Maximus Cybersecurity Capabilities

Integrated, agile cyber defense for resilient, scalable enterprise security postures

Digital transformation is critical to enhancing organizational efficiencies, providing better customer experiences, and achieving greater mission outcomes. But as new technological advancements are enabling new possibilities, they are bringing increased complexity to modern IT architectures. Advanced endpoint systems, cloud environments, networks, and third-party applications are creating new pathways for bad actors to exploit. As IT architectures continue to evolve, it is becoming clear that traditional perimeter-based network security alone is insufficient at protecting against today's sophisticated cyber adversaries.

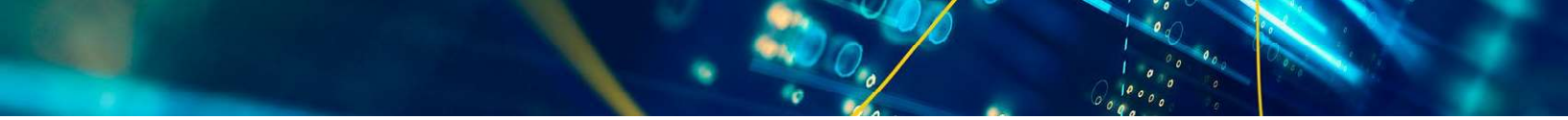
At Maximus, we are relentless in our pursuit of protecting enterprise assets, data, and operations Trusted to manage some of the government's largest security operations, we leverage our deep knowledge of agency mission and extensive technical expertise to create integrated cyber solutions that bolster enterprise cyber defenses for continual mission protection. Founded on security risk-based approach methodologies, and designed for NIST and FISMA compliance, we harden enterprise security postures by:

- Proactively identifying system and software weaknesses, reducing risks, and removing vulnerabilities
- Rapidly collecting and analyzing security data to understand and predict a threat actor's behaviors - before they can strike
- Automating the continuous authentication and validation of every request for access – regardless of user, endpoint, system, or service, removing gaps in security
- Putting security at the forefront of system development, layering security controls throughout the Software Development Life Cycle (SDLC)

Through emerging cyber technologies, including advanced analytics, Artificial Intelligence, and deep learning, we automate threat detection, mitigation, and response, while providing greater visibility across the enterprise, thus strengthening security postures. Our expertise lies in delivering the most advanced cyber solutions in:.

Benefits

- Unified and centralized visibility of security posture across the enterprise
- 24/7 security monitoring, response, and remediation
- Comprehensive threat intelligence into threat risks and user behaviors
- Modern, agile secure software development
- Automation anywhere with continuous authentication and monitoring
- Hybrid multi-cloud security for scale



Governance and Policy

We ensure operational and technical security compliance across the enterprise. Our Governance and Policy service provides a framework that helps agencies to manage their IT assets effectively, ensuring compliance with relevant regulations and industry standards while mitigating risks. We work closely with our customers to understand their requirements and address their challenges by providing tailored solutions for the strategic development of policies, procedures, as well as controls across security, incident response, risk management, and compliance frameworks.

Security Operations

We safeguard enterprise operations for continuous mission delivery. Our Security Operations Center Services provide a team of cybersecurity experts for 24/7 security monitoring, incident response, as well as threat hunting to rapidly identify and remediate potential security risks. Our deep knowledge of agency mission enables us to continuously secure agency enterprises while keeping government apprised of the current state of their security postures.

Cloud Security

We enable consistent, integrated security across hybrid multi-cloud environments. Our Cloud Security solutions offer advanced protection of government data, incorporating advanced encryption, access control, and incident response for secure enterprise scalability. Our solutions seamlessly integrate into existing government architectures to support the agility, flexibility, and security required to meet mission objectives.

Zero Trust Architectures

We go beyond traditional network security, protecting critical data, systems, and users – no matter where they are located. We implement a full spectrum Zero Trust security model to protect critical infrastructures, providing increased visibility and control over enterprise networks. Built on industry standards, and designed to meet compliance requirements, our Zero Trust implementations ensure resilient enterprise environments.

Threat Hunting and Remediation

We dive deep into the network to uncover the unknown. Our Threat Hunting and Remediation services leverage advanced techniques and integrated security tools to proactively identify threats before they cause damage. Our services provide continuous monitoring and real-time reporting to ensure our customers know the current state of their security posture, always.

Sample Customers

- Cybersecurity & Infrastructure Security Agency
- Defense Information Systems Agency
- Internal Revenue Service
- Transportation Security Administration
- Environmental Protection Agency

Cyber Analytics

We learn and analyze cyber threats and vulnerabilities in a way traditional security cannot. Our Cyber Analytics services leverage advanced algorithms, statistical analysis, behavioral analytics, and machine learning to provide greater insight into the data generated by government networks, identifying potential threats, and anomalies, and providing agencies with a better understanding of the security posture. Incorporating continuous monitoring and real-time reporting, we ensure agencies remain informed.

DevSecOps & Continuous Authorization to Operate (cATO)

Modern systems require modern software development. Our DevSecOps services assist agencies in identifying and addressing security risks throughout the entire Software Development Life Cycle (SDLC). We bring security teams into the planning at the start, working closely with development teams to integrate security tools and automated testing throughout the development process, which ensures more secure software deployments and faster time-to-market. Our cATO offering uses automated tools and processes to continuously assess the security of the systems and networks and provide regular reporting to ensure that they are in compliance with relevant regulations.