Securing the Government Enterprise

The Case for Managed Security Services

Federal government agencies face unique and growing challenges in securing their enterprise from cyberattacks. They have a higher threat profile than many of their commercial counterparts, coupled with institutional constraints in acquiring, hiring, and implementing the critical resources needed to fully protect their agency.

Against these challenges, managed security services like extended detection and response (XDR) can dramatically improve their overall cyber resilience, enabling them to detect, defeat, and recover from increasingly sophisticated attacks faster and more confidently.

By standardizing and automating core security operations and integrating streaming analytics and threat intelligence, XDR can improve overall performance, financial predictability, and cost-effectiveness.

Federal cybersecurity’s persistent challenge

While federal agencies perform admirably in protecting their environments, many are asking if their current cybersecurity cost structure is sustainable, especially as attacks become pervasive. According to Accenture’s Third Annual State of Cyber Resilience Report—Federal Edition, most (75 percent) federal agencies report year-over-year cost increases for cybersecurity, with 1 in 5 reporting cost increases exceeding 25 percent. Leading this charge were higher costs for network security, threat detection, and security monitoring. As a result, 60 percent of these federal leaders say these cost increases are unsustainable.

Federal agencies face a host of inherent constraints that make protecting their networks and infrastructure both costly and challenging. These factors include an inability to readily hire qualified talent, an overly complicated IT architecture and environment that is expensive and difficult to protect, pervasive compliance mandates, and a procurement system not conducive to agility.

These factors leave too many federal agencies reliant on highly manual processes, outdated technologies, and understaffed and undertrained security operations centers (SOC) to protect their exceedingly fragmented environment against a growing number of more sophisticated attacks.


**Zero trust takes center stage**

Federal agencies are also shifting their focus from perimeter security to more adaptive approaches like zero trust that offer more multifaceted and pervasive defenses. This is driven by the need to protect their increasingly distributed and virtual cloud-based environments from more numerous and cunning cyber-attacks. Continued reliance on firewalls and similar border protections alone leaves the enterprise vulnerable and unprotected.

What adaptive security models like zero trust argue is that adversaries will eventually breach an agency. As a result, there is increasing recognition that detection and response speed is the new battlefield, as this can dramatically reduce the potential damage and impact. According to Accenture research, cybersecurity leaders detect and mitigate attacks faster, which means they are four times less likely to suffer a significant breach, and their cost to defend and mitigate a successful attack is 72 percent lower.

**XDR is built for zero trust**

This shift has put analytics, artificial intelligence (AI), and automation at the forefront of cybersecurity. These technologies allow security teams to detect and respond to attacks faster and scale their efforts to protect even more of the enterprise (in our study, leaders actively safeguard 85% of the enterprise versus 55% for non-leaders).

Approaches like XDR [or earlier managed detection and response (MDR)] industrialize this next-generation security operations center into either Software-as-a-Service (SaaS) or fully managed service offerings. It takes advantage of a platform-based approach that integrates specialized cybersecurity tools together to provide a highly automated, insight-driven, active cyber defense. When adopted as a managed service, agencies further benefit from teams of highly trained cyber analysts using established best practices to address the full cybersecurity lifecycle.

XDR is built for zero trust, as it brings all of the pillars of trust together as an integrated security model.

---

*Solutions like XDR automatically handle up to 80 percent or more of alerts, allowing analysts to quickly converge on the remaining threats that represent the highest enterprise risk.*
Accenture XDR for Government in action

Accenture XDR for Government is a FedRAMP-authorized security operations center (SOC) delivered by U.S. citizens as a fully managed service. It provides 24/7/365 security monitoring and incident response to detect, respond, and eradicate threats and intrusions at machined speed.

What sets Accenture XDR for Government apart

- It has fully automated over 80 percent of all alert responses for clients—delivering operational security at unprecedented speed.
- All detections are mapped to the MITRE ATT&CK framework—expediting analysis and adapting defenses using AI.
- The customer portal delivers streaming security intelligence—providing a comprehensive, real-time view of your security posture.
- It is a FedRAMP-authorized platform and can be fully operational in 90 days.
The mission case for managed security services

Managed security services like Accenture XDR for Government offer a highly industrialized approach to cybersecurity, driven by its widespread use of analytics, AI, and automation. These technologies allow Accenture XDR for Government to provide broader coverage of the enterprise, detect threats more effectively, and remediate breaches faster. Overall performance is tied to specified service level agreements (SLA) with real-time reporting providing added visibility and assurance.

As a cloud-based, open platform, agencies can automatically deploy Accenture’s federal offering across a variety of environments for 24/7/365 continuous monitoring in just hours and its fully operational in 90 days. It can provide up to 100% enterprise and ecosystem coverage, including Internet-of-Thing (IoT) and operational technology (OT) systems.

The integration of end-to-end monitoring, real-time threat intelligence, and preprogrammed incident responses means that the preponderance of low-level and repetitive alerts are handled automatically. In the case of Accenture XDR for Government, up to 80 percent or more of these event alerts are resolved, with a 95 percent true positive rate (vs. 75 percent industry average), without human intervention. The remaining alerts are sent to tier 2 and 3 analysts. This approach ensures 100% alert coverage and continuous vigilance while decreasing alert fatigue, which is a hidden threat in many organizations.

Accenture XDR for Government also delivers faster incident response and remediation. It detects an incident in production environments, on average, in under one minute and offers a service level objective (SLO) defined response time of fifteen minutes or less. It also follows US-CERT SLA and reporting requirements. This performance compares very favorably with an industry average of often days or weeks to detect, respond, and remediate attacks and breaches.

A recent Ponemon Institute report, The Cybersecurity Illusion: Enterprise Security Remains Reactive, showed that only 24 percent of organizations have a robust cyber metrics program in place, and only 60 percent tracked any meaningful metrics at all. Accenture XDR for Government works to fill this gap by mapping all detections to the MITRE ATT&CK framework for further analysis, while a customer portal provides a real-time view of an agency’s security posture.

The end result is that managed security services like Accenture’s federal offering not only provide more extensive coverage with better threat detection and faster remediation in many cases, but this improved performance is backed by measurable key performance indicators (KPI) and enforceable SLAs.
The business case for managed security services

As with other outsourced services like cloud, managed security services offer better performance at a lower cost. These savings are driven by reliance on common, best-of-breed infrastructure, the widespread use of analytics, AI and automation, and operational economies-of-scale that reduce the cost to provide true 24/7/365 coverage with highly skilled threat analysts.

Consider, for example, a 3,000-person federal agency with 5,000 endpoints under management. Analysis indicates that they could achieve a $3.4M cumulative net benefit over the first three years of implementing Accenture XDR for Government. These benefits include a 32 percent reduction in operating costs that creates $1.5M in direct cost savings and avoidance. The added value derives from quantifiable performance improvements and risk reduction.

Another agency with 4,500 employees forecasted $10M in hard cost savings over five years with Accenture XDR for Government. The agency would also enjoy a $5M added value benefit from automated incident response and integrating threat intelligence to improve operational efficiency and effectiveness.

Getting started

Managed security services can serve as the SOC for an agency or augment existing security structures. Smaller agencies that must meet the same compliance mandates and standards of their larger peers may want to go with a fully managed solution. Larger agencies—those that may want to or must legally keep some data on-premises—should consider a hybrid approach that allows data to reside on site but still leverage the efficiency gains from a managed service.

The expanded use of managed security services will grow in federal agencies as it did with other outsourced technologies. The undeniable business case will ultimately push the service-model forward. Government agencies already benefit from outsourced services. It is time the security stack joins the other groundbreaking technologies agencies benefit from because of the “as-a-service” model.
Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. Our 514,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

Accenture Federal Services, a wholly owned subsidiary of Accenture LLP, is a U.S. company with offices in Arlington, Virginia. Accenture’s federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations. Learn more at www.accenturefederal.com.

Authors

Aaron Faulkner
Managing Director
Accenture Federal Services, Cybersecurity Lead

Dave Dalling
Cyber Chief Technology Officer
Accenture Federal Services

Nate Morin
Managing Director
Accenture Federal Services, Cloud Security Lead

Michael Goodman
Associate Director
Accenture Federal Services, Federal Zero Trust Lead

About Accenture

About Accenture Federal Services

Contributors

John Conley
Andrew Girgis
Andrew Kim
Riley Panko
Christian Stephenson

Copyright © 2020 Accenture. All rights reserved. Accenture and its logo are trademarks of Accenture.