Skyhigh Security

Skyhigh Data Security Posture Management (DSPM)

When Data Broke Free and Security Fell Behind

Cloud, SaaS, cloud-native development, and AI have transformed how data behaves. Instead of residing in a few secure systems, data now spreads across backups, logs, collaboration tools, analytics platforms, and AI pipelines—often beyond the visibility of security teams. It is created, copied, and moved faster than organizations can govern or secure it, creating a growing gap between where data exists and how well it is protected. This gap increases the risk of breaches and compliance failures.

Traditional security tools were not designed for this reality. They focus on access, movement, and configuration, but fail to determine whether sensitive data is unnecessarily duplicated or exposed at rest, or if misconfigurations truly put critical data at risk.

DSPM (Data Security Posture Management) addresses this challenge by making data sensitivity central. It enables organizations to identify, understand, and prioritize risks based on the data itself, providing clearer, more effective data protection.

Starting With The Data: How DSPM Redefines Security Posture

Data Security Posture Management (DSPM) continuously discovers data across cloud, on-premises, and hybrid environments, classifies it by sensitivity, and maps access, exposure, and risks such as misconfigurations or excessive permissions. By linking data sensitivity to security posture, DSPM prioritizes real risks over noisy alerts and enables proactive remediation. It answers critical questions: what data exists, where it resides, who can access it, and what its risk level is. DSPM delivers unified visibility, strengthens compliance through continuous assessment, and transforms data security into a strategic advantage for organizations.

Turning Data Sprawl Into Strategic Control

Leading organizations adopt Skyhigh DSPM for its data-centric approach to securing modern, distributed environments. Sensitive data now spans multi-cloud systems, SaaS applications, shadow databases, and more often beyond traditional visibility. Skyhigh DSPM continuously discovers and classifies sensitive data wherever it resides, bringing hidden risks into scope. It enhances decision-making by correlating data, access, and threat context, transforming raw findings into actionable risk intelligence so teams can prioritize critical exposures. Its proactive, visibility-driven approach strengthens protection for data at rest, while integration with Advanced DLP enables real-time control of data in motion, preventing leaks and misuse. With periodic scanning, continuous enforcement through Skyhigh's SSE and Advanced DLP, and audit trails that sustain compliance, protection remains consistent as environments evolve. Closed-loop remediation and near real-time protection turn insights into action, delivering measurable risk reduction and enduring control in a rapidly changing data landscape.

KEY ADVANTAGES

Skyhigh DSPM's advantages cluster around clarity, context, and control, cutting through data chaos without adding noise.

- **Data-first visibility:** Continuously discovers and classifies sensitive data across environments, revealing hidden risk.
- **Context-driven risk intelligence:** Correlates data, access, and behavior to surface real risks.
- **Proactive risk reduction:** Identifies exposure early and drives remediation before breaches occur.
- **Evidence-based compliance:** Maps data to regulations with continuous assessments and audit-ready compliance proof.
- **SSE-enabled Skyhigh DSPM:** Posture intelligence guides SSE and DLP enforcement across data movement.

FedRAMP

Skyhigh DSPM achieved FedRAMP High Authorization in March 2026, reinforcing Skyhigh Security's ongoing commitment to serving federal customers. Additionally, Skyhigh Advanced DLP and SWG (authorized in 2023), as well as Skyhigh DLP and CASB (authorized in 2020), have also received FedRAMP Authorization. Learn more.

KEY VALUE PROPOSITION

Risk That is Quantifiable and Comparable:
Translate abstract exposure into measurable data-risk, enabling teams to compare, rank, and track improvement over time.

Security That Scales With Data Growth:
As data multiplies across clouds, SaaS, analytics, and AI pipelines, Skyhigh DSPM scales visibility and governance without relying on tribal knowledge.

Faster, Smarter Incident Response:
When incidents occur, Skyhigh DSPM provides instant clarity on what data is involved, its sensitivity, and exposure history, cutting investigation time dramatically.

Better Decisions With Fewer Policies:
By using data context instead of broad rules, Skyhigh DSPM enables precise controls that reduce policy sprawl and operational friction.

From Detection to Direction:
Skyhigh DSPM doesn't just flag issues, it provides clear prioritization and remediation guidance, turning findings into forward momentum instead of backlog.

A Deep Dive Into the Foundations of Skyhigh DSPM

Here is how we at Skyhigh keep your data posture strong and why it makes a difference for you.

Visibility Of Sensitive Data Across Cloud Environments

We can discover data both at-rest and in-motion in real time—because we believe real control begins with visibility. By automatically discovering and classifying sensitive data across cloud, SaaS, and hybrid environments, enterprises gain a living view of data as it is created, moved, or forgotten, eliminating blind spots. Skyhigh DSPM enables this proactive risk management, surfacing misconfigurations and excess access early, ensuring continous compliance with clear data accountability and reduces audit stress. With this level of insight, operations become focused, prioritizing high-impact risks, allowing organizations to innovate, scale, and share data with confidence.

Controlled Data Flow Into AI Pipelines

AI has raised the stakes for data security because once sensitive data enters an AI pipeline, it cannot be reversed. With strong visibility and governance, organizations control data flows into AI systems, preventing irreversible loss. Skyhigh DSPM helps block sensitive data from unmanaged tools, reducing exposure, while turning shadow AI into a governed activity. Even sanctioned tools remain secure through controls like DLP and masking, enabling innovation without compromising data ownership, compliance, or security.

Extend Data Protection Beyond Boundaries with Inline Visibility

Secure data without any boundaries. Organizations can integrate Skyhigh DSPM with third-party proxy solutions using ICAP to gain real-time visibility into data movement, extending protection beyond native environments. This enables continuous discovery and safeguarding of sensitive data across inline platforms while eliminating blind spots and enforcing consistent policies. Enhanced visibility also strengthens access management by exposing hidden risks from outdated permissions and revealing true usage patterns. Skyhigh DSPM helps reduce over-sharing through precise controls and enforces least-privilege access as data and users evolve. The result is unified protection and secure, confident data operations.

Governing the Data Estate with Clarity, Control and Intent

Contextual data governance begins with understanding what data exists, how sensitive it is, who can access it, and why. Skyhigh DSPM enables this visibility by continuously discovering and classifying data across environments. The platform also delivers comprehensive remediation and protection from a single system, addressing risks identified by its analysis engine. Grounded in this context, governance moves beyond checkbox compliance to support business goals. Policies align with data sensitivity and real usage, strengthening protection for high-value data while maintaining accessibility. Continuous visibility enables defensible compliance, while a shared view across teams reduces friction and improves control.

Object-level Classification for Audit-Ready Compliance

Compliance is simpler when it starts with data, not audits. By making sensitive data visible, Skyhigh DSPM transforms compliance into continuous assurance. It classifies data at the object level, files, tables, and datasets, based on sensitivity, regulatory relevance, and exposure, enabling proportional, defensible controls. With continuous data context, compliance evidence updates automatically as environments change, simplifying audits and reducing disruption. By linking sensitivity to real exposure and enforcement across the SSE fabric, it delivers always-on, verifiable compliance grounded in actual protection.

Capabilities

Following is a sneak peak on few capabilities offered by Skyhigh DSPM:

Capabilities	Description	Benefit
Comprehensive Enterprise Data Visibility	Delivers a single-pane-of-glass view into data-risk across sanctioned cloud services, on-premises private applications, and Shadow IT and AI, identifying movement of sensitive to personal unsanctioned apps like personal Dropbox or Google Drive.	Security teams can identify sensitive data across all environments, including unsanctioned apps, reducing blind spots and enforcing security policies consistently.
Secure AI & GenAI Governance	Enforces “Least Privilege” for internal tools like Microsoft Copilot to prevent unauthorized training and blocks sensitive data uploads to external GenAI services like ChatGPT in real-time.	Prevent unauthorized access of sensitive data, control how internal tools use information, and block risky data uploads to external AI services in real-time, reducing exposure and potential breaches.
Context-Aware Destination Risk Blocking	Prevents the upload of highly confidential files to web applications identified as high-risk by dynamically correlating data sensitivity with the destination service’s risk score.	Mitigate accidental data leaks and reduce exposure to cyber threats.
Insider Threat & High-Risk User Monitoring	Instantly isolates and monitors all data accessed, created, or shared by high-risk users, such as leavers, allowing for immediate access revocation and download prevention.	Stop high-risk users from exfiltrating sensitive data, thus maintaining control over critical information.
Continuous Compliance & Residence Monitoring	Continuously audits data ownership and volume to identify compliance violations, such as unauthorized access by non-certified analysts or service accounts interacting with regulated PCI data.	Identifies policy breaches, helping ensure sensitive data is managed properly and remains aligned with PCI requirements.
Strategic Data Asset Management	Analyzes data distribution by object type and size to uncover hidden vulnerabilities, such as intellectual property (IP) concealed in CAD files or massive unencrypted database backups.	Proactively uncover vulnerabilities to safeguard critical assets ahead of potential exposure.
Forensic Search & Integrity Validation	Locates every instance of exfiltrated data using cryptographic hashes and checksums, ensuring detection even if files have been renamed to bypass standard DLP filters (e.g., renaming a database to an image file).	Strengthens DLP with advanced detection and enforcement capabilities that stops unauthorized data movement.
Data Proliferation & Duplicate Investigation	Identifies “digital twins” and modified copies of sensitive files across the enterprise to track data proactively.	Enhanced data control and risk management and aids in redundant data removal.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com

April 2026. DS-EN-000054-01