Accenture Federal Services | Google Public Sector

Reinventing Federal Cybersecurity: MxDR for Government

The Managed Extended Detection and Response (MxDR) for Government solution, powered by Google's advanced Security Operations (SecOps) platform, utilizes security-specific generative artificial intelligence (Gen AI) to enhance threat detection and response. MxDR offers modernized response automation and customizable dashboards specifically designed for federal use cases. Whether serving as your primary security operations center or complementing your existing security framework, MxDR provides streamlined security analysis, intuitive interfaces, and AI-assisted investigations that improve operational efficiency while reducing costs. Together, we deliver immediate value and a clear path to long-term cybersecurity objectives through the strategic deployment of our core services.

KEY CHALLENGES

Escalating Cybersecurity Costs: Federal agencies report unsustainable increases in cybersecurity expenditures, with some experiencing rises exceeding 25%.

Talent Acquisition and Retention: Lengthy hiring processes and competition from the private sector make it difficult for agencies to attract and retain skilled cybersecurity professionals.

Legacy Systems Vulnerability: A significant portion of federal systems are outdated, more vulnerable to attacks, and costly to secure, posing risks if not modernized.

Compliance-Driven Security: Numerous federal mandates often lead to a compliance-focused rather than a risk-based approach, hindering the development of agile security ecosystems.

KEY SOLUTIONS

Advanced Threat Detection and Automated Response: MxDR provides comprehensive security platforms with advanced threat detection and automated response capabilities.

Seamless Integration with Existing Infrastructure: These solutions integrate seamlessly with legacy systems, addressing challenges related to system vulnerabilities.

Cost Savings and Predictable Budgeting: The as-a-service model of MxDR offers significant cost benefits, reducing capital expenditures and maintenance overhead.

Flexible Deployment and Enhanced Agility: Offers flexible deployment options that can either replace or augment existing security operations centers.

FEDERAL USE CASES

Enhanced Threat Detection and Response:
Federal agencies can detect more threats with less effort using an integrated library of detections and AI-assisted query refinement.

Streamlined Security Analysis:
Analysts can conduct efficient investigations with an intuitive interface and AI-generated case summaries.

Real-Time Intelligence-Based Threat Detection:
Agencies benefit from real-time threat updates and tailored response strategies through modernized orchestration and customizable dashboards.

Compliance with Federal Cybersecurity Controls:
The FedRAMP High Authorized MxDR solution ensures compliance with federal cybersecurity regulations and provides a seamless 24x7 upgrade path.

Proactive Cyber Resilience:
Agencies can proactively address evolving threats and support rapid modernization with intelligent automation and a robust security posture.

Why Accenture Federal Services

Accenture Federal Services is a leading US federal services company and subsidiary of Accenture LLP. We empower the federal government to solve challenges, achieve greater outcomes, and build a digital core that is agile, smart, and secure. Our 15,500 people are united in a shared purpose to advance our clients' mission-critical priorities that make the nation stronger and safer, and life better for people. See how we make change that matters at accenturefederal.com.

Proven track record in RMF, FISMA, and FedRAMP implementations

30+ years supporting Federal agencies and delivering critical mission technology

Accenture Named Overall Leader in the Everest Group Managed Detection and Response Services 2025

CONNECT WITH US TODAY

Dan Matlick
Cyber Operations Lead
daniel.matlick@afs.com

Drew Epperson
Cyber Technical Director
andrew.epperson@afs.com