Cisco Identity Services Engine
Security Technical Alliance

Benefits

Get Answers Faster
Organize relevant threat information on one platform instead of having to conduct lengthy investigations, traversing from system to system.

Stop Attacks Faster
Stop a threat immediately by directing ISE to contain the device. Automate your responses so you don’t have to spend time on threats that are clearly identified.

Protect Critical Data Faster
Change users’ access privileges before or after they get on the network, based on their threat score. If a device starts to act suspiciously, you can automatically deny it access to critical resources such as finance or patient records while allowing access to noncritical resources.

The Cisco® Identity Services Engine (ISE) Security Technical Alliance comprises partners whose technologies integrate with ISE. Its aim is to help improve the visibility and control of threats and vulnerabilities in the network.

Overview
The enterprise network continues to grow in complexity, with more connected devices and applications to manage than ever before. The increase in devices and applications has led to less visibility into who and what is connecting to the network and how threats can be controlled. IT departments have generally addressed these security concerns by continually adding more security systems and vendors to their networks.

However, multiple solutions from multiple vendors also produce disconnected repositories of information. All these disparate systems generate disparate data that needs to be manually pieced together to accurately identify a network threat and determine which remediating action should be taken.

Cisco ISE can help streamline this process. ISE collects valuable contextual data from across the network. This data can then be consolidated and shared across multiple systems and vendors by the Cisco Platform Exchange Grid (pxGrid). You can get answers faster. And you can use the Cisco ISE Rapid Threat Containment feature to stop security threats using the network as an enforcer.

In addition, ISE enables Security Technical Alliance partner technologies to use Structured Threat Information Expression (STIX) threat scores and the Common Vulnerability Scoring System (CVSS) to change or mitigate the access status based on a threat score. You can give access to devices that have a low risk score while denying access to devices with a higher risk score.
Cisco pxGrid

Cisco pxGrid is an open, scalable, and IETF standards-driven data-sharing and data-control platform. It allows multiple security products to work together. Security operations can automate to get answers faster and contain threats faster.

How pxGrid Improves Your Security

**Simpler integration:** Use one API for open, automated data sharing and control between more than 50 security products.

Cisco pxGrid helps enable an entire ecosystem of dissimilar IETF standards-compliant technologies to work together. You have to manage and maintain only a single interface instead of a collection of unrelated APIs.

**Instant visibility:** See all contextual and relevant data on a single screen improves time and people efficiencies.

Customize the way you share and view security data. See your security posture more clearly and concisely, including provocative events on your network. Improve staff efficiency.

**Fast investigations:** Conduct a full analysis on one system for faster answers.

Security intelligence can be shared automatically between virtually any pxGrid-integrated technologies. You don’t have to conduct lengthy investigations. Your security operations can come up with answers.

**Even faster responses:** Stop threats instantly using the network as an enforcer.

pxGrid allows any integrated and capable technology on a pxGrid instance to instruct ISE to contain a threat using the network as an enforcer so Any attack anywhere in the network can be immediately stopped.

Cisco ISE partners offer the following integrations:

- **User and entity behavior analytics (UEBA)**
  Track, collect, and assess user data and activities.

- **Mobile device management (MDM)**
  Assess posture compliance and apply network access control.

- **SIEM and threat defense**
  Gain visibility into security events throughout your network.

- **Identity access management**
  Adjust authentication policies based on risk levels and offer single sign-on.

- **Vulnerability assessments**
  Get a complete view of your vulnerabilities in a single pane.
Cisco Cloud Access Security
Protect your business from risky cloud apps.

Network and application performance
Expedite troubleshooting and resolve issues fast.

Firewall and access control
Detect and contain botnets quickly with precise policy management.

Cisco Rapid Threat Containment
Automatically contain malware to mitigate network risks.

Next Steps
To learn more about the Cisco Identity Services Engine (ISE) visit www.cisco.com/go/ise
To learn more about Cisco Rapid Threat Containment visit www.cisco.com/go/rtc
To view the list of Cisco ISE Security Technology Alliance Partners go to www.cisco.com/go/csta
Additional detailed information regarding specific partners is searchable in the Cisco Marketplace Solutions Catalog at http://marketplace.cisco.com/catalog