Securing the Government Enterprise

The Case for Managed Security Services

accenture

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 advanced analytics and threat intelligence, XDR can improve overall performance, financial predictability, and cost-effectiveness. For example, federal agencies can reduce security operations center (SOC) costs by a third or more with a managed option. The end result is enabling a more strategic, agile, and sustainable approach to cybersecurity, empowering federal agencies to stay ahead of threats and operate with greater assurance.

Federal cybersecurity's persistent challenge

Federal agencies currently find themselves chasing a security finish line that is constantly moving.

The number and ingenuity of attacks continue to increase as part of an ever-evolving threat environment. According to Accenture's Third Annual State of Cyber Resilience Report—Federal Edition, federal leaders report that the average number of targeted attacks they face grew 53 percent year-over-year to a total of 320.

These targeted attacks are more likely to be conducted by foreign adversaries and other sophisticated actors, with a far greater potential to disrupt operations and extract high-value assets from an agency. Accenture's 2020 Cyber Threatscape Report notes that "suspected state-sponsored and organized criminal groups were observed using a combination of off-the-shelf tooling and open-source penetration testing tools at an unprecedented scale to carry out cyberattacks and hide their tracks." Agencies must also contend with existing advanced persistent threats (APTs) that may linger within their enterprise undetected, doing untold damage. The challenge is that most cyber teams are consumed instead by continuous firefighting, responding to a deluge of hundreds or thousands of speculative attacks daily.

Further complications arise from federal agencies' reliance on extended supply chains, third-party contractors, and affiliates like state governments. Our research found that nearly half (45 percent) of federal agencies' security breaches are now indirect. As a result, 85 percent of federal executives in our research believe they must go beyond guarding their enterprises to securing their ecosystem as well. These risks may grow with a widespread shift to work-from-home.

This is driving increasing interest across the federal government in zero trust and other adaptive security strategies that offer more multifaceted and pervasive defenses. These frameworks argue that trust in the security of the network is misplaced, with organizations requiring a more data-centric strategy instead. Specifically, this means implementing a layered, risk-based approach using integrated threat intelligence, automation, and analytics to detect and eradicate threats anywhere in the environment more quickly.

Federal agencies are evolving towards this model and have performed admirably against this threat environment, outperforming their commercial counterparts and reducing successful attacks by 43 percent year-over-year. However, this success is not without cost. Most (75 percent) federal agencies report year-over-year cost increases for cybersecurity, with twenty percent reporting cost increases exceeding 25 percent. Leading this charge were cost increases for network security, threat detection, and security monitoring. As a result, 60 percent of these federal leaders say these cost increases are unsustainable.

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

The demand for qualified cybersecurity professionals continues to grow. Agencies cannot find enough candidates to fill open positions. When they come across a potential candidate, they face fierce competition from the private sector and other government organizations. For example, the average time-to-hire is more than twice as long for the federal government (98 vs. 42 days) versus the private sector. Since federal agencies typically cannot offer the types of salaries or benefits available in the private sector, it can be even more challenging to attract qualified talent.

The preponderance of legacy systems across the federal government creates additional challenges. According to Accenture's Decouple to Innovate report, federal leaders describe approximately one-third (32.9 percent) of their core systems as legacy. These systems are often more vulnerable to attack and more costly to secure. For example, 46 percent report that an outage in these systems involved a security breakdown, with 85 percent believing their agency's future will be threatened if they do not update their technology.

At the same time, agencies face many unique federal compliance mandates that can draw attention away from larger security goals and provide false confidence. Specifically, these mandates may promote a compliance-driven versus risk-based approach to cybersecurity, making it more difficult to foster an agile security ecosystem that can quickly adapt to changes in the threat landscape.

Government agencies must also contend with procurement hurdles that makes it difficult to quickly acquire innovative technologies to counter new threats. The federal acquisition process typically takes a year or longer to complete, leaving agencies exposed in the interim.

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. Given the exposure they face, where even one successful attack is too many, these challenges represent unacceptable risk in far too many cases.

As-a-Service takes center stage

The federal government's long pursued "cloud first" strategy has recently reached an inflection point. Projected federal spending on commercial cloud technology reached an all-time high in FY20, and the number of FedRAMP-authorized offerings has doubled to 200 over the past two years. The Department of Defense has also indicated that accelerated cloud adoption is a national security imperative.

By shifting to an as-a-service model for applications and computing infrastructure, federal agencies have benefited in several ways, including improved performance and agility, faster access to commercial innovation, and more cost-effective operations with better predictability. Instead of owning, operating, maintaining, and updating commodity technology solutions, they shifted their focus to more strategic objectives and outcomes.

Services like XDR bring a similar dynamic to the cybersecurity field. Federal agencies can access best-of-breed security technologies as a fully integrated and supported service offering. In cases like the Accenture XDR for Government managed service, these cybersecurity platforms offer the same FedRAMP and other certifications as a leading cloud service provider (CSP).

The next generation of cybersecurity

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

What they have discovered 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, with 88 percent of breaches detected in one day versus 22 percent for non-leaders. As a result, leaders are four times less likely to suffer a significant breach, and their cost to defend and mitigate a successful attack is 72 percent lower.

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 percent of the enterprise versus 55 percent 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, and 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.

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.

Automation serves as one of the critical components of managed security services. The current threat environment requires cybersecurity systems to move at machine speed as human analysts cannot keep pace. By using automation to remediate many of the threats and alerts, managed security services only rely on human intervention when truly needed.

Managed security services like XDR can replace an agency's security operations center (SOC) or work in concert with existing security operations, providing an instant upgrade to defense, threat detection, risk mitigation, and cyber resilience. For many agencies, the transition to a managed security services platform can serve as a leapfrog event, allowing them to improve cyber resilience drastically in just a few months.

XDR is built for zero trust, as it brings all of the pillars of trust together as an integrated security model. And as we will discover, XDR is the rare solution that can deliver, as a managed service, significantly better protection at lower (and more predictable) cost. It also allows federal agencies to extend coverage very quickly while increasing their operational maturity.

Simply put...what is XDR?

XDR brings together traditional security information and event management (SIEM) and security orchestration, automation, and response (SOAR) with real-time threat intelligence to provide an end-to-end, fully managed solution. As its name suggests, XDR services build upon earlier MDR with broader enterprise coverage, capturing and normalizing data from various sources, such as endpoint detection and response (EDR), network analysis, user behavioral analysis, and cloud workload monitoring, into a shared repository. XDR then uses advanced analytics and continuous monitoring to isolate real threats from the noise more quickly and effectively. By doing so, it allows security organizations to move from simply cataloguing events to actively prioritizing, analyzing, and eradicating actual threats.

FedRAMP

Accenture XDR for Government

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 machine speed.

This pioneering solution offers:

SOC Operations & Monitoring
Dedicated personnel with diverse skillsets continuously monitor the environment to quickly identify and address a wide variety of alerts and threats in real-time.

High-Fidelity Threat Intelligence
Continuous open- and closed-source threat intelligence is used to enhance monitoring and response and to conduct forensic investigations within the network.

Intelligent Threat Detection
Automate response and remediation using streaming analytics and improve detection capabilities through deep learning techniques to help agencies remain vigilant and proactive.

Threat Hunting
Identify compromises through targeted, preemptive discovery across the kill chain, isolating known and unknown threats with integrated malware detonation capabilities.

Behavioral Analytics
Use machine learning to identify anomalous activity and quarantine potential insider threats.

Automated Incident Response (IR)
SOAR technologies are used to immediately and independently mitigate incidents with the required resources at machine speed.

Targeted Response Playbooks
IR is guided by detailed playbooks that are continuously updated with new insights and methods through regular training and simulation to optimize performance.

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.

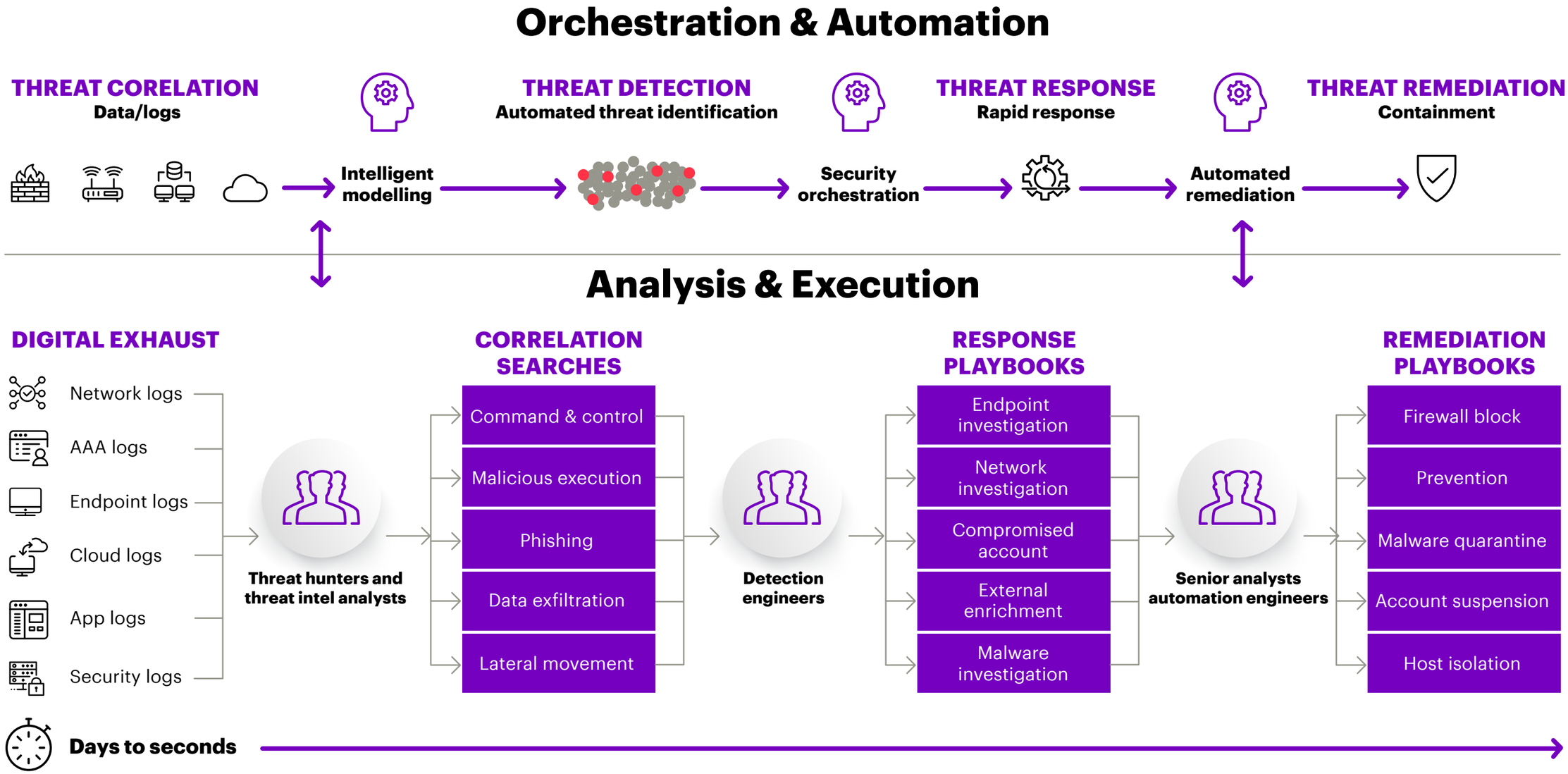
All detections are mapped to the MITRE ATT&CK framework–expediting analysis and adapting defenses using AI.

The customer portal delivers streaming security intelligence–providing a comprehensive, real-time view of your security posture.

Accenture XDR for Government is FedRAMP–authorized and can be fully operational in 90 days.

FedRAMP

Accenture XDR for Government in action



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 additional 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 it's fully operational in 90 days. Existing FedRAMP authorization aids speed of deployment. It pulls and correlates all relevant log data, including multiple APIs—endpoints, networks, cloud monitoring, applications, security devices, and more—and can provide up to 100 percent enterprise and ecosystem coverage, including Internet-of-Thing (IoT) and operational technology (OT) systems. This approach maximizes existing investments while delivering more comprehensive insight into the full threat environment.

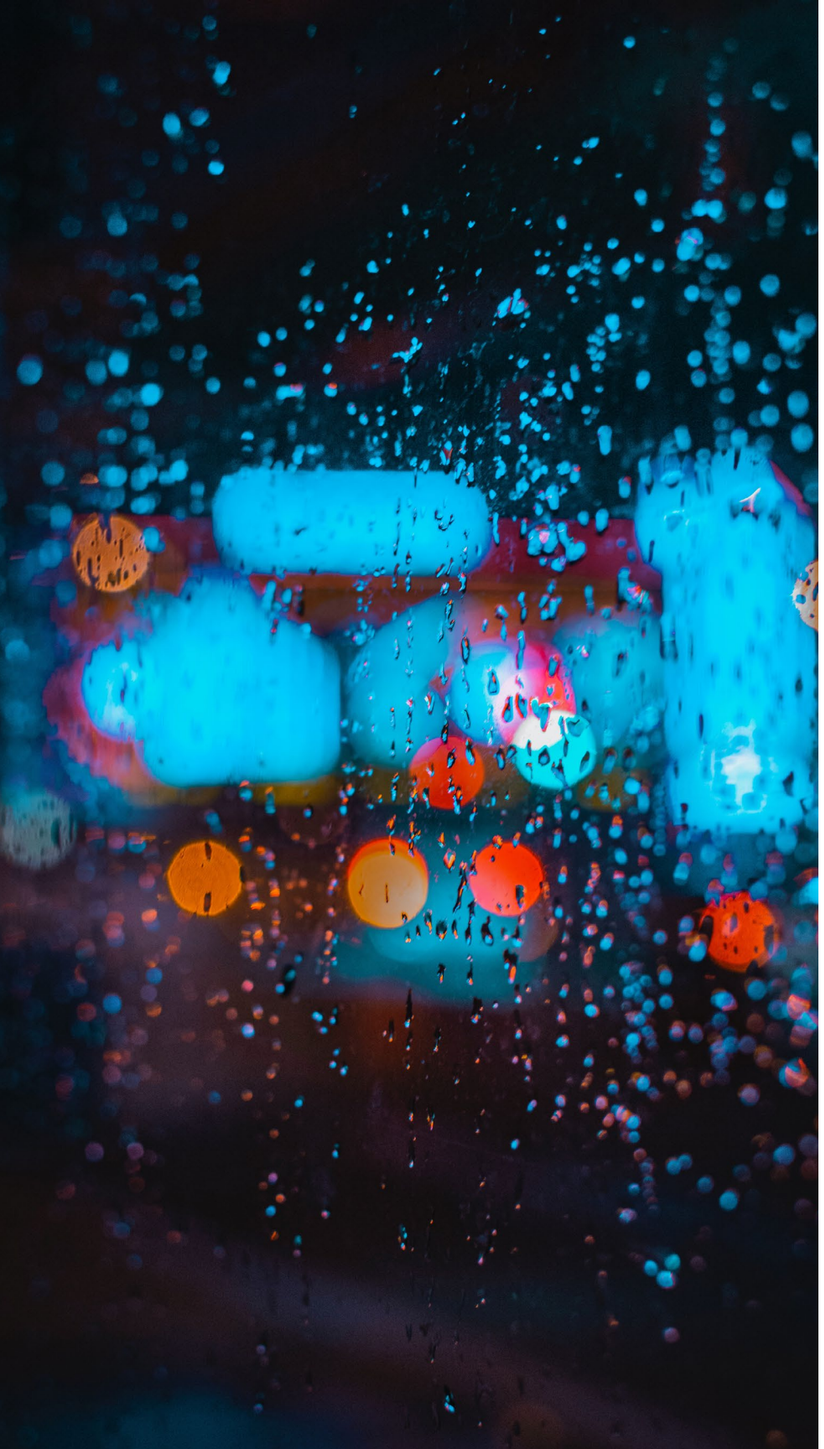
The integration of end-to-end monitoring, real-time threat intelligence, and preprogrammed incident responses means that the preponderance of low-level and repetitive alerts typically assigned to tier 1 analysts are handled automatically. In the case of Accenture XDR for Government, up to 80 percent 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 percent 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 service level objective (SLO) defined response time of fifteen minutes or less. It 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.

This approach builds collective knowledge of the threat environment's true nature and sets the stage for continuous performance improvement. For example, different technologies can be deployed against the most common threat types to improve detection and accelerate the response.

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 an undeniable business case, namely 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 additional 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.

This makes Accenture XDR for Government the rare solution that delivers better performance and protection at less cost.

Managed security services as a framework for growing maturity

Federal agencies vary significantly in their cybersecurity risk profile and maturity.

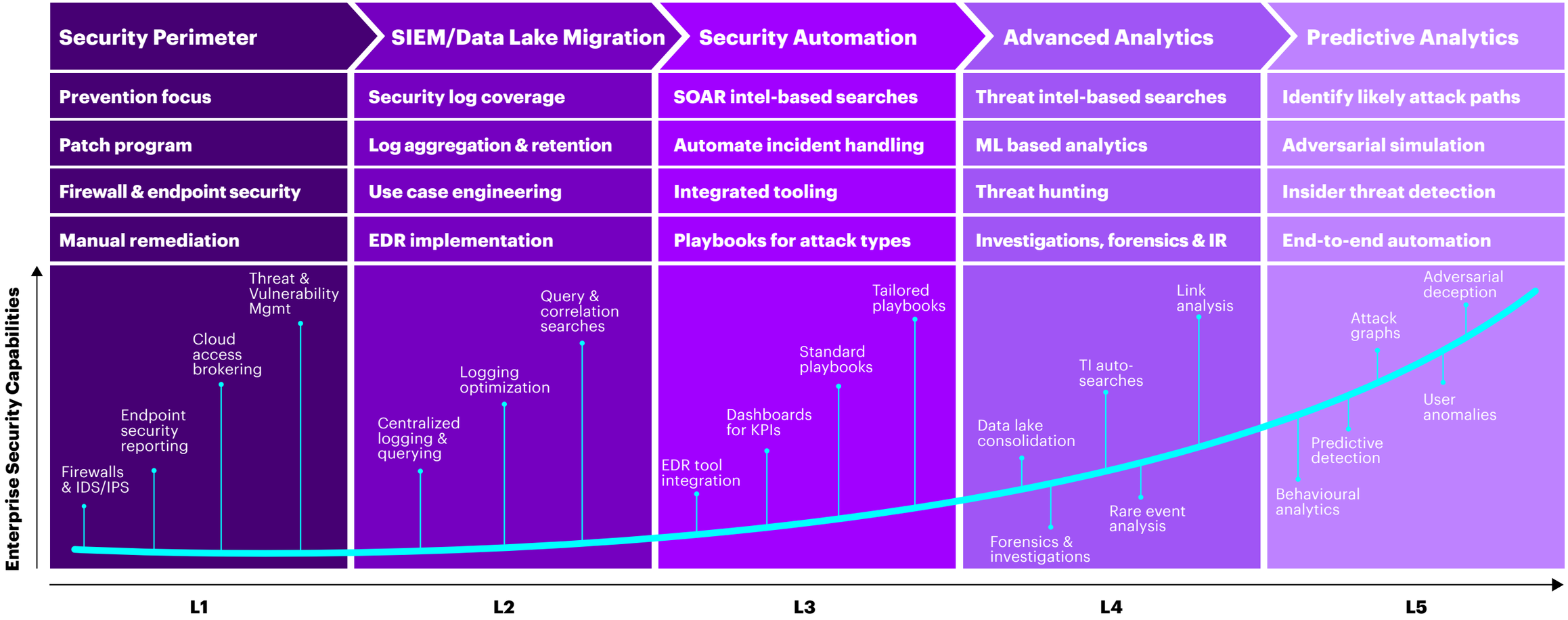
Many smaller and midsize agencies struggle to find sufficient talent and funding to implement more adaptive and predictive strategies. And larger agencies are often challenged by uneven or inconsistent execution across their environment. In either case, budget is consumed by maintaining inefficient processes instead of making investments to grow competency and improve performance.

As part of its XDR engagements, Accenture can help agencies create and execute a strategic roadmap to break this bottleneck and quickly make material improvements in their overall cyber maturity.

Designed for the chief information security officer (CISO), the Level-Up framework aligns security requirements with business priorities, and includes a detailed, stepped progression for growing cybersecurity capacity.

Level-Up SOC maturity progression

Define your journey to the SOC of the future



Level-Up uses a unique toolkit to evaluate more than 800 unique characteristics that define an agency's current SOC capabilities. This enables a strategic enterprise risk assessment of existing security capabilities to determine the robustness of current security operations. Based on this gap analysis, a to-be state is defined with agency-specific KPIs and a detailed program implementation timeline.

Getting started

Federal technology leaders who want to implement managed security services will face the same embedded cultural resistance to new technology they face when implementing other outsourced services such as the cloud. As with other outsourced services, technology leaders may want to build confidence in the solution before advancing to larger deployments.

One way to start is with small projects or security systems that protect lower-stakes levels of data. As the business case builds over time, agency leaders can confidently add managed security services to more programs and offices.

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 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.

Author

Dave Dalling
Cyber Chief Technology Officer
Accenture Federal Services

Contributors

John Conley

Andrew Girgis

Andrew Kim

Riley Panko

Christian Stephenson

About Accenture

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 506,000 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.**

About Accenture Federal Services

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**.