Cisco TrustSec accelerates and simplifies network security

BENEFITS

- Centrally apply and enforce consistent policies across wired, wireless, and remote-access users and devices
- Reduce operational expenses by simplifying network segmentation and defining security groups based on business roles not IP addresses
- Limit the impact of a data breach through more effective segmentation and by quickly isolating and containing threats using your network
- Reduce the scope of regulatory compliance by protecting sensitive information from inappropriate access

Your organization is dealing with more devices and more threats against its critical assets. Both expand your risk and compliance challenges. But what if you could regain control of your network?

Cisco TrustSec® technology helps protect critical assets from malware and bad intent by controlling access to your applications, equipment, and users. Cisco TrustSec software-defined segmentation simplifies the security controls in your network and provides consistent, automated policy across campuses, branches, and data centers whether users connect through wired, wireless, or VPN. Automation is enabled through the distribution of rich contextual information to network decision points.

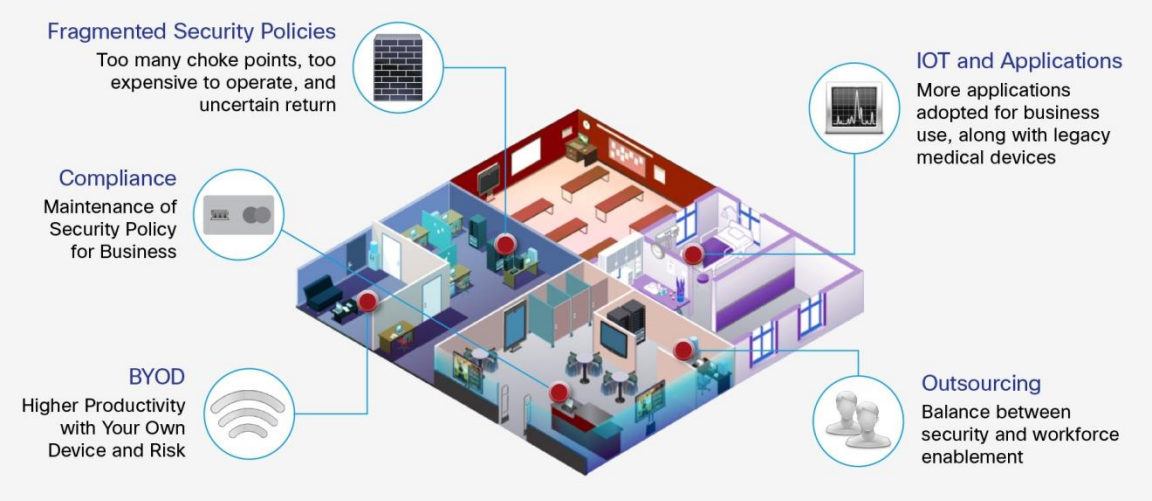
Unsegmented network means unfettered network access

In an open network, engineers can access financial records, disgruntled employees can access proprietary information, and even third-party contractors are sometimes given complete system access. Such an environment creates massive concerns in terms of intellectual property protection, regulatory compliance, and overall network security. A simple breach can leave the network exposed.

Network growth requires flexible and scalable policy enforcement

In most organizations, networks continually grow. New applications are hosted on new clusters of servers. New network connections, new subnets, and new endpoint platforms are added every day. Firewall policies and access control lists (ACLs) struggle to keep up. The natural tendency to deploy the network infrastructure in the simplest way possible works during the initial deployment. But as applications, roles, and device types multiply, increasing demands are put on security controls. Policy management and segmenting the network then become more and more onerous. (See Figure 1.)

Figure 1. Complex Challenges for Business

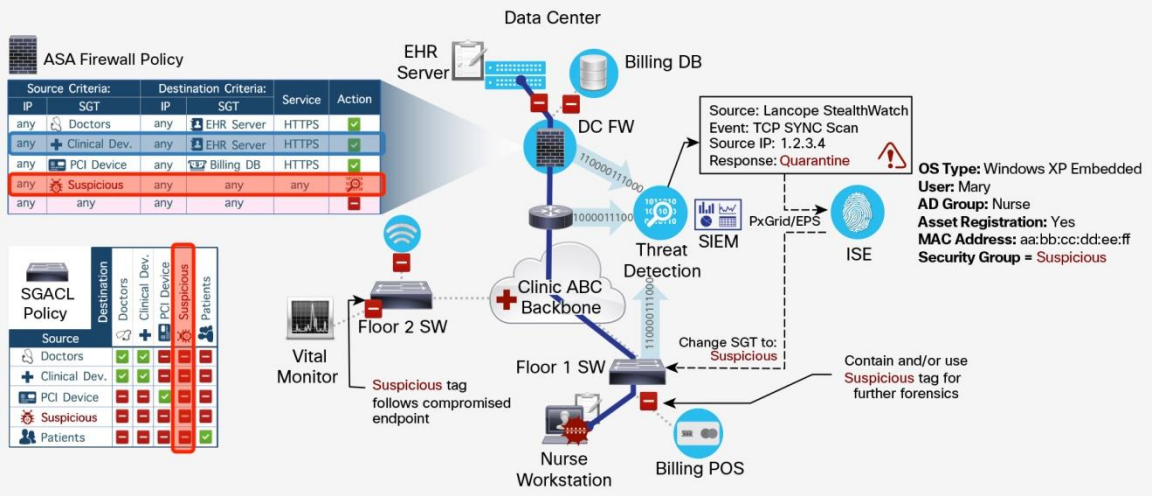


By abstracting security policies away from individual components of the network such as switches, routers, and firewalls—and by centrally defining those policies—vast improvements in manageability and control are possible. Simplicity leads to better security. With a centrally defined security policy—essentially network segmentation by policy—comes more control and flexibility without redesigning the network.

How it works/key features/components

Cisco TrustSec technology is embedded in Cisco switches, routers, wireless, and security devices. It is available as open-source in the Open Daylight SDN and is used by partners and other vendors. It is an IETF internet draft. It provides a scalable mechanism for the enforcement of policies that are centrally created to be automatically and dynamically provisioned across wired, wireless, and VPN devices. It is a highly secure network architecture that extends security across the network from campus to branch to data center. Cisco TrustSec technology is the foundation of the Cisco Network as an Enforcer initiative and mitigates risk by reducing the attack surface through better segmentation while also increasing operational efficiency and making compliance goals easier to achieve. (See Figure 2.)

Figure 2. Threat Detection and Remediation Using Cisco TrustSec Technology



Cisco TrustSec software-defined segmentation

Cisco TrustSec software-defined segmentation reduces the risk of malware propagation, simplifies security operations, and assists in meeting compliance goals. Resource classification is based on business roles, not IP addresses. Business roles can be based on contextual information including user role, device type, posture, location, time, and type of access.

Cisco TrustSec segmentation uses what are called security group tags (SGTs) to represent logical groups. A SGT represents a set of network endpoints, users, or servers with common entitlements. The SGT provides a layer of policy abstraction that works independently of the underlying network and avoids the need for IP address-based or VLAN-based mechanisms traditionally used for access control. Policies for wired, wireless, or VPN remote access can be managed consistently and centrally to avoid the operational cost associated with topology-based policy management.

> “What Cisco technology will let us do is to scale as big as the mind can imagine. I can’t know everything that the business will want to do in six months, or next year, or the year after. But what I can do is build us a network that will scale and let us do pretty much anything we want to do with limited investment in the next four years.”
>
> **— Bill Dugger, Senior Network Engineer, Beachbody**

Taking complexity out of network security

The Cisco Identity Services Engine (ISE), Cisco’s market-leading policy management platform, gathers advanced contextual data about who and what are accessing your network. It then defines role-based access using SGTs to segment your network. Embedded in your existing Cisco infrastructure, Cisco TrustSec technology simplifies the provisioning and management of network access making security operations more efficient. It helps enable security policies to be enforced consistently everywhere in the network.

Simplify access management

- Create and manage policies in a simple matrix using plain language
- Easily manage access control and segmentation across the enterprise
- Control access to critical assets by business role, device type, and location

Gain consistent policy across the network

- Consistently enforce policies across the network and scale from mobile users to the data center
- Define policies in Cisco ISE, which are applied across wired, wireless, and VPN access methods

Reduce operational expenses

- Limit the impact of data breaches and prevent the lateral movement of threats and compromises across your network with microsegmentation
- Reduce the need for costly and time-consuming moves, adds, and change management by automating firewall rules and ACL administration
- Easily comply with audits and avoid a costly network redesign to meet compliance requirements

Use Cases

Vertical	
Healthcare	• Protect electronic medical records (EMRs) • Protect medical equipment and data from malware with microsegmentation
Retail	• Scope reduction for PCI compliance • Protect sensitive information from other connected devices
Financial	• Control access to regulated applications • Simplify audits and compliance • Accelerate security policy provisioning for new applications
Education	• Control student access to classroom media and resources • Scale segmentation for students, staff, and faculty roles
Manufacturing	• Improve security controls for the Internet of Things (IoT) • Simplify segmentation for manufacturing zones • Simplify vendor access controls • Simplify supply-chain partner security
Horizontal	
Consistent policies	• Apply policies across campus, branch, and data center environments • Gain consistent policies across Cisco TrustSec-enabled enterprise networks and Cisco Application Centric Infrastructure (ACI) data centers
Highly secure BYOD	• Increase investments in bring-your-own-device (BYOD) policies while protecting sensitive information
Threat mitigation	• Mitigate malware scanning and propagation • Provide rapid threat containment
Simplified firewall rule management	• Speed data center service and application provisioning • Dramatically simplify firewall rule tables • Avoid repetitive adds, moves, and changes of firewall rules
Highly secure vendor access	• Differentiate access for contractors and partners

Why Cisco?

With so many access attempts occurring within and beyond the traditional enterprise network perimeter, you need security everywhere. Fortunately, your Cisco network already contains what you need to do the job. By simply activating the embedded security capabilities in your Cisco network, you can transform your network into a full-blown security monitoring system that gives you broad, deep visibility into your network and everything that connects to it.

Security advisory services

To safeguard the connections among people, processes, data, and things, security needs to be as pervasive as the Internet of Everything (IoE).

Cisco Security Advisory Services' strategic and technical advisors help you identify opportunities to:

- Align security to business imperatives
- Create a competitive advantage
- Capture business value from emerging technologies

Security integration services

Cisco Security Integration Services address solution-level architectural challenges. We are experts at delivering integrated security solutions across the network. We partner with you to transform your business requirements into security solutions that accelerate the adoption of technology with little or no disruption.

Our experts will help you:

- Assess strategies and recommend the best approaches for new technology deployments in your environment
- Test and deliver new solutions with proven processes and tools that reduce business disruption
- Migrate from older security solutions
- Partner with your in-house security and IT talent

> "The Cisco solution gives us a very precise way, from the wireless access point or the switch, to identify who is trying to access what. It allows us to place users in the right category and have the right policy to match information security demands."
>
> **— Roman Scarabot-Mueller, Head of Infrastructure, Mondi Group International**

Major Cisco TrustSec deployment models

User-to-data-center access control	• Context-based access control • Compliance requirements of PCI, HIPAA, and export-controlled information • Merger and acquisition integration, divestments
Data center segmentation	• Server zoning and microsegmentation • Production versus development server segmentation • Compliance requirements such as PCI and HIPAA • Firewall rule automation
Campus and branch segmentation	• Line-of-business segregation • PCI, HIPAA, and other compliance regulations • Malware propagation control and quarantine

Next Steps

For more information about successful real-world examples of this solution, visit http://www.cisco.com/go/trustsec

To learn more about how to deploy the Cisco TrustSec solution, contact your Cisco Services 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 C22-737173-02 06/17