Solution Overview

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

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, 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 networks are more complex and distributed than ever. As organizations acquire new businesses and expand branch and remote locations, the network perimeter extends which makes it more difficult to defend. And more users are connecting to these networks with more devices, from more places than ever before. As the network continues to expand, visibility into what is happening will continue 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. And a lack of visibility effectively limits the ability to deliver network diagnostics and compliance validation. It complicates your ability to protect the interior of the network from threats both inside and outside the network. Visibility into all activity is critical to securing complex networks. You need to see traffic flows, applications, users, and devices, known as well as unknown, to determine whether there may be anomalous behavior.

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. And with Cognitive Analytics, a cloud-based threat detection and analytics capability, you can get deep visibility into both web and network traffic. This additional contextual information helps you identify and prioritize new and emerging threats across the extended network.

> "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.

Post-Incident Forensics

The 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 post-incident forensic investigations.

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

Analyzing encrypted traffic for improved security

Encryption is important in security. But although you may use encryption to protect data and privacy, attackers use it to conceal malware and evade detection by network security products. With Stealthwatch and its enhanced analytics capabilities, you can better understand whether encrypted traffic on the network is malicious. Stealthwatch applies machine learning and statistical modeling for encrypted traffic analytics to enhance NetFlow analysis. Cognitive Analytics can learn from what it sees and adapt to changing network behavior over time. The network telemetry is collected through the Flow Collector and is sent to Cognitive Analytics for further analysis. Stealthwatch with Cognitive Analytics improves visibility into traffic flows by centralizing the management of network and web traffic within the Management Console. Rather than decrypt the traffic, Stealthwatch with Cognitive Analytics pinpoints malicious patterns in encrypted traffic to identify threats and accelerate the appropriate response.

Stealthwatch Versus Other Security Technologies

The Stealthwatch system collects and analyzes network telemetry such as flow (NetFlow, sFlow, JFlow, IPFIX, 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 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, 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 Stealthwatch alarm.

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**

Architecture and Components

The Stealthwatch system can be customized, but its required core components are the Flow Rate License, Flow Collector, and the Management Console. Here is how the components work together:

- 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).

- The Flow Collector leverages NetFlow, IPFIX and other types of flow data from existing infrastructure such as routers, switches, firewalls, proxy servers, endpoints and other network infrastructure devices. The data is collected and analyzed to provide a complete picture of network activity.
- 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 Flow Sensor is used in places on the network where flow telemetry data is not supported. It uses a combination of Deep Packet Inspection (DPI) and behavioral analysis to identify applications and protocols in use across the network.
- 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 Stealthwatch Cloud License is an add-on license offering greater visibility and enhanced awareness of the activity and potential threats to existing implementations across public, private, and hybrid cloud network infrastructures.
- The Stealthwatch Endpoint License is an add-on license that provides more efficient, context-rich investigations into end user devices that are exhibiting suspicious behavior. The license permits endpoint data collected by the AnyConnect NVM to be exported and analyzed in the Management Console.
- The 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.
- The Threat Intelligence License taps into global threat intelligence feeds to generates alerts and a Concern Index of events to flag suspect communications so they can be swiftly investigated.

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 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 Stealthwatch system to meet the intense demands of today's advanced threat environment.

Stealthwatch 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

Visit http://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 www.cisco.com/go/offices.

Printed in USA C22-736505-02 06/17