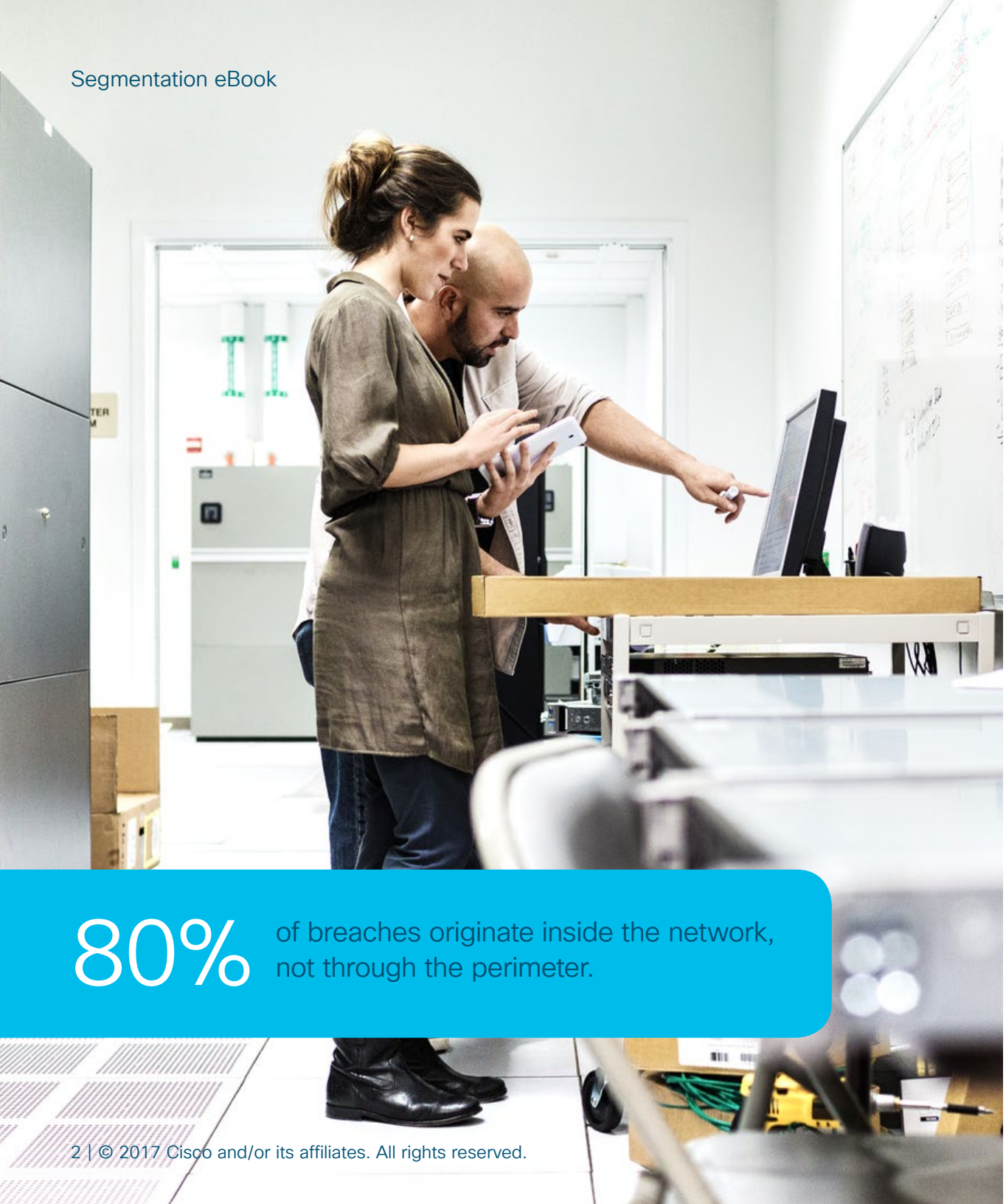
Segment Your Network for Stronger Security

Protecting Critical Assets with Cisco Security



80% of breaches originate inside the network, not through the perimeter.

The threat landscape continues to evolve.

We know that perimeter defenses, however necessary, cannot do it all. Attackers will get into your network, and oftentimes, they will bypass the perimeter altogether.

ZK Research estimates that 80% of breaches originate inside the network, not through the perimeter. According to Cisco principal engineer TK Keanini, “Threat actors are not breaking in anymore. They are simply logging in.”

So what can we do about it?

One essential way to protect your network from intruders is through network segmentation. In fact, several of the most high-profile data breaches in recent years could have been prevented this way.

Network Segmentation can secure critical assets, but it has its shortcomings...

Segmentation involves the partitioning of your network into various zones. You restrict access for each zone to only those users, applications, and devices that require it to run the business. That way, if attackers slip into the network undetected, they will be able to access only a small portion of your data and assets, instead of gaining the keys to your entire kingdom.

"Network segmentation has been around for a long time, but many organizations have forgone implementing it because traditional methods have some key shortcomings," said Keanini. "The main challenge of conventional network segmentation is that it is impractical to implement and maintain in large corporate environments."

Due to such shortcomings, VeraQuest Research found that only one in four companies employ an end-to-end segmentation strategy.

Networks continue to modernize, digitize, and expand. How can we properly segment them to keep them secure without unnecessary cost and complexity? The answer lies in software-defined segmentation.

Software-defined segmentation changes the game

Traditionally, network segmentation has been done through firewalls, virtual LANs (VLANs), and extensive access control lists (ACLs). But according to Keanini, “In networks with thousands of users and multiple environments, such as the cloud and specialized IoT networks, this quickly becomes nearly impossible to manage.”

Segmentation policies become outdated as users and assets are added to a network. To protect themselves effectively, organizations need to constantly adjust segmentation policies as the network evolves.

Software-defined segmentation enforces policies based on user, application, or device instead of IP address. You can centrally manage policies across the network, so segmentation is more effective and can more easily adapt to changes in network topology. You can implement and alter segmentation policies without reconfiguring network devices, amounting to massive operational improvements.

Network as an Enforcer solution allows for better segmentation

The Network as an Enforcer solution from Cisco embraces your existing network infrastructure to deliver better, more streamlined segmentation and security. The Network as an Enforcer consists of four main offerings: **Cisco TrustSec® technology, Cisco IOS® NetFlow, Cisco® Stealthwatch, and the Cisco Identity Services Engine (ISE)**.

Cisco TrustSec technology

Embedded in more than 40 Cisco product families and third-party offerings, Cisco TrustSec software-defined segmentation provides a role-based approach to policy enforcement. It does this by defining roles through security groups. Traffic from a set of network endpoints, users, or servers is assigned a security group tag (SGT) for enforcement. You don't have to whitelist IP addresses manually across every switch.

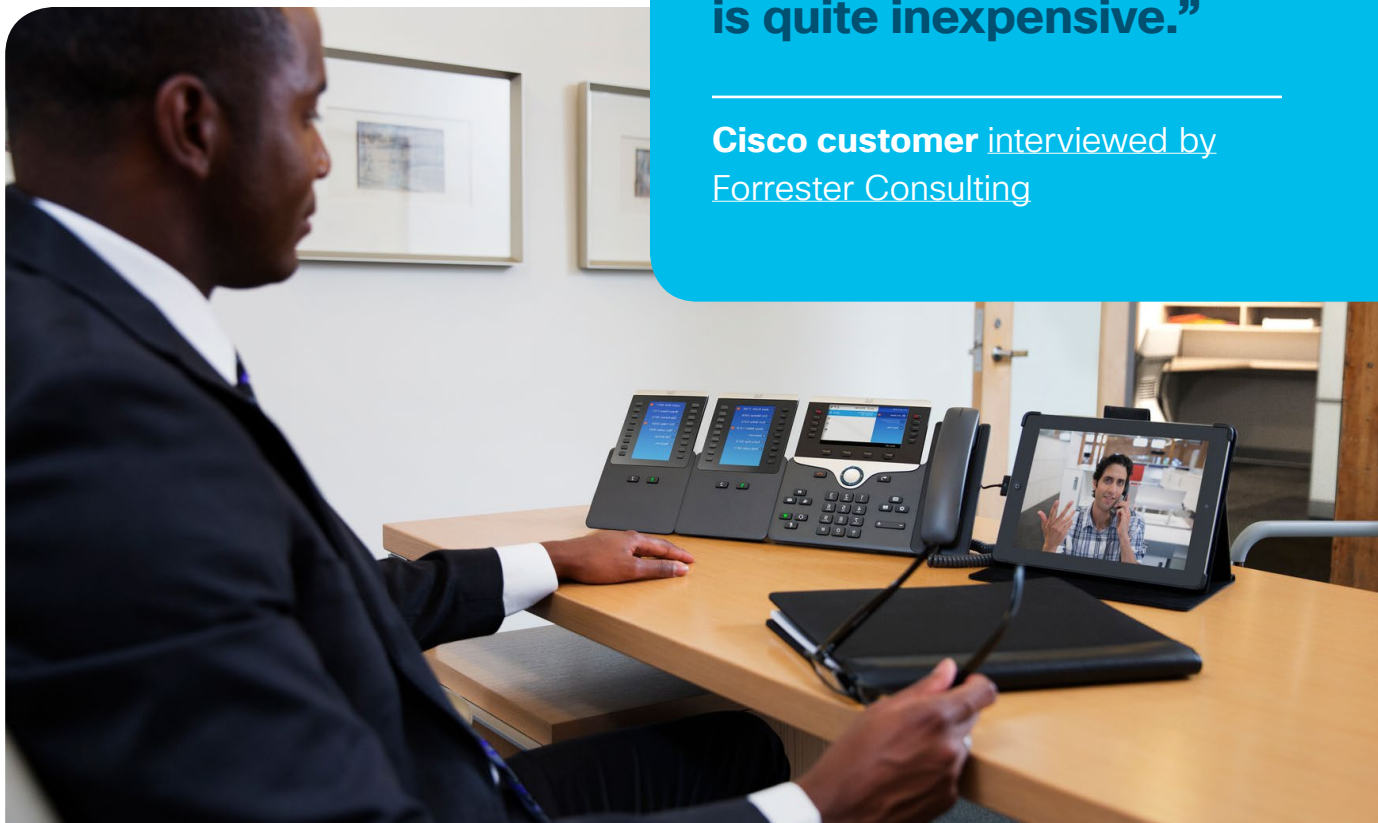
A study by Forrester Consulting found that with Cisco TrustSec technology, customers can experience an 80 percent reduction in operational costs and a 98 percent reduction in time to implement policy changes.

Cisco IOS NetFlow

Cisco IOS NetFlow was created by Cisco to track network conversations. It delivers valuable details including the source, destination, timing, and protocol. It can tell who is talking to whom, with which device, from where, and for how long, and can measure how much data is exchanged. NetFlow is embedded in Cisco routers, switches, and other networking devices. It simply has to be turned on to begin delivering network insight.

"With TrustSec, you have no bandwidth restrictions versus the firewall approach. So we have less investment risk with TrustSec. And from an operational cost point of view, TrustSec is quite inexpensive."

Cisco customer interviewed by Forrester Consulting



76% of IT professionals say visibility is their biggest security challenge, according to the Ponemon Institute.

“The guest network should never talk to internal services – like budgetary and personnel systems... Stealthwatch can tell us if this happens.”

Passaic County Technical Institute

Cisco Stealthwatch

Once NetFlow is turned on, the data needs to be collected and analyzed so security teams can easily digest and understand it. The Cisco Stealthwatch solution collects and analyzes large amounts of NetFlow data to provide a comprehensive picture of network activity.

To create segmentation policies that do not impede security or hinder business productivity, you need to know exactly which users and devices are on your network, and what each of them is doing. The visibility provided by Stealthwatch is critical for building and testing segmentation policies, and monitoring their efficacy once in place.

Cisco Identity Services Engine (ISE)

Cisco ISE is a secure access control platform used by more than 17,000 organizations to help ensure that only authorized users and devices can access their network infrastructure. Providing secure access requires insight into user and device details. ISE gathers this information to deliver valuable context that can be shared with other network and security solutions. ISE also serves as the controller for defining and enforcing segmentation policies through technologies like Cisco TrustSec software-defined segmentation.

“The Cisco solution gives us a 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.”

Mondi Group International

How do these technologies work together?

Here's how these technologies work together to provide effective network segmentation:

Organizations get in-depth network visibility from NetFlow and Stealthwatch, which is enhanced by user and device context from Cisco ISE. This combination is known as the Cisco Network as a Sensor solution. It plays a key role in helping organizations develop accurate segmentation policies.

Hosts are segmented according to Cisco TrustSec SGTs.

Cisco ISE uses TrustSec technology to define and enforce network segmentation policy, allowing or denying access to specific users, devices, applications, or whole areas of the network.

Cisco Stealthwatch continues to monitor network and user behaviors. It alerts administrators if segmentation policies are violated so that they can be quickly reconfigured. When Stealthwatch identifies a security event that requires investigation or remediation, it can also automatically notify Cisco ISE to change the device or user policy to contain the threat.

Professional Services

If you wish to simplify segmentation even further, Cisco also offers a service that can automatically segment the network on your behalf. This service builds segments based on Stealthwatch flow traffic analysis. It gets additional context from Cisco ISE, customer IP address management systems, and/or customer domain controllers. The service can then develop segmentation enforcement policies or build Stealthwatch host groups to segment assets based on various criteria.

Contact Stealthwatch-CustomerSuccess@cisco.com for more information on this option.

A practical process for segmentation

Cisco's Keanini recommends the following process for implementing network segmentation:

Model:
Model your digital business. Try different segmentation policies and see the results without disrupting operations.

Implement and enforce:
Use the power of Cisco ISE and Cisco TrustSec technology to enact the segmentation models that fit your organization.

Monitor:
Use Stealthwatch to detect any network behavior that violates your segmentation policies either by mistake or with malicious intent.

Simplicity leads to improved security

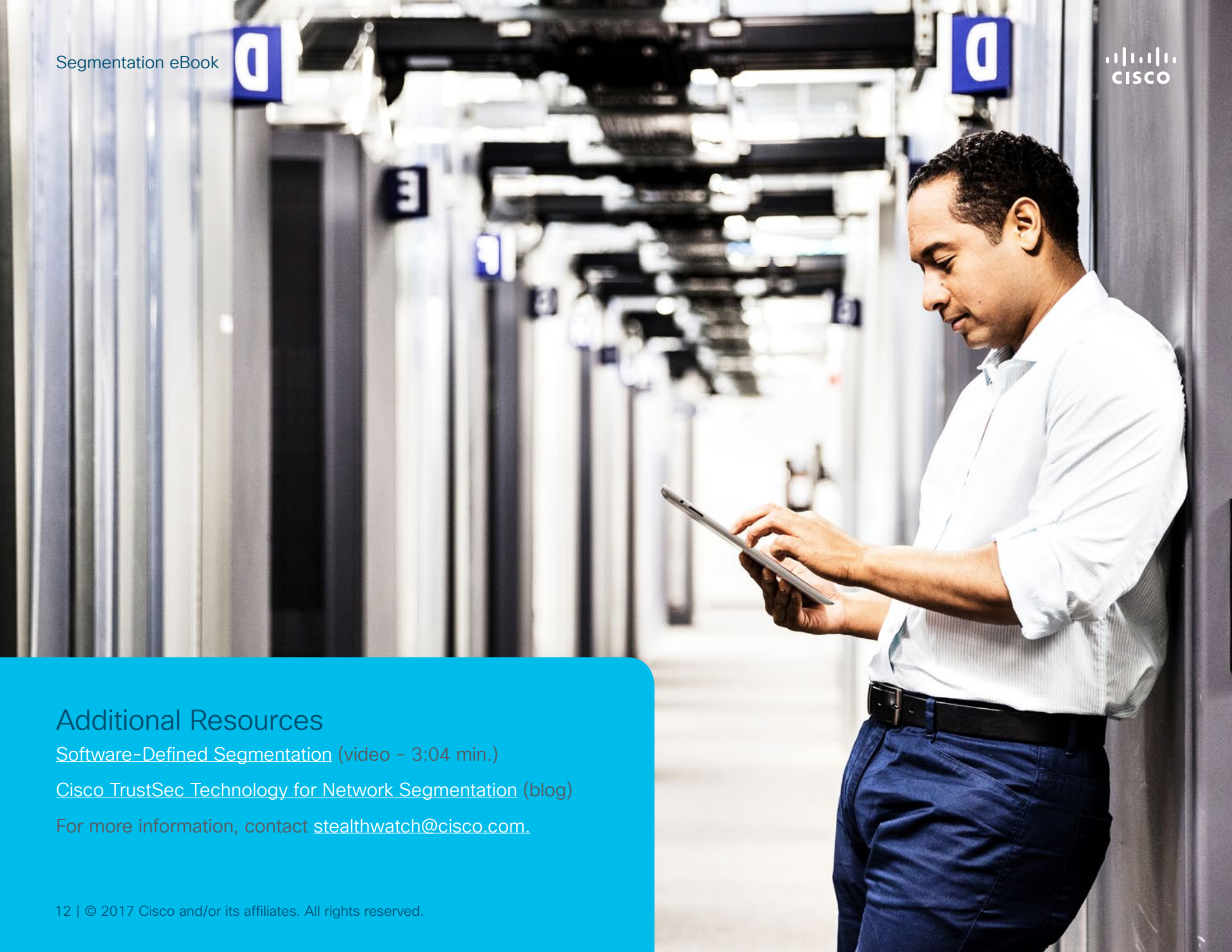
Cisco's network segmentation solutions bring many benefits to an enterprise. With these solutions, you can:

- Restrict the lateral movement of attackers across the network, thwarting a wide range of attacks such as malware and insider threats.
- Streamline network and security operations, resulting in a dramatic savings of time, cost, and resources.
- Better comply with industry and government regulations by walling off sensitive parts of the network from the rest of your environment.
- More easily digitize and expand your network infrastructure through cloud, personal device onboarding, and the Internet of Things (IoT).

Prestigious hospital, outdated network

A large national hospital system was lagging far behind on security. It had a flat network without segmentation. Doctors, staff, students, and medical equipment all shared the same network, multiplying the attack surface and exposing the hospital to threats. The hospital system transformed its environment with the Cisco Network as an Enforcer solution. Now, even if attackers get in, their access is limited to one network segment.

Read the full case study.



Additional Resources

Software-Defined Segmentation (video - 3:04 min.)

Cisco TrustSec Technology for Network Segmentation (blog)

For more information, contact stealthwatch@cisco.com.