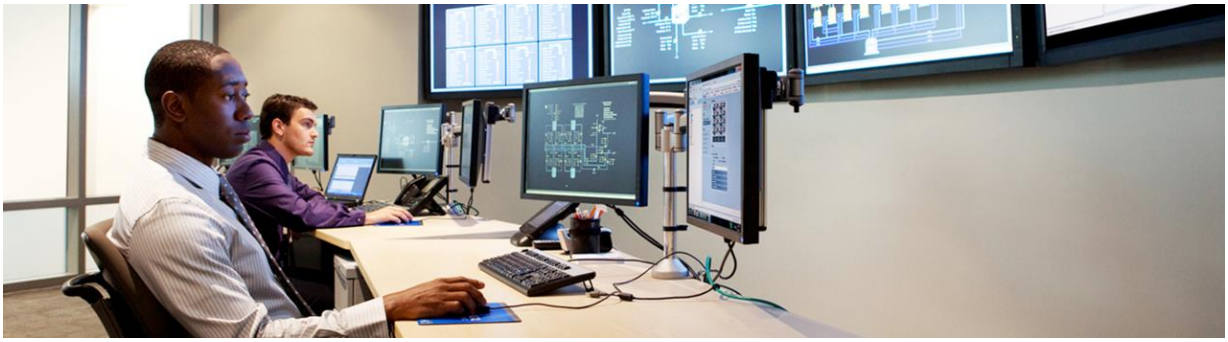


Cisco Rapid Threat Containment

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 Cisco or technology partner product.

Stop Attacks Faster
When you've recognized a threat, you can take immediate action to stop it by directing the Cisco Identity Services Engine 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. This flexibility allows you to protect critical data while limiting the impact on your users' productivity.

What if your network security could sense and immediately stop flagrant threats? Now it can with Cisco® Rapid Threat Containment.

Today's advanced malware threats are increasing in sophistication, stealth, and speed. The proliferation of lightly protected devices in the Internet of Things (IoT) is expanding the attack surface. Because many organizations already have anomaly-detection capabilities, adversaries who want to steal valuable data now develop malware to evade detection. Effectively detecting and stopping threats has thus become a race against time for IT, security, and incident response teams.

Companies must start automating their security operations to quickly detect and automatically stop ever-changing threats. Imagine advanced threat sensors continually updating your threat intelligence to identify malware. Containing obviously compromised endpoints is then fast and efficient. This is what Rapid Threat Containment is: a complete, open, and semi- or fully automated capability to get ahead of the quantity and elusiveness of threats and vulnerabilities in your company network.

The Threat Landscape Continues to Evolve—Your Environment Must as Well

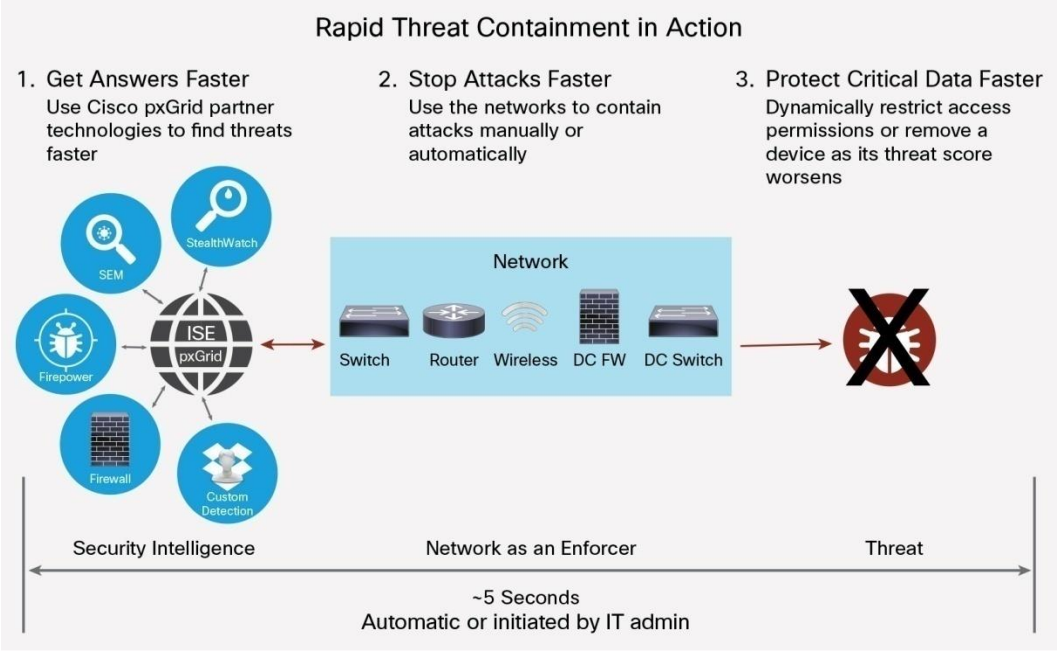
As explained in our 2016 Cisco Midyear Security Report, attackers are using innovative tactics such as exploit kits, ransomware, and advanced malware in order to evade detection. Without visibility, context, and control as part of your security features it's extremely difficult to combat these threats. Organizations today are using as many as 60 standalone security solutions. They don't work together. They are typically point solutions that, alone, have limited impact against well-funded cybercriminals. And they typically generate vast numbers of alerts, many of which are not related to malware or exploits.

On average, large organizations have to sift through nearly 17,000 alerts each week to find the 19 percent that are security related, and security professionals have time to investigate only 4 percent of the warnings. [1]

The longer the threat goes undetected, the greater the potential for damage. Also noted in the Midyear Security Report, the current industry average for time to detection is 100 to 200 days. That's far too long. By the time a breach is discovered, the damage has already been done.

Cisco Rapid Threat Containment lets you get to the heart of what matters: detecting and containing critical threats fast enough so that you can mitigate your security exposure and risk (Figure 1).

Figure 1. Step-by-Step Rapid Threat Containment Process



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

How It Works

First, the Cisco Platform Exchange Grid (pxGrid) helps you share security information between multiple products. IT security teams can find answers faster without having to conduct lengthy and time-consuming investigations.

Upon detecting a flagrant threat on an endpoint, a pxGrid Security Technical Alliance integration partner technology, the Cisco Firepower™ Management Center, Cisco Stealthwatch, or Cisco Advanced Malware Protection can instruct the Cisco Identity Services Engine (ISE) to contain the infected endpoint either manually or automatically. The containment can involve moving the device to a sandbox for observation, moving it to a remediation domain for repair, or removing it completely. ISE automatically updates the endpoint's access policy to one that is more restricted, thus effectively quarantining the endpoint from the network. The endpoint can then be remediated or completely blocked from accessing the network.

ISE can also receive the standardized Common Vulnerability Scoring System (CVSS) classifications and the Structured Threat Information Expression (STIX) threat classifications, so you can make graceful manual or automatic changes to a user's access privileges based on their security score. For instance, if a user's device is clean, you can give it full access to all authorized services and data. But if the device starts behaving suspiciously you can have its access to critical data restricted while allowing access to less critical applications such as email. The user can still work while you protect assets that you can't afford to lose to malware or ransomware. Now if the device really acts up and malware is detected, the network can immediately move the device to a quarantine before it can cause further damage.

Cisco Rapid Threat Containment includes:

- **Context and control:** The Cisco Identity Services Engine (ISE) provides contextual identity data (user, device type, and posture). It contains threats by using the network as an enforcer with VLANs or Cisco TrustSec® software defined segmentation.
- **Integration:** Cisco 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 Security Technical Alliance partners who are integrated with pxGrid's Rapid Threat Containment capability can share their data and use ISE to control network access to threatening devices.
- **Cisco security technologies:** With the Cisco Firepower Management Center and Stealthwatch behavior analysis, you can share security intelligence and the ability to request threat containments through ISE.
- **Threat-centric NAC technologies:** You can use the standard STIX expressions for threats and CVSS classifications for vulnerabilities to help ensure consistent categorization and responses. Today Qualys is integrated with pxGrid for vulnerabilities and Cisco AMP for threats.

Table 1 explains the benefits of Rapid Threat Containment in more detail.

Table 1. Benefits

Threat visibility provides IT security teams with a comprehensive view of threats on the network and the information needed to make rapid, automated decisions	The collective market-leading security intelligence technologies in Cisco Security Technical Alliance partners, Firepower Management Center, Cisco Stealthwatch, and Cisco AMP allow you to put more pieces of the security puzzle in one place. They dramatically speed your ability to get answers to such questions as: What is the threat? Where is the threat? Who owns the device? What is their policy? and Where are they? It's easier and faster to draw conclusions and take action.
Enforcement automation helps ensure that compromised endpoints are rapidly contained upon threat detection	The technologies supporting automatic enforcement are: **Cisco Security Technical Alliance partner and Cisco security technologies:** When a threat or indicator of compromise of sufficient severity is discovered, one of the integrated technologies can direct ISE to take a containment action. **Cisco ISE:** The network controller function of ISE allows it to instruct the network, whether Cisco or multivendor, to contain the infected endpoint. This can be either manual or automated. **Cisco TrustSec® technology:** This software-defined segmentation technology offers the most flexible and advanced way to contain infected endpoints. The enforcement can take place either at the network access switch or controller that the infected endpoint is connected to, or at a downstream device such as a Cisco Adaptive Security Appliance (ASA), Cisco Web Security Appliance, or Cisco Integrated Services Router (ISR). **Downloadable access control list (dACL):** Cisco ISE can push a dACL or named ACL to a switch or controller to block or contain a device at the switch or wireless controller. **VLAN:** ISE can force an infected device to a quarantined VLAN.

Why Cisco?

Cisco is no longer just a world leader in network and switching products. We are guided by the imperative that security must be open and everywhere and by the knowledge that our customers need a business partner to help them with their security complexity. Today only Cisco has the breadth of capability and credibility to address security as a fully integrated architecture to help businesses go faster and capture the opportunity ahead.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Solution Support

The Rapid Threat Containment solution is tested, documented, and supported by Cisco customer service. Cisco customer service helps ensure your security operation is operating and will help resolve challenges on Cisco-on-Cisco and Cisco Security Technology Alliance partner-on-Cisco integrations.

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

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

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 on Cisco's extensive and market-leading security technologies, go to: http://cisco.com/go/security.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-736229-02 01/17