FORTINET FEDERAL

ISSUE BRIEF

IT Modernization Brings Benefits, Challenges to Federal Agencies

Early in 2023, the Federal Aviation Administration's Notice to Air Missions (NOTAM) system failed, causing thousands of flight delays and cancellations. The agency attributed the outage to human error. Yet the system's three-decade-long tenure reinforced an essential truth in the Federal technology space: At some point, agencies will no longer be able to support legacy systems. They struggle to find engineering staff to support antiquated programming languages while the cyber threat landscape grows more ominous, endangering already fragile operations. Combine these factors with the growing importance of technology to citizen services plus cybersecurity priorities established by recent executive orders, and agencies face an urgent need for nimble and focused IT modernization.

The Benefits of Modernization

IT modernization is both a necessity and an opportunity. Due in part to fiscal constraints and lengthy procurement processes, the government often lags at least three to five years behind the leading edge of the private sector in IT and security. By modernizing systems and fortifying them with flexible IT infrastructure and security based on principles such as zero trust, Federal leaders can close that gap.

Federal mandates, especially executive orders requiring zero trust security architectures and improved customer experience, are the impetus for many agency modernization efforts. Modernization brings many additional opportunities:

- **Heightened organizational resilience.** Multiple connectivity options and a common operating picture of IT performance and threats across networks and devices enable agencies to recover quickly from unplanned service outages and cyber incidents.
- **Bigger bang for technology bucks.** Convergence of security products and vendors means that one new product can potentially replace a dozen functions performed by legacy systems. An agency might only need to replace one product now, but when it's ready to refresh other products, the functionality to do so may already be built in. For budget-conscious Federal officials, that means spending smarter and getting better results for taxpayer dollars.
- **Increased employee productivity.** Cloud migration and growing implementation of software-defined networking are combining to connect data, devices, and robust, secure computing resources to users in any location. Expanding use of robotic process automation to automate routine, repetitive, and often tedious tasks is further increasing productivity and freeing employees to focus on more complex tasks. These technology trends offer agencies increased agility and flexibility and can also bring cost savings.

The Challenges of Modernization

The escalating Federal IT modernization effort has brought some notable successes: in particular, the Technology Modernization Fund, with an infusion of $1 billion through the American Rescue Plan Act, has helped agencies accelerate legacy system transformation. Yet some experts say they would give the government a grade of B, at best, on its modernization pace so far. Federal leaders' challenges include:

- **Modernizing not only to meet a mandate, but also to meet a mission.** This requires intensive planning based on specific agency circumstances.
- **Ensuring security across cloud environments.** Though it improves security overall, modernization also brings potential security risks. Because cloud environments themselves are more complex, security becomes more complicated as agencies move more functions to the cloud. This is compounded when agencies operate simultaneously in multiple public cloud infrastructures as well as their own private or hybrid cloud. Differences in security capabilities and policies across clouds can create gaps and vulnerabilities, while multi-cloud environments can obscure visibility across the organization. The chain of cloud security is only as strong as its weakest link, and malicious actors can take advantage of any gaps and inconsistencies they find.
- **Incorporating digital innovation at remote and branch locations.** The limitations of legacy wide-area networking infrastructures can lead to performance issues due to traffic bottlenecks, and many organizations experience sticker shock when modernizing branch offices. They also find that upgrading wired solutions at branch offices does little to help remote or mobile users.
- **Funding uncertainty.** Federal agencies are unable by law to initiate spending on new activities during a continuing budget resolution – and with the Federal government operating under continuing resolutions more often than not in recent years, many new IT initiatives have remained on the drawing board.

As agencies grapple with these challenges, they also face ambitions deadlines laid out in government modernization mandates, such as the Biden administration's 2021 executive order on cybersecurity.

Fortinet Federal Solutions Help Address Modernization Challenges

Agencies with agile infrastructures can readily optimize bandwidth and cloud resources with built-in, enterprise-class security. Automation, deep analytics, and automatically adaptive network infrastructure can deliver significant operational efficiencies and help agencies more effectively manage evolving computing requirements. Fortinet Federal provides all of these capabilities – and more – to Federal agencies seeking to modernize for greater agility, resiliency, efficiency, and security.

For more than 20 years, Fortinet Federal has been a driving force in the evolution of cybersecurity and networking and security convergence. More than a dozen years ago, Fortinet Federal recognized the need for automation amid pressing cybersecurity talent shortages and the torrent of data overwhelming IT personnel. Today, its comprehensive on-premises and cloud-based networking and security solutions enable IT and security staff to automate the design, deployment, and operation of large-scale IT environments. Its cloud presence is so strong that Fortinet hardware is often the default technology in many public cloud-based solutions. Fortinet Federal's offerings include:

- **The Fortinet Security Fabric,** a broad, integrated, and automated cybersecurity mesh platform that is essential to reducing complexity and increasing overall security effectiveness across today's expanding networks. Utilizing advanced AI, the fabric is a portfolio of more than 50 security and networking technologies – the largest in the industry – that share threat intelligence, correlate data, and automatically respond to threats as a single, coordinated system.

Gartner recently named this approach a "cybersecurity mesh architecture" and called it a top cyber trend for 2022. Fortinet pioneered it nearly a decade ago with an open architecture designed to connect traditionally disparate security solutions into a unified framework. The Fortinet Security Fabric is built on three key attributes: It is broad, detecting threats and enforcing security everywhere; it is integrated, closing security gaps and reducing complexity; and it is automated, enabling faster time-to prevention and efficient operations. It is an open ecosystem, integrating more than 500 products and services from other security and IT vendors. The Fortinet Security Fabric provides an automated solution that serves as an essential force-multiplier for short-staffed IT and security teams.

> By 2024, organizations that adopt a cybersecurity mesh architecture to integrate security tools, so that they work together as an ecosystem, will reduce the financial impact of individual security incidents by 90 percent, on average.
>
> – Gartner

- **FortiGate Next-Generation Firewall,** which delivers seamless AI/ML-powered security and networking convergence over a single operating system (FortiOS) and across hardware appliances, virtual machines, and SASE services. This provides users with powerful security and networking convergence, industry leading price-per-performance, and AI/ML-powered threat protection.

  FortiGate offers key practical benefits at a time when the Federal government is rapidly moving toward adopting zero trust architecture: It is the only firewall product to natively integrate zero trust network access policy enforcement points. The FortiOS operating system can automatically trigger user verification and device risk assessment for each application session, providing the foundation for building a zero trust edge strategy that enables the increasingly hybrid Federal workforce to connect to applications, while maintaining consistent security.

- **Fortinet Secure SD-WAN,** which combines the protections of a FortiGuard NGFW appliance with built-in advanced SD-WAN networking capabilities to eliminate MPLS-required traffic backhauling, prioritize business-critical applications, and improve the user experience without compromising security.

  The limits of traditional WAN infrastructure and its legacy routers paved the way for software-defined wide-area networking (SD-WAN), which has quickly become the de facto solution for legacy WAN infrastructure replacement. Yet not all SD-WAN approaches are the same. Some simply add basic SD-WAN capabilities to existing legacy routers, adding infrastructure complexity and exposing branch and remote locations to security risks. Fortinet Secure SD-WAN, by contrast, securely consolidates networking, routing, and security infrastructure in a single, organically developed solution.

> Fortinet was named a leader in the 2022 Gartner® Magic Quadrant™ for Network Firewalls and the 2022 Gartner® Magic Quadrant™ for SD-WAN.

To learn more about how your agency can modernize with efficient IT solutions that boost security, conserve budget dollars, amplify the capabilities of IT staff, and improve the end-user experience, visit www.FortinetFederal.com.

FORTINET FEDERAL®

March 8, 2023 9:39 AM