Skyhigh Security

Skyhigh Data Loss Prevention (DLP)

KEY ADVANTAGES

- Protect sensitive data with confidence and ease, regardless of where it resides.
- Enhance sensitive data detection, prevent data leakage and stop insider threats.
- Simplify DLP using AI powered technology.
- Reduce signal to noise ratio in DLP incidents by leveraging AI.
- Gain confidence by testing data policies and rules before applying them broadly.
- Increase efficiencies with unified data protection across your entire SSE portfolio
- Reduce the number of alerts and incidents with automatic threat protection controls.
- Tackle emerging threats such as ransomware and extortion.

Advanced, Simplified, and Unified Data Protection for Today's Modern Enterprise

We make DLP Effortless

Organizations need data protection solutions that meet the ever-evolving needs of modern businesses, including protecting data stored in hybrid and multi-cloud environments, as well as data being accessed by remote employees on managed and unmanaged devices, while meeting compliance regulations. Businesses need future-facing DLP solutions that support emerging technologies, such as artificial intelligence applications, because cyberattacks take advantage of these new technologies. As organizations increasingly move to hybrid, multi cloud environments with remote/hybrid workforces, they are discovering that on-premise DLP solutions do not protect data in these scenarios. As a result, trying to protect data across all environments has become extremely complex, cumbersome and time consuming. DLP should not be a burden and Skyhigh provides a simplified way to secure an organization's data effectively, efficiently and effortlessly. With a unified approach, Skyhigh Security applies DLP rules consistently across sanctioned applications, unsanctioned applications, unmanaged devices, and a remote workforce.

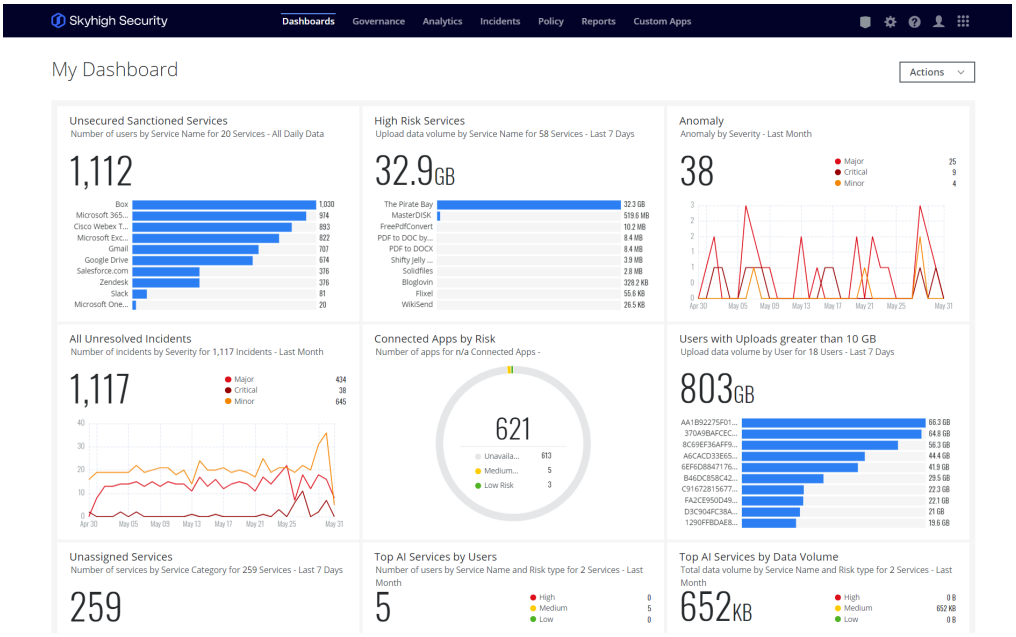

Figure 1. Skyhigh Security Dashboard

KEY USE CASES

- Detect and protect sensitive data regardless of where it resides.
- Secure your remote workforce; protect data being accessed by unmanaged devices.
- Ensure compliance with evolving regulatory compliance requirements.
- Protect against ransomware and other web-based threats in real time.
- Extend zero-day threat protection without degrading user experience.
- Identify and prevent insider threats.

Advanced Detection and Protection

Skyhigh DLP helps organizations protect their sensitive and confidential data using multiple advanced content-matching techniques, including real time Exact Data Matching (EDM), Indexed Document Matching (IDM), Optical Character Recognition (OCR) and AI-ML Auto Classifiers. These techniques increase accuracy, efficiency, and compliance within a wide range of industries and contexts - enabling organizations to better detect sensitive data, enforce policies, and prevent data leakage. They also tackle emerging threats such as ransomware, extortion, and identify insider threats.

Exact Data Matching (EDM)

Skyhigh's highly scalable EDM detects personally identifiable information (PII) and other confidential data stored in structured repositories with a very high detection accuracy and low false positive rates. EDM removes the manual burden on DLP administrators, reduces false positives and improves the overall security posture while providing the highest level of adherence to compliance requirements.

Indexed Document Matching (IDM)

Skyhigh's enhanced IDM protects unstructured data in text-based documents and image files through fingerprinting and indexing. Once your data is fingerprinted, you can add a DLP policy rule to leverage that indexed data for a complete or percentage match to protect your most sensitive documents. IDM complements exact data matching techniques to further reduce false positives by using exact hashes and taking away the guesswork out of a policy.

Optical Character Recognition (OCR)

OCR technology protects data that is stored in digital format, such as images of drivers licenses, passports or tax documents. OCR is a text extraction process that pulls text out of documents and images and feeds the plain text into the DLP engine for scanning to take place. OCR prevents data loss, misuse and theft by scanning images for sensitive information.

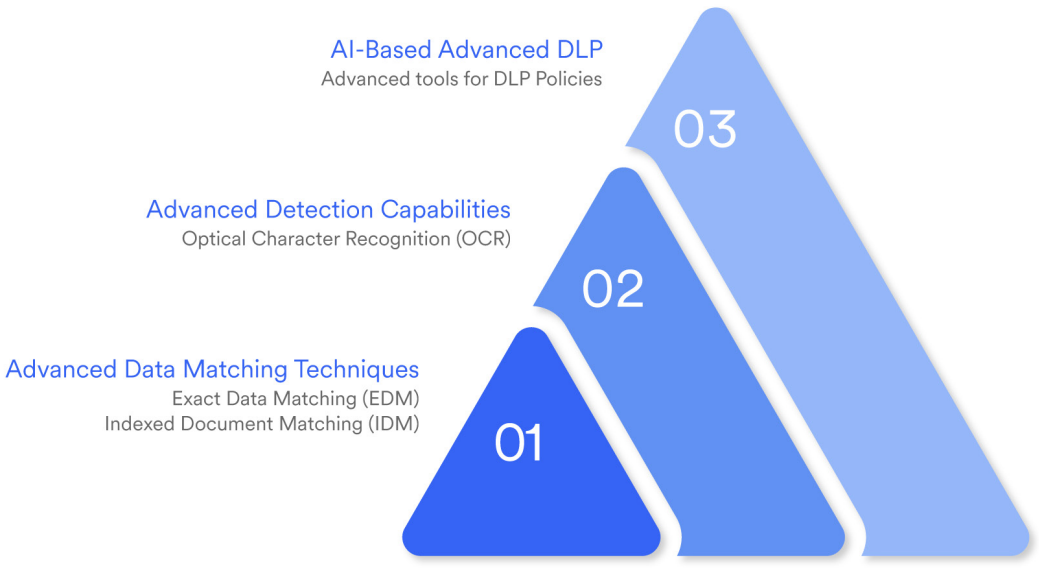

Figure 2. Skyhigh DLP Pyramid

Simplified DLP

Manually classifying sensitive data for DLP is a complex and time-consuming process. Creating accurate and comprehensive DLP rules requires specialized expertise, often unavailable in busy IT teams. Inconsistent classification leads to security gaps and potential data breaches. The burden of managing and maintaining numerous DLP rules is a drain on resources. We make DLP easy and effortless with best of breed capabilities such as AI Powered Classification Builder, AI/ML Powered Auto Classifiers and the Classification Tester.

AI Powered Classification Builder

Skyhigh is first-to-market an advanced AI-based RegEx Generator enabling users to swiftly create complex classifications based on regular expressions, improving productivity and efficiency. This new feature minimizes inaccuracies arising from human errors leading to imminent data loss, false positives and false negatives, and also enables zero day protection with complex and accurate policies, while supporting native non-English language queries to build DLP workflows.

AI-ML Based Data Policies

Leveraging Skyhigh's ML-powered auto-classifiers in data policies enables enterprises to define simpler policies without the need for complex data matching rules. Pre-trained machine learning models handle the grunt work, automatically identifying and classifying sensitive content with unmatched accuracy, removing the need for DLP expertise. Out-of-the-box protection gets you up and running quickly with pre-configured models for common data types like PII (Personally Identifiable Information), PCI DSS (Payment Card Industry Data Security Standards), and HIPAA (Health Insurance Portability and Accountability Act).

Classification tester functionality

One of the most common reasons for an ineffective DLP solution is the lack of a sandboxing tool. Complex policies and classifications are prone to human error, resulting in significant loss of sensitive data.

The Skyhigh Security classification tester utility provides this much needed capability to allow admins to test their data policies and rules before deploying them broadly. Our sandboxing tool addresses testing data classifications so admins can confidently apply them, to protect sensitive data across CASB, SWG, on-premises and ZTNA use cases.

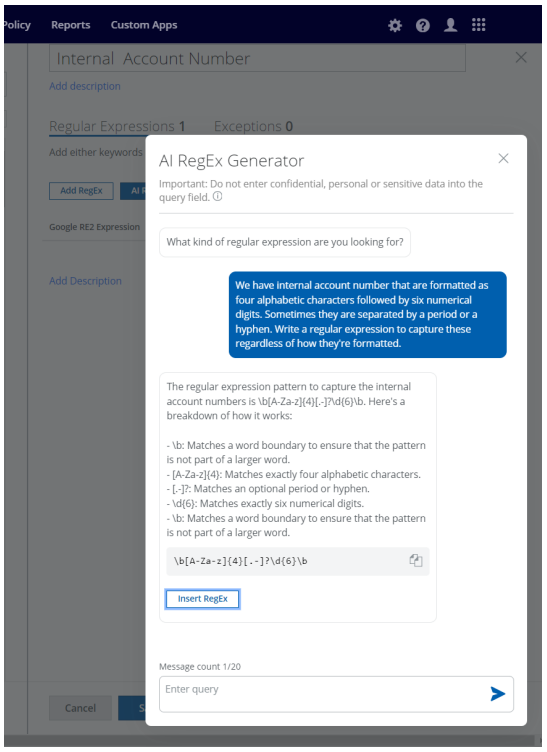

Figure 3. AI Powered RegEx Generator

Unified Data Protection

Skyhigh Security's unified data protection delivers a visual representation of sensitive information, identifying where it has been distributed, how it is being used and where it has been exfiltrated - across all cloud applications, web, private apps, email and endpoints, while highlighting data compliance risks. Skyhigh Security protects against data loss by applying classifications to data protection policies that trigger actions, generating incidents when sensitive data is identified.

Skyhigh Security is the industry's first vendor to provide unified data protection across the entire SSE portfolio, converging SWG, CASB and ZTNA using a single data classification and access policy while unified incident management makes it easy to administer data violation events by bringing them together in one dashboard.

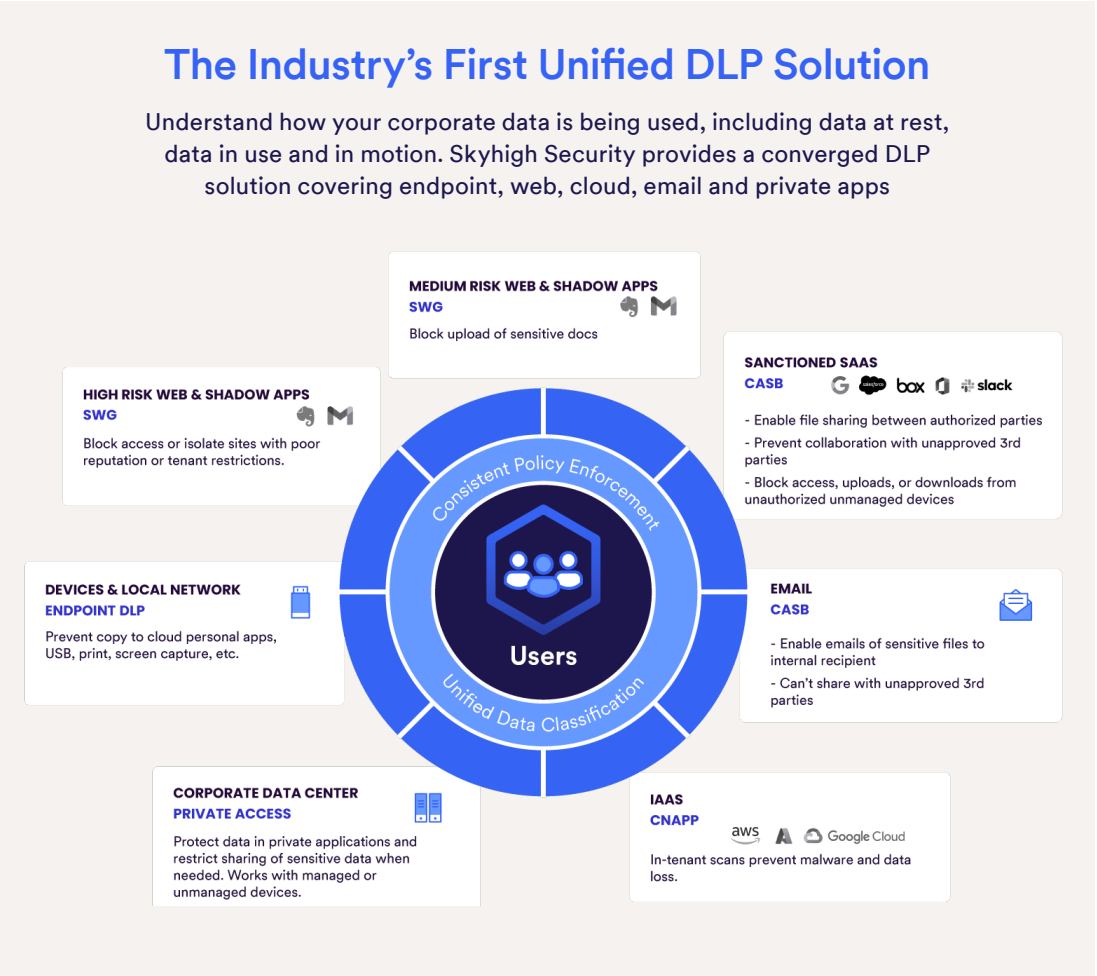

Figure 4. Skyhigh Security's Unified DLP Solution

After using our Advanced DLP capabilities to detect sensitive content, Skyhigh Security enables you to protect your data using these techniques:

- Apply encryption
- Quarantine
- Delete
- Send email notifications
- End use remediation (EUR)
- Bot notifications
- Apply DRM rules
- Block sensitive traffic
- Collaboration controls

For more information visit Skyhigh DLP or contact your sales representative.

Multi-Vector Data Protection

Skyhigh Security's unified DLP Solution helps you understand how your corporate data is being used, including data at rest, data in use and in motion. Skyhigh Security provides a converged DLP solution covering web, cloud, email, private apps and endpoints with unified data classification, policy enforcement, and incident management with pervasive DLP, real-time collaboration control, adaptive risk-based enforcement (40,000+ apps), and guided policy advisor.

Proactively Minimize Insider Risk

Skyhigh Security enables organizations to significantly improve their security posture by proactively minimizing insider risk through the use of Unified user risk scores. User risk scores identify and address potential insider threats before they result in data breaches by allowing enterprises to take different actions for risky users. Skyhigh Security continuously monitors and assesses the activities, access behavior of users to compute user risk scores that are used to prevent risky activities.

This targeted approach enhances the overall efficiency of security measures, as it allows for the prioritization of high risk individuals and the deployment of tailored interventions. The dynamic nature of user risk scores ensures that security protocols remain adaptive to evolving insider risks, reducing the likelihood of data exfiltration and ensuring compliance with regulatory requirements.

Leveraging user risk scores significantly improves an organization's overall security posture, protects sensitive information and improves compliance. Benefits include proactive insider threat detection, an adaptive security posture that evolves in real-time, accelerated incident response with additional context, reduced alert fatigue by streamlining false positives and more.

Enterprise Grade Threat Protection

Skyhigh Security DLP provides zero-day malware protection by integrating remote browser isolation, machine learning, emulation-based sandboxing, and real-time global threat intelligence. Fully integrated RBI technology provides the most powerful form of web threat protection available, eliminating the opportunity for malicious code to touch any end user device. Risks from new cloud threats are mitigated, enabling users to productively and safely use web and cloud apps from anywhere. Automated threat protection controls reduce the number of alerts and incidents for security teams to investigate and respond. Consistent policies, data protection, and visibility across isolated and non-isolated traffic, improve overall operational efficiency.

Skyhigh Security DLP safeguards your sensitive data, no matter where it's stored or how it's being used or shared. Managed from a single cloud-native console, Skyhigh DLP prevents data leakage, loss and misuse while ensuring compliance, and prevents data breaches using multi-vector data protection. With Skyhigh DLP you get advanced detection and protection, simplified DLP and unified data protection.

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

June 2024. DS-EN-000030-01