Five Signs It's Time to Step up your Network Security

The modern network is expanding rapidly. It connects multiple branches, mobile users, the cloud, and data centers. Organizations are moving away from traditional IT infrastructure towards a digital-ready network infrastructure. From streamlining operations and inventory management to offering new value-added services, many businesses are realizing significant benefits from digitization.

However, the rate of digital transformation is moving at an unprecedented pace – and challenging security. Mobility, the Internet of Things (IoT), Bring-Your-Own-Device (BYOD) access, and the move to the cloud are critical ingredients in growing a digital business. Yet this additional complexity is making it difficult for organizations to secure their networks. Consider these challenges:

A growing attack surface

More devices are going online at a staggering pace. In fact, 26 billion networked devices and connections will exist by 2020[1] and 2 billion BYOD devices will be in the workplace by 2020[2].

Delayed visibility

The average industry breach time-to-detection is 191 days[3].

Inevitable and costly attacks

One in every four companies will experience a major breach, and the consequences are serious. The average cost of a data breach has risen to US$3.62 million[3], and 60 percent of digital businesses[4] will suffer major service failures due to the inability to manage digital risk.

As traffic volumes grow, it is easier for organizations to lose sight of exactly what and who is on their network. As more devices access the network, not only in quantity but also in variety, it can be difficult to manage policy enforcement. And more complexity makes it harder to segment and maintain your network effectively.

Almost every organization faces these challenges. But as your network grows and the threat landscape evolves, many organizations simply don't know where to begin when it's time to step up their network security.

[1] Cisco VNI Forecast
[2] Mind Commerce
[3] Ponemon Institute
[4] Gartner

Contents

Securing your digital network: the five signs

It's clear that you need to secure your digital network—and everything that touches it. In this white paper, we'll show you how to determine when your network security needs attention. Here are the top five signs it's time to step up your network security:

Your network is growing

Nearly every environment is experiencing an expanding network. Whether it's the hospital that hosts medical devices and guest devices, or the global business launching a BYOD policy, billions of new devices are being added to networks around the globe.

Connected devices have great advantages, but can cause device overload, which may threaten security. You know you are experiencing device overload when you can't tell which devices are touching your network or manage their level of access to your network and sensitive data.

Managing a large number of endpoints obscures visibility, makes threats harder to identify, widens the attack surface area, and introduces new backdoor vulnerabilities. Stealthy attackers will use whatever means possible to gain access to your network. A growing number of devices can seem like an open invitation to enter.

Something as simple as managing guest access can increase your attack surface and threaten security. When you grant a guest access to your network, can you provision the right level of access quickly and easily? Do you know how many and what types of devices are being used? Do you know how and when to decommission access? A global organization may host hundreds or even thousands of guests each week. Without the proper tools, managing access can be time consuming and leave you open to attack.

You can't tell if you've been breached

Do you think there's a threat inside your network? How do you know? If you think there is a threat, chances are you're right. According to a study from Cisco, 100 percent of organizations surveyed were hosting some sort of malware on their networks. That means it's only a matter of time before you experience a significant breach.

Breaches take organizations by surprise and are expensive in terms of lost productivity, cost to remediate, service failures, and reputational damage. Sophisticated threat actors can infiltrate your network where they can live for months, or even years, without being detected.

Once inside, attackers have free reign to explore your network for critical data and the best way to extract it without your knowledge. That's why it's important to be able to identify suspicious behavior before it becomes a full-blown breach. Organizations need to see all network traffic, continuously monitor it for suspicious activity, and pinpoint areas that need immediate attention.

Consider the large technology company that discovered almost half of its end-user workstations were infected with a custom piece of malware written just for its network. The malware had been quietly stealing information for an unknown period of time. Or think about the healthcare provider that fell victim to an attack because it couldn't detect malicious activity in its encrypted data flows.

These are true stories from organizations that had numerous security tools but lacked visibility into the network interior. And with the growing frequency and severity of attacks, a lack of visibility can be the difference between a near miss and a costly attack.

Your infrastructure is very old—or very new

Aging routers, switches, and other network infrastructure are red flags that your network may not be as secure as it could be. Misconfiguration, old policies, and outdated software and operating systems are just a few of the ways your old gear can leave you vulnerable to attack.

Unfortunately, many organizations are relying on infrastructures built on outdated components running vulnerable operating systems. In its 2016 Cybersecurity Report, Cisco performed an analysis of 115,000 devices and found that 92 percent of the sample devices had known vulnerabilities in the software they were using.

It's important to identify your most vulnerable gear and prioritize it for upgrade. And while you're waiting for the upgrade, ask yourself if you have the ability to automatically baseline device behavior and detect anomalies. If you do, you will be able to detect potential threats on these older devices.

On the other end of the spectrum, if you are planning, currently working on, or have recently refreshed your network, it's a good time to take advantage of your investment in security-enabled network devices. Advanced networking products, such as Cisco® Catalyst® 9000 Switches, have capabilities that enhance network security and integrate with other tools to reduce your attack surface and augment malware detection.

With a little planning, an upgrade is also an opportunity to ensure your network is configured to provide awareness of all users and devices hitting it, continuously monitor their behavior, and manage their access efficiently. Otherwise, you're opening thousands of doors to attackers.

You are losing control in an unsegmented environment

An unsegmented network means unfettered network access: 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 entire network exposed.

Network segmentation is essential for protecting critical business assets. It limits the lateral movement of threats across your network and controls access to sensitive data. But traditional segmentation approaches are operationally complex and time consuming to implement and update. As the number of roles and endpoints increase within an organization, the time and cost of managing technologies such as virtual LANs (VLANs) can be significant.

What you need is the ability to scale your network and reap the benefits of segmentation without the headaches. Ideally, segmentation tools should help you map your network, classify devices into logical groups, and manage those devices at scale while restricting access to critical applications.

You can't tell if you have policy violations

Should your CFO's smartphone have access to financial data? At 3:30 AM? From China, when your CFO lives in Texas?

Detecting policy violations means identifying attempts to access sensitive data and restricted areas of the network, in real time. With a properly configured network, you should be able to continuously monitor and detect suspicious activity and attempts to access critical assets. And wouldn't it be nice to have the control to deny access to users and devices quickly and easily as they come online?

Compliance verification is also an important part of the equation. Can you verify compliance as your network changes? Can you get the contextual information necessary to understand what is interacting with data and devices on the network? Can you ensure you have limited access to sensitive data?

Network growth requires flexible and scalable policy detection and enforcement. As the network scales, policy management can become more onerous, costly, and potentially risky. Without centralized access control, understanding what entities are interacting with sensitive data and accurately alarming on violations can be nearly impossible.

Security that's woven into the network

Now you know how to tell when it's time to step up your network security. You should also know there's a solution that can give you:

- The visibility to see what is happening on your network and automatically identify threats
- The control to defend your network against complex and persistent threats
- The ability to segment and simplify network operations for improved contextual awareness and reduced operational burden

The solution is woven into the very fabric of your network, and it's called Network Visibility and Segmentation.

What is Network Visibility and Segmentation?

The components

Our Network Visibility and Segmentation solution combines our Cisco Stealthwatch™, Cisco Identity Services Engine (ISE), and Cisco TrustSec® products.

Product	Description	Primary Benefits
Cisco Stealthwatch	Stealthwatch gathers telemetry from across your network and detects malicious activity using machine learning.	• Extend visibility and threat detection across the network, including encrypted traffic. • Get accelerated incident response and forensics.
Cisco Identity Services Engine (ISE)	Contain threats quickly. ISE shares user and device details and controls access across wired, wireless, and VPN networks.	• See and share user and device details. • Get secure access from one place. • Reduce risk, and contain threats by dynamically controlling network access.
Cisco TrustSec	Software-defined segmentation reduces your attack surface, simplifies access control, and streamlines compliance.	• Simplify network segmentation to reduce risk and protect business assets. • Implement and enforce policies without reworking the entire network. • Lower operational expenses and make policy changes quickly.

Used separately each of these tools is powerful. When used together with your network, these three products form an integrated solution with benefits that increase exponentially, without impeding performance, adding complexity, or creating blind spots.

An integrated solution

In the digital era, balancing the demands for agility and security requires a new approach. Cisco Network Visibility and Segmentation offers integrated threat detection and containment. Users get a 360-degree view of the distributed network by monitoring traffic behaviors enriched with user and device context. Secure access through software-defined segmentation simplifies policy management and helps you contain threats quickly.

With Network Visibility and Segmentation, organizations can:

Gain 360-degree visibility	Achieve dynamic control	Attain rapid threat containment:
Identify who is on your network with advanced contextual data, detect unauthorized access, and find potential threats before they escalate to a full-blown breach.	Control who gets on your network, enforce consistent policies with centralized control, and simplify network access control with software-defined segmentation.	Automatically detect, mitigate, and remediate security threats and vulnerabilities on the network, and bring down your overall time to detection.

Network visibility and segmentation solution benefits

360-degree visibility

Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources. Cisco Stealthwatch gathers telemetry from network traffic for advanced threat detection and detailed forensics.

Secure access

Get consistent access control across wired, wireless, and VPN networks with 802.1X, MAC, and web authentication. Connect easily for admission control. For segmentation, ISE controls policy for Cisco TrustSec to enforce within the network. With Stealthwatch, you can to monitor your traffic for segmentation assurance.

BYOD access and compliance

ISE simplifies BYOD management with built-in Certificate Authority (CA) and third-party Mobile Device Management (MDM) integration for onboarding and self-service of personal mobile devices.

Rapid threat containment

Stealthwatch analyzes network traffic using machine learning and behavioral modeling for advanced threat detection. Integration with ISE helps you block threats immediately by dynamically quarantining the suspicious endpoint.

The solution in action

How about that healthcare organization that wants to host medical devices, point-of-sale technology and guest devices on one network? It's Sentara Healthcare, and they are using Network Visibility and Segmentation to enjoy the benefits of a digital network without compromising security.

Another company taking advantage of Network Visibility and Segmentation is Wargaming, the award-winning online game developer and publisher that needed to secure its large, distributed global network, in a way that provided centralized visibility across the environment.

Cost savings and business benefits

Not only does Network Visibility and Segmentation provide visibility, control, and the ability to segment and simplify network operations, according to studies from Forrester, it can save your organization money and has numerous other business benefits:

Used together, Stealthwatch and ISE can provide cost savings to an organization. According to Forrester, using the two tools together can save an organization $1.6 million through avoiding security events, $892,000 in IT resources, and $1.4 million due to increased employee productivity.

Forrester Consulting conducted an analysis of customers using TrustSec software-defined segmentation in production networks. The findings: TrustSec reduced operational costs by 80 percent and accelerated policy changes by 98 percent.

Are you ready?

Are you ready to step up your network security? Here are two ways to get started:

If you believe you lack visibility, start by taking our visibility assessment. This free assessment provides insight into network blind spots. It will give you recommendations on what you can do to enhance your visibility and threat detection capabilities.

If you want to know what users and devices are hitting your network, and to manage access consistently and efficiently, check out one of these demonstrations of Cisco ISE.

C11-740303-00 03/18