The Five Signs: A Network Security Checklist

The modern network is expanding rapidly. It connects multiple branches, mobile users, the cloud, and data centers. Mobility, the Internet of Things (IoT), Bring-Your-Own-Device (BYOD) access, and cloud services are critical for business growth. Yet this complexity is making it difficult to secure a network. Many organizations may not even know where to begin when it's time to strengthen their network defenses.

This checklist is designed to help you understand when your network security needs attention. Take a look at these top five signs and see if they apply to you.

Your network is growing

Connected devices have great advantages, but they can cause device overload, which can threaten security. You know you are experiencing 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 more backdoor vulnerabilities. Stealthy attackers will use whatever means possible to gain access to your network. A growing number of devices can present an invitation to enter.

You suspect you've been breached but lack visibility

Attacks are growing in frequency and severity. How do you know if there's a threat inside your network? If you think there is, chances are you're right. Sophisticated threat actors can infiltrate your network and live for months, or even years, without being detected. Once inside, they are free to find critical data and the best way to extract it without your knowledge.

You need to see all network traffic and identify and remediate suspicious behavior before it becomes a full-blown breach. A lack of visibility can be the difference between a near miss and a costly attack.

Did you know?

- **The attack surface is growing:** 26 billion networked devices and connections will exist by 2020 and 2 billion BYOD devices will be in the workplace by 2020.
- **Threats are hard to find:** The average industry breach time-to-detection is 191 days.
- **Attacks are inevitable and costly:** One in every four companies will experience a major breach, the average cost has risen to US $3.62 million, and 60 percent of digital businesses will suffer major service failures due to the inability to manage digital risk.

Getting started

Are you ready to revive your network security? Here are two ways to begin:

- Read our white paper to learn more about the five signs and our solution called Network Visibility and Segmentation, which can help you find threats faster and enhance your network security.
- Take 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.

C96-740432-00 05/18

Your infrastructure is very old—or very new

Aging infrastructure is a sign 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 networking gear can leave you vulnerable to attack.

On the other hand, if you have recently upgraded your network or are planning to do so, now is a good time to make sure your network is configured to let you see all the users and devices hitting it, continuously monitor their behavior, and manage their access efficiently. Otherwise, the new devices you add could open 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 third-party contractors can be granted complete system access. Such an environment creates massive concerns in terms of intellectual property protection, regulatory compliance, and overall network security.

Network segmentation 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. What you need is the ability to scale your network and reap the benefits of segmentation without the headaches. Otherwise, a simple breach could leave your entire network exposed.

You can’t tell if your policies are violated

Should your CFO’s smartphone have access to financial data? At 3:30 a.m.? 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. As the network grows, policy management can become more and more onerous, costly, and risky. Without centralized access control, getting accurate alerts on violations and understanding what entities are interacting with sensitive data can be nearly impossible. What should be a routine denial of access when the CFO’s smartphone is communicating from China could be a misstep that leads to the next inevitable breach.