Cisco Stealthwatch

Improving visibility across your business

Know every host

Record every conversation

Understand what is normal

Be alerted to change

Respond to theats quickly

Secure Digital Businesses Demand Increased Visibility

Today's enterprise network is expanding rapidly. It connects multiple branches, mobile users, the cloud, and data centers. Organizations are moving away from traditional IT infrastructure and towards a digital-ready network infrastructure to change the way business is done. From streamlining operations and inventory management to offering new value-added services, many businesses are realizing significant benefits from digitization.

But as companies change to digital businesses and adopt new practices and technologies, they require increased visibility to maintain security.

76% of IT professionals say visibility is biggest challenge.
Source: Ponemon Institute

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, including encrypted traffic
- **Enable deeper forensic investigations** with audit histories of network activity
- **Simplify** network segmentation, performance monitoring, and capacity planning
- **Ensure enterprise compliance** by identifying the extent as well as the quality of encryption in the network
- **Achieve greater visibility and anomaly detection** with global and local traffic correlation
- **Identify insider threats** by obtaining contextual information from cloud services

Cisco Stealthwatch

Monitor · Detect · Analyze · Respond


Extended Network


Data Center


Branch


Cloud

Cisco Stealthwatch provides continuous real-time monitoring of, and pervasive views into, all network traffic. It dramatically improves visibility across the extended network and accelerates response times for suspicious incidents. It creates a baseline of normal web and network activity for a network host, and applies context-aware analysis to automatically detect anomalous behaviors. Stealthwatch 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.

Now, with Cognitive Analytics, a cloud-based threat detection and analytics capability, Cisco Stealthwatch can get additional contextual information to identify and prioritize new and emerging threats across the extended network. Stealthwatch with Cognitive Analytics has additional visibility and context into global and local traffic, and utilizes machine learning for continuous analysis and detection of command and control communications. Now, you can detect threats that have bypassed existing security controls and identify data exfiltration to legitimate cloud services.

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 Cisco 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 intraflow metadata or Encrypted Traffic Analytics to enhance NetFlow analysis. Cognitive Analytics can learn from what it sees and adapt to changing network behavior over time.

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.

Using Encrypted Traffic Analytics, Stealthwatch also ensures enterprise compliance with cryptographic protocols and visibility into and knowledge of what is being encrypted and what is not being encrypted on your network.

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 Stealthwatch, you have all the network visibility, threat detection, and analytics capabilities in public, private, and hybrid cloud environments. You gain real-time situational awareness and enhanced security across your entire infrastructure.

Extending Visibility to the Endpoints

In our connected world, mobility is king. More users are connecting to corporate networks with more devices, from more places than ever before. But to truly monitor all network activity, security professionals need the ability to look into the applications and processes that occur at the network edge, down to remote devices. With Cisco Stealthwatch Endpoint License, security professionals can conduct more efficient, context-rich investigations into user machines that exhibit suspicious behavior, accelerate incident response, and remediate policy violations quickly.

Extending Visibility to Branch Locations

Gaining network visibility across a branch network, particularly a distributed branch with multiple locations, can be complex as well as costly. Cisco Stealthwatch Learning Network License is a cost-effective solution for extending network security to branch and remote networks. You can take advantage of your existing

“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. Learn more

Cisco networking investment by using NetFlow data generated by Cisco devices to improve visibility and security on your network. It embeds security anomaly detection into the network element itself, using packet capture along with intelligent detectors to identify, mitigate, and remediate threats. The solution provides visibility without affecting bandwidth and requires interaction and data movement only when an action needs to be taken.

Security Designed to Work Together

Cisco Stealthwatch enhances visibility across the entire business by leveraging your existing network infrastructure. It turns NetFlow data into actionable intelligence, and helps to turn your network into a sensor. You gain deep visibility into all network traffic to identify potential network threats.

By integrating Stealthwatch with other Cisco Security solutions, you can gain enhanced segmentation, threat detection, and forensics capabilities across your extended networks, branches, data centers, and cloud.

The integration of Cisco Stealthwatch with the Cisco Identity Services Engine helps organizations get a 360-degree view of their extended network. Now, you can gain unique visibility across your business using your existing network as a sensor, simplify segmentation throughout your networks with centralized control and policy enforcement, and address threats faster, both proactively with threat detection and retroactively via advanced forensics.

Cisco has now combined the capabilities of NetFlow analysis and packet analysis. We have integrated Cisco Stealthwatch and the Cisco Security Packet Analyzer. Both technologies can assist in troubleshooting security and network incidents, but one is often sacrificed for the other, usually because of budget concerns or 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

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

Cisco Stealthwatch

- 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