BEDROCK SECURITY

A New Era for Data Security: Are You Ready for EO 14117?

The U.S. Department of Justice's new data protection rule, issued under **Executive Order 14117**, is now live, and it's reshaping how organizations handle sensitive data. Whether you're a data controller, processor, SaaS vendor, or U.S.-based affiliate of a global enterprise, this rule applies to you. And the stakes are high: organizations must be fully compliant by **October 6, 2025**, or risk **civil fines of up to $374,474 per violation** (or **twice the transaction value**) and **criminal penalties of up to 20 years in prison** for willful breaches.

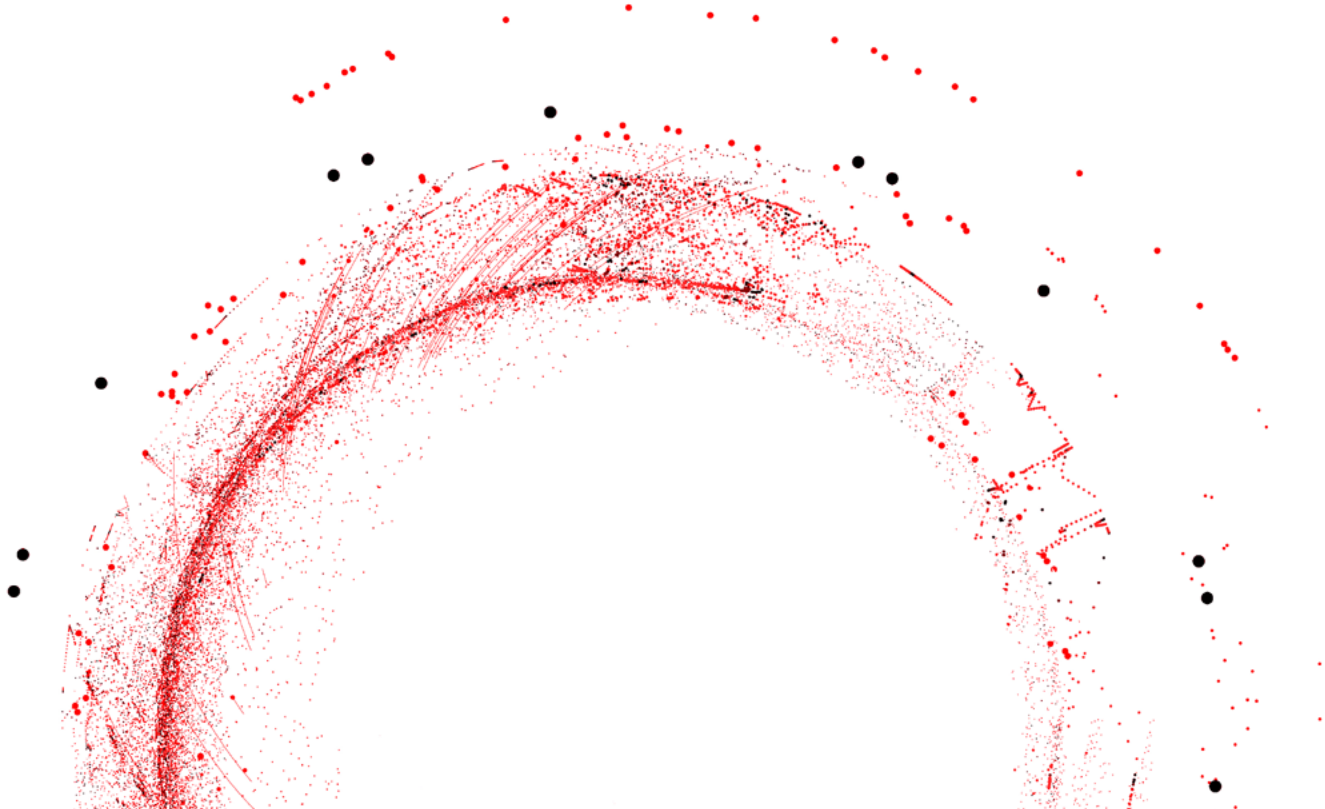
At its core, the regulation demands continuous visibility into what data you hold, how it moves, who can access it, and whether your policies actually protect it. Most organizations aren't there yet, especially across cloud and SaaS environments.

That's where Bedrock Security comes in.

Unlike traditional DSPM solutions that struggle to scale or keep up with AI-fueled, multi-cloud environments, **Bedrock was purpose-built to meet this moment**. Our platform gives you:

- **Scalability** – Serverless architecture that handles petabytes without tradeoffs
- **Accuracy** – AI-driven classification that reduces noise and improves precision
- **Context** – A continuously updated metadata lake that links data, access, usage, and risk
- **Efficiency** – Automated enforcement that shrinks the compliance burden

EO 14117 isn't just a policy; it's a national security mandate. Below, we break down each DOJ requirement and show how Bedrock helps your team stay compliant, audit-ready, and in control.



BEDROCK SECURITY

A New Era for Data Security: Are You Ready for EO 14117?

4 Ways Bedrock Can Help You Achieve Compliance

REQUIREMENT (EO 14117)DOJ	REQUIREMENT SUMMARY	WHERE ORGANIZATIONS FALL SHORT	HOW BEDROCK HELPS ACHIEVE COMPLIANCE
Sensitive personal and government-related data types and volume, transaction parties' identities, data end-use and transfer methods, and vendor identities.	Know exactly what kind of sensitive data is involved and how much, who is sending or receiving it, how and why it's being used or shared, and which third-party vendors (if any) are involved.	**82%** of cybersecurity professionals say they face visibility gaps in data discovery and classification. Only **24%** of organizations can produce a timely, complete data inventory.	**1) Deep Data & Identity Insight:** Bedrock discovers and classifies sensitive data across your data stores, so you know what data you have and how much of it. It also tracks identities and access (from employees to service accounts) and maps their data interactions, showing who is involved in each data transfer. Bedrock links this context with data flow monitoring, so you can see the purpose and method of each transfer and identify any external (vendor) access, giving full visibility into "who, what, how, and why" for every sensitive data transaction.
Risk-based procedures to verify and log data flows.	Continuously monitor and record how sensitive data moves, with extra focus on higher-risk data transfers.	**53%** of security teams lack real-time visibility into how sensitive data moves across environments. **62%** say the complexity of data formats and systems makes monitoring too manual.	**2) Continuous Data Flow Monitoring:** Bedrock automatically maps data flows across all cloud/SaaS environments, logging where sensitive data travels and detecting any unauthorized or risky transfers. It enforces data movement policies (e.g. "trust boundaries") to prevent sensitive data from going to unapproved locations and alerts security teams to unusual activity.
Written policies on data security and compliance that are certified annually by a responsible officer or employee.	Maintain formal data security and compliance policies in writing, and have an authorized executive review and officially attest to them every year.	**66%** of organizations cite lack of people and process as a barrier to effective enforcement. **79%** of teams say AI and SaaS usage is creating new blind spots in identity access control.	**3) Unified Compliance Dashboard:** Bedrock provides a real-time, unified view of your data security posture across all environments. This continuous visibility ensures your data protection policies are consistently enforced and documented. As a result, the responsible officer can easily review Bedrock's reports and dashboards to confirm that policies are being followed, making the annual certification process straightforward and backed by data.
Retaining the results of an annual audit by an internal or external independent auditor to verify compliance with the security requirements established by CISA.	Conduct an independent audit each year to confirm you're meeting the required security standards, and keep the audit report on file (e.g. for at least ten years as mandated).	Only **28%** of security leaders are confident they can detect and remediate policy violations in real time. **84%** say traditional tools make audit prep too slow and fragmented.	**4) Audit-Ready Evidence & Records:** Bedrock continuously logs all relevant data security activities and controls, creating an auditable trail automatically. It automates compliance documentation, freeing teams from manual spreadsheet tracking. With always-on monitoring, Bedrock drastically reduces the time needed to prepare for audits and provides reports that can be retained to meet long-term record-keeping requirements. Auditors can rely on Bedrock's collected evidence (e.g. data flow logs, access records, classification reports) to verify compliance with CISA's security standards, streamlining the annual audit process.

About Bedrock Security: Bedrock Security, the ubiquitous data security and management company, accelerates enterprises' ability to harness data as a strategic asset while minimizing risk. Its industry-first metadata lake technology and AI-driven automation enable continuous visibility into data location, sensitivity, access and usage across distributed environments. Bedrock's platform continuously catalogs data, enabling security, governance and data teams to proactively identify risks, enforce policies and optimize data usage — without disrupting operations or driving up costs. Trusted by leading financial institutions, healthcare providers and Fortune 1000 companies, Bedrock Security empowers organizations to improve data security posture management (DSPM), confidently deliver Responsible AI initiatives, and manage the exponential data growth. Learn more at https://bedrock.security.

BEDROCK SECURITY

Learn More

REQUEST A DEMO