Solution Brief

Manage Risk in an Expanding Data Landscape

Maintain control of intellectual property and ensure regulatory compliance with scalable data access governance tailored to your unique business needs

Challenge

- The faster people can create, use, and share data the more productive organizations can be, but this can greatly increase attack surfaces and liability for the business.
- Sensitive data is rapidly moving between on-prem repositories, SaaS services, and end-user devices, with risk potential at every turn.

Solution

- A holistic platform to automatically discover, classify, prioritize, remediate, and protect sensitive data across your environment.
- Risk prioritization and remdediation workflows enable you to mitigate risks like overexposure of regulated data as soon as possible.

Outcome

- Visibility and control over proprietary and regulated data across the organization for safer collaboration and minimized compliance risk.
- Significantly reduce data breach potential as you navigate AI and cloud transformation projects.

The Challenge: A Risk-Heavy Data Landscape

Today's data environment is sprawling, fast-moving and increasingly hard to govern. Enterprises are experiencing:

→ **Data sprawl and fragmentation**
Most organizations can't tell you where all their sensitive data is, much less what kinds of regulated data or intellectual property are accessible by various people. Data visibility is often limited to generic or narrow views that lack context, or only have meaningful insights on a small fraction of the enterprise.

→ **Data hungry AI**
AI promises improved productivity but this depends on access to large amounts of data and introduces a much larger risk surface.

→ **Increasing regulatory pressure**
GDPR violations can result in fines of up to 4 percent of annual global revenue, and most regulations now demand real-time visibility and control.

Organizations cannot afford to rely on outdated governance models. Scaling effective data access governance is essential to reduce risk, satisfy regulatory demands and avoid the negative consequences of data overexposure.

What Is Data Access Governance?

Data access governance refers to the policies, procedures and technologies organizations use to control:

→ Who can access what data

→ Under what conditions

→ How access is monitored and remediated

A foundational principle of data access governance is the **Principle of Least Privilege** (PoLP), which states that users, applications and systems should only have the level of access needed to perform their roles.

Employee workarounds, often in an attempt to streamline collaboration, end up working against this principle, underlining the need for active enforcement.

While enforcing the principle of least privilege may introduce some rigidity to workflows, the alternative – a breach or regulatory non-compliance – can be catastrophic. The key is to leverage technologies that can be tailored to your specific needs so that you can avoid any unnecessary friction.

Forcepoint's Approach: Scalable Governance That Works

Forcepoint provides a scalable, integrated approach to data access governance through two key solutions:

→ Data Security Posture Management (DSPM)

→ Data Detection & Response (DDR)

Together, they enable GRC and security teams to implement, automate and scale effective data access governance across complex hybrid environments.

Step 1: Discover and Classify With DSPM

Forcepoint DSPM offers visibility and control over sensitive data across cloud and on-prem infrastructure.

Key Capabilities:

→ **Automatic discovery and classification**
Classifies up to 1 million files per hour using a customizable AI mesh featuring small language models (SLMs) that identify business-critical content accurately and efficiently.

→ **Permissions mapping and analysis**
Maps user access permissions for files to detect over-permissioned access and identify excessive risk for remediation.

→ **File lineage**
Enables a view of the history of the file, including who has access and how the file has been shared, copied, or downloaded over time.

→ **Duplicate analytics**
Shows how many duplicates of a given file exist and how they are spread across the environment.

→ **Remediation workflows**
Connects security and business stakeholders to address risky access configurations with workflows for adjusting or revoking permissions and moving files to more secure locations.

With DSPM, organizations can pinpoint where regulated and proprietary data lives, understand how it's used and enforce least privilege policies at scale.

Step 2: Monitor and Enforce With DDR

Forcepoint DDR builds on DSPM's foundation by adding real-time behavior monitoring, automated risk detection and responsive controls.

Core Features:

→ **Live access monitoring**
Tracks data usage patterns in real-time – including opening, moving, sharing and renaming – to detect anomalies.

→ **Risk detection and response**
Identifies potential risks to sensitive data before damage occurs.

→ **Remediation assistance**
Enables rapid responses to data security risks as they unfold by initiating remediation workflows as security policies are violated.

→ **Controlling data movement**
Combine DSPM and DDR with Forcepoint's Data Security Cloud to prevent sensitive data from leaving the organization's control with the industry's most trusted solution for DLP blocking.

With DDR, organizations can complement periodic scans of data-at-rest with continuous monitoring for data risk, helping contain threats, prevent data loss and support ongoing compliance.

Solving the Governance Gap

GOVERNANCE GOAL	ACHIEVED WITH DSPM	ENHANCED WITH DDR
Find and classify data	AI-driven periodic data discovery scans and classification	Continuous data risk monitoring
Map and remediate access	Permissions inventory and workflows	Live access monitoring and alerts
Reduce risk surface	ROT analysis and blast radius cleanup	Threat detection and policy enforcement
Enforce least privilege	Access governance automation	Continuous monitoring and response

Benefits of Scaling Data Access Governance with Forcepoint

Reduce Risk

- → Identify sensitive data and over-permissioned files across more locations
- → Stop risk as it starts unfolding, before damage occurs

Simplify Compliance

- → Streamline audits and policy enforcement across GDPR, HIPAA, CCPA and more
- → Maintain consistent controls across hybrid environments

Improve Efficiency

- → Cut review time with AI-powered remediation and direct remediation
- → Focus analyst time on prioritized, high-impact issues

Scale with Agility

- → Support growing data repositories with rapid, high-volume scanning

Conclusion: Unified Governance That Works

Forcepoint DSPM and DDR work together to deliver:

- → **Actionable visibility** across all sensitive data
- → **Remediation** of permissions and exposure risks
- → **Continuous monitoring and control** for rapid enforcement of governance

This integrated platform equips GRC, compliance and security leaders with the tools needed to control access, manage risk and maintain compliance – at the pace modern business demands.

Next Steps: Get a Data Risk Assessment

Discover how Forcepoint can help your organization unlock data access governance at scale.

Request a free Data Risk Assessment

Get a personalized snapshot of your data risk posture, including shadow data, ROT and overexposed files – plus expert guidance on how to reduce your risk and improve compliance.

forcepoint.com/contact