DATASHEET

Mimecast Incydr Gov

Addressing Today's Data Protection Challenges

Federal agencies are increasingly vulnerable to data exfiltration, with sensitive information like classified data, citizen records, and operational plans at risk. Insider risk means employees accidentally or maliciously share files and sensitive data through:

- Unsanctioned AI tools
- Private email or cloud storage
- Personal code repositories
- USB drives, printing, AirDrop, and more

Common Gaps in Data Protection Strategies

Agencies often face several challenges with traditional solutions like Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), User Behavior Analytics (UBA), and User Access Monitoring (UAM) that are policy-based, reactive, and resource-intensive:

- **Lack of visibility into unknown risks:** Shadow IT and unsanctioned AI tools create blind spots, while a policy-based monitoring approach misses key risk areas.
- **Complex classification processes:** Lengthy, manual classification efforts delay effective protection, especially for unstructured data
- **Ineffective controls:** Basic block/no-block responses lead to false positives, disrupt productivity, and fail to adapt to and change user behavior.
- **Inefficient incident response:** It can take weeks to determine the "who, what, where, when, and how" of data exfiltration incidents.

How Incydr Gov Solves These Challenges

Incydr is purpose-built to help federal agencies quickly identify and mitigate data exfiltration risks. The solution aligns with the National Security Agency's (NSA) Zero Trust model and meets the requirements of the Cybersecurity Executive Order (EO).

Incydr provides comprehensive visibility across all file movements within an agency's environment from day one, shifting the focus from unclear user behavior to actual risk-indicating activity. It doesn't rely on traditional data-at-rest scanning but instead monitors endpoint, cloud, browser, and email activity in real-time. It automatically captures exfiltrated files for forensic analysis, allowing analysts to confirm the sensitivity of data involved in incidents immediately.

The platform uses AI-powered risk prioritization to automatically build a behavioral baseline and evaluate incidents based on file sensitivity, user behavior, file origin, and destination risk indicators. These risk indicators are pre-configured, but fully customizable. Teams can, for instance, setup tracking of movement and exposure of Controlled Unclassified Information (CUI).

Investigations are seamless, offering full contextual details —"who, what, where, when, and how"— in just a few clicks. Historical lookback is available for up to three years. The available Mihra Investigation Agent for Incydr offers built-in triage, contextual enrichment, and recommendations for incident response, saving teams valuable time.

Incydr provides a flexible suite of adaptive controls to protect data and educate employees. With real-time blocking and targeted in-the moment education, employees can learn and correct risky behavior over

time – directly addressing the 68% of insider incidents caused by accidental or negligent behavior. Watchlists allow agencies to apply controls to sensitive data sources or high-risk users, helping balance security with productivity.

Incydr works as a standalone tool or integrates seamlessly with existing tools like Security Information Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) systems. A Model Context Protocol (MCP) Server integration is available for customers to bring their own large language model (LLM) AI tool to accelerate workflows, check adherence to acceptable use policies, and even build custom reports.

Why Federal Agencies Choose Incydr

Incydr's capabilities are tailored to address the unique needs of government agencies, including a FedRAMP-authorized moderate SaaS solution to meet stringent U.S. Federal government requirements:

- **Comprehensive visibility:** Detect exfiltration risks involving sensitive data, shadow AI, and other unsanctioned tools from day one.
- **Immediate ROI:** Agencies reduce investigation times by up to 50% and realize payback in less than six months.
- **Tailored protection:** Adaptive controls like real-time blocking and education ensure secure access to data without disrupting mission-critical work, and curve employee behavior over time.
- **Seamless integration:** Pre-built connections with EDRs, SIEMs, IAMs, LLMs via MCP Server, and other tools fit into existing security & AI ecosystems.

Use Case: Combatting Shadow IT and AI Risks

Unsanctioned AI tools and shadow IT are growing threats to government data security. Employees often upload or paste sensitive information to these tools to improve productivity, but traditional DLP solutions fail to detect or protect against such risks.

Incydr Gov provides unmatched visibility into these activities, detecting risky behaviors such as pasting data into generative AI tools, uploading files to personal cloud storage, and sharing sensitive information via Airdrop, USB drives, & printing. Adaptive controls allow agencies to block these activities, protect sensitive data, educate employees, or apply targeted restrictions to minimize disruption while maintaining security.

Use Case: Protecting Data from Departing Employees

Departing employees and contractors often pose a significant risk to sensitive government information. Incydr automates monitoring of departing employees or contractors by integrating with HR systems and ticketing tools. It identifies anomalous behavior, builds a comprehensive activity history, and provides detailed reports to HR and legal teams to help agencies take swift action.

Why Incydr is the Right Solution for Government Data Protection

Incydr Gov empowers federal agencies to tackle data protection effectively, all while adhering to Zero Trust principles. By combining data visibility with contextual insights, the solution delivers a proactive, efficient approach that safeguards sensitive information, fosters secure collaboration, and ensures compliance with critical cybersecurity requirements.

Key Benefits:

- Comprehensive data protection across all environments.
- Streamlined and simplified risk management processes.
- Seamless integration with existing tools and workflows.
- Compliance with federal cybersecurity mandates, including FedRAMP authorization.

With Incydr Gov, agencies can confidently address insider risk while maintaining operational efficiency and meeting the highest security standards.