WHITEPAPER

Securing Government Networks

Cybersecurity tops the list of federal concerns for 2022, as it has for many previous years. But with the expanded attack surfaces that come with remote work, and increasing migration to the cloud, it's getting more complicated.

Report after report finds not only escalating numbers of cyberattacks, but more sophisticated attacks as more devious hackers, nation-state involvement and insidious trends like ransomware-as-a-service take a deeper and deeper hold.

As the workforce embraces remote work as a ready alternative to office work, we can add that to the list of perennial worries. Unfortunately, bad actors have found remote work easier to disrupt, given its broader attack surface. With many public sector employees determined to continue working remotely at least part of the time, the threat isn't likely to go away soon.

Yet another factor contributing to remote work cybersecurity concerns is the growth of cloud computing. The expansion of cloud computing has essentially eliminated network perimeters. Finally, the trend toward greater collaboration and data-sharing has helped bring the issue of cybersecurity to the fore.

"There has been a significant shift in mindset by the adversary; today, every target is a value target," said **Chris Roberts**, federal technology director at Quest Software. "That makes security broader than just an IT responsibility. We now recognize the role that every user and corresponding endpoint plays within the complete information security model for operations."

While agencies have made significant headway in securing their networks, most still have work to do. For example, the switch to remote work compelled agencies to better understand which devices are on their networks. At the same time, agencies can't know exactly how remote employees are connecting—whether the network or WiFi connection, for example, is fully secure.

Truly securing federal networks requires embracing zero trust in a big way. Zero trust addresses security at all levels of the agency by refusing access until anything attempting to use the network—APIs, nodes, people or devices—is fully authenticated.

A four-pronged approach to securing government networks

Fully protecting networks requires comprehensive zero trust at every point. "You can't effectively secure something if you don't know where or what it is," Roberts said. In other words, a full inventory of assets and users is a critical first step. Without that, full security will remain elusive.

1. Know what data is in your network and who has permission to access it. More than anything else, hackers want data they can use for purposes of extortion or to aid in launching even more lucrative cyberattacks on agencies. Cyberthieves will go after any type of data they consider potentially valuable, from classified military data to health and financial information of government employees and private citizens.

PRODUCED BY: FCW SPONSORED BY: DLT A TECH DATA COMPANY | Quest Public Sector

The first step in protecting that data is knowing what type of data you have, where it is located and who has access to it. Doing this effectively requires good data governance—understanding exactly who has specific rights to view, access or manipulate the data based on their role, and whether the person is in a secure place to access the data. This involves cataloging the data and applying metadata to it. With this structure, it's much easier to classify data properly, determine where it is at all times, who controls it, and who is authorized to access it.

That's where role-based access comes in; only users with the right roles should be able to access the data. "There should be no assumptions about who I am or what my role is," Roberts explained. "If I'm not a fuel tech on the runways, I have no business grabbing a gas tank and attaching it to an F-15. It's the same with any type of data."

2. Know your nodes. Unlike the past, when nodes were basically endpoints, nodes today can be just about anything with an IP address on a network. That means not only PCs, tablets and smartphones but IoT devices like smart thermostats, security systems, and even intelligent Heating Venting and Ai Conditioning (HVAC) systems. Smart hackers know how to infiltrate these devices. That means agencies must be able to scan them, patch them and block ports on the devices.

Protecting all nodes requires knowing every IP address and node and whether there is anything at the end of the IP address like a port scanner listening on specific ports. With that information, network administrators can proactively shut down certain ports. It's virtually impossible to account for all nodes manually, but there are tools that help automate the process.

3. Know your APIs. Older systems typically operated in closed network environments with defined perimeters, making security relatively straightforward. In these environments, ports generally covered all connectivity options. Modern architectures are different. Most are integrated with services built on open standards, running on the Internet in some type of cloud environment. Agencies also use more cloud-based services than ever before, from software-as-a-service (SaaS) to platforms and infrastructure as a service. These use APIs to provide interconnectivity. In most cases, APIs are baked into the applications and services agencies are using.

All of this means that it's as important to apply zero trust to APIs as it is to apply zero trust to other parts of network security. It can get complicated, especially when agencies use external services or SaaS-based applications but aren't aware of the APIs. Yet APIs are critical entry points today. To make sure you have a full inventory of APIs, Roberts suggests communicating

USE FEDERAL SECURITY GUIDANCE TO YOUR ADVANTAGE

Agencies looking for inspiration to improve network security have no shortage of guidance. Here are four great sources:

- Executive Order on Improving the Nation's Cybersecurity. This is a good place to start. It explains why modernizing and implementing stronger cybersecurity standards is so critical, and emphasizes the importance of a zero trust approach. It also strongly advises agencies to embrace multifactor authentication and encryption and accelerating the move to secure cloud services.
- CISA's guidance on securing federal networks. CISA provides practical implementation guidance around how to patch, inventory and block threats.
- NSA's Network Infrastructure Security Guidance. This report outlines best practices around perimeter and internal network defenses to improve monitoring and access controls throughout the network.
- NIST's Zero Trust Architecture Model. Also called NIST SP 800-207, the model explains how to achieve zero trust.
- TIC 3.0 The latest version of the Trusted Internet Connection (TIC) expands the idea of securing an agency's perimeter based on a traditional network architecture to one that accounts for multiple and diverse architectures. This flexibility enables agencies to implement security capabilities in the way that best fits their network architectures, IT modernization roadmaps and risk management approaches. TIC 3.0 also broadens the concept of TIC to include cloud, mobile and encrypted applications, services and environments. environments.

> **"It ensures that if you have a domain administration account, you know exactly who will be using it, what time they can use it, or what location or machine they can use it on."**
>
> CHRIS ROBERTS
> Federal Technology Director, Quest Software

with all vendors supplying technology to your environment. To really make sure, however, he also recommends using technology to deeply inspect every application.

4. Know your users. Identity itself is a critical attack vector, prized by adversaries, who steal credentials to impersonate users and infiltrate networks or launch full-scale social engineering attacks. Most important, Roberts said, is knowing the authenticity of a user before authenticating the user. That means understanding what they do, whether they are coming from an accepted IP range or block of addresses, where they are geographically located, and how they are connecting.

That's why so many organizations today have turned to tactics like multi-factor authentication (MFA) to verify identity, and behavioral analytics to get down to the details, such as how specific users use their mouse and keyboard. This information can form a baseline for how specific users behave over time. With this information, it's easier to spot unusual behavior and when spotted, agencies can lock the user out, restrict their access or require an additional layer of authentication.

Yet many organizations make assumptions about secure identities that can lead to big problems. For example, it's not uncommon for IT operators to assume that if users are listed on Active Directory, there is no need for additional security. While identity in Active Directory is critical, it's more than a network authentication tool. At its core, it's a relational database with username principles, machine IDs and other directory-based information.

For hackers, the real prizes to be won through Active Director or LDAP are domain controllers, because that's where the database of user accounts is located. They can often get there by compromising domain administrators themselves. If the wrong people access privileged accounts, they can do real damage. They can reroute application changes or network paths, for example.

Preventing this requires privileged account management, which allow agencies to secure, control and audit privileged accounts by providing appropriate access. "It ensures that if you have a domain administration account, you know exactly who will be using it, what time they can use it, or what location or machine they can use it on," Roberts explained.

Network security is non-negotiable

While it can be a bit overwhelming to address all the angles necessary to truly secure agency networks, there is really no choice. One way to simplify it is to bring it back to basics—zero trust, for everything from data, APIs, nodes and ports to users.

That means avoiding superusers whenever possible. There are always at least a few people in any organization who want access to everything, but providing that freedom is dangerous. "The more superusers you have, the more at risk you are, because you have now moved away from a role-based authentication model to a trust model where you are giving people the keys to the kingdom," Roberts said. "It's the opposite of zero trust."

It will get easier, Roberts expects, as vendors continue to improve security capabilities. Today, for example, machine learning and artificial intelligence are going a long way toward improving network management and security. It's just a matter of accepting that these technologies are an important path forward.

"We have to get more prescriptive about letting machines analyze data. It's the perfect application for machine learning," he said. "The more analytics we get, the better and faster our responsiveness to cyber incidents will become."

Learn more at questpublicsector.com Quest Public Sector

About Quest Software Public Sector, Inc.
Quest Software Public Sector, Inc., part of Quest Software, provides software solutions that make the benefits of new technology real in an increasingly complex IT landscape. With 30+ years' experience, Quest is a global provider to more than 130,000 organizations across 100 countries. From database and systems management, Active Directory and Office 365 management, and cyber security resilience Quest Software Public Sector, Inc. helps government agencies tackle their next organizational initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com/fed.