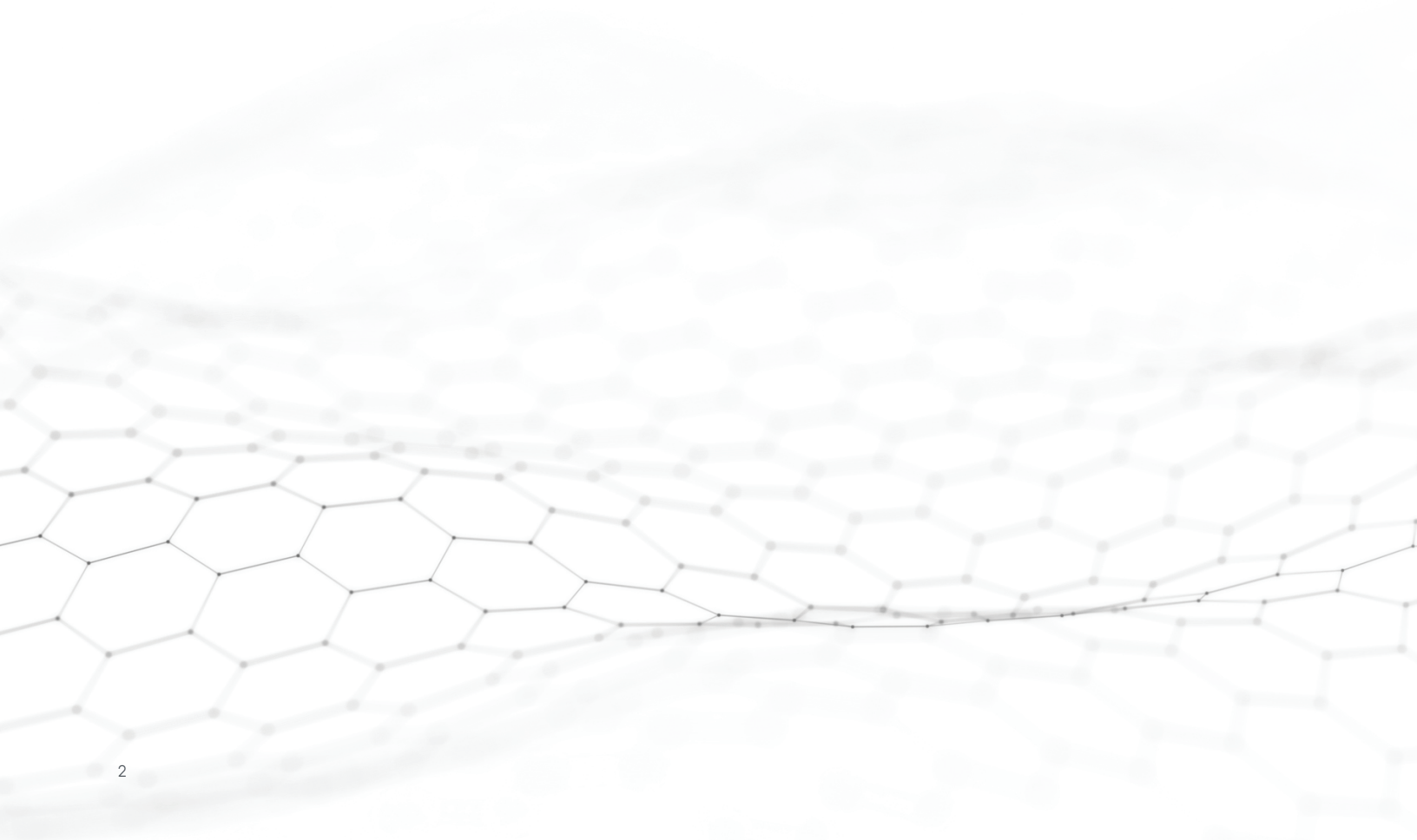
Forcepoint Product Reference Guide

Data Security for Federal and Defense Missions

Forcepoint

Federal Edition



Data Security for the Federal Mission

Federal missions depend on data that is constantly in motion, across mission systems, distributed sites and now AI workflows that request broad access to sensitive and controlled information. For agencies advancing Zero Trust initiatives and standing up new AI governance programs, the challenge is not only knowing where sensitive data lives but demonstrating control over it on infrastructure the agency owns.

This guide covers the Forcepoint capabilities relevant to federal civilian, defense and public sector environments. For each capability, this guide covers its positioning, key differentiators, mission relevance and a recommended federal deployment model, drawn from current Forcepoint product documentation.

Why These Capabilities

This guide focuses on Forcepoint capabilities that support deployment within agency-controlled environments, including on-premises data centers, Government Cloud, Private cloud environments, disconnected networks and other high-security government environments. These capabilities let agencies maintain control over infrastructure, data and policy enforcement while meeting mission and compliance requirements.

Forcepoint capabilities built primarily around a shared, vendor-hosted cloud service (SaaS), such as Forcepoint CASB and Risk-Adaptive Protection, are outside the scope of this guide for that reason.

Supporting Federal Priorities

The capabilities in this guide map to common federal mission priorities as follows.

FEDERAL PRIORITY	RELEVANT CAPABILITIES
Protect Controlled Information	DSPM, Data Classification, DLP
Improve Data Visibility	DSPM, DDR
Reduce Data Exfiltration Risk	DSPM, DDR, DLP, DLP for Email, Web Security
Secure AI Adoption	DSPM, Data Classification, Web Security
Threat Prevention	Forcepoint Network Security Platform (FNSP), RBI, Web Security, AMDP
Zero Trust Access Control	Forcepoint Network Security Platform (FNSP)

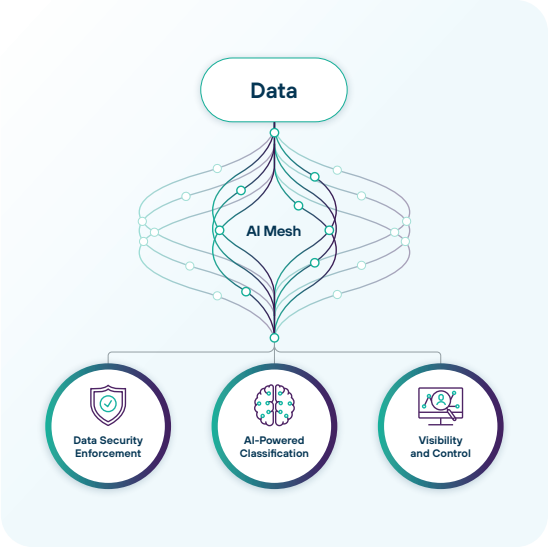
Capabilities at a Glance

The following Forcepoint capabilities are covered in detail in this guide.

CAPABILITY	CATEGORY	RELEVANT CAPABILITIES
DSPM	Data Security Posture Management	Discovery, classification, and remediation software deployed on agency-hosted servers.
DDR	Data Detection and Response	Continuous monitoring on agency-controlled infrastructure, integrating with existing SIEM/SOAR tooling.
DLP	Data Loss Prevention	Centrally managed through the Forcepoint Security Manager (FSM), across endpoint, network, discovery, and email channels.
DLP for Email	Email Data Loss Prevention	Email inspection and enforcement integrated with existing mail infrastructure and centrally managed through FSM
Data Classification	AI-Assisted Data Classification	Classification engine operating on agency-hosted repositories.
Network Security	Forcepoint Network Security Platform (FNSP)	Physical or virtual appliances. Bare-Metal (Ruggedized) and Public/Private Cloud support
Web Security	Secure Web Gateway	Physical, virtual, or endpoint-agent deployment. RBI, AMDP sandboxing, and advanced DLP classifiers are add-ons.
AMDP	Advanced Malware Detection and Protection	Keeps file submissions inside the agency data center. Supports Windows, Linux, and Android; macOS sandboxing is cloud-only.
RBI	Remote Browser Isolation	Deployed as an add-on within Forcepoint Web Security or as a standalone web security solution to isolate web sessions from user devices.

AI-Native Data Security Posture Management (DSPM)

Discover, classify and remediate risks to structured and unstructured data at scale with Forcepoint's AI Mesh.



Overview and Positioning

Forcepoint DSPM automatically discovers and classifies sensitive data at scale, covering structured and unstructured data. Its AI Mesh uses a highly efficient Small Language Model (SLM) architecture, rather than a general-purpose LLM, to deliver speed and explainability and to enable customization without extensive model retraining. Remediation capabilities enable file movement with file stubbing and data access governance.

Key Capabilities and Differentiators

- → Rapid discovery and automatic classification of sensitive data across agency file shares, on-premises SharePoint, and local directories (LDAP), with optional connectors into cloud repositories where an agency's accredited environment includes them
- → Least-privilege enforcement through built-in permissions remediation, plus overexposed-data analysis (publicly shared, shared externally, or overshared internally)
- → Identification and removal of redundant, outdated, and trivial (ROT) data to reduce risk and storage burden
- → Free Data Risk Assessments (DRA) to baseline an organization's current data security posture before a full deployment

Mission Relevance and Use Case

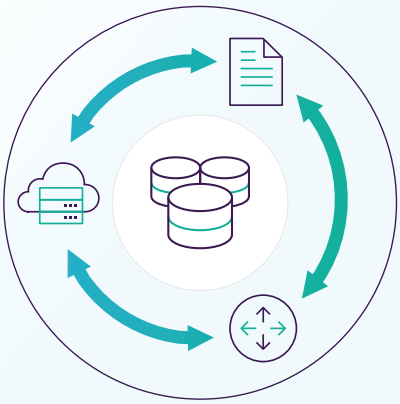
Agencies managing controlled unclassified information (CUI), PII, or mission data across legacy file shares and modernized repositories need continuous, automated visibility to support federal Zero Trust initiatives and the data inventories that agency AI governance programs require. DSPM gives data owners a prioritized view of where risk concentrates, ahead of a spillage or breach, rather than after one.

Recommended Federal Deployment Model

Appliance or virtual deployment within the agency data center, scanning local storage and directories.

Forcepoint Data Detection and Response (DDR)

Continuous detection and response to protect your most sensitive information.



Overview and Positioning

Forcepoint DDR extends DSPM's visibility into continuous, near real-time monitoring of data in use across endpoints and the cloud applications an agency has authorized. Unlike a posture tool that depends on a completed discovery scan, DDR begins monitoring for new data risks immediately after deployment.

Key Capabilities and Differentiators

- → Continuous, near real-time monitoring of data activity, with full data lineage tracking across a file's lifecycle
- → AI Mesh-powered classification with dynamic incident alerts and forensic-level detail for investigating incidents
- → Automated alerts and policy-violation enforcement to reduce time to response
- → Integration with third-party SIEM and SOAR platforms for incident response and threat management

Mission Relevance and Use Case

For components working to meet federal requirements for effective logging and network visibility, DDR's unified incident workflow and file lineage tracking help reduce false positives while giving security operations centers a documented, continuously updated record for compliance reporting and incident response.

Recommended Federal Deployment Model

Deployed alongside DSPM on agency-controlled infrastructure, feeding the agency's existing SIEM or SOAR tooling.

Forcepoint Data Loss Prevention (DLP)

Industry-leading Data Loss Prevention with unified management across all channels.

Overview and Positioning

Forcepoint DLP delivers comprehensive data loss prevention, managed through the Forcepoint Security Manager (FSM), without sacrificing performance or productivity. It extends consistent policy enforcement across endpoint, network, web and email channels while simplifying policy management.

Key Capabilities and Differentiators

- → AI-guided policy recommendations help administrators identify, refine and deploy the right DLP policies from more than 1,800 predefined templates, policies, and classifiers covering 90+ countries and 160+ regions
- → Rich forensic investigations with detailed timelines and evidence to accelerate response and support compliance, audits, and legal proceedings
- → Advanced detection including OCR for data in images, exact data matching, fingerprinting of structured and unstructured data, custom-encryption identification, cumulative (drip) DLP detection and advanced file scanning for partial exfiltration
- → Flexible policy actions including user coaching, justification, monitoring, blocking, quarantine and encryption to balance user productivity with data protection
- → Executive-level dashboards that translate DLP activity into risk reduction, policy effectiveness and program value for leadership
- → Integration with Forcepoint Data Classification and Microsoft Purview Information Protection for automated labeling

Mission Relevance and Use Case

This deployment model lets agencies enforce consistent data protection policies across networks that cannot route content through a public cloud, supporting insider-threat and CUI-handling requirements. As agencies expand the use of AI, Forcepoint DLP applies those same policies to AI interactions on the endpoint, helping prevent sensitive data from being exposed while keeping policy management, incident data and forensic investigations within the agency environment to support data sovereignty requirements in highly regulated environments.

Recommended Federal Deployment Model

Forcepoint DLP is designed for deployment within the agency accreditation boundary, keeping policy management, enforcement, incident data and forensic investigations under agency control. Whether protecting enterprise, disconnected, or air-gapped environments, agencies can apply consistent data protection policies across multiple security domains.

Forcepoint DLP for Email

Secure your organization's most vulnerable data channel: email.

Overview and Positioning

Forcepoint DLP for Email extends granular, agentless data protection to outbound email traffic, inspecting messages and attachments as they move through the agency's existing mail infrastructure. It integrates with Microsoft 365, Google Workspace, and other popular email platforms while allowing agencies to manage DLP policies and incidents through Forcepoint Security Manager.

Key Capabilities and Differentiators

- → Mail client-agnostic, agentless coverage across managed devices and BYOD, with no agent required
- → The same 1,800+ predefined policies, templates and classifiers used across Forcepoint DLP
- → Manager approval workflows, encryption and quarantine, with incidents managed in the same console as other channels
- → Agency-controlled inspection that keeps policy enforcement and incident data within the protected environment

Mission Relevance and Use Case

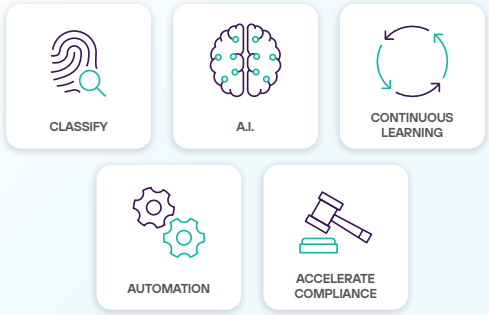
Email remains one of the primary channels for accidental data loss and deliberate exfiltration. On-premises deployment keeps the email connector and policy decisions inside agency infrastructure, supporting data sovereignty requirements for agencies that cannot route mail content through a public cloud scanning service.

Recommended Federal Deployment Model

Forcepoint DLP for Email integrates with the agency's existing email infrastructure, including Microsoft 365, Google Workspace, Exchange, and other supported platforms, while keeping policy management, enforcement and incident visibility within Forcepoint Security Manager. This enables agencies to extend consistent DLP policies across email and other data channels while supporting agency-controlled deployments.

Data Classification

Combining AI Mesh and a Small Language Model to deliver highly accurate data classification.



Overview and Positioning

Forcepoint Data Classification uses AI Mesh, a networked AI architecture built around a GenAI Small Language Model (SLM), to classify unstructured data and feed accurate labels back into DSPM and DLP policy enforcement. Forcepoint states the SLM is roughly one-tenth the size of the smallest general-purpose LLMs, runs on standard compute without requiring GPUs, and classifies within roughly 200 milliseconds.

Key Capabilities and Differentiators

- → AI-generated classification recommendations with a confidence level, alongside user review and correction, embedded directly in the Microsoft Office ribbon
- → Configurable classification tiers from Public through Regulated or Protected, including export-controlled categories such as ITAR/EAR (see table below)
- → Visual labels and metadata for policy enforcement, with mapping to Microsoft Purview Information Protection (MIP) tags and integrations with Azure RMS, Seclore, SealPath and Ionic
- → Granular user-activity reporting and a no-code analytics builder for compliance audits

Forcepoint Data Classification Types

CLASSIFICATION	ACCESS	EXAMPLE
Public	No restrictions	Marketing collateral
Internal	Restricted to staff and non-employees by role	Internal policies and procedures
Restricted or Sensitive	Restricted to approved individuals	Personal/employee data; business/financial data
Confidential	Restricted and distribution-limited to authorized personnel	Payroll and salary information; intellectual property; detailed budgets
Regulated or Protected (optional)	Restricted to a small number of entitled users	Medical research (HIPAA); PCI-covered card data; export-controlled research (ITAR/EAR)

Mission Relevance and Use Case

Forcepoint positions Data Classification explicitly for government use: categorizing information by sensitivity and regulatory requirement, automatically tagging datasets to facilitate audits and transparency and supporting export-control categories such as ITAR/EAR alongside HIPAA and GDPR-style regimes. Agencies implementing CUI marking requirements need classification that reflects their own category structure, not a generic commercial sensitivity label.

Recommended Federal Deployment Model

Classification engine integrated with agency file repositories and existing DLP or DSPM policy stores. Pattern-based classification suggestions are available offline, while ML-based (AI Mesh) suggestions are described in Forcepoint documentation as available only when online.

Forcepoint Network Security Platform (FNSP)

The Forcepoint Network Security Platform delivers a unified, policy-driven security architecture purpose-built for government agencies, defense contractors and regulated enterprises operating in high-assurance environments. Designed from the ground up to meet the most stringent federal security mandates, the platform integrates next-generation network protection with validated cryptographic controls, continuous compliance monitoring and AI-powered threat intelligence.

The Forcepoint Network Security Platform has been architected to natively satisfy the requirements of four foundational compliance frameworks mandated across U.S. federal, defense and intelligence community environments. The following table summarizes the platform's alignment across each framework:

COMPLIANCE FRAMEWORK	SCOPE AND APPLICABILITY	FORCEPOINT ALIGNMENT
Common Criteria (CC)	DoD, Intelligence Community, NATO-aligned procurements	Independently evaluated and certified security functional requirements; supports Protection Profiles for network devices and firewalls
FIPS 140-3	Federal agencies, defense contractors, financial institutions requiring cryptographic assurance	All cryptographic modules validated at Level 2+; AES-256, SHA-2/3, RSA-4096 enforced across data in transit and at rest
NIST SP 800-53 Rev. 5	Federal civilian agencies (FedRAMP, FISMA), DoD RMF, and enterprise risk management programs	Controls mapped across AC, AU, CA, CM, IA, IR, RA, SC, SI, and SI families; supports continuous monitoring and authorization-to-operate (ATO) packages
CMMC 2.0 (Level 2 & 3)	Defense Industrial Base (DIB) contractors handling CUI and...	Addresses all 110 NIST 800-171 practices required for Level 2 certification; advanced...

NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations, defines the baseline control catalog used across federal civilian agencies (FISMA, FedRAMP) and the Department of Defense Risk Management Framework (RMF). The Forcepoint Network Security Platform directly implements or supports controls across the following control families

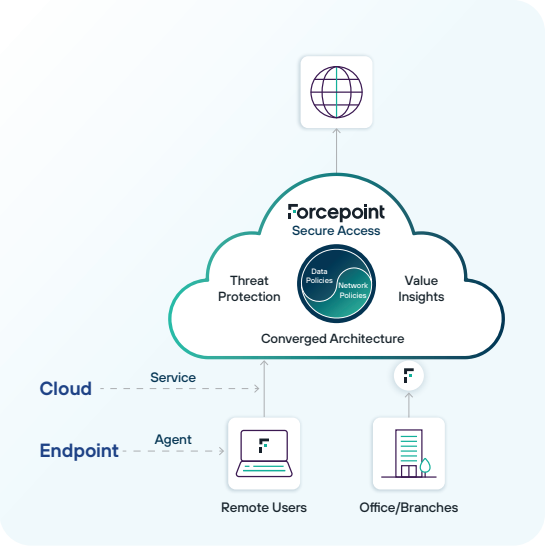
FAMILY	CONTROL FAMILY	PLATFORM COVERAGE
AC	Access Control	ZTNA enforcement, role-based access, least-privilege network segmentation, remote access controls
AU	Audit and Accountability	Tamper-evident audit logging, real-time SIEM integration, log retention management, non-repudiation
CA	Assessment and Authorization	Continuous monitoring, automated control testing, ATO evidence generation, POA&M management
CM	Configuration Management	Baseline configuration enforcement, change detection, golden configuration comparison, drift alerting
IA	Identification and Authentication	Multi-factor authentication, PKI/CAC integration, certificate validation, identity-based policy enforcement
IR	Identification and Authentication	Automated threat containment, forensic packet capture, incident timeline reconstruction, SOAR integration
SC	System and Communications Protection	Encrypted communications, network segmentation, boundary protection, covert channel prevention
SI	System and Information Integrity	IPS/IDS, malware detection, software integrity verification, spam and malicious code protection

The Forcepoint Network Security Platform supports flexible deployment models designed to integrate seamlessly with existing federal and defense IT environments, including on-premise data centers, classified air-gapped networks, hybrid cloud environments, and tactical edge deployments.

- → On-Premises and Air-Gapped Networks: Both hardware and virtual appliance form factors that support classified network environments including NIPRNet, SIPRNet, and JWICS-adjacent deployments. Bare-Metal option for ruggized tactical deployment.
- → Cloud and Hybrid Integration: FedRAMP-authorized cloud service integrations with AWS GovCloud, Azure Government, and DoD IL4/IL5 environments.
- → SIEM and SOAR Integration: Native integration with Splunk, Microsoft Sentinel, IBM QRadar, and ServiceNow for unified security operations.
- → Identity and Access Management: RADIUS/TACACS+ and SAML 2.0 integrations with DoW Enterprise Identity platforms, Microsoft Entra, and Ping Identity.
- → Orchestration and Automation: REST API, Ansible and Terraform libraries supporting automated deployment, policy updates and playbook execution.

Forcepoint Web Security (SWG)

Forcepoint cloud and on-premises web security.



Overview and Positioning

Forcepoint Web Security is built on a distributed enforcement architecture, giving agencies the option to inspect traffic in the cloud, on-premises, at the endpoint, or a mix of all three. Real-time analysis runs through Forcepoint's Advanced Classification Engine (ACE), a decision engine that routes content to the most effective of eight defense assessment areas (anti-malware, anti-spam/phishing, reputation analysis, behavioral sandboxing, and real-time security, content, and data classification, among others).

Key Capabilities and Differentiators

- → Built-in machine learning and heuristics identify new threats, not just known ones, backed by Forcepoint ThreatSeeker Intelligence across more than 900 million endpoints
- → Shadow IT visibility: discover cloud and GenAI applications in use and restrict access based on assessed risk
- → In the on-premises deployment mode, core threat prevention (proxy inspection, classification, anti-malware) is included; File Sandboxing (AMDP), Remote Browser Isolation, and advanced DLP classifiers are licensed add-ons (see table below)

Feature Availability by Deployment Mode

CAPABILITIES	ON-PREM	HYBRID	CLOUD
Proxy (SSL) inline inspection, real-time security/content classification, anti-virus/anti-tmalware	Included	Included	Included
File Sanboxing (AMDP)	Add-on	Add-on	Add-on
Remote Browser Isolation	Add-on	Add-on	Add-on*
Cloud Application Risk Database	Included	Included	Included
Standard Compliance DLP (PII/PHI/PCI, password files)	Add-on (Web, DLP module or full DLP Suite)	Add-on (limited)	Included
Advance DLP Classifiers (fingerprinting, ML)	Add-on	Add-on (limited)	Add-on
Granular web/social media controls, SSO (SAML 2.0)	Included	Included	Included

Mission Relevance and Use Case

As agencies expand GenAI access under federal AI governance and acquisition guidance while remaining accountable for the data those tools touch, Web Security's shadow AI detection and data theft controls give agencies guardrails to allow broader GenAI use without allowing sensitive or controlled data to leave agency control.

Recommended Federal Deployment Model

Physical, virtual, or endpoint-agent deployment for sensitive networks, avoiding routing of web traffic through a shared cloud proxy where policy requires it to stay on agency infrastructure. Confirm which add-on modules (RBI, AMDP sandboxing, advanced DLP) an agency needs, since these are not bundled by default

Advanced Malware Detection and Protection (AMDP)

An advanced sandbox solution engineered to detect and protect against advanced malware and zero-day threats.

Overview and Positioning

AMDP, powered by Hatching, a Recorded Future company, is Forcepoint's advanced sandbox: it executes suspicious files in an isolated, controlled environment to detect malware designed to evade signature-based and static-analysis tools, then shares malicious file signatures across Forcepoint's product portfolio.

Key Capabilities and Differentiators

- → Dynamic, behavior-based analysis detects zero-day and polymorphic malware that traditional antivirus, which relies on known signatures, cannot catch
- → Comprehensive file support for Windows, Linux, and Android; macOS analysis is available only through Forcepoint's cloud deployment, not on-premises
- → Detects over 350 malware families and their derivatives, with detailed forensic and MITRE ATT and CK-mapped reporting
- → Deployment options are cloud (SaaS) and on-premises, with Forcepoint describing the same capabilities across both

Mission Relevance and Use Case

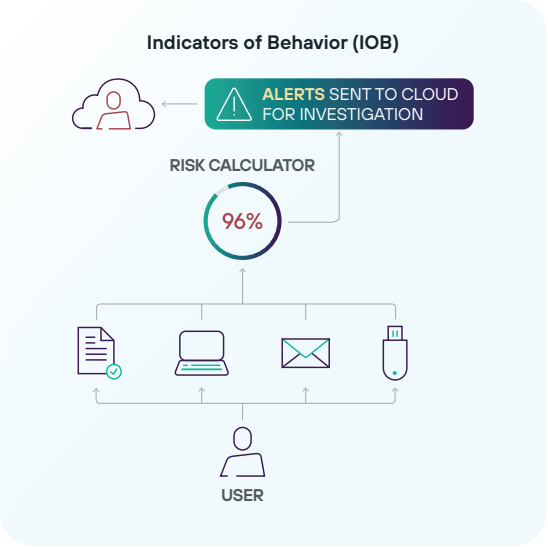
Forcepoint's own AMDP materials list central and federal government, alongside local and state government, among the top targeted industries for advanced malware, and note AMDP as the number-two optional capability Gartner identifies for SSE, after RBI. The On-Premises Manager stores detection and analysis information inside the agency's own data center, fitting environments with stringent privacy and policy constraints where files cannot be submitted to an external, vendor-hosted sandbox..

Recommended Federal Deployment Model

On-premises Manager and Engine components, with the Engine network isolated per Forcepoint deployment guidance (the Engine cannot run on a VM), integrated with NGFW and Secure SD-WAN for inline blocking. Forcepoint's data retention model for AMDP keeps only the file hash and threat score, with threat reports retaine for one year.

Remote Browser Isolation (RBI)

Isolate the web session from the user's device for high assurance web browsing.



Overview and Positioning

Forcepoint RBI renders risky or uncategorized websites inside an isolated remote container so malicious code never reaches the endpoint; the container and anything in it, is discarded when the session ends. RBI is licensed as an add-on to Forcepoint Web Security or as a standalone offering, and is available within Web Security's on-premises, hybrid, and cloud deployment modes.

Key Capabilities and Differentiators

- → Two isolation modes: Secure Streaming (image/pixel streaming, the highest-assurance mode) and Secure Rendering (sanitized HTML/CSS for a faster, native-like experience); Smart Isolation selects automatically based on assessed risk
- → Content Disarm and Reconstruction (CDR): rather than trying to detect malware, it extracts and verifies valid content from a document, then reconstructs a new file to carry it, eliminating document-borne risk including steganographic uploads
- → Licensing tiers: Full RBI (up to 100 percent of web traffic, unlimited categories) or Selective RBI (up to 10 licensed web categories)
- → Clipboard control and Safe Surf (read-only browsing with no data entry) for high-risk destinations

Mission Relevance and Use Case

Forcepoint positions RBI for both distributed businesses and government agencies. It lets agencies extend safe access to uncategorized or higher-risk destinations, such as open-source research sites, for the analysts and leadership who need that access, while reserving full isolation for high-value targets (for example, senior leadership) and selective isolation for the broader user population.

Recommended Federal Deployment Model

Deployed as a licensed add-on within Forcepoint Web Security, so session rendering and CDR processing occur on infrastructure the agency controls rather than a shared public isolation service. Confirm current system and browser requirements with the Forcepoint public sector team.

Forcepoint

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-Product Reference Guide-Federal-EN] 20Jul2026