Cisco Stealthwatch Improves Threat Defense with Network Visibility and Security Analytics

BENEFITS

- Gain visibility across all network conversations, including east-west and north-south traffic, to detect 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 to reduce enterprise risk
- Enable deeper forensic investigations with audit histories of network activity
- Simplify compliance, network segmentation, performance monitoring, and capacity planning by extending visibility across the network

If you're looking for comprehensive network visibility across internal and distributed networks, look no further. Using sophisticated behavioral analytics, the Cisco Stealthwatch™ system transforms data into intelligence you can use. You strengthen your security and can respond to incidents faster.

Today's enterprise network is more complex and distributed than ever before. New security challenges arise weekly. The ever-evolving threat landscape, along with trends such as cloud computing and the Internet of Things, further complicates the situation. Unfortunately, as 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.

Cisco Stealthwatch collects and analyzes massive amounts of data to give even the largest, most dynamic networks comprehensive internal visibility and protection. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic on the extended network so they can quickly and effectively respond to threats.

With continuous monitoring and intelligence, you can detect a wide range of attacks. You can identify behaviors related to zero-day malware, insider threats, advanced persistent threats (APTs), distributed denial of service (DDoS) attempts, and other attacks before they wreak havoc on your network. Unlike other security monitoring solutions, Cisco Stealthwatch monitors not only traffic going in and out of the network but also lateral, or east-west, traffic inside the network to identify network abuse and insider threats.

More Attacks, Less Visibility

Today's threat surface has never been bigger or more complex. Networks are everywhere, and companies are continuously acquiring new companies, adding new locations, and opening branch offices. Users access your network from their own smart devices, from wherever they are. Corporate apps, servers, and data are in the cloud. As the network continues to expand, visibility into what is happening on the network continues to be more challenging.

Simultaneously, attackers are more sophisticated, agile, and organized than ever before, so visibility into any hallmark of suspicious behavior on the network is critical for defense against attacks. In security, understanding comes from visibility.

In order to get to more effective security, we need visibility to see what is occurring across the entire network. A lack of visibility effectively limits the ability to deliver network diagnostics and compliance validation. And it complicates your ability to protect the interior of the network from threats both inside and outside the network. Visibility into the network is critical to securing the complex enterprise. You need to see traffic flows, applications, users, and devices, known as well as unknown, to determine whether there may be anomalous behavior.

Cisco Stealthwatch dramatically improves network visibility, security, and response across the entire network. It helps security operations teams gain real-time situational awareness of all users, devices, and traffic on the network, in the data center, and in the cloud, so they can quickly and effectively respond to threats.

Architecture and Components

The Flow Collector, Flow Sensor, and Management Console are the core elements needed for the Cisco Stealthwatch system to provide visibility across the network. These elements can be delivered as physical or virtual appliances, along with their respective licenses.

The Flow Collector ingests telemetry from network devices and mechanisms. These include the Cisco Network Based Application Recognition (NBAR), NetFlow Security Event Logging (NSEL), NetFlow, and syslog. Data is collected, analyzed, and stored. A minimum of one collector is required, and up to 25 Flow Collectors can be supported in a deployment

The Flow Sensor is useful in areas of the network where devices do not natively support NetFlow. Flow Sensors gather application information, along with packet-level performance statistics, from business-critical, peer-to-peer, social media, and mobile applications. URL information is also provided in flow records generated by the Flow Sensor. Traffic data can be sent to the Flow Sensor, and the sensor can then send it on to a Flow Collector.

All this information from the Flow Collectors are brought into a central point, the Management Console, and only one console is needed to visually represent all the data collected.

> "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**

Continuous Network Monitoring

With in-depth insight into everything going on across the network, you can quickly baseline your environment's normal behavior, no matter what your organization's size or type is. This knowledge makes it easier to identify something suspicious. You can also identify and appropriately segment critical network assets to improve access control and protection.

Postincident Forensics

The Cisco Stealthwatch system goes beyond improving real-time threat detection. It dramatically speeds up incident response time, often reducing troubleshooting from days or months to minutes. The ability to store network data for months or even years provides an invaluable audit trail of all network activity, so you can easily conduct precise postincident forensic investigations.

Besides providing a comprehensive view of network traffic, Cisco Stealthwatch offers additional levels of security context. These include user and device awareness, cloud visibility, application awareness, and threat feed data.

Cisco Stealthwatch Versus Other Security Technologies

The Cisco Stealthwatch system collects and analyzes network telemetry such as flow (NetFlow, sFlow, JFlow, etc.) from your routers, switches, and firewalls to monitor network and user behavior. The system conducts sophisticated, proprietary analytics on network data to automatically detect abnormal behaviors that may signify an attack.

Sometimes Cisco Stealthwatch is compared with other monitoring solutions such as security information and event management (SIEM) and full packet capture. SIEM technology tracks syslog from network assets and issues alerts and alarms from signature-based tools. Unfortunately, syslog originating from compromised machines is unreliable, and signature-based monitoring tools can see only what they have access to, missing behavioral changes.

Meanwhile, full packet capture can be deployed only in limited areas of the network due to its extremely high cost and complexity. Supplementing these information sources with pervasive, behavioral-based monitoring is critical for filling in dangerous security gaps. Additionally, Cisco Stealthwatch can be used along with the Cisco® Security Packet Analyzer to capture and examine packets correlated to an anomalous traffic flow generated by a Cisco Stealthwatch alarm.

Cisco Stealthwatch capabilities also surpass those of competing security technologies (including other flow-based monitoring tools) because it is so scalable. The ability to de-duplicate and stitch together unidirectional flow records results in cost-effective flow monitoring and storage for even the largest, most complex enterprise networks.

> "[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**

Components

The Cisco Stealthwatch system can be customized, but its core components are the Flow Collector, Flow Sensor, and the Management Console. As noted, these are delivered as either physical or virtual appliances, along with the appropriate licenses. Here is how the components work together:

- Flow Collectors draw on NetFlow, IPFIX, and other types of telemetry data from your existing infrastructure. They give you cost-effective, end-to-end visibility across the enterprise network.

- The Management Console manages, coordinates, and configures all Cisco Stealthwatch products to correlate real-time security and network intelligence across the enterprise.
- Flow Sensor uses a combination of deep packet inspection (DPI) and behavioral analysis to identify applications and protocols in use across the network. It is used in places on the network where NetFlow is not supported.
- UDP Director is a high-speed, high-performance appliance that receives essential network and security information from multiple locations. It forwards the information in a single data stream to one or more destinations such as the Flow Collector.
- The Threat Intelligence License taps into global threat intelligence. It generates alerts and a Concern Index of events to flag suspect communications so they can be swiftly investigated.
- The Proxy License ingests proxy records and associates them with the flow records. It delivers the original user, application, and URL information for each flow so you can monitor network conversations that pass through web proxies.
- Endpoint solution components include the Endpoint License and Endpoint Concentrator. The 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 Flow Collector to provide visibility to analyzed endpoint data in the Management Console.
- The Cloud License is a virtual license add-on to the Cisco Stealthwatch system. It extends your network as a sensor into the cloud, so you can see flows within a virtual instance within the Management Console.
- The 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 detection of threats at the branch level.

Use Cases

All industries	• Continuously monitor the extended network • Detect threats in real time • Speed incident response and forensics • Simplify network segmentation • Meet regulatory compliance requirements • Improve network performance and capacity planning
Retail	• Remotely monitor hundreds of systems for security and performance issues • Safeguard point-of-sale (POS) terminals • Maintain PCI compliance
Healthcare	• Protect patient records • Thwart cyber attacks on life-saving medical equipment • Maintain HIPAA compliance • Safeguard intellectual property • Maintain high levels of performance • Quickly discover and safeguard new network devices
Financial services	• Detect both outsider and insider threats • Protect customer data • Uphold strict compliance requirements • Maintain 24-hour access to critical financial information • Find and fix threats and performance issues before they become crises
Government	• Continuously monitor across networks for advanced attacks • Protect confidential information • Maintain compliance with stringent security regulations • Detect insider threats

Higher education	• Safeguard mobile devices • Detect peer-to-peer (P2P) file sharing • Protect sensitive information • Prevent network misuse and abuse • Maintain high levels of availability and performance • Streamline security workflows • Meet regulatory compliance demands

Why Cisco?

As the inventor of NetFlow, Cisco is uniquely positioned to offer a security solution that uses flow data for network visibility. Beginning in 2000, Lancope pioneered the use of telemetry data to gain in-depth network and security insight with its StealthWatch system. By collecting and analyzing NetFlow, IPFIX, and other types of network telemetry data, StealthWatch turned the network into an always-on virtual sensor and applied sophisticated behavioral analytics to detect a wide range of attacks and elevate the security posture of hundreds of enterprises worldwide. Now, Cisco Stealthwatch provides you with the best of these two parallel technology development efforts.

Deploying Stealthwatch Simply and Professionally

Certified professional services organizations and certified partners offer years of experience designing, deploying, and managing the Cisco Stealthwatch product family. With broad customer and industry experience, an outside services team can help you optimize deployments to meet specific business requirements, increase productivity, and reduce risk. Using a unique combination of network and security skills, the team quickly and effectively implements a Cisco Stealthwatch system to meet the intense demands of today's advanced threat environment.

Cisco professional services include initial installation, health check and tuning, host group automation, proxy integration, and system training, as well as custom consulting and integration services.

> "[Stealthwatch] allows us to gain internal network visibility … and easily audit our secure zones to ensure certain types of traffic are not leaving those networks."
>
> **— Ryan Laus, Network Administrator, Central Michigan University**

Cisco Capital

Financing to Help You Achieve Your Objectives

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.

Next Steps

To learn more, visit http://www.cisco.com/go/stealthwatch or contact your local Cisco account representative.

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.

Printed in USA C22-736505-01 03/17