Making Smart Use of One-Time Cybersecurity Funding:

Tactics for Sustainability and Ongoing Success

Funding from the American Rescue Plan Act and the Infrastructure Investment and Jobs Act provides state and local governments a critical opportunity to catch up on modernization and long overdue investments in cybersecurity. As IT and cybersecurity leaders strategize on how to spend this funding, they must also prepare for what happens once investments are in place. It's all too easy to focus on the new technology and overlook its impact on the organization's people and processes. In addition, organizations that adopt an upgrade/refresh mentality may miss out on the flexibility, scalability and stronger risk posture that a long-term roadmap for cybersecurity provides.

Given the high stakes that go along with receiving potentially millions of dollars in taxpayer money, many leaders are asking how they can set themselves up to successfully manage and maintain technology investments even as funding runs out, staff headcounts remain the same and cybersecurity challenges continue to grow. Key tactics for ongoing success include simplifying management, leveraging intelligent automation, and educating business and IT staff. A fabric-based cybersecurity platform powers these tactics and ensures technology investments stand up to change, growth and innovation while minimizing impact on staff.

The never-ending cybersecurity workday

Cybersecurity teams face the following challenges on a daily basis:

New vectors and an expanding attack surface. Remote work, cloud environments, digital services and operational technology (e.g., transportation control systems and water management systems) have greatly magnified the attack surface and pushed it beyond the perimeter of traditional cybersecurity controls.

Financially motivated cybercriminals with state-of-the-art arsenals. Criminals are using artificial intelligence, machine learning and other advanced technologies to act as force multipliers and ferret out vulnerabilities inside organizations. Ransomware-as-a-service makes it easier than ever to execute an attack, and criminals are demanding ransoms both to unlock encrypted systems and prevent exposure of breached data.

Overwhelming volume of alerts. As the attack surface expands, cybersecurity incident response teams must manage an increasing volume of information coming from device logs. Filtering and analyzing alerts to prioritize and act on the most relevant events is tedious and stressful and contributes to "alert fatigue" and errors.

Lack of security visibility. Many organizations use a patchwork of standalone security products, which creates potential gaps in security and makes it cumbersome to accurately determine and address the organization's security posture across all domains within the enterprise (e.g., data centers, wide area networks, the cloud and edge computing environments).

Staffing and skills shortages. Smaller local governments may have very few (if any) personnel devoted full time to cybersecurity. The more thinly stretched they are, the more difficult it becomes to maintain and manage new technology investments.

WHAT IS A SECURITY FABRIC?

A security fabric is a technology solution and approach where a range of cloud-native cybersecurity solutions are designed from the ground up to work together seamlessly across environments (i.e., domains) regardless of their physical or virtual location. A security fabric simplifies navigation between security devices, consolidates device data and centralizes policy management. Unlike best-of-breed solutions that often leave gaps in security, a security fabric ensures full coverage across any application or deployment environment. In addition, it creates efficiencies and synergies that are difficult to achieve otherwise. A similar concept is a security mesh architecture, which focuses on defining the security perimeter around the identity of a person or thing, regardless of where they exist in the enterprise.[1]

Essential tactics for scaling staff and sustaining new technologies

The following tactics help organizations scale staff capabilities and sustain investments. The foundation of their success is a security fabric.

Cross-domain visibility

Because tools in the security fabric are seamlessly integrated across the enterprise, staff can see and manage cybersecurity for the entire range of domains through a single pane of glass. This centralized system reduces management complexity, enables security teams to share threat intelligence across solutions and helps teams more easily protect the entire attack

surface. Instead of focusing on individual enforcement points and appliances, security personnel can operate from a higher-level perspective that takes into account all relevant events and enables personnel to prioritize activities based on complete data.

Artificial intelligence and machine learning

AI and ML enable organizations to scale staff capabilities and continuously improve threat response through adaptive security orchestration, automation and response (SOAR). Instead of having security staff manually sift through security alerts and mitigate routine incidents (for example, phishing emails), organizations can automate filtering workflows and create self-healing networks. On the back end, organizations can incorporate AI and ML to correlate and analyze suspicious behavior, threat intelligence, security device data and other contextual information. As security operations mature, organizations can feed that intelligence back into an AI engine to automate intelligent event response workflows while also creating a virtuous cycle of improvement.

Tutorials and training

If cybersecurity teams don't know how to use technology properly and aren't leveraging all its features, an organization can't realize the full potential of its investment. Worse, leaders may have a false sense of security about the organization's risk posture. Training and support help staff get up to speed quickly on new products. A trusted partner can be a valuable resource for training and support materials such as user guides, videos and online tutorials that walk staff through issues when they arise. In many cases, these materials enable staff to resolve issues more quickly and cost-effectively than they could if they had to bring in third-party support — all while building the internal skillset.

Getting the most mileage from investments

The following best practices help organizations maximize technology investments and sustain them over time:

- Gain executive sponsorship to ensure the entire organization is properly prepared for change and embraces new technologies.
- Develop a long-range view of revenue and expenditures to ensure funds will be available to maintain technology investments once federal funding runs out.
- Work with lines of business and other functions to clarify and prepare for other teams' potential technology investments.
- Focus on a long-range security roadmap versus refresh and upgrade cycles to help advance security goals overall.
- Team with a trusted partner to fill in gaps in expertise, staffing and technology and for specialized tasks such as DevOps, training and incident response.

SCALING CAPABILITIES WITHOUT ADDING STAFF

The Spring Branch Independent School District in Texas serves about 35,000 students and 6,000 staff. The district is using Fortinet's Security Fabric tools to keep students, staff and systems secure across its 47 campuses.

"The advantage of the Fortinet security fabric is the single pane of glass," says Troy Neal, executive director of cybersecurity and technology operations for the district. "I do not want to have to go to five different interfaces to figure out a problem. With a team as lean as ours, we cannot be there in person every time someone has a security question."

The Fortinet management tools save about four hours a day for his team of two. These capabilities, along with FortiSOAR and other security fabric tools, ensure Neal's team can continue to carry out its mission even as the district grows and new technologies are added.

"I am not going to get a bigger security team, and frankly I do not even want a bigger team. School districts have to maximize the dollars that are available to us, and to my mind, the best way to do that is through automation and streamlining management processes as much as possible," Neal says.[2]

Money well spent

Federal funding gives state and local governments an important opportunity to transform their cybersecurity programs. Organizations that invest strategically in a security fabric can address immediate issues while also setting themselves up to function more efficiently and innovatively in the years ahead.

This piece was developed and written by the Government Technology *Content Studio, with information and input from Fortinet.*

1. Gartner, Inc. Top Strategic Technology Trends for 2021. https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021
2. Fortinet Case Study. How a Lean Team Is Keeping K-12 Students and Staff Secure. July 2021. https://www.fortinet.com/content/dam/fortinet/assets/case-studies/cs-spring-branch.pdf

PRODUCED BY: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education. **www.govtech.com**

FOR: FORTINET

Fortinet secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network — today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. To learn more, visit **www.fortinet.com**.

IMAGE PROVIDED BY: SHUTTERSTOCK.COM