Government Data Security Solutions with Forcepoint

Challenges and compliance mandates in government

Forcepoint

Brochure

Government organizations face strict regulations and challenges when it comes to data protection. Sensitive information such as classified data, national security information and personally identifiable information (PII) must be safeguarded against threats ranging from malicious insiders to cyberattacks. Regulatory mandates such as FISMA, NIST SP 800-53 and CMMC require comprehensive data security measures, making compliance difficult with disparate solutions.

Forcepoint Data Security Overview

Forcepoint Data Security provides an integrated platform that enables government organizations to protect sensitive data across endpoints, cloud, web and network environments. This unified platform integrates critical Forcepoint capabilities including Data Security Posture Management (DSPM), Data Detection and Response (DDR), and Data Loss Prevention (DLP) – into one cohesive system.

DSPM, DDR, DLP Core Capabilities

1. **DSPM:** Discovers and classifies sensitive data across repositories, ensuring full visibility of where data resides and how it's used. Provides both remediation of risky data (ROT, over-permissioned data, misplaced data) and enforces policies to secure an organization's overall security posture.
2. **DDR:** Provides continuous monitoring and dynamic response to suspicious data activity across endpoints and cloud locations, providing swift responses to potential data breaches.
3. **DLP:** Enforces protective policies across all digital channels to ensure data remains secure, preventing exfiltration of sensitive information.

Enhanced Security Capabilities for Government Organizations

Digital Security is National Security

Hackers can bypass traditional security measures and gain access to classified data through weak credentials, supply chain vulnerabilities and misconfigurations. Forcepoint DSPM scans data repositories (on-prem file servers and cloud storage) to discover and classify sensitive information with AI-driven accuracy. With this proactive approach, Forcepoint DSPM can highlight where data is stored, who has access and any misconfigurations, providing a solid foundation for governance by fixing risky data such as ROT, data sovereignty and over-permissioned data. In addition to that, Forcepoint DDR provides continuous monitoring of data activity across endpoints and cloud services, instantly alerting on suspicious behavior or policy violations. DSPM and DDR together ensure that sensitive data remains protected, even if external threats bypass physical security.

Insider Threats: A Hidden Danger

In addition to external threats, insider threats represent a significant risk to government data security. Forcepoint DDR helps detect and stop unauthorized access from within the organization, such as accidental or deliberate leaks of sensitive data by employees or contractors through external or public sharing. DDR's data lineage capability tracks document movement and provides forensic visibility into where data travels, ensuring that even internal threats are neutralized before they can cause damage.

Preventing Unauthorized Data Access and Sharing

Government employees may unintentionally download sensitive data to personal devices or share it via emails. With Forcepoint DLP, organizations can inspect real-time data movements across cloud services and endpoints, blocking risky user activities that could lead to data loss incidents. Forcepoint DLP leverages over 1,700 pre-built classifiers and policy templates to detect and remediate risky actions. Additionally, the adaptive access control policies of Forcepoint DLP help prevent anomalous and unusual login attempts to cloud applications, ensuring data remains protected from unauthorized access.

Benefits for Government Organizations

1. **End-to-End Protection:** Ensure all data is discovered, protected and monitored across all environments, reducing the risk of data breaches and non-compliance.
2. **Unified Visibility and Control:** Provide government agencies with a single pane of glass to monitor and enforce security policies, significantly reducing administrative complexity.
3. **Simplified Compliance:** Easily meet regulatory requirements such as NIST SP 800-53, FISMA and CMMC by using pre-built templates and classifiers for data protection and reporting.

Key Use Cases in Government

1. **Classified Information Protection:** Protect sensitive government data such as national security information and classified records, ensuring compliance with ITAR and export control regulations.
2. **Secure Collaboration:** Ensure that sensitive government data shared in collaborative tools (email, cloud applications) is secure and meets regulatory standards.
3. **Insider Threat Detection:** Detect and prevent malicious insider threats through real-time monitoring and automated responses to anomalous data access patterns.

Regulatory Compliance Alignment (e.g., NIST, CMMC, FISMA)

Forcepoint's platform is built to align with key government regulatory frameworks, ensuring organizations can meet their compliance obligations effectively.

1. **NIST SP 800-53:** Forcepoint helps implement the security controls required to safeguard federal data, ensuring compliance with NIST's cybersecurity framework.
2. **Cybersecurity Maturity Model Certification (CMMC):** Protects controlled unclassified information (CUI) across defense contractors and ensures compliance with CMMC requirements.
3. **Federal Information Security Modernization Act (FISMA):** Forcepoint's platform helps government agencies comply with FISMA's mandates for safeguarding federal

For government organizations, Forcepoint provides the most complete data protection and compliance platform to safeguard data. By unifying DSPM, DDR, and DLP, Forcepoint enables organizations to know their data, secure it everywhere, and rapidly respond to risk, all from a single, integrated solution. This unified approach empowers CISOs and compliance officers to manage risk proactively while confidently meeting the requirements of NIST SP 800-53, CMMC, FISMA and beyond. The result is a stronger security posture, simplified compliance, and end-to-end protection. In an era of escalating threats and regulations, Forcepoint Data Security offers a smarter path to protecting data and maintaining compliance.

Get a Free Data Risk Assessment

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-Brochure-Government DSS with FP] 02Jun2025