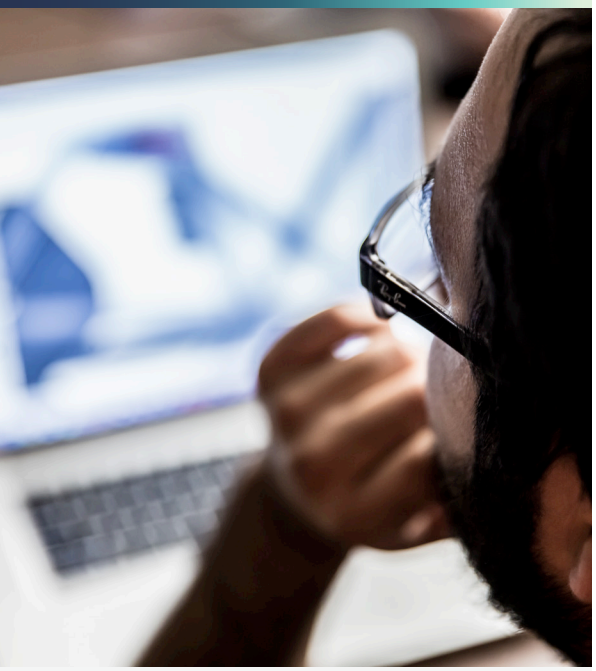
At-a-Glance



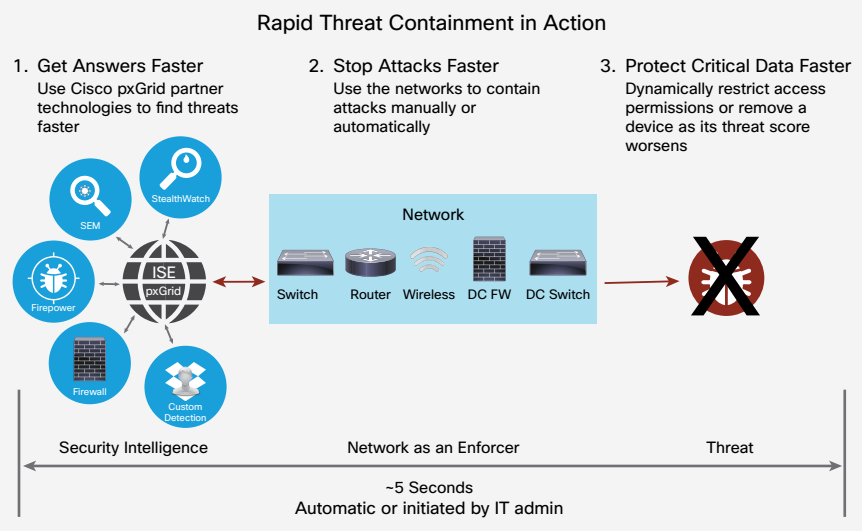
Cisco Rapid Threat Containment

Stop Threats Before They Stop You

Cisco® Rapid Threat Containment makes it easy to get fast answers about threats on your network and to stop them even faster. It uses an open integration of Cisco security products, technologies from Cisco partners, and the extensive network control of the Cisco Identity Services Engine (ISE).

With integrated network access control technology, you can manually or automatically change your users' access privileges when there's suspicious activity, a threat. or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.

Rapid Threat Containment turns your security intelligence and response technologies into an integrated operation to see and stop threats wherever and whenever they occur in your network.



Note: In this figure, the network comprises switches, routers, wireless controllers, data center firewalls, and data center switches.

Benefits

- **Get answers faster:** You can organize all relevant threat information on one analysis platform instead of having to conduct lengthy investigations, traversing from system to system. It's easier to see and understand threats and vulnerabilities on a single product.
- **Stop attacks faster:** When you've recognized a security event, you can take immediate action to stop it by directing ISE to contain the device from your analysis platform. You can also automate responses so you don't have to spend time on threats that are clearly identified.

- **Protect critical data faster:** You can change users' access privileges before or after they get on the network, based on their threat score. So if a device starts to act suspiciously you can have its access to critical resources such as finance or patient records automatically denied while allowing access to noncritical resources. This flexibility allows you to protect critical data while limiting the impact to your users' productivity.

What's Inside

Cisco Rapid Threat Containment includes:

Context and control: The Cisco Identity Services Engine provides contextual identity data (user, device type, and posture). It contains threats by using the network as an enforcer with VLANs or Cisco TrustSec® security groups.

Integration: Cisco Platform Exchange Grid (pxGrid) provides an open, highly secure system for security technologies to exchange intelligence, obtain contextual information from ISE, and direct ISE to contain threats. Cisco pxGrid is consistent with Internet Engineering Task Force (IETF) standards.

Intelligence: Cisco pxGrid technology partners integrate with ISE to share their data and control network access.

Cisco security technologies: With Cisco Firepower™ Management Center and Stealthwatch, you can share security intelligence and the ability to request threat containments through ISE.

Threat-Centric NAC technologies: You can use the standard expressions of the Structured Threat Information Expression (STIX) for threats and the Common Vulnerability Scoring System (CVSS) for vulnerabilities to help ensure consistent categorization and responses.

Next Steps

The Rapid Threat Containment solution is tested, documented, and supported by Cisco customer service.

For more information on Cisco's support for multi vendor solutions go to http://www.cisco.com/c/en/us/services/support/solution-support.html.

For a complete listing of Cisco security technology partners who support ISE pxGrid and Rapid Threat Containment go to: www.cisco.com/go/csta.

For design and deployment guides go to: http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html.

For more details about Cisco's extensive and marketing-leading security technologies, go to: http://cisco.com/go/security.

C45-735770-04 05/17