibility across the network perimeter, interior, data center, and private and public clouds, and down to the endpoint
- A simplified understanding of normal network behavior, with NetFlow establishing a baseline for pinpointing anomalous behavior
- Continuous monitoring of devices, applications, and users throughout distributed networks
- Advanced security analytics and intelligence to detect a wide range of behaviors that could signify an attack
- Acceleration of incident response times with real-time threat detection
- Superior forensic investigations with comprehensive network audit trails
- Simplified capabilities for network segmentation, compliance validation, and troubleshooting and diagnostics

"When I walk into an organization and I know I need a basic understanding of what's happened or [what's] going on, Stealthwatch has always come through for me. ... Stealthwatch's greatest asset for my team has been [that] when no one's paying attention, Stealthwatch is in the background still watching."

– Phil Agcaoili.
CISO, Elavon

"[Stealthwatch] has provided us with better visibility into network activity across our global enterprise. The near real-time data reporting and alerting capabilities enable our team to detect and respond quicker to security incidents as they occur."

– Jeff DeLong.
Information Security Architect, Westinghouse Electric Company, LLC

"[Stealthwatch] is a product that provides so much insight into what is really happening within your network, and gives the best blend of advance notice of problems combined with historic reporting using standard flow data. Couple this with outstanding support, sales, marketing, and active collaboration with customers and it's a winning solution."

– Steve Mould.
Senior IT Architect, Experian

Integration Across the Cisco Portfolio

Cisco Stealthwatch enhances our "Security Everywhere" strategy and supports network security and visibility across the extended enterprise.

As a critical part of our Network as a Sensor and Network as an Enforcer initiatives, Cisco Stealthwatch turns NetFlow data into actionable intelligence. It helps you turn your network into a sensor. You gain deep visibility into all network traffic to identify potential network threats.

The combination of Cisco Stealthwatch and the Cisco Identity Services Engine helps organizations get a 360-degree view, respond to threats faster, and protect a growing digital business. By using these two solutions together, you can see details about each individual device: type, operating system, compliance status, connection method, geographical location, and more. Discover anomalous traffic in your environment and know exactly when an individual user's behavior becomes suspicious.

Cisco has now combined the capabilities of NetFlow analysis and packet analysis: We have integrated the Cisco Stealthwatch solution and the Cisco Security Packet Analyzer. Both of these types of technologies can assist in troubleshooting security and network incidents, but one is often sacrificed for the other, usually because of budget concerns or a lack of resources. Our targeted approach enables you to store only packets of interest, reducing storage costs while providing a more detailed, context-rich record of what happened on the network. The added visibility and security context provided by NetFlow is combined with a more precise and cost-effective means of obtaining packet-level data to help you further investigate a specific issue when necessary.

Next Steps

The Cisco Stealthwatch solution collects and analyzes massive amounts of network data to deliver comprehensive visibility and protection for even the largest, most dynamic networks. To learn more, visit http://www.cisco.com/go/Stealthwatch or contact your local Cisco account representative.

C45-736510-01 03/17