Get True Visibility with Cisco Secure Network Analytics and Cisco Identity Services Engine (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 Secure Network Analytics (formerly Stealthwatch) and Cisco Identity Services Engine (ISE) helps organizations get a 360° view, respond to threats faster, and secure a growing digital business.

Get a 360º view

Respond to threats faster

Secure a growing digital business

Get a 360° view

Gain unmatched visibility and control with integration between Secure Network Analytics and Identity Services Engine (ISE).

- Continuously monitor, analyze, separate, categorize, and store host and user information from your network with Secure Network Analytics.
- Enable administrators to see details about each individual device – type, operating system, compliance status, connection method, geographical location and more with Identity Services Engine.
- Discover anomalous traffic in your environment. Applying context-aware security analysis to automatically detect anomalous behaviors, Secure Network Analytics can identify a wide range of attacks, including malware, zeroday attacks, Distributed Denial-of-Service (DDoS) attempts, Advanced Persistent Threats (APTs), and insider threats.
- Know exactly when individual user behavior becomes suspicious. Secure Network Analytics enables admins to set their own behavior thresholds, once a user crosses the threshold it triggers an alert unditatius.

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

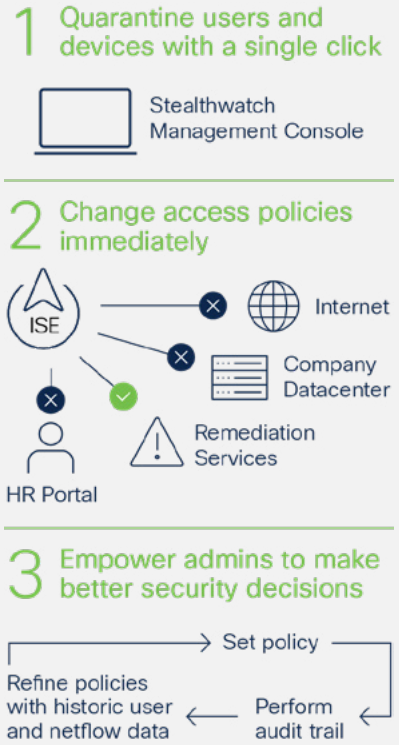
Mike Sheck
Incident Response Team, Cisco CSIRT

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 Secure Network Analytics detects anomalous traffic, it issues an alert, giving the admin the option to quarantine the user. pxGrid enables Secure Network Analytics to hand off the quarantine command directly to Identity Services Engine.
- New pxGrid enhancements found in Cisco ISE 3.3 gives a Network Admin the ability to peer into the network and locate the data needed to optimize their network and boost efficiency. Network attributes are displayed in a manner that frames the data in ways that customers can truly use, so that they are able to run their network security more effectively, leading to safer networks and less time spent on translating data.
- A Cisco-only feature called Wi-Fi Edge Analytics will allow network admins to mine data from Apple, Intel and Samsung devices to better improve profiling. Cisco Catalyst 9800 wireless controllers will pass along endpoint-specific attributes, such as model, OS version, firmware, among others, to ISE via RADIUS. From there this information will be used to profile common endpoints found on the network.
- Admins can make a decision based on analysis, revoking users access and quarantining through Identity Services Engine them with a single click. Admins don't need to modify or change the overall system policies in place because Identity Services Engine reassigns the access policy of the quarantined individual.
- Find the root cause of a breach with post-incident audit trails. Secure Network Analytics stores records of all network activity for months or years.

Learn more on responding to threats faster at:
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 and 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 **Cisco Identity Services Engine**.
- Scale the environment without creating blind spots. A deployment of **Secure Network Analytics** 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 **Secure Network Analytics** Management Console. Easily integrate 3rd party technologies and services through a REST API.

At-a-Glance

A leading healthcare company uses **Cisco Identity Services Engine** and Secure Network Analytics to gain visibility and get ead of cyber attacks.

Challenge	Solution	Results
Secure 500 sites and 250,000 devices across the network	Network as a Sensor and Network as an Enforcer with **Cisco Identity Services Engine** and **Secure Network Analytics**	Deployed across all sites 6 months ahead of schedule
Gain visibility and control over network threats	Enforce network segmentation and user access control policies	Cut threat response time from days to minutes
Meet HIPAA compliance requirements		Ensured safety of information and compliance to HIPAA standards

Learn more: cisco.com/go/SecureNetworkAnalytics and cisco.com/go/SecureNetworkAccess