DATA SHEET

Commvault® Data Posture 360

Understand sensitive data. Reveal exposure. Act with confidence.

OVERVIEW

Data Posture 360 helps organizations understand what sensitive data they have, where they might be exposed, and prioritize actions to help reduce risk. By enabling unified visibility into critical information and the context needed to evaluate it, Data Posture 360 helps security, governance, and data teams make more informed decisions, focus remediation efforts, and strengthen data hygiene across the organization.

THE DATA VISIBILITY GAP

Sensitive data is increasingly distributed across cloud, SaaS, on-premises, and protected environments, making it difficult for organizations to understand what data they have, where it resides, who can access it, and how it may be exposed. Excessive permissions, data sprawl, orphaned data, and a lack of visibility expand attack surface while creating governance, compliance, and AI-readiness challenges.

Without the context needed to understand exposure and prioritize risk, security and data teams struggle to focus remediation efforts where they can have the greatest impact.

$4.99M

global average cost of a data breach

72%

of organizations surveyed report they can't see how users interact with sensitive data across endpoints, cloud services, or SaaS platforms

SOLUTION

Data Posture 360 delivers Data Security and Posture Management (DSPM) capabilities that help organizations discover sensitive data, understand where it is exposed, and prioritize the actions that can help reduce data risk across cloud, on-premises, SaaS, and protected environments. By correlating data sensitivity, exposure indicators, and contextual risk insights, Data Posture 360 helps teams focus remediation efforts where they matter, improve data readiness, and support governance, compliance, AI, and cyber resilience initiatives.

With Data Posture 360, you can:

- Discover and classify sensitive data across your environment
- Gain insights into data exposure and prioritize remediation efforts
- Support attack surface reduction through improved data hygiene
- Help detect exposed secrets, including API keys and credentials

1 IBM, Cost of a Data Breach Report 2025, April 2026
2 2 Fortinet, 2025 Data Security Report, Aug 2025

KEY OUTCOMES

- Gain unified visibility into sensitive data across your production and protected environments
- Focus remediation efforts where they matter and help limit ROT data
- Improve data hygiene
- Help reduce exposure and storage costs

IDENTIFY SENSITIVE DATA

Data Posture 360 helps security, governance, and data teams build a trusted inventory of sensitive information across structured and unstructured environments. With greater visibility into critical data assets, organizations can help reduce blind spots, establish stronger governance foundations, and make more informed data security decisions before, during, and after a breach.

UNDERSTAND DATA RISK

Armed with greater visibility into sensitive data, organizations can better support data security, governance, compliance, and legal initiatives across the data lifecycle. Teams can investigate potential exposure, support audit and compliance initiatives, help accelerate eDiscovery and legal workflows, and use risk-based prioritization to focus remediation efforts on the areas with the greatest business impact and potential exfiltration risk.

STRENGTHEN CYBER RESILIENCE

Cyber resilience starts with understanding your data. By identifying sensitive, exposed, redundant, outdated, and orphaned data, Data Posture 360 helps organizations improve data hygiene, reduce unnecessary exposure, and support more informed protection and resilience strategies across the data lifecycle.

KEY CAPABILITIES

Capability	Feature	Benefits
• Automate data identification and classification	• Discover and classify sensitive data across production instances and protected data	• Build a unified inventory of sensitive data • Identify PII, PCI, PHI, intellectual property, and exposed secrets • Support governance, compliance, and AI initiatives
• Highlight data exposure and correlate risk signals	• Data inventory with related exposure and risk signals	• Reveal potential sources of exposure across sensitive data • Correlate sensitivity, exposure, and risk context
• Guide remediation actions	• Identify and remediate ROT data	• Help reduce unnecessary data exposure • Strengthen data hygiene • Help reduce attack surface • Can help lower storage costs

TURN DATA INSIGHTS INTO ACTION

Data Posture 360 is designed to help organizations turn sensitive data insights into action. By combining discovery, classification, risk insights, and remediation prioritization across production and protected environments, security, governance, and data teams gain the context needed to help reduce exposure,

> **With Commvault, we are able to help customer control their data and eliminate unpredictability.**

Chris Kiaie
Managing Director, ORIIUM, a Commvault customer

1. KNOW WHAT MATTERS

Organizations cannot protect what they cannot understand. Data Posture 360 helps security and governance teams identify sensitive data, understand where it resides, and uncover potential sources of exposure across production and protected environments. By building a trusted view of critical information assets, teams gain the context needed to make more informed data security and governance decisions.

2. ADAPT TO HELP REDUCE RISK

As environments evolve, teams need to focus attention on the risks that matter most. Data Posture 360 helps organizations investigate exposure, support audit and compliance initiatives, accelerate eDiscovery and legal workflows, and prioritize remediation efforts based on potential business impact. This helps teams reduce unnecessary exposure while supporting ongoing governance and data security programs.



Identify Potential Exposure



Focus Remediation Efforts



Support Audit and eDiscovery

3. STRENGTHEN DATA READINESS

Data Posture 360 helps organizations identify sensitive, redundant, outdated, and orphaned data that can increase risk and complicate data management decisions. By improving visibility into data quality, exposure, and lifecycle status, teams can strengthen data hygiene, help reduce attack surface, and establish a stronger foundation for data security, governance, AI, and resilience initiatives.

Learn more, visit **commvault.com**

© 2026 Commvault. See here for information about our trademarks and patents. 10_26