BROADCOM

Executive Summary

Data Security Posture Management: Modernizing Data Defense

Data is one of the most critical assets in modern organizations—powering operations, decision-making, and innovation. Yet as data expands across on-premises systems, cloud platforms, SaaS applications, and emerging technologies like GenAI, protecting it has become increasingly complex. Traditional security approaches, which treat data protection as a byproduct of other controls, are no longer sufficient.

This shift introduces a fundamental challenge: organizations are responsible for protecting vast amounts of distributed data but often lack visibility into where that data resides, what it contains, and who is accountable for securing it. As a result, data security programs can become fragmented, reactive, and difficult to scale—leading to gaps in protection, compliance risks, and missed threats.

To address this, organizations must move beyond ad hoc or tool-centric approaches and adopt a structured, lifecycle-driven model for data security. Data security posture management (DSPM) enables this shift by providing a continuous, holistic framework for discovering data, classifying its sensitivity, and assessing risk based on exposure and access. Rather than functioning as a standalone tool, DSPM serves as a discipline that integrates governance, risk management, and security operations into a unified data protection strategy.

At its core, DSPM empowers organizations to treat data as assets that need to be managed—applying consistent controls, aligning with regulatory requirements, and enabling more effective prioritization of security efforts. By integrating with existing technologies such as DLP, SIEM, and cloud security tools, DSPM enhances—not replaces—existing investments, ensuring that controls are applied where they matter most.

Leading organizations recognize that data security must be proactive, measurable, and aligned with business risk. By adopting a DSPM approach, they can reduce risk, improve compliance outcomes, and build trust in cloud and SaaS adoption—while enabling security teams to operate more efficiently and strategically.

The Data Visibility Gap

Data is distributed across cloud, SaaS, on-prem, and shadow IT

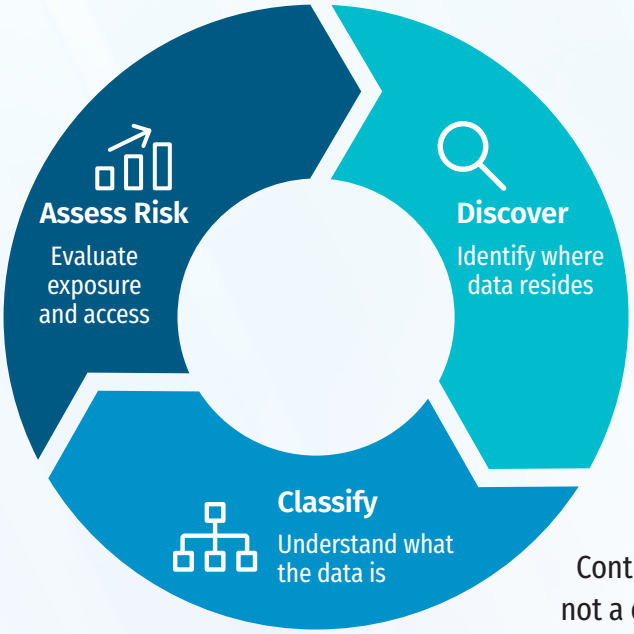
Organizations often don't know where data resides

Ownership and accountability are unclear

Undiscovered data remains unprotected and high risk

RESULT:
You can't protect what you don't understand

The DSPM Lifecycle Model



RESULT:
Continuous lifecycle, not a one-time process

Key Capabilities of DSPM

- Enterprise-wide data discovery
- Data classification by sensitivity and type
- Risk-based analysis aligned to threats
- Integration with governance and compliance frameworks
- Alignment with enterprise risk management (ERM)

DSPM + Existing Security Investments

- Enhances DLP, SIEM, and cloud security tools
- Enables better policy definition and enforcement
- Aligns technical controls with business risk
- Turns tools into a cohesive data security program

Bottom Line for Executives

Data security can no longer be reactive or fragmented. By adopting a lifecycle-based DSPM approach, organizations can gain visibility, reduce risk, and build a scalable, business-aligned data protection strategy.

SANS | Research Program

What's at Stake

Data Breaches
Sensitive data exposed or misused

Compliance Failures
Inability to meet regulatory requirements

Operational Inefficiency
Overwhelmed teams and missed alerts

Business Risk
Loss of trust, IP, and competitive advantage