Cisco Stealthwatch

Scalable visibility and security analytics


Extended Network


Data Center


Branch


Cloud

Have you been compromised? How would you know?

You have already invested heavily in the IT infrastructure and security for your organization. Yet, attacks are getting through and hostile internal actors operate with impunity. Moreover, it takes months or even years to detect threats[1]. This lack of threat visibility is a function of growing network complexity as well as constantly evolving attacks. And security teams, with their limited resources and disjointed tools, can only do so much. How do you know if your current security controls are working, managed, and configured properly? And how do you know these tools are doing the job that you need them to do?

The solution: Network + Security

Network packet metadata can provide useful insights about who is connecting to the organization and what they are up to. Everything touches the network, so these insights can extend from the HQ to the branch, public cloud and private data centers, roaming users, and even Internet of Things (IoT). Analyzing this data can help detect threats that may have found a way to bypass your existing controls, before they are able to have a major impact. It can also detect questionable behavior undertaken by hostile insiders. And, importantly, properly functioning analytics can lessen the burden on your security team and provide them with more opportunity to concentrate on high probability threats. This approach to advanced threat detection is:

Integrated
with your current infrastructure

Agentless
without the need for sensors to be deployed everywhere

Flexible
in terms of deployment and consumption options: on-premises or cloud, hardware/virtual appliance or SaaS

Gain confidence in your security effectiveness

Cisco Stealthwatch provides enterprise-wide visibility, from the private network to the public cloud, and applies advanced security analytics to detect and respond to threats in real-time. It continuously analyses network activities and creates a baseline of normal network behavior and then uses this baseline, along with advanced machine learning algorithms, to detect anomalies. However, not everything *weird* is malicious and Stealthwatch can quickly and with high confidence correlate anomalies to threats such as C&C attacks, ransomware, DDoS attacks, illicit cryptomining, unknown malware, as well as insider threats. With a single, agentless solution, you get comprehensive threat monitoring across the data center, branch, endpoint and cloud, regardless of the presence of network encryption.

Benefits

Know every host. See every conversation. Understand what is normal. Be alerted to change. Respond to threats quickly.

- **Continuously monitor and detect** advanced threats that have either bypassed existing security controls or originate from within
- **Focus on critical incidents, not noise** with contextual, high-fidelity alarms prioritized by threat severity
- **Respond quickly and effectively** with complete knowledge of threat activity, network audit trails for forensic investigations, and integrations with existing security controls
- **Leverage existing investments** into the IT infrastructure and use the rich network telemetry for better security
- **Scale security with growing business needs** whether you are adding a new branch or a data center, moving workloads to the cloud, or simply adding more devices
- **Ensure compliance** with policy violation alarms that can be tuned to the business logic

1. Average time to detect a breach is 197 days according to the Ponemon 2018 report.

“Cisco Stealthwatch has helped us gain visibility into the internal traffic by 100% which has resulted in the identification of threats that were extremely difficult to detect previously.”

IT Architect, Large Enterprise Industrial Manufacturing Company

Next Steps

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

C45-736510-05 11/18

Contextual network-wide visibility

Stealthwatch provides **agentless enterprise-wide visibility,** across on-premises, as well as in all public cloud environments. With knowledge of who is on the network and what they are doing, it also helps organizations to implement **smarter segmentation** customized to the business logic. And it provides **actionable intelligence** enriched with context such as user, device, location, time-stamp, application, etc.

Predictive threat analytics

Stealthwatch uses a pipeline of analytical techniques to detect advanced threats before they can turn into a breach. Using **network behavior analysis,** it can pinpoint anomalies, which are further analyzed using a combination of **supervised and unsupervised machine learning** for high-fidelity threat detection. This allows your security team to focus on the most critical threats. The Stealthwatch security analytics engine is also powered by the industry-leading **Cisco Talos threat intelligence,** that has the most up-to-date information for local-to-global threat correlation.

Automated detection and response

The combination of this context-driven enterprise-wide visibility and the application of advanced analytical techniques helps organizations to detect threats like **unknown or encrypted malware, insider threats, policy violations,** anything that “hits the wire”. Security teams can see **alarms that are prioritized by threat severity,** and have additional information to take actions easily. Stealthwatch also has the capability to store telemetry at scale, and provides network audit trails for **forensic investigations** into past events and for **compliance monitoring.** Finally, it integrates with your existing security controls in order to respond to the threat, without any business shutdown.

Analyzing encrypted traffic for improved security

The rapid rise of encrypted traffic is changing the threat landscape. While encryption is great for data privacy and security, it has also become an opportunity for cyber criminals to conceal malware and evade detection. Gartner forecasts that by 2019, 80% of all web traffic will be encrypted and 70% of the attacks will use encryption. It isn’t feasible to decrypt and analyze encrypted traffic, and soon, with the emergence of TLS 1.3, it won’t even be possible. Cisco has introduced a revolutionary technology, **Encrypted Traffic Analytics (ETA),** that is enabled by the next-generation Cisco network and Stealthwatch, to analyze encrypted traffic without any decryption. This allows organizations to 1) detect threats in encrypted traffic, and 2) perform cryptographic compliance to know how much of their digital business uses strong encryption and to audit for policy violations. To learn more, go to https://www.cisco.com/go/eta