At-a-Glance

"The Cisco Identity Services Engine prevented any unauthorized access to the network while providing highly flexible operational access management."

Mirko Berlier,
Cisco Engineer and Expo 2015 Architect

"The behavioral alarms built in to Stealthwatch gave us a whole new detection capability that we never had before."

Mike Sheck
Incident Response Team
Cisco CSIRT

Get true visibility with Stealthwatch and ISE

Use security as a growth enabler

Organizations are racing to reap the benefits of digitization, fueled by trends such as mobility, IoT, cloud, and advanced analytics. The key to these benefits is adapting networks to operate at digital speeds and keeping them secure against threats. When companies are confident about their security, they are able to innovate, adopt new technologies and develop new services. Unfortunately, in a recent survey 39% of organizations have halted a mission-critical initiative due to cybersecurity concerns.

Even when people know their system is compromised, they don't always know where it's happening and how, making them susceptible to network abuse and insider threats. Organizations need a solution that provides extensive network visibility enhanced by rich user and device details to speed up threat detection and response.

Only the combination of Stealthwatch and Cisco's Identity Services Engine helps organizations get a 360° view, respond to threats faster, and secure a growing digital business.

Get a 360° view

Respond to threats faster

Secure a growing digital business

Get a 360° view

Gain unmatched visibility and control with integration between Stealthwatch and ISE.

- Continuously monitor, analyze, separate, categorize, and store host and user information from your network with Stealthwatch.
- Enable administrators to see details about each individual device – type, operating system, compliance status, connection method, geographical location and more with ISE.
- Discover anomalous traffic in your environment. Applying context-aware security 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.
- Know exactly when individual user behavior becomes suspicious. Stealthwatch enables admins to set their own behavior thresholds, once a user crosses the threshold it triggers an alert.

A leading healthcare company uses ISE and Stealthwatch to gain visibility and get ahead of cyber attacks.

Challenge:

- Secure 500 sites and 250,000 devices across the network
- Gain visibility and control over network threats
- Meet HIPAA compliance requirements

Solution:

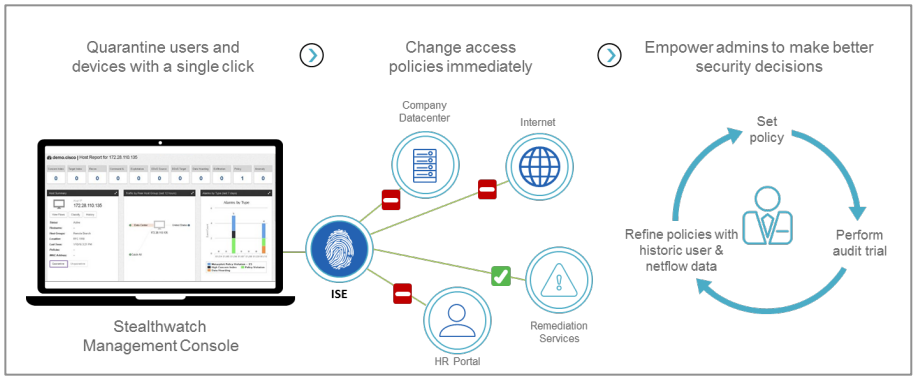
- Network as a Sensor and Network as an Enforcer with Cisco ISE and Stealthwatch
- Enforce network segmentation and user access control policies

Results:

- Deployed across all sites 6 months ahead of schedule
- Cut threat response time from days to minutes
- Ensured safety of information & compliance to HIPAA standards

Respond with Rapid Threat Containment

No matter how advanced the security, some threats will still get in. The solution isn't to build larger walls, it's about speeding up the way you respond.



- Once Stealthwatch detects anomalous traffic, it issues an alert, giving the admin the option to quarantine the user. pxGrid enables Stealthwatch to hand off the quarantine command directly to ISE.
- Admins can make a decision based on analysis, revoking users access and quarantining through ISE them with a single click. Admins don't need to modify or change the overall system policies in place because ISE reassigns the access policy of the quarantined individual.
- Find the root cause of a breach with post-incident audit trails. Stealthwatch stores records of all network activity for months or years.

For more on responding to threat faster go to: www.cisco.com/go/rtc

Secure your growing digital business

To move forward with new initiatives or technologies confidently, businesses must know they can scale without creating new security issues.

- Stop thinking about security as an obstacle and provide a foundation for network segmentation for secure access & visibility.
- Enable admins to carefully control access to sensitive assets, know precisely when someone tries to access information, and extend that visibility to any new area of the network, environment or cloud.
- Add users, devices and business without compromising network visibility. Reduce the administrative burden of setting up new devices with constantly updating device profile feeds from ISE.
- Scale the environment without creating blind spots. A deployment of Stealthwatch can process data from 50,000 flow sources at 6 million flows per second (fps) all while stitching and de-duplicating flows.
- Reduce the administrative burden associated with silo'd management sources. Network-wide flow is centrally displayed in the Stealthwatch Management Console. Easily integrate 3rd party technologies and services through a REST API.

Next Steps.

To learn more visit www.cisco.com/go/Stealthwatch, www.cisco.com/go/ise