



Skyhigh Data Security Posture Management: Modernized Data Security

Organizations are increasingly adopting multi-cloud and hybrid cloud architectures, along with AI/ML programs and new collaboration initiatives, to drive innovation and stay competitive. However, this data explosion, coupled with continuous innovation, expands attack surfaces and creates challenges in discovering and securing vast, distributed datasets. Simultaneously, organizations struggle to control access to this data and ensure proper configuration of their cloud services. This expanded attack surface has serious implications for security, introducing new vulnerabilities, reducing visibility, and increasing complexity, which can result in security gaps.

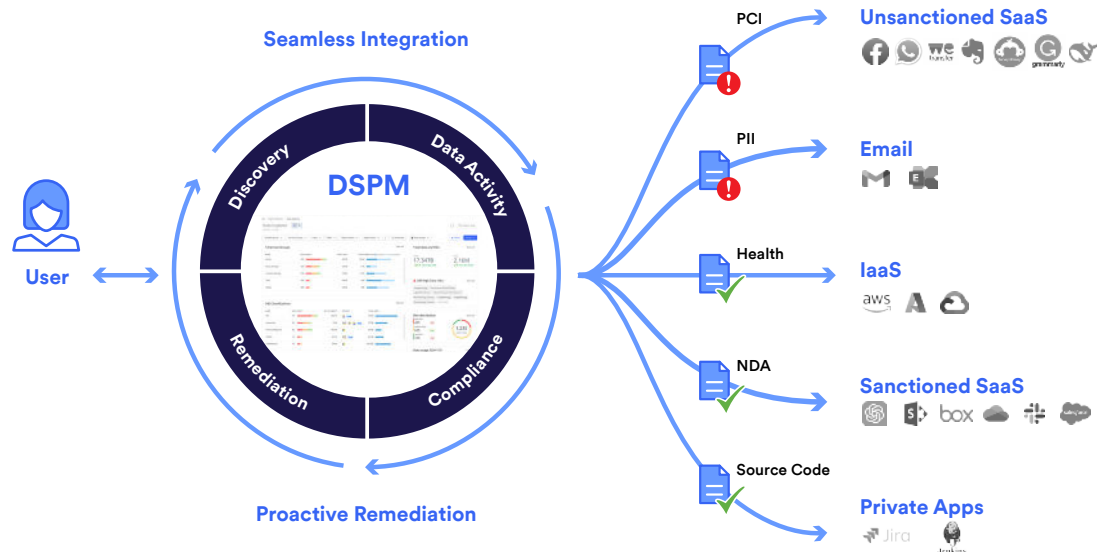
Skyhigh's SSE enabled DSPM solution allows customers to start their DSPM journey leveraging tools they already trust, reducing operational complexity and accelerating time to value, all from a single console.



Key Challenges in Data Security

- **Lack of visibility** into where sensitive data resides across hybrid, multi-cloud environments, email and Private Applications, as well as within shadow IT systems and GenAI applications. This lack of visibility increases the risk of data exposure or misuse.
- **Complex data access governance**, making it difficult to track how data is used, who has access to sensitive information, whether that access is appropriate, and how to enforce the principle of least privilege.
- **Increasing data risks**, including data explosion, misconfigurations, insider threats, and compliance violations. The lack of automated risk assessment leads to security gaps.
- **Lack of comprehensive data risk remediation**, makes it difficult for organizations to remediate and secure sensitive data vulnerabilities, misconfigurations, and improper data handling across cloud environments.
- **Fragmented security tools**, requiring multiple solutions to monitor and protect data across diverse cloud environments, leads to inefficiencies and additional cost.
- **Challenges maintaining and proving compliance**, enterprises struggle to efficiently comply with multiple regulatory requirements while managing audit costs and mitigating compliance risks.

Figure 1. Skyhigh DSPM.





How Skyhigh DSPM Solves These Challenges

1

Comprehensive Data Visibility and Classification

- Discovers and maps sensitive data across SaaS and IaaS environments.
- Tracks data movement and usage across web, private apps, email, and cloud platforms, including GenAI applications and Shadow Data
- Comprehensive data categorization using advanced AI-ML driven classification, fingerprinting (EDM and IDM), Optical Character Recognition (OCR) and more.
- Integration with third-party labeling and classification vendors, such as Microsoft Purview Information Protection and Titus, to identify sensitive data labeled by these solutions.

2

Data Access & Activity Monitoring

- Track data usage by analyzing who has access to sensitive data and monitoring their activity.
- Identify data sharing risks, including external exposure and data leaving enterprise boundaries.
- Detect anomalies and potential threats in real-time to prevent data breaches.
- Discover high-risk users based on their behavior and access patterns.

3

Risk Assessment & Compliance Auditing

- Gain full visibility into data exposure risks across your data sets, including:
 - **Risky Users:** Detect sensitive data accessed by high-risk users.
 - **Risky Storage:** Identify misconfigurations and vulnerabilities in cloud platforms.
 - **Risky Shadow IT:** Discover shadow data and sensitive data being shared with unauthorized and risky cloud applications.
- Provides an intelligent incident management platform that streamlines SOC analysis, enabling faster investigation and response to data risks.
- With actionable intelligence, organizations gain visibility into threats to their sensitive data and their compliance posture.

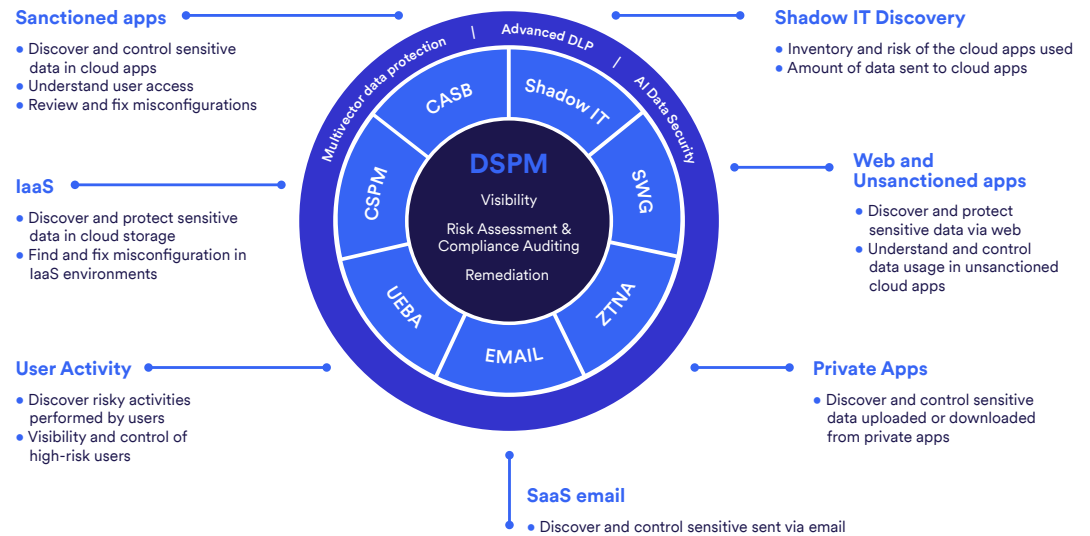


4

Remediation & Protection

- Automated remediation to prevent data loss and unauthorized access.
- Policy-based protection to secure sensitive data across all enterprise data sets.
- Granular controls over data exfiltration across web, cloud applications, GenAI applications, private apps, and email.
- Comprehensive protection for both managed and unmanaged devices using RBI, reverse proxy, and cloud app isolation.
- Resolve any possible misconfigurations in your corporate SaaS and IaaS to secure the data.
- Protect sensitive data by integrating with Rights Management Solutions (RMS) such as Microsoft Purview Information Protection and Seclore

Figure 2. SSE driven DSPM solution.





Why Skyhigh DSPM?

- **Comprehensive data security approach:** Skyhigh's Secure Service Edge (SSE) solution extends naturally into DSPM by leveraging our strong data security capabilities in AI/ML driven classification, compliance, and threat prevention.
- **Built on market leading SSE components:** Existing SSE features like SWG, CASB, CSPM, SSPM, UEBA, activity monitoring, and Shadow IT control, position Skyhigh to provide a seamless DSPM solution without requiring extensive new deployments, all managed from a single console.
- **Sanctioned and unsanctioned app coverage:** In addition to providing visibility into all structured and unstructured data on sanctioned cloud services and infrastructure, Skyhigh's proven SSE technologies ensure that customers can also monitor and control data leaving the enterprise into Shadow services, detecting Shadow Data and applying sophisticated controls to secure it.
- **Visibility and control of GenAI application:** Skyhigh enables enterprises to harness the benefits of Generative AI, sanctioned and unsanctioned, while minimizing risks and ensuring compliance with data protection standards
- **Optimized risk reduction:** These technologies enable enterprises to react quickly and efficiently to emerging threats by significantly reducing false alerts through exact data fingerprinting and machine learning, thereby optimizing SOC workflows.

Skyhigh's Data Security Posture Management (DSPM) solution sets the industry standard for protecting sensitive data across your cloud, private apps and more. With an industry leading classification platform that goes beyond traditional data security to accurately classify and safeguard data at rest and in motion. Fully integrated within our Secure Service Edge (SSE) platform, it delivers seamless data security without adding complexity. Skyhigh SSE driven DSPM platform provides end-to-end visibility and comprehensive protection across all data exfiltration points, ensuring no blind spots. With multiple proactive remediation options, including automated enforcement and guided responses, and a unified console for streamlined management, Skyhigh Security offers the most effective, scalable, and intelligent approach to data security in today's evolving threat landscape.



Get Started Today

Gain full visibility and control over your data with **Skyhigh DSPM**. Contact us to learn how you can simplify data security, reduce risk, and ensure compliance.

Learn more

For more information please visit skyhighsecurity.com or invite us for a demo at <https://skyhighsecurity.com/demo>.



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