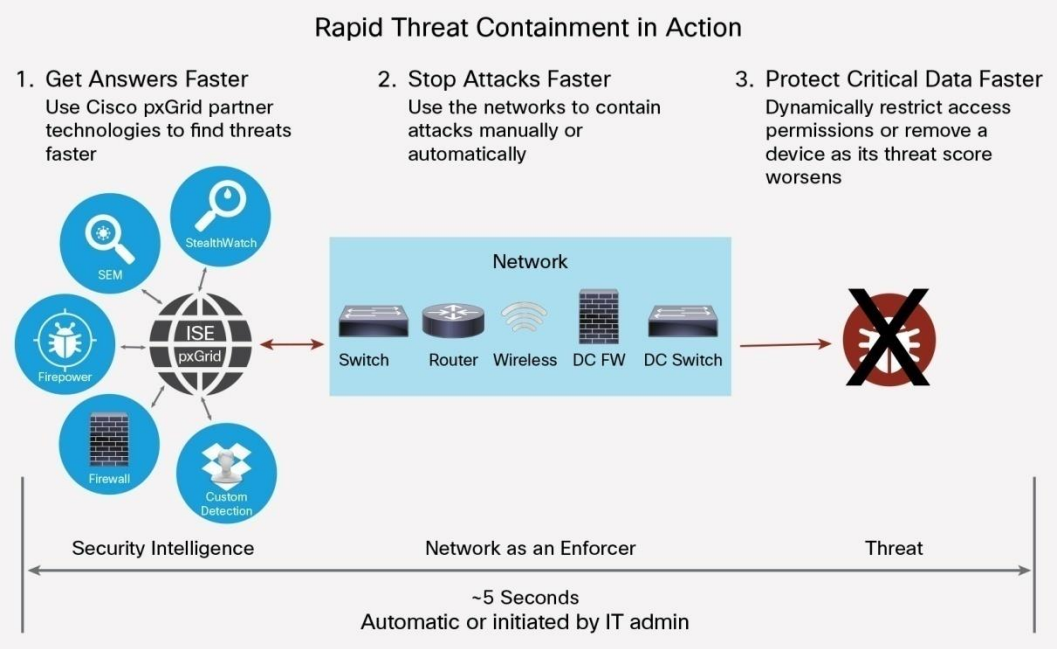
Cisco Rapid Threat Containment

The Cisco® Rapid Threat Containment solution 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 Rapid Threat Containment you can turn your security intelligence and response technologies into an integrated operation to see and stop threats wherever and whenever they occur in your network.

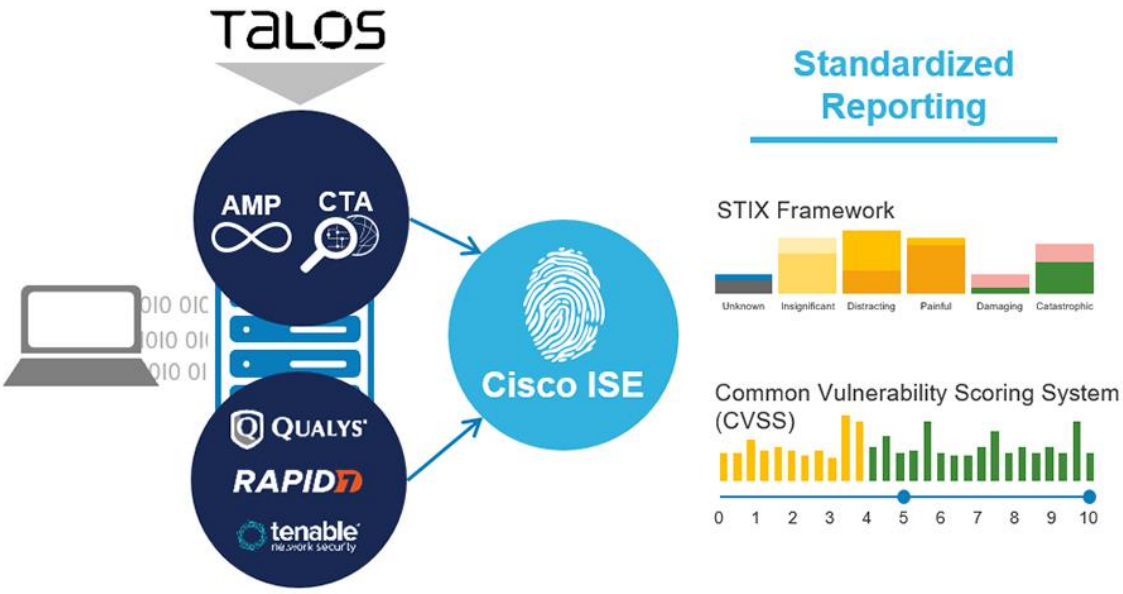


Note: In this figure, the network comprises switches, routers, wireless controllers, data center firewalls, and data center switches.

Features and Benefits

Feature	Benefit
Richer visibility	Improves clarity from bidirectional data sharing of Cisco Identity Services Engine (ISE) contextual data
Advanced threat sensors	Detects advanced malware and indicators of compromise from the network and a pool of the industry's most advanced security technologies
Network threat enforcement	Helps you quickly stop threats using the network as an enforcer
Threat-centric NAC	Update your policies dynamically based on indications of compromise (IoC) coming from vulnerability assessments and threat incident intelligence

Threat-centric NAC Diagram



Stop Attacks Faster

When you've recognized a threat, you can take immediate action to stop it by having your threat sensors directly to Cisco ISE to contain the device. You can also automate responses so you don't have to spend time on threats that are clearly identified.

Infected endpoints are quickly and automatically removed as threats. Depending on the severity of the threat or indicator of compromise, Cisco ISE to contains the compromised endpoints dynamically. Cisco ISE then automatically pushes an enforcement instruction to a router, switch, firewall, or wireless controller. Enforcement options include Cisco TrustSec® software-defined segmentation, a downloadable access control list (dACL), or a quarantined VLAN. The endpoints can then be remediated or completely blocked from accessing the network.

Lower Costs

Operational overhead, malware-related costs, and capital expenses are reduced. Automated responses are based on the policies you set, so you can limit the need for IT security staff involvement while mitigating the damage and financial impact.

Capital expenses are reduced because you can use your existing network devices for enforcement.

Platform Support and Compatibility

Product Family	Platforms Supported
Cisco Identity Services Engine	**1.3, 2.0, 2.1, 2.2, 2.3**
Network threat enforcement	Cisco TrustSec technology: Software-defined segmentation offers the most flexible and advanced way to contain infected endpoints. The enforcement can take place either at the network access switch or controller to which the infected endpoint is connected, 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.

Product Family	Platforms Supported
Cisco Threat Sensors	Cisco Advanced Malware Protection (AMP) Cisco Firepower Management Center Cisco Stealthwatch Cisco Cognitive Threat Analytics Cisco Web Security Appliance
Technology Partner Integrations	Attivo Networks, Bayshore. E8 Security, Elastica, Exabeam, Greenlight Technologies, HanSight, Hawk Defense, Huntsman, Infoblox, illusive, Infocyte, Intelliment, Invincea, LemonFish, LogRhythm, NetIQ, Qualys, Rapid 7, RedShift Networks, SAINT, Splunk, Tenable, ThreatTrack, TrapX, tripwire

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.

For More Information

For more information, learn more at http://www.cisco.com/go/rtc or speak with your Cisco sales representative or Cisco authorized channel partner.

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 C78-736242-02 06/17