Growing Zero Trust with XDR

Extended Detection & Response offers federal agencies the speed, agility, and intelligence needed to stay ahead of the threat.

accenture

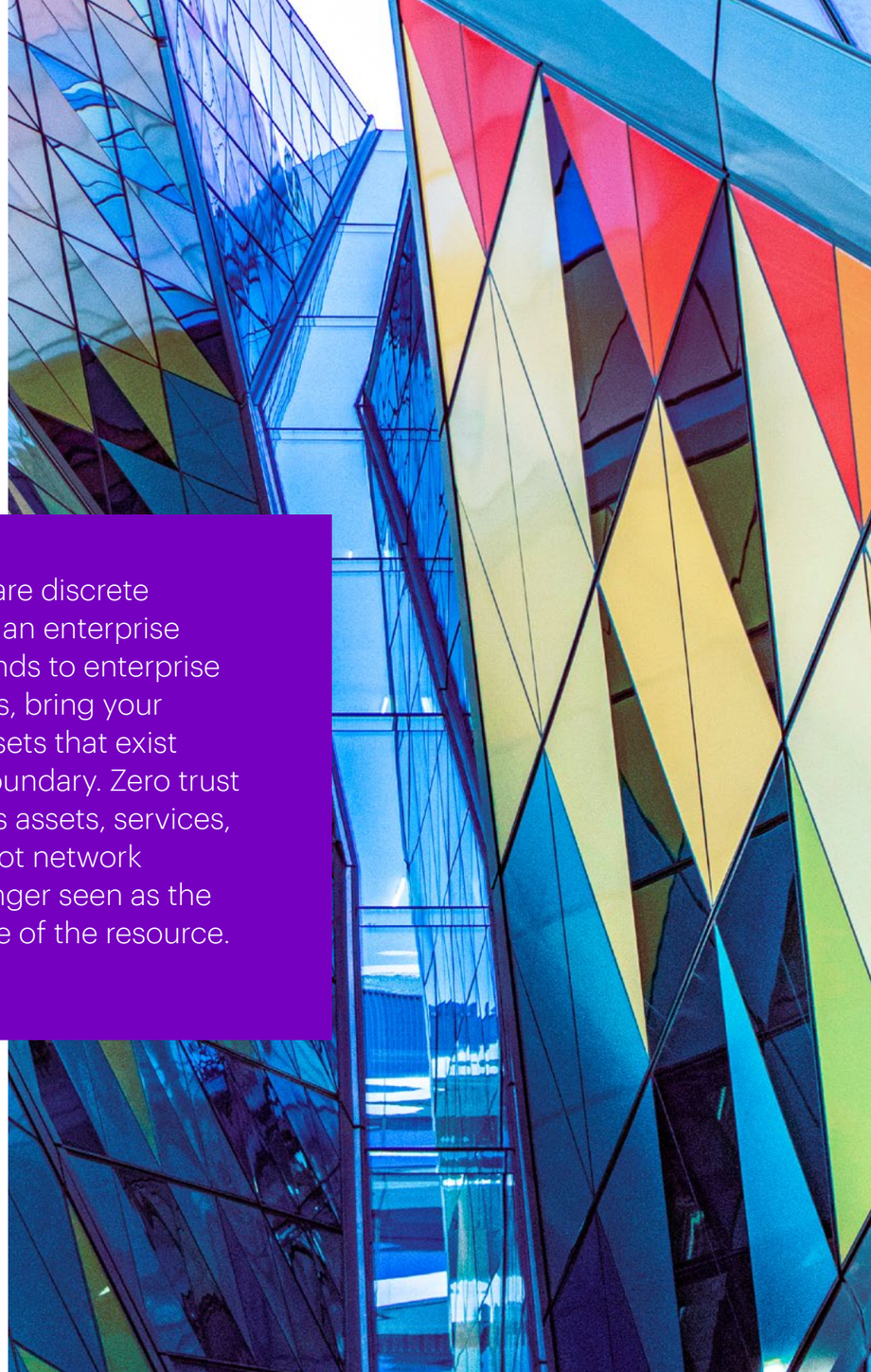
With dramatic changes taking place throughout the federal computing environment, security goalposts are shifting. A government-wide move towards more open and cloud-based systems expands the attack surface and explodes the traditional notion of perimeter security. More recent events, such as the shift to work-from-home, the emergence of the Internet-of-Things (IoT), and 5G and IPV6 are accelerating this trend. As a result, new cybersecurity risks are emerging as adversaries evolve their approaches to target these growing vulnerabilities.

Given this new landscape, federal agencies are embracing zero trust architectures (ZTA) as their new cybersecurity framework. First coined by John Kindervag (with Forrester Research at the time), zero trust holds that no environment is entirely secure and therefore, trust within the network is often misplaced. Furthermore, it recognizes that most investments focus on securing devices and networks at the expense of the enterprise data that are the organization's crown jewels.

Building on this initial concept, Forrester recently described zero trust (content accessible to Forrester client or via purchase) as "...a conceptual and architectural model for how security teams should redesign networks into secure micro-perimeters, use obfuscation to strengthen data security, limit the risks associated with excessive user privileges, and use analytics and automation to dramatically improve security detection and response." [1]

The National Institute of Standards and Technology (NIST) has further codified (NIST SP 800-207) the zero trust approach for the federal government, describing it as follows:

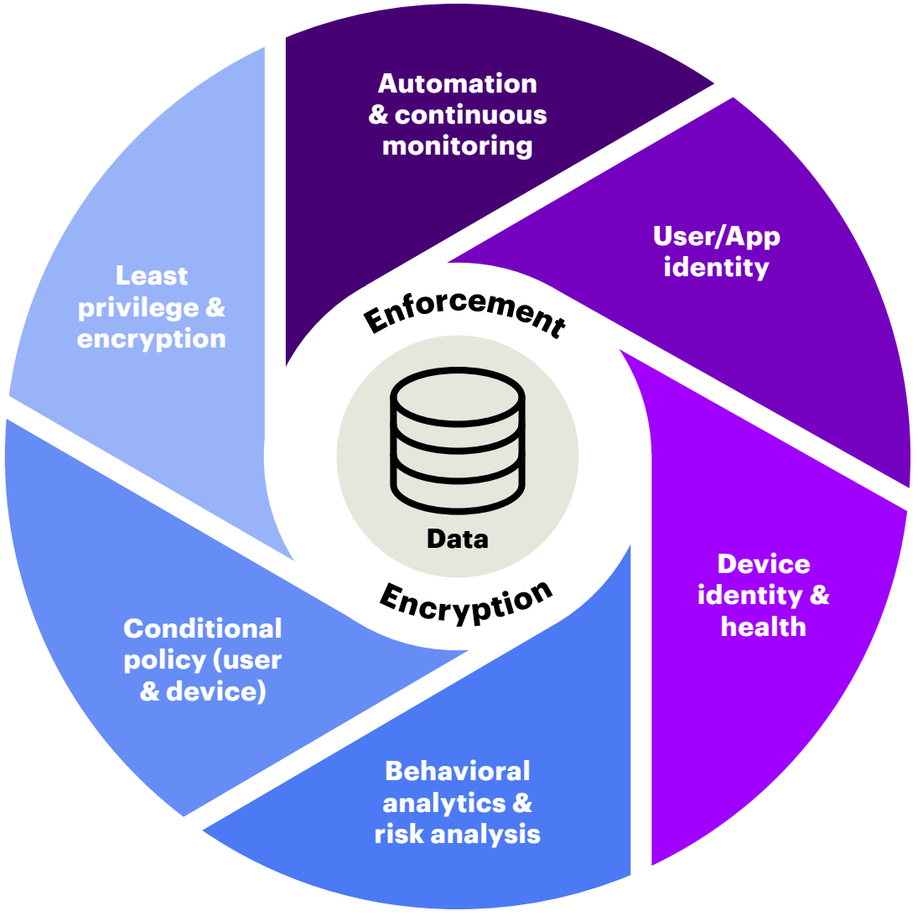
Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust responds to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that exist outside an enterprise-owned network boundary. Zero trust focuses on protecting resources, such as assets, services, workflows, and network accounts, and not network segments. The network location is no longer seen as the prime component to the security posture of the resource.



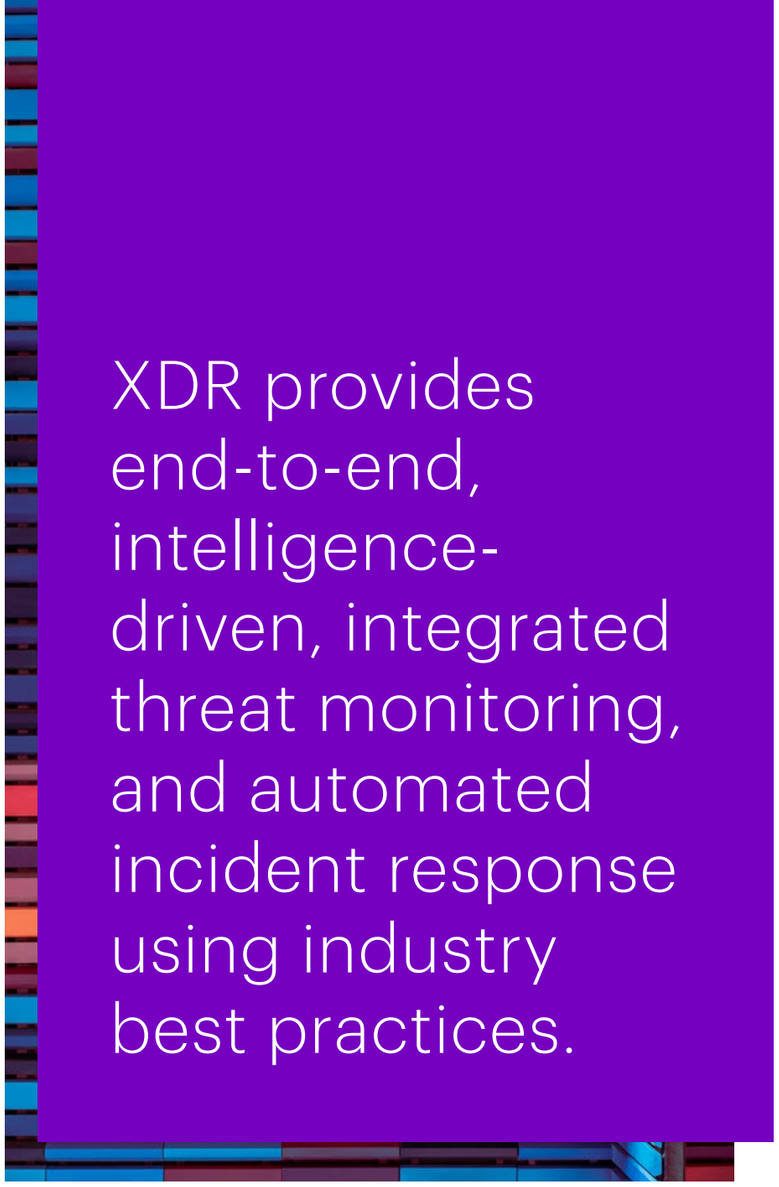
In practical terms, implementing an adaptive security architecture like zero trust means taking a data-centric approach to cybersecurity. Agencies must effectively catalog their digital assets and intellectual property in terms of potential risk and implement procedures to identify, manage, and monitor the users, devices, and applications accessing this data. This method creates a more layered approach to protecting assets coupled with an enhanced ability to detect and respond to rogue actors within the enterprise.

Extended Detection & Response (XDR) can play a pivotal role in enhancing a zero trust architecture when coupled with more fine-tuned Identity and Access Management (IdAM). Solutions like Accenture's XDR for Government provide comprehensive security monitoring through flexible as-a-service delivery that focuses on data and identity monitoring. By offering state-of-the-art technologies as a fully managed service, agencies can take advantage of advanced analytics and automation to identify and mitigate cyber threats at machine speed.

This high degree of automation is key to supporting the zero trust framework. Under zero trust, monitoring extends beyond the network perimeter to encompass a wide range of activities and endpoints as well as the supply chain. In this significantly broader landscape, speed to react and an automated response is essential. XDR enhances the zero trust effectiveness by elevating the speed and volume of anomaly detections and rapid responses.



Adaptive Security – A Zero Trust Model



XDR provides end-to-end, intelligence-driven, integrated threat monitoring, and automated incident response using industry best practices.

Introducing XDR

Security breaches and advanced persistent threats (APTs) are assumed in a zero trust architecture, making detection and response speed critical to eradicating the threat before significant damage occurs.

XDR addresses this need, using automation, artificial intelligence (AI), and analytics to quickly address spurious attacks and more effectively isolate and remediate the sophisticated, targeted attacks that can cause real damage.

XDR provides end-to-end, intelligence-driven, integrated threat monitoring, and automated incident response using industry best practices. It brings together advanced security operations center (SOC) components, including real-time threat intelligence, user and entity behavior analytics, AI-driven event correlation, and security orchestration, automation and response (SOAR) capabilities, to address the full cyber threat lifecycle.

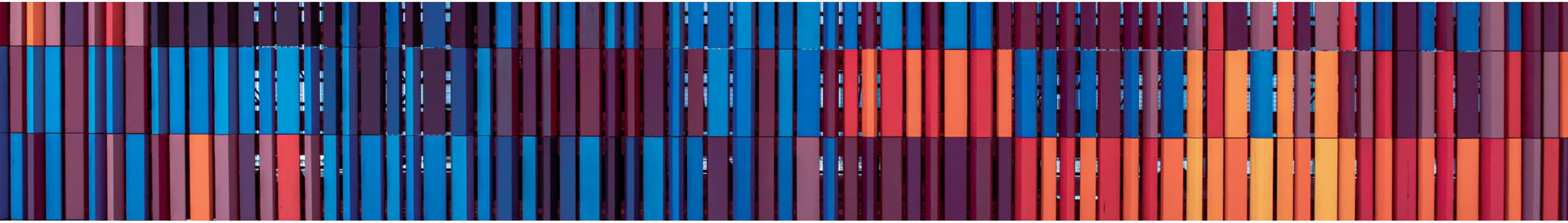
To ensure that these various tools work together as a cohesive whole, XDR is often delivered as a fully integrated Platform-as-a-Service (PaaS) or managed service offering. By opting for XDR as a managed service, agencies can also utilize highly skilled, multidisciplinary teams and documented playbooks to further accelerate threat detection and resolution.

XDR builds upon traditional endpoint detection & response (EDR) and more recent network detection & response (NDR) solutions to address today's digital government's broader footprint. Specifically, it operates across the entire IT ecosystem, including operational technology (OT) and IoT systems, collecting and correlating data across endpoints and servers, cloud workloads, and networks.

Gartner notes that (content accessible to Gartner clients) " ...[t]he primary value propositions of an XDR product are to improve security operations productivity and enhance detection and response capabilities by including more security components into a unified whole that offers multiple streams of telemetry, presenting options for multiple forms of detection and concurrently enabling multiple methods of response." [2]

This broader view gives defenders greater visibility into emerging threats, which can be analyzed, prioritized, and addressed in real-time, thus mitigating potential data loss and minimizing security breaches. In practical terms, this means that many tier-one alerts are resolved automatically, while real-time correlation is used to identify more sophisticated attacks.

For the CISO, XDR significantly enhances their ability to track threats across the enterprise while also empowering them to hunt for more sophisticated, hidden dangers proactively. It also provides better real-time visibility and therefore, greater operational confidence. CIOs value XDR's extensibility, as it can be readily extended to cloud workloads and public APIs, third-party supply chains, and remote workforces, facilitating both agile and secure operations. In terms of the CFO, they view the combination of potential cost-savings and overall risk mitigation as especially compelling.



XDR in action

For example, Accenture XDR for Government is a FedRAMP-authorized solution explicitly built around government agencies' needs.

It brings together best-of-breed SOC components and investigatory tools as a fully managed service to measurably improve cyber resilience while lowering operating costs in most cases. It integrates natively with existing security systems and can serve as either a primary SOC or as a strategic component of a multitiered defense.

Key capabilities for Accenture XDR for Government include:

SOC Operations & Monitoring

Maintain 24/7/365 cyber resilience with continuous monitoring by U.S. persons of the environment to quickly identify and address a wide variety of alerts and threats; this includes surge capacity to escalate threats to tier 2 or 3 response quickly.

High-Fidelity Threat Intelligence

Actively fuse open and closed-source intelligence to better understand the threat environment, adapt defenses, and guide forensic investigations.

Intelligent Threat Detection

Streaming analytics and machine learning are used to automate and improve threat detection to recognize even unknown threats.

Threat Hunting

Target APTs using proactive, intelligence-driven exploration with integrated malware detonation capabilities across the entire cyber kill chain.

User & Entity Behavioral Analytics

Flag abnormal or risky user and device activity and isolate potential insider threats.

Automated Incident Response (IR)

Leverage integrated SOAR technologies to automatically counter and mitigate detected threats at machine speed.

Targeted Response Playbooks

Regular training and simulation with continually enhanced scenario playbooks works to further improve incident response.

Real-time Visibility

Customized portal provides a comprehensive, real-time view of the organization's security posture, including risk scoring, detailed analysis of incidents, and tailored recommendations.

Tool Agnostic Integration

XDR leverages existing customer investments by integrating data from current security tools to provide a single point of visibility.

FedRAMP

The XDR approach

In the case of Accenture XDR for Government, 80 percent of all alert responses are automated—delivering operational security at unprecedented speeds and significantly reducing the time-and-effort requirement of chasing spurious alerts, freeing highly skilled experts to tackle more high-value tasks.

This widespread adoption of analytics and automation allows Accenture XDR for Government to deliver significantly faster incident response and remediation. In production environments, it detects incidents, on average, in under one minute. Response time is based on a service level objective (SLO) of eight minutes or less, with an average time to resolution of 15 minutes. In contrast, Accenture's Third Annual State of Cyber Resilience Report – Federal Edition found that most federal agencies currently take days or weeks to find and fix security breaches in their enterprise.

XDR detections are mapped to the MITRE ATT&CK framework, using artificial intelligence to expedite analysis and adapt defenses. Typically, XDR will deliver a customer portal that presents IT leaders with streaming security intelligence, providing a more complete view of the organization's overall security posture.

XDR's customer value ultimately depends on the end user's technology deployment and data availability. With this in mind, the Accenture XDR team can work with customers to assess their technology and help them maximize capability coverage and integration. A FedRAMP-authorized XDR service will integrate seamlessly into the existing security fabric and can provide first- or second-line defense, serving as either a primary SOC or as a strategic component of a multitiered defense.

XDR detections are mapped to the MITRE ATT&CK framework, using artificial intelligence to expedite analysis and adapt defenses.

How is XDR different?

A number of other security infrastructure offerings go partway toward meeting the demands of a highly complex security landscape. The government has pursued these solutions with varying degrees of success. It's instructive to take a look at how XDR does and does not resemble these alternate methodologies.

EDR

With its focus on the growing universe of endpoint devices, Endpoint Detection & Response (EDR) can be a powerful tool for managing security at the endpoint. However, EDR cannot effectively peer into network traffic and cloud workloads, which means it provides a more limited view, leading to unverified alerts that can overwhelm a traditional SOC. By providing a more granular and contextual perspective, XDR can automatically resolve many of these alerts and prioritize those deemed the most significant risk.

MDR

Managed Detection & Response (MDR) is precisely that—a managed service offering that delivers SOC capabilities as a service around a specific tool. Given the constraints on cybersecurity talent, this can be a valuable and cost-saving alternative to in-house staffing.

Most MDR offerings don't provide the defense-in-depth offered by employing various cybersecurity tools, have limited visibility into network traffic and cloud workloads, and lack sophisticated data integration, correlation, and analysis.

SIEM and SOAR

At a casual glance, XDR may resemble components of both SIEM (secure information and event management) and SOAR (security, orchestration, automation, and response), as it leverages both technologies. However, XDR adds additional capabilities to provide a more robust and resilient monitoring and response solution.

Why “as-a-service”?

By acquiring XDR as a managed service, organizations can leverage several significant advantages.

In an environment where cybersecurity talent is scarce, agencies can take advantage of highly skilled and trained, multidisciplinary teams addressing the full cybersecurity lifecycle. Coupled with the use of analytics and automation, these economies of scale can deliver better coverage at a lower cost.

An as-a-service model also makes it easier to stay ahead of the threat. Near-term, agencies benefit from the collective knowledge and specialization enabled by a shared service model, which means that new risk areas can be quickly identified and responded to. Thinking about the longer-term effects, the shift to an outcome-based model with defined SLAs can drive continuous performance improvements. For example, a managed service provider has the incentive and the ability to quickly procure and implement new tools to maintain or bolster cyber defenses in the face of emerging threats.

Finally, working with a managed service provider can be a leapfrog event for agencies seeking to grow their cybersecurity maturity. For example, Accenture’s companion Level-Up framework assesses 800 characteristics to chart a five-step cybersecurity maturity progression to bring federal agencies to a fully predictive model.

XDR and zero trust

An adaptive security model like zero trust is a lifestyle. By definition, it's about maintaining a constant state of risk-based vigilance. And as both the technology and threats evolve, strategies and privileges need to change with them.

For federal agencies, this reinforces the need to layer in zero trust capabilities and controls over time, building from the inside/out and outside/in simultaneously to secure the enterprise. This approach will help agencies reduce risk and better protect critical assets by improving identity management and device security while also implementing more agile and intelligent detection capabilities to respond faster to the inevitable breach and limit its impact. For example, should an alert identify suspicious activity attached to elevated account privileges, XDR can implement an automated playback to halt that activity, leveraging user identity as a cue to initiate corrective action automatically.

In this context, XDR can play a critical role, acting as the central nervous system that integrates an end-to-end zero trust architecture. Specifically, it provides real-time visibility and alerting across the entire network and environment, monitoring enforcement of core policies, providing insight with context, and empowering teams to take fast action when required.

Furthermore, solutions like Accenture XDR for Government, a cloud-based, FedRAMP-authorized platform, use open standards to integrate across endpoints, networks, cloud workloads, applications, security devices, and users, and can become fully operational in 90 days or less. With its integrated capabilities mapped against a defined maturity curve, agencies can use Accenture XDR for Government to develop their zero trust competency and grow their maturity.

Authors

Aaron Faulkner
Managing Director
Accenture Federal Services
Cybersecurity Lead

Dave Dalling
Cyber Chief Technology Officer
Accenture Federal Services

Michael Goodman
Associate Director
Accenture Federal Services
Federal Zero Trust Lead

Michael Fluharty
Principal Director
Accenture Federal Services
Cybersecurity Innovation

Citations

[1] Joseph Blankenship, Heidi Shey, *Defend Your Digital Business From Advanced Cyberattacks Using Forrester's Zero Trust Model* (July 2, 2020), Forrester

[2] Peter Firstbrook, Craig Lawson, *Innovation Insight for Extended Detection and Response* (March 19, 2020), Gartner

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 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**.

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**.