Modernizing government security operations

How to build a strategy for the challenges of today and tomorrow

verizon

The digital landscape has entered a new era

Today, our digital world is being shaped by the exponential growth in Internet of Things (IoT) devices, large quantities of data sourced from an endless stream of individual and group activities, rapid emergence of artificial intelligence (AI), changes to how work is performed, and rising expectations from people on how data and technology can aid and transform their day-to-day lives.

Federal, state and local governments are at the forefront of these trends, as policy-makers and technology leaders seek to not just better manage the flow of information and deliver services the public expects and needs, but also better secure the vast amounts of data being shared and the networks they rely on.

According to Gartner, global government IT spending is poised to grow by 7.3% and reach nearly $590 billion in 2023.

For the U.S. government, the Biden administration is seeking to increase federal IT spending for civilian agencies by 13% to $74 billion. The total amount of the increase is directed towards securing networks, applications and data.

Meanwhile, at the state and local government level, projections foresee steady growth in IT spending from roughly $137 billion in 2023 to $177 billion by 2028. Federal stimulus funding from programs like the Bipartisan Infrastructure Law (BIL), also known as the Infrastructure Investment and Jobs Act (IIJA), are expected to provide state and local governments with additional funding to improve internet access and enhance cybersecurity.

However, even as federal and state governments have increased spending on technology and networks, several problems remain.

Not enough cybersecurity and IT professionals to fill crucial roles

One of the most significant problems facing all industries, including the public sector, is that there are not enough cybersecurity and technology professionals to fill essential roles.

According to Cybersecurity Ventures, there are about 3.5 million open cybersecurity jobs worldwide. Data from Cyberseek, a cybersecurity industry research company, says that in the U.S. there are about 770,000 open roles across all industries.

When it comes to the federal government, there are an estimated 39,000 unfilled cybersecurity jobs. The cybersecurity staffing gap has reached the point where Department of Commerce CIO, Andre Mendes, pointed out in 2022 that federal agencies are hiring people from different federal agencies. He said, “We’re stealing people from each other, that’s what it’s come down to.”

State and local governments do not have it any easier. Retention of skilled IT and security professionals has proven to be especially difficult. During the Public Sector Workforce Summit in Washington, D.C. in August of 2023, speakers noted that IT and cybersecurity staff are often retiring faster than agencies can replace them. While vacancies in cybersecurity create challenges, they are not the only problem as state, county and local governments are struggling to hire people with experience in application development, data analytics, systems integration and enterprise architecture.
For federal and state government agencies responsible for large and critical systems that process vital data, this shortage of skilled in-house technology professionals reduces the effectiveness of network and security operations by overloading understaffed teams and slowing down both the accuracy of and responsiveness to problems and threats.

770,000

open roles across all industries in the U.S.

39,000

estimated open roles in the federal government.

Lack of automation and data-driven decision making

In addition to staffing challenges, the lack of automation and data-driven decision making has weakened the security posture for many agencies.

Legacy systems are more dependent on human-led observations and a manual setting of security rules, which can lead to errors or omissions. What's more, these systems do not have the deep analytics needed to pull insights from all the interactions taking place across a network and process how data and workloads are moving from the edge to the cloud and whether or not threats are encountered along the way.

In other cases, legacy systems are simply not designed to see newer technologies, like IoT devices, on the network, which means they can neither protect them nor can they spot breaches that allow malware to infiltrate and move laterally through the network.

Attack surface vulnerable to breach is growing

One of the most significant challenges to cybersecurity strategy and operations has been the union of IT networks and Internet-enabled Operational Technology and IoT devices. The data and workloads from these systems and devices use networks, but are often not visible to legacy IT security solutions.

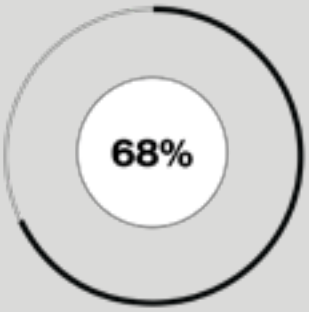
To make the situation more difficult for security teams, these systems and devices are growing exponentially, often lack their own encryption, and possess vulnerabilities that can be exploited by bad actors as data and workloads move from the edge to the cloud. In short, the attack surface security operations teams need to manage is constantly growing and becoming more complex. Government agencies can no longer take a human-centric and network-centric view to cybersecurity. The growing and multifaceted nature of these challenges underlines the need for a holistic and scalable approach to security that addresses both external and internal threats at the same time as aligning with the demands of the cloud and connected device era.

Cybersecurity threats are increasing on all fronts

The threats to government agencies also have increased, but prevention has not significantly improved.

Government agencies are challenged by a lack of visibility to their ecosystems from the edge to the cloud. The ability to avoid false positives, or respond to serious threats, exceeds the ability of many agency security teams.

According to the United States Government Accountability Office (GAO), Federal Agencies reported 32,511 cyber incidents in 2021, a 59% increase from 19,060 reported in 2016.



68% of all public sector breaches involved the human element – whether through error, privilege misuse, stolen credentials use, or social engineering.

2024 DBIR

31% of all breaches over the past 10 years have involved the use of stolen credentials.

2024 DBIR

61% of CISOs, and 53% of CEOs, feel unprepared for a targeted cyberattack in the next 12 months.

2023 MSI

Meanwhile, a study by Sophos in 2023 indicated “the rate of ransomware attacks in state and local government has increased from 58% to 69% year over year, contrary to the global cross-sector trend, which has remained constant at 66% in [their] 2023 and 2022 surveys.”

Attackers continue to exploit vulnerabilities and compromise sensitive information. The methods used by these bad actors range from the simple (using known vulnerabilities that businesses and government agencies fail to patch in a timely manner) to the complex (using an API equipped with AI capabilities to secure unauthorized access).

At one point, data exfiltration was a technology professional’s biggest threat. Now, bad actors are trying to attack and take control of the infrastructure. To do this, they are expanding their targets to coincide with the growing attack surface available to them.

Executive orders and policy mandates

To address the growing threats, the Biden administration has signed several executive orders and issued memorandums that create new mandates for federal agencies, which could filter down to state governments and private sector businesses. While these initiatives are important steps to better security, mandates or requirements also represent a challenge for federal and state government agencies with limited resources.

For example, President Biden's Executive Order on Improving the Nation's Cybersecurity seeks to improve supply chain software security, increase agency sharing of breach information, advance the movement to secure cloud services and implement zero trust architecture across the government.

The movement to adopt zero trust cybersecurity principles in a memo from the Office of Management and Budget requires agencies adopt zero trust architecture (ZTA) and meet other "specific cybersecurity standards and objectives" by September 30, 2024.

And the executive orders on quantum technology and artificial intelligence also create guidelines and standards for AI safety and security.

Rethinking security operations for today and tomorrow

In order to address these challenges, the approach to security operations needs to evolve for the future.

Traditionally, government agencies have relied on internal Security Operations Centers (SOCs) staffed with a mix of government employees and contracted cybersecurity professionals. This was designed to help SOCs achieve better staffing and maximize expertise on-site.

However, the need to support legacy hardware and software alongside data and workloads from the digital edge to the cloud, combined with securing a growing attack surface, has caused the more manual and human-led security model to break down.

The scale and complexity of securing legacy and cloud infrastructures simultaneously have rendered traditional security operations teams insufficient for both effectively managing their networks and adequately detecting, isolating and responding to threats, attacks and breaches.

To keep up, agencies are starting to rethink their security operations model and adopt a managed security services model that enables a continuous evolution of security tools and processes, integrating automation into every aspect of cybersecurity.

Managed security services provide government agencies access to state-of-the-art technologies they may not have, as well as enhanced automation and specialized expertise. This allows agencies to swiftly adapt, enhance security capabilities, bridge the talent gap, and ensure cost-efficiency.

With a managed services model, agencies can seamlessly integrate people, processes and technology to create an efficient, effective, highly responsive, and transparent security operations environment.

The Verizon Threat Intelligence Platform Service (VTIPS) enables the transformation of threat data from a variety of sources into real-time, actionable intelligence. VTIPS accomplishes this by providing functional tools required to build a unified threat library and share knowledge about adversaries, threat, and vulnerabilities.

Threat intelligence analysts can leverage VTIPS to enrich Indicators of Compromise (IOC) and correlate threats through actively sharing threat intelligence among Trusted Circles of partnering organizations.

VTIPS seamlessly integrates with an organization's security infrastructure to provide accurate and timely alerts needed to detect and stop malicious attacks.

See Verizon Threat Intelligence Services for more information.

Benefits of adopting a managed security services approach

Here are some examples of how integrating a managed services approach can benefit your agency.

Reduce False Positives

With threats spreading across cloud environments, mobile endpoints, industrial control systems and supply chains, machine-based solutions have emerged as game-changers in the landscape of cybersecurity. Their scalability is a key advantage, enabling efficient processing, analyzing, and correlation of complex data at a scale beyond human capabilities.

Machine learning algorithms excel at detecting abnormal traffic patterns, user behavior anomalies, and potential threats that might have otherwise remained concealed. This predictive analysis enables proactive threat mitigation that empowers government agencies to more effectively manage security across diverse infrastructures and stay one step ahead of adversaries.

Improve Threat Detection

How do machine-based solutions enable security analysts to become more effective in their roles? One way is through comprehensive threat intelligence.

Threat Intelligence plays a critical role in determining Indicators-of-Compromise (IOC) that enrich security environments. Experienced Managed Security Service Providers (MSSP) leverage threat intelligence to offer agencies a stand-alone capability for enriching their security environments and delivering timely security alerts that incorporate data from incident responders, malware analysts, dark web threat hunters, and curated open-source feeds. Policy and behavior-based alerting, combined with advanced automation incorporating AI and ML, can offload repetitive tasks (e.g., vulnerability scanning, patch management, blocking and quarantining, threats, log analysis, etc.).

Accelerate Incident Response

Automation is used to enrich ticket information and recommend mitigation techniques for analysts, accelerating incident response. This shift not only frees up valuable human resources, but it also allows for more informed decisions based on enriched ticket information containing actionable intelligence.

Artificial Intelligence (AI) is employed to identify and respond to sophisticated threats by using advanced analytics and intelligent algorithms. By combining human expertise with machine capabilities, security operations centers can accelerate incident response, minimize human error, improve operational efficiency, ensure consistent adherence to security protocols, and swiftly counteract attacks.

Transform security operations with managed security services

As cybersecurity measures continue to evolve, managed services provide a solution capable of adapting to future threats quickly, efficiently, and cost-effectively.

Adopting managed security services involves partnering with experienced teams that are responsible for managing and optimizing an agency's security posture. Partnering with a trusted managed services provider offers unparalleled advantages in navigating the intricacies of modern security challenges. Agencies can tap into a wealth of expertise, resources, and industry best practices.

Below are key benefits of choosing a managed services provider to address pressing cybersecurity challenges:

1. Innovation and Automation Tailored to Mitigate and Defend the latest Threats - A reputable managed services provider empowers agencies with a comprehensive suite of continuously evolving tools and specialized services tailored for hybrid environments. By prioritizing continuous evolution and advanced automation of the security, managed service providers offer cost-efficient security solutions that are scalable to agencies' specific needs, leveraging expertise and partnerships with leading vendors for best-in-class protection in the ever-changing threat landscape.

   What's more, a managed service provider continually updates their analytical tool suite to take advantage of new releases, products, and best practices. Instead of a one-off solution, they build a reusable suite that is cost effective by spreading the cost across multiple customers for the betterment of all.

2. Leverage Advanced Technologies and Expertise from Experienced Professionals - Agencies seek managed service providers that have a demonstrated track record of recruiting and retaining top tier talent, often from government agencies and military units, where they have security clearances and hands-on experience defending against nation state attackers. Partnering with managed services providers grants agencies access to skilled professionals who possess in-depth knowledge of cutting-edge security technologies. By tapping into this collaboration, agencies can bridge the security skills gap, stay ahead of evolving threats, and benefit from advanced solutions and valuable insights.

3. Gain Comprehensive Threat Intelligence - Choosing the right Managed Security Service Provider (MSSP) involves evaluating who can deliver the most comprehensive and actionable threat intelligence, equipping agencies with real-time insights into the ever-changing threat landscape. Proactive identification of emerging risks strengthens defenses and enables rapid response, minimizing the impact of security incidents.

4. Offload Security Management Tasks - Entrusting security management to a managed service provider enables agencies to focus on their core competencies and mission. This streamlines resource allocation, enhances operational efficiency, and ensures visibility and control over the security posture through the provider's expertise.

5. Achieve Full Transparency and Control - Managed services offer agencies transparent visibility through role-based access controls and intuitive dashboards, providing comprehensive insight into all aspects of cybersecurity. This transparency empowers organizations to effectively monitor, manage, and make informed decisions about their cybersecurity posture.

Transforming security strategy for a resilient future

Cybersecurity has changed, because the nature of the threats have changed.

The exponential growth of internet-enabled Operational Technology, Internet of Things and mobile devices, and their integration with the network, is expanding the attack surface beyond the ability of any organization to manage without assistance.

What's more, the scarcity of skilled professionals, the need for big data security analytics, the growing number of insider assisted attacks, and the complexities of managing diverse infrastructures have only increased the urgency for a new approach to security.

To be more successful in this evolving digital age, federal, state and local government agencies need to shift their mindset and embrace a managed services framework that combines humans and machines to identify and analyze attacks utilizing a knowledge base of threat intelligence and attack behaviors.

By pairing an in-house SOC team with managed security services, agencies can leverage the innovation, expertise and resources of trusted partners. By finding the right managed services partner that aligns with an agency's friction points, agencies can access tailored security solutions, advanced technologies, and comprehensive threat intelligence, cost effectively. Most importantly, this is accomplished with security through a fiscal partnership, allowing an agency to have full control over their environment without the costs or risks associated with contract staffing. With managed services and machine-based security solutions combined, agencies create a strong security posture that can effectively mitigate risks and respond to emerging threats.

As agencies navigate the path toward a more resilient future, they must embrace the innovative, collaborative, and the transformative power of managed services. By doing so, they can enhance their security capabilities, protect sensitive information, and adapt to the ever-changing cybersecurity landscape.

For more information on Verizon security solutions for your public sector organization, visit us at: verizon.com/business/solutions/public-sector/security-resources/