The Top 10 Benefits of Cisco Stealthwatch and ISE

Today’s rapidly growing enterprise networks are becoming more digitized and dynamic.

The Result: A plethora of new security challenges. One of the most worrisome of these challenges is a lack of network visibility.

By using Cisco Stealthwatch™ technology together with the Cisco® Identity Services Engine (ISE), you can obtain critical network visibility, better control access to data and resources, and gain the upper hand against attackers. The integrated solution offers many benefits.

Here are the Top 10:

   The Cisco Stealthwatch system collects and analyzes NetFlow from your routers, switches, and firewalls. It then delivers comprehensive visibility at the network core, edge, data center, and cloud. Cisco ISE adds to this visibility with in-depth device and user data.

2. More detailed security context.
   By integrating Stealthwatch and ISE, you can see a myriad of details about network traffic, users, and devices. Instead of just a device’s IP address, Cisco ISE delivers other key details, including user name, device type, location, the services being used, and when and how the device accessed the network.

3. Faster threat detection.
   With the combination of network visibility and security context, you can detect threats faster and more comprehensively.

4. Effective network segmentation.
   Cisco ISE can help you create and enforce segmentation policies to keep unauthorized users and devices from accessing restricted areas of the network. Stealthwatch’s expansive visibility can help you determine how to most effectively segment the network, and help monitor the efficacy of your policies when they are in place.

5. Unified access control.
   With Stealthwatch and ISE, you can create, enforce, and monitor role-based access control policies throughout the entire network all from one place. ISE grants appropriate network access to users and devices based on advanced profiling capabilities. It then shares this data with Stealthwatch for more precise threat detection. Stealthwatch feeds user behavior back to ISE to immediately update access policies for suspicious or compromised users.
Dramatically improved incident response and forensics.
Stealthwatch and ISE help you quickly identify the source of an incident. When Stealthwatch detects anomalous traffic, it can send an alert to Cisco ISE to automatically quarantine the user.

Actionable security intelligence.
Use your entire network as a sensor and an enforcer by turning massive amounts of data from existing network infrastructure into actionable security intelligence.

Greater operational efficiency.
The combined solution significantly reduces the manual actions needed to detect, investigate, and remediate threats. The device onboarding burden for your IT staff is eased with self-service onboarding through ISE.

Ability to harness security as an enabler for your digital business.
With effective, scalable security across the entire network, you can more confidently expand and enhance your network through initiatives such as digitization, mobility, cloud, and the Internet of Things (IoT).

Enhanced regulatory compliance.
More easily pinpoint and remediate any violations of industry regulations such as PCI and HiPAA.

For more information about Cisco Stealthwatch and Cisco ISE, visit www.cisco.com/go/stealthwatch and www.cisco.com/go/ise, or contact stealthwatch@cisco.com.