StealthWatch Improves Threat Defenses with Pervasive Network Visibility and Security

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 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 complicate 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.

StealthWatch alleviates this problem. It collects and analyzes massive amounts of data to give even the largest, most dynamic networks comprehensive internal visibility and protection. StealthWatch 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 StealthWatch's continuous monitoring and intelligence, you can detect a wide range of attacks. You can thwart 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 governments and corporations face an ever-increasing deluge of cyber attacks. It is painfully clear that conventional security solutions like firewalls, antivirus tools, and intrusion prevention systems (IPSs) are no longer enough to keep confidential data out of the hands of attackers. No matter how many technologies a company deploys at the edge of its network, intruders will get in one way or another. They’ll use zero-day attacks, stolen access credentials, infected mobile devices, a vulnerable business partner, or other methods.

More and more, attackers aren’t even hacking. They simply access readily available credentials and log in. An attacker just has to find the right employee to manipulate, and suddenly he or she has all the benefits of an inside user. As a result of this social engineering trend, employees are increasingly becoming insider threats, often without their knowledge. Companies are suffering because they are too focused on securing the perimeter and take too long to detect an attacker within their networks.

If you want to win the cyberwar, you have to know what is going on inside your network, not just what is happening outside the perimeter. This is especially true today. More than 80 percent of network traffic travels east to west inside the data center, never crossing the perimeter. Unfortunately, traditional security technologies like security information and event management (SIEM) systems and full packet capture provide little visibility into the internal network. Moreover, these approaches are not often feasible when scaled beyond limited deployments.

StealthWatch Architecture and Components

The two-tier StealthWatch architecture includes the StealthWatch FlowCollector and the StealthWatch Management Console appliances. They are delivered as either physical or virtual appliances along with flow collection licenses.

The StealthWatch FlowSensor delivers comprehensive visibility of the network and server performance metrics through deep packet inspection (DPI). If an organization’s network does not support NetFlow, the FlowSensor is deployed as an appliance that generates network telemetry data. The FlowSensor’s telemetry data is sent to the FlowCollector, which conducts behavioral analysis. It identifies applications and protocols to optimize security, network operations, and application performance.

With the FlowCollector, StealthWatch can store and analyze as many as 4000 telemetry sources at 240,000 sustained flows per second. As many as 25 FlowCollectors can be aggregated on the same network for up to six million flows per second.

> “StealthWatch reduces problem-solving from days to seconds. With StealthWatch, we can stay ahead of potential attacks and breaches.”
> **— Edge Web Hosting**

Main Capabilities

StealthWatch uses your existing infrastructure investments to provide truly pervasive visibility and security intelligence across the entire enterprise network.

Continuous Network Monitoring

With in-depth insight into everything going on across the network, organizations of any type and size can quickly baseline their environment’s normal behavior. This knowledge makes it easier to identify something suspicious. Organizations can also identify and appropriately segment critical network assets to improve access control and protection.

Early Threat Detection

StealthWatch applies context-aware security analysis to automatically detect anomalous behaviors. It can identify a wide range of attacks, including malware, zero-day attacks, DDoS, APTs, and insider threats. Unlike other security monitoring solutions, it monitors not only traffic going in and out of the network but also lateral (east-west) traffic. It thus uncovers network misuse and abuse as well as attackers operating inside the network.

Post-Incident Forensics

StealthWatch 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, making StealthWatch critical for conducting 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.

StealthWatch Versus Other Security Technologies

StealthWatch 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 StealthWatch is compared with other monitoring solutions such as 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.

StealthWatch's capabilities also surpass those of competing security technologies (including other flow-based monitoring tools) because it is so highly 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.

> "Lancope's solution 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 quickly to security incidents as they occur."
>
> **— Jeff DeLong, Information Security Architect, Westinghouse Electric Company, LLC**

StealthWatch Components

StealthWatch can be customized, but its core components are the FlowCollector and the Management Console. As noted, these are delivered as either physical or virtual appliances. Here is how the components work together:

- FlowCollectors 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 entire enterprise network.
- The Management Console manages, coordinates, and configures all StealthWatch products to correlate real-time security and network intelligence across the enterprise.

- FlowSensor uses a combination of 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 then forwards the information in a single data stream to one or more destinations such as the FlowCollector.
- The StealthWatch Labs Intelligence Center (SLIC) Threat Feed taps into global threat intelligence. It generates alerts and a Concern Index of events to flag suspect communications so they can be swiftly investigated.
- ProxyWatch 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.

Use Cases

All industries	• Continuously monitor the extended network • Detect threats in real time • Speed up incident response and forensics • Simplify network segmentation • Meet regulatory compliance requirements • Improve network performance and capacity planning
Retail	• Remotely monitor hundreds of remote 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 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 StealthWatch. By collecting and analyzing NetFlow, IPFIX, and other types of network telemetry data, StealthWatch turns the network into an always-on virtual sensor and applies sophisticated behavioral analytics to quickly detect a wide range of attacks to elevate the security posture of hundreds of enterprises worldwide. Now a Cisco product, StealthWatch provides you with the best of these two parallel technology development efforts.

Deploying StealthWatch Simply, 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 organizations optimize StealthWatch 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 StealthWatch 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 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 about StealthWatch, 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 C22-736505-00 01/16