Leveraging your network to fortify cybersecurity

By CyberScoop | FedScoop Staff

Enterprise CIOs and CISOs face a constant barrage of challenges, often leaving them little choice but to rely on cybersecurity approaches that address specific concerns. The need to react quickly to new attacks can tempt IT professionals to focus on best-of-breed point products to shore up their organization's cybersecurity posture.

In today's fast-changing threat landscape, however, that can be a dangerous gamble.

Whether you're trying to modernize your IT, lower your operating costs or improve cybersecurity, how you build your network is often the determining factor in whether you succeed or fail.

And it's perhaps more crucial than ever to move towards a fully automated and integrated network that not only improves performance and lowers cost, but brings to bear modern, sensor-aware servers, switches, routers and security devices enabling a holistic cybersecurity strategy.

Start with the network

One of the biggest misperceptions about IT modernization is that it only refers to emerging technologies that are on the bubble of realization. Artificial intelligence and blockchain technology, for example, are highly promising, but they are not starting points for improving cybersecurity.

Government agencies, in many instances, are still playing catch-up with their commercial sector counterparts. When Congress passed the Modernizing Government Technology Act (MGT Act) into law in December 2017, it was an acknowledgement that federal agencies must immediately focus their attention on the nuts and bolts of their IT environments. The law acknowledged the need for working capital funds at the agency level that can be used to improve, retire or replace existing IT systems, in order to enhance cybersecurity and improve efficiency and effectiveness.

But to realize the potential modernization and cybersecurity improvements promised by the MGT Act, agencies and commercial enterprises alike should recognize there's only one place to start: the network.

Strategically enabling the security features of existing switches and routers and replacing the older ones with new, smart, intuitive versions immediately multiplies security, speed and efficiency, making other steps in modernization easier. Taking an integrated architectural approach can ensure your network is better prepared for the future.

Functionality and security

An integrated architecture takes advantage of end-to-end solutions, including endpoints, cloud and security, that communicate with one another. That makes it easier to leverage and respond to global threat intelligence. It also makes it possible to gain system-wide visibility. These are the enablers of both modernization and better security.

The challenge for many CIOs, however, is determining what features and functionality in networking products, such as switches, are essential when budget resources are tighter than ever. Another challenge is determining what minimum specifications commercial sector and government decision makers should accept when looking to upgrade their networks.

HERE ARE SOME CORE QUESTIONS TO ASK WHEN CONSIDERING NEW INVESTMENTS:

- Are your network switches designed for security, mobility, IoT and the cloud?
- Can you centrally manage policy enforcement for simpler control?
- Is automation built-in to handle mundane day-to-day operations, allowing you to shift IT time and money to focus on creativity and design?
- Are your switches gathering information, making correlations, learning about threats across the world and automating responses to threats before, during and after an attack?
- Does your network infrastructure provide true visibility into wired and wireless networks, creating a single network fabric?
- Does your network switch have the ability to report 100 percent net flow without hindering performance?
- Does your network support Encrypted Traffic Analytics, Trustworthy Systems and advanced security capabilities that help enable segmentation and micro-segmentation?

The architectural approach — what Cisco calls simple, open, automated — enables organizations to undergo modernization and security improvements in a more holistic manner. All Cisco products, for instance, leverage open APIs. But the ultimate goal is automation, whether those functions are between Cisco products exclusively or with other products.

For example, Cisco's Digital Network Architecture (DNA) gathers information from a constellation of devices and device types, streamlining the ability to correlate data and apply insights. It can identify otherwise invisible threats and automate security responses. And it constantly adapts and protects by learning about threats across the world to stay ahead of potential attacks.

The architecture builds on a BDA strategy—Before, During and After. Before an attack, Cisco software provides comprehensive visibility and awareness of what's on your extended network so you can implement policies and controls to defend it, according to Peter Romness, Cisco cybersecurity solutions lead for U.S. Public Sector. Continuous monitoring across all of the possible attack vectors during an attack enables IT security leaders to thwart the attack and gather information about it. After the attack, the software helps you know what hit you, repair the damage it did and get back to the mission of your agency, Romness said.

5 STEPS TO NETWORK MODERNIZATION AND SECURITY

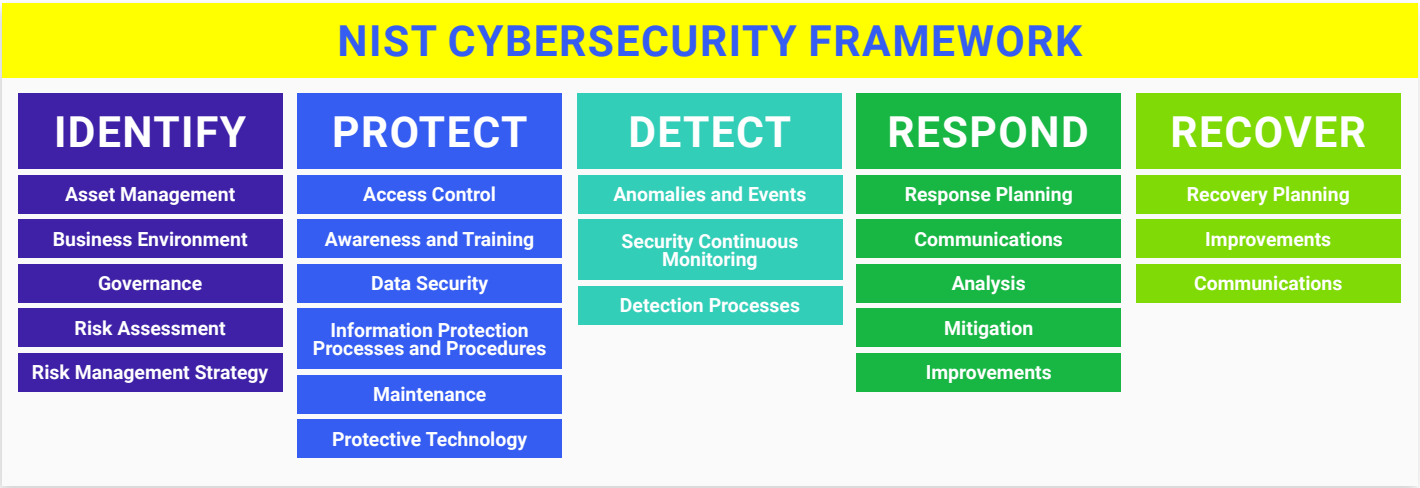
1. **Develop a plan.** Using an architectural approach, plot out the systems, processes and job categories that you need to modernize. Prioritize them so that you can tackle them in manageable increments. Include obtaining leadership buy-in and cybersecurity in the planning stage.

2. **Start with the network.** The network is the backbone of everything you do in IT. It should usually be the first thing you modernize. Replacing older switches and routers with new, smart, intuitive versions immediately multiplies security, speed and efficiency to make other steps in modernization easier.

3. **Leverage software and services.** Many things that used to be hardware based are controlled by software now. A Software Defined Network (SDN), for example, reduces agency costs through policy-enabled workflow automation. Switches based on a Digital Network Architecture with Software Defined access turn a network from simple connectivity to a platform for delivering services.

4. **Integrate the cloud into your migration plans.** The cloud enables modernization without the need to "rip and replace" on-premises systems. Cloud services that comply with the Federal Risk Authorization and Management Program (FedRAMP) offer added assurance that a cloud offering meets federal requirements.

5. **Deploy security from core to edge.** By increasing visibility across your entire network and using a network-as-sensor approach, you can block malware before it enters your network, detect malicious code hiding in encrypted data and even analyze data to better understand threats and improve future defenses.



Future proof and alignment

The central question facing CIOs and CISOs — "Are we secure?" — can never be answered definitively. But the correct answer for enterprise IT leaders, especially in light of the National Institute of Standards and Technology's Cybersecurity Framework, is to ensure that they have used a risk-based approach to determine their IT risks in order to prioritize investments.

The NIST Cybersecurity Framework, which was released in 2014 and revised in December 2017, is quickly becoming the de facto standard for both government and industry. Cisco has aligned its products to the NIST framework. It is important to understand that the Cybersecurity Framework is guidance, not a step-by-step roadmap. Organizations must make risk-based decisions to fit their own individual circumstances. Used correctly, though, it helps you understand, manage and reduce your cybersecurity threat exposure. The framework can help you determine your most urgent needs so that you can invest intelligently.

Increasingly, that also means assessing how your network connects to the cloud service providers. While federal agency CIOs and CISOs need to be sure cloud services meet federal risk and authorization management (FedRAMP) standards, commercial sector enterprises are likely to see added security benefits from working with cloud providers that have received FedRAMP authority to operate.

FedRAMP authorization means that cloud offerings meet the federal government's stringent security requirements, as verified by an independent auditor. Cisco's FedRAMP-certified cloud solutions, for instance, feature extensive security controls and processes that meet federal cloud security standards.

In addition, Cisco offers Cloudlock, a multi-mode, cloud-native Cloud Access Security Broker that helps organizations, including federal agencies, securely leverage the cloud for apps they buy and build. Cisco Cloudlock delivers security for any cloud application and platform, including IaaS, PaaS, and IDaaS, and orchestrates security across existing investments, using open, automated APIs.

The cloud enables modernization without the need to "rip and replace" on-premises systems. In many cases, government agencies as well as commercial enterprises can replicate and even enhance the functionality of a legacy system by subscribing to it as a service via the cloud. This makes modernization possible without accepting additional risk.

But without a strategic approach to using network architecture, enterprises will find it difficult to keep up and adapt as the threat landscape changes. They won't be able to simplify and automate security processes to ensure rapid and remote policy enforcement. By increasing visibility across your entire network and using a network-as-sensor approach, enterprises can also isolate malware before it enters their networks, detect malicious code hiding in encrypted data and even analyze data to better understand threats to improve future defenses.

This article was produced by cyberscoop | fedscoop *for, and sponsored by,* CISCO