Network Access Control: Your First Line of Cyber Defense

MARKET TRENDS REPORT

govloop

FORCE 3
A SIRIUS COMPANY

Introduction

Every day, the Department of Defense (DoD) blocks an estimated 36 million emails containing malware, sent in hopes of gaining unauthorized access to military systems and national security data, according to the Defense Information Systems Agency (DISA).

When national and citizen security is at stake, the ability to control who has access to federal agencies' networks is critical — and growing evermore complicated.

These networks provide the backbone for creating, storing and transmitting personnel records, intellectual property, healthcare data and our country's most sensitive information. It's the kind of data that could be detrimental to your agency, not to mention national security, should it falls into the wrong hands.

For the IT professionals charged with permitting and denying access to those networks, the job has become increasingly complex.

Today's more mobile and connected workforce introduces new challenges for government agencies trying to permit sufficient access to the required resources and to restrict access only to those who truly require it. Agencies must balance the need for network access by employees alongside the requirements to defend the network against a barrage of cyberthreats and risks. On top of that, agencies must adhere to strict compliance regulations.

As network boundaries increasingly extend beyond physical walls, network access control provides a first line of defense from insider and external threats. To take advantage of the security provided by network access control, agencies must ensure they're properly defining network boundaries to include remote and field workers, while also exploring opportunities to automate security processes where possible.

In this report, GovLoop partnered with network security company Force 3 to examine and define the current challenges agencies face when securing their networks. We'll also highlight the comprehensive approach required to address evolving security needs and challenges.

BY THE NUMBERS

33,632

security incidents reported by federal agencies to the Homeland Security Department's U.S. Computer Emergency Readiness Team in 2016.

Source: Government Accountability Office

70%+

of federal agencies have employed strong anti-phishing and malware capabilities to help safeguard their networks from malicious activity.

Source: Fiscal 2016 E-Gov report to Congress

82,384

publicly known cybersecurity vulnerabilities and exposures were identified by the National Institute of Standards and Technology as of Feb. 9, 2017, with more being added each day.

Source: Government Accountability Office

$15 billion

is the amount requested in the president's fiscal 2019 budget for cybersecurity, a 4 percent increase above the fiscal 2018 estimate.

Source: The President's Fiscal 2019 Budget Request

"Strengthening the cybersecurity of federal networks, systems and data is one of the most important challenges we face as a nation."

- THE PRESIDENT'S FISCAL 2019 BUDGET REQUEST

THE CHALLENGE

Monitoring and Controlling Network Access

Identifying and correcting network vulnerabilities is a 24/7 operation that must evolve as cyberthreats evolve. To stay current with ever-changing commercial and government regulations, agencies can't rely on antiquated solutions and operational procedures.

Such a reactive approach to security focuses on addressing current and near-term cyber issues, but does not include longer-term planning or responses for future threats. It also doesn't position agencies to proactively comply with security requirements that govern how they should manage network access across multiple devices and users.

To prevent the risks of unauthorized access to high-value assets or the loss of sensitive data, network access control is mandated by Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standards (FIPS) guidelines, along with various DoD regulations. There are also network access requirements set by the Federal Risk and Authorization Management Program (FedRAMP), which developed a governmentwide baseline for securing cloud products and services used across agencies.

But implementing and enforcing these mandates requires sufficient funding and skilled professionals who understand the right tools and techniques. "The biggest challenge that we're seeing is either a lack of resources or a lack of the training and knowledge necessary to keep the network running or to be able to secure it," said Pete Burke, security practice team lead at Force 3.

This is especially challenging because a number of agencies have cybersecurity-related spending and duties that extend beyond the protection of their own networks, instead serving a broader cybersecurity mission. For example, DHS is charged with overseeing various programs aimed at improving network security and protecting government data across civilian and defense agencies alike.

Failure to implement these types of programs exposes federal agencies to greater cyber risks at the network, system and data levels.

THE SOLUTION

Agencies need a comprehensive, multi-faceted strategy — one that provides the broadest, most inclusive view of their network.

But to get there, agencies must first understand who and what is trying to connect to their network. When it comes to regulating the continuous flow of activity, the first line of defense is network access control. Having this capability empowers agencies to immediately deny unidentified users, thus eliminating the potential for unauthorized access to data or other resources. Ultimately, strong network access control allows agencies to remain compliant.

The network access control solutions agencies adopt should authenticate that users are who they claim to be, and that the devices they use comply with agency security requirements. They should also account for different user types within the government workforce. For example, two people may perform the same job, but one is a government employee, and the other is a contractor.

"What we're able to do by utilizing network access control is to have those users identified automatically when they connect to the network and have a policy applied to both users that is slightly different to allow access to what they need," Burke said.

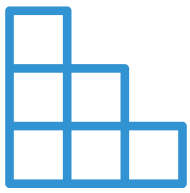
By coupling automation with network access control, agencies will see even greater benefits. Having automated capabilities in place standardizes how network access is managed, and it also frees IT personnel to work on more complex tasks that require the expertise of skilled professionals.

Implementing network access control comes in different stages, Burke said. "First, make sure you're comfortable with the authentication piece, then on to automating access control and finally adding the ability to remediate machines based on compliance. It's a crawl, walk, run mentality."

Next, let's review several best practices for implementing a comprehensive approach to network defense.

BEST PRACTICES

Developing a Comprehensive Approach to Network Defense



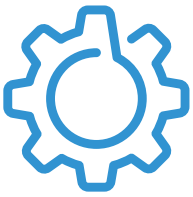
1. Set a solid foundation

When implementing network access controls, you have to ensure the technology you implement properly enforces security polices and that users are authenticated before gaining network access. When the time comes for your agency to undergo auditing procedures, you must be able to show these security measures are in place and effective.

2. Focus on authentication and access control

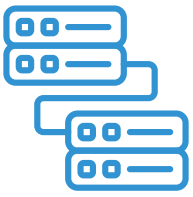
The network access control solution you use should be able to identify users by their unique profile and the device they are using. Once that is determined, access can be granted or denied. As a best practice, Burke recommends that once users are authorized on the network, they be given access only to what they need.

It isn't enough to simply authenticate users' identities before giving them network access. Controlling what they can and cannot do within the network is also critical to security. "We've seen where different agencies are authenticating the assets and users on the network, but they're not enforcing any access control, which defeats the purpose," Burke said. Authentication is part of the process, but it isn't the only step.



3. Automate network access control

Over time, agencies should reach a point where they can automatically remediate network access issues. That includes quarantining devices that are trying to connect to the network, but don't meet an agencies standard levels of compliance. As your implementation of network access control evolves, you should consider how these and other tasks can be automated.

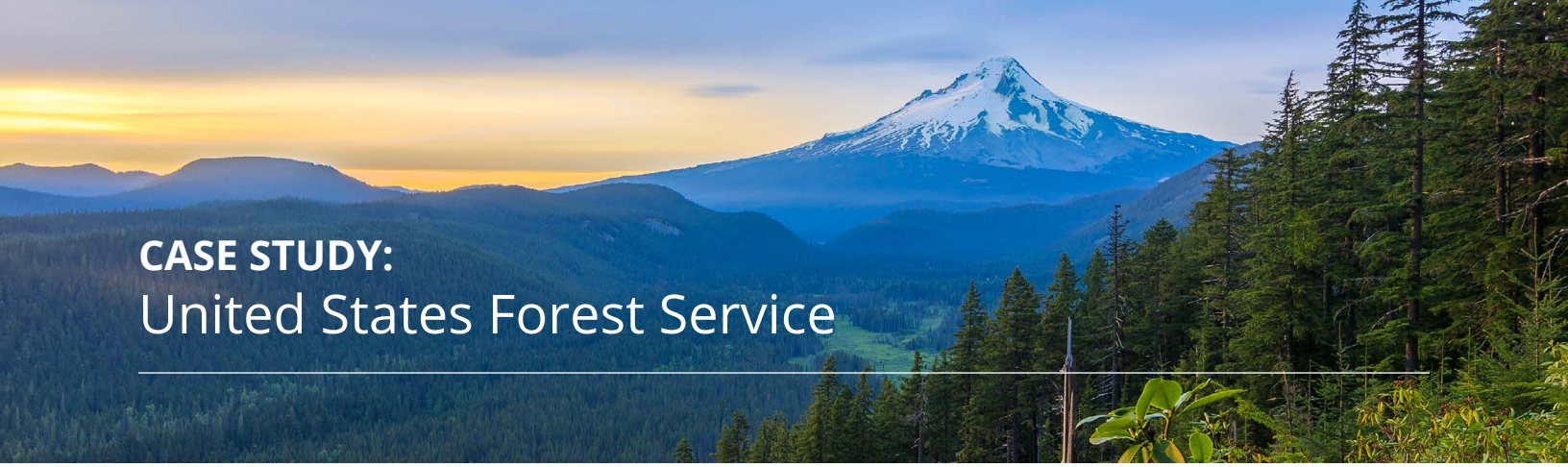


4. Increase network visibility

Burke recommends that agencies also improve the level of visibility that IT teams have into all of the traffic moving across the network. Boosting visibility involves monitoring network traffic flows, controlling network access, ensuring connected devices are compliant, performing remediation requirements and tracking which applications and systems that users can access. By doing so, agencies can create a baseline of network behavior and heuristics, enabling them to identify insider threats or malicious network activity that deviates from normal behavior.

5. Provide adequate training for your workforce

Identify opportunities to train or re-train IT personnel who will be involved in implementing network access controls. Ensure they have the knowledge and resources they need to maintain network security and availability. Through industry partnerships, you can learn new skills and also supplement your current workforce.



CASE STUDY:
United States Forest Service

The U.S. Forest Service faces a unique challenge when it comes to maintaining government-issued devices and ensuring they are secure and compliant before firefighters use them on the network.

In addition to the Forest Service's full-time staff, there are also seasonal employees who need access to technology and the network at various times throughout the year. Some employees work for a limited number of hours during the summer, which is peak fire season. Other permanent seasonal positions require employees to work for 26 weeks and have 26 weeks off.

"For six months out of the year, their laptops and tablets are sitting on the shelf," Burke said. "They are expected to grab those devices and to immediately be able to start working remotely wherever they are needed at the time. They need access to internal networks and different data points."

This creates a large undertaking for the IT department. They have to bring the laptops in for patching, antivirus updates and any necessary upgrades to ensure the devices comply with agency security requirements.

The Forest Service partnered with Force 3 to implement a governmentwide program called Comply to Connect.

Here's how it works: Let's say an employee uses a smartphone to remotely connect to the agency's network. When that employee's device requests network access, that action activates a scan of the device to ensure compliance.

The scan, Burke explained, determines if software patches are updated, if the antivirus software is current and running, and if any security vulnerabilities are present. That kind of integrated scanning is a feature of a network access solution provided by Cisco called Identity Services Engine, or ISE. Cisco ISE helps ensure that only authorized users gain network access and that those users have approved computers that meet the agency's security policies.

"We've integrated that VPN [virtual private network] connection in with the network access control solution," Burke said.

When employees bring those devices online for the first time, they are often noncompliant because they've been out of use for an extended time. ISE quarantines the machines until they are updated and only allows users to access what they need on the network to do their jobs.

HOW FORCE 3 HELPS

As a leading network security company, Force 3 provides the experience and expertise agencies need to implement effective, efficient and powerful access control. Its team of highly trained and highly specialized engineers provide technical expertise and a comprehensive, vendor-agnostic approach to providing technology solutions that align with federal compliance requirements.

The goal, Burke explained, is not to sell a particular solution. "The first thing that we do," he said, "is try to find an agency's pain points, the problem they need resolved and where they're having issues across their network."

When partnering with Force 3, agencies will review what mandates or compliance measures they need to meet and timelines they must adhere to. "We're trying to identify the customer issue," Burke said. "Once we do, we'll build a solution that resolves the problem." Learn more here: www.force3.com

Conclusion

Strengthening the security of government networks, systems and data is one of the most pressing challenges agencies face. It requires a comprehensive approach to security, and it starts with managing who has access to your agency's most valuable asset: data.

To guard against insider and external threats, agencies need a network security strategy that goes beyond authentication. That strategy must account for the level of access users have to agency data and systems once they are connected to the network.

Implementing these security measures will ultimately ensure your agency is in compliance with government standards and better equipped to defend against evolving cyberthreats.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

ABOUT FORCE 3

Force 3 is *the* Network Security Company. We provide secure IT solutions and services for clients who demand value and reliability. Together with our parent company, Sirius Computer Solutions, we offer a wide range of solutions and services backed by expert engineers and strategic partnerships.

From design to deployment, support and maintenance, we constantly focus on supporting our customers' missions and promoting the best possible outcomes. Your success is critical to us—and we don't succeed unless you do.

To learn more, visit www.force3.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop