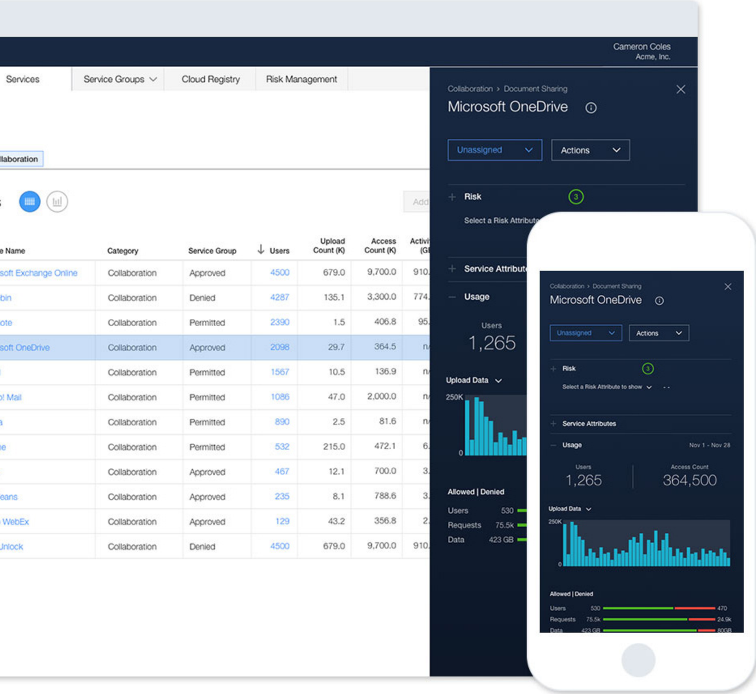
skyhigh

Cloud Access Security Broker

Skyhigh Cloud Access Security Broker enables organizations to enforce security, compliance, and governance policies across all cloud services, all users, and all devices.



e Name	Category	Service Group	↓ Users	Upload Count (K)	Access Count (K)	Activi (GE
soft Exchange Online	Collaboration	Approved	4500	679.0	9,700.0	910.
bin	Collaboration	Denied	4287	135.1	3,300.0	774.
ote	Collaboration	Permitted	2390	1.5	406.8	95.
soft OneDrive	Collaboration	Approved	2098	29.7	364.5	n/
	Collaboration	Permitted	1567	10.5	136.9	n/
o! Mail	Collaboration	Permitted	1086	47.0	2,000.0	n/
a	Collaboration	Permitted	890	2.5	81.6	n/
ne	Collaboration	Permitted	532	215.0	472.1	6.
	Collaboration	Approved	467	12.1	700.0	3.
eans	Collaboration	Approved	235	8.1	788.6	3.
WebEx	Collaboration	Approved	129	43.2	356.8	2.
Unlock	Collaboration	Denied	4500	679.0	9,700.0	910.

Skyhigh is the leading cloud access security broker (CASB) trusted by over 600 enterprises to enforce security policies across thousands of cloud services:

Visibility

Gain continuous visibility into SaaS, PaaS, and IaaS usage, understand data flowing outside the organization, and enforce governance policies

Compliance

Identify sensitive data in motion or at rest in cloud services and enforce data loss prevention policies to comply with industry regulations and internal policies

Threat Protection

Identify, mitigate, and remediate insider threats, compromised accounts, privileged user threats, and malware across cloud services

Data Security

Enforce data-centric security policies including encryption with your own keys, tokenization, contextual access control, and information rights management

FEATURED CUSTOMERS

DIRECTV

WESTERN UNION

Aflac

KAISER PERMANENTE

Honeywell

Booz Allen

COMCAST

hp

aetna

AstraZeneca

General Mills

RBC

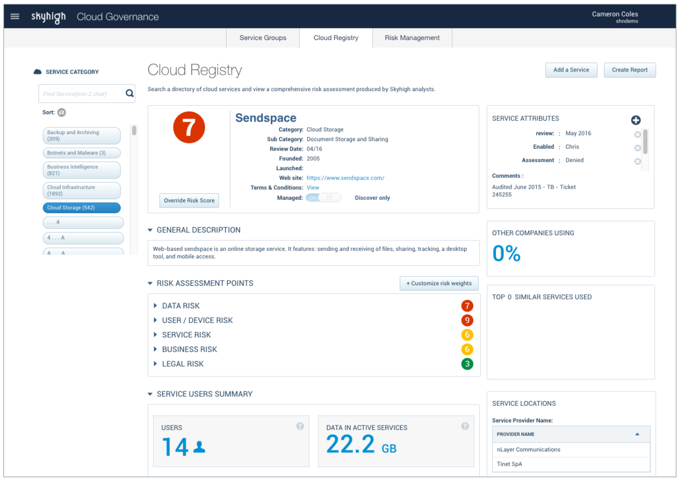
VISIBILITY

Cloud Usage Discovery

Discovers all SaaS, PaaS, IaaS, and custom applications in use and visually summarizes traffic patterns, access count, and usage over time.

Cloud Registry

Provides the world's largest and most accurate registry of cloud services, including thousands of services uncategorized by firewalls and proxies.



Cloud Registry

Search a directory of cloud services and view a comprehensive risk assessment produced by Skyhigh analysts.

Sendspace

Category: Cloud Storage
Sub Category: Document Storage and Sharing
Review Date: 04/16
Founded: 2005
Launched:
Web site: https://www.sendspace.com/
Terms & Conditions: View
Managed: ON Discover only

SERVICE ATTRIBUTES

review: : May 2016
Enabled : Chris
Assessment : Denied

Comments :
Audited June 2015 - TB - Ticket 245255

GENERAL DESCRIPTION

Web-based sendspace is an online storage service. It features: sending and receiving of files, sharing, tracking, a desktop tool, and mobile access.

OTHER COMPANIES USING
0%

RISK ASSESSMENT POINTS

DATA RISK	7
USER / DEVICE RISK	9
SERVICE RISK	6
BUSINESS RISK	6
LEGAL RISK	3

TOP 0 SIMILAR SERVICES USED

SERVICE USERS SUMMARY

USERS 14

DATA IN ACTIVE SERVICES 22.2 GB

SERVICE LOCATIONS

Service Provider Name:

PROVIDER NAME
nLayer Communications
Tinet SpA

Cloud Registry: Provides a 1-10 CloudTrust Rating

CloudTrust Ratings

Assigns a risk rating for each service based on 50 attributes. Modify attribute weights and add custom attributes to generate personalized ratings.

Cloud Service Governance

Provides a workflow to automatically or manually classify services based on risk criteria and enforce acceptable use governance policies through coaching and/or blocking.

Cloud Enforcement Gap Analysis

Presents allowed and denied statistics and highlights gaps in cloud policy enforcement along with recommendations to close gaps.

AI-Driven Activity Mapper

Leverages artificial intelligence to understand apps and map user actions to a uniform set of activities, enabling standardized monitoring and controls across apps.

On-Demand Data Scan

Identifies sensitive data stored at rest with the ability to target scans based on cloud service, date range, user, sharing status, and file size.

Collaboration Analytics

Visually summarizes sharing with third-party business partners, personal emails, and internal users and reports on policy exceptions.

COMPLIANCE

Cloud Data Loss Prevention

Enforces DLP policies based on data identifiers, keywords, and structured/unstructured fingerprints across data at rest and uploaded or shared in real time.

Secure Collaboration

Enforces external sharing policies based on domain whitelist/blacklist and content and educates users on acceptable collaboration policies.

Pre-Built DLP Templates

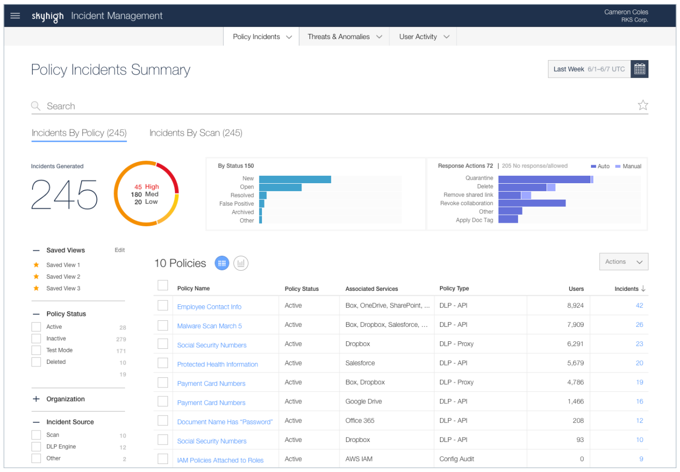
Provides out-of-the-box DLP templates and a broad range of international data identifiers to help identify sensitive content such as PII, PHI, or IP.

Multi-Tier Remediation

Provides coach user, notify administrator, block, apply rights management, quarantine, tombstone, and delete options and enables tiered response based on severity.

Policy Violation Management

Offers a unified interface to review DLP violations, take manual action, and rollback an automatic remediation action to restore a file and its permissions.



Policy Incidents Summary

Policy Status

□ Active	28
□ Inactive	279
□ Test Mode	171
□ Deleted	10
	19

+ Organization

Incident Source

□ Scan	10
□ DLP Engine	12
□ Other	2

10 Policies

□	Policy Name	Policy Status	Associated Services	Policy Type	Users	Incidents ↓
□	Employee Contact Info	Active	Box, OneDrive, SharePoint, ...	DLP - API	8,924	42
□	Malware Scan March 5	Active	Box, Dropbox, Salesforce, ...	DLP - API	7,909	26
□	Social Security Numbers	Active	Dropbox	DLP - Proxy	6,291	23
□	Protected Health Information	Active	Salesforce	DLP - API	5,679	20
□	Payment Card Numbers	Active	Box, Dropbox	DLP - Proxy	4,786	19
□	Payment Card Numbers	Active	Google Drive	DLP - API	1,466	16
□	Document Name Has "Password"	Active	Office 365	DLP - API	208	12
□	Social Security Numbers	Active	Dropbox	DLP - API	93	10
□	IAM Policies Attached to Roles	Active	AWS IAM	Config Audit	0	9

Policy Violation Dashboard: Summary view of all policy violations and remediation status

Match Highlighting

Displays an excerpt with content that triggered a DLP violation. Enterprises, not Skyhigh, store excerpts, meeting stringent privacy requirements.

Closed-Loop Policy Enforcement

Optionally leverages policies in on-premises DLP systems, enforces policies, and registers enforcement actions in the DLP system where the policy is managed.

THREAT PROTECTION

Cloud SOC

Delivers a threat dashboard and incident-response workflow to review and remediate insider threats, privileged user threats, and compromised accounts.

Cloud Activity Monitoring

Provides a comprehensive audit trail of all user and administrator activities to support post-incident investigations and forensics.

User Behavior Analytics

Automatically builds a self-learning model based on multiple heuristics and identifies patterns of activity indicative of a malicious or negligent insider threat.

Account Compromise Analytics

Analyzes login attempts to identify impossible cross-region access, brute-force attacks, and untrusted locations indicative of compromised accounts.

Privileged User Analytics

Identifies excessive user permissions, inactive accounts, inappropriate access, and unwarranted escalation of privileges and user provisioning.

Malware Protection

Identifies and blocks known signatures, sandboxes suspicious files, and detects behavior indicative of malware exfiltrating data via cloud services and ransomware.

Guided Learning

Provides human input to machine learning models with real-time preview showing the impact of a sensitivity change on anomalies detected by the system.

DATA SECURITY

Security Configuration Audit

Discovers current cloud application or infrastructure security settings and suggests modifications to improve security based on industry best practices.

Contextual Access Control

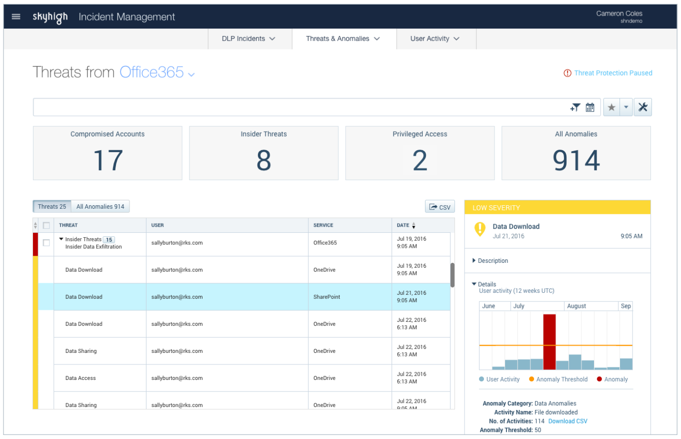
Enforces policies based on user, managed/unmanaged device, personal/corporate account, and geography with coarse and activity-level enforcement.

Contextual Authentication

Forces additional authentication steps in real-time via integration with identity management solutions based on pre-defined access control policies.

Encryption and Tokenization

Delivers peer-reviewed, function-preserving encryption schemes using enterprise-controlled keys, and tokenization for structured and unstructured data.



Threats from Office365

Threat Protection Paused

Compromised Accounts	Insider Threats	Privileged Access	All Anomalies
17	8	2	914

THREAT	USER	SERVICE	DATE
Insider Threats 15 Insider Data Exfiltration	sallyburton@rks.com	Office365	Jul 19, 2016 9:05 AM
Data Download	sallyburton@rks.com	OneDrive	Jul 19, 2016 9:05 AM
Data Download	sallyburton@rks.com	SharePoint	Jul 21, 2016 9:05 AM
Data Download	sallyburton@rks.com	OneDrive	Jul 22, 2016 6:13 AM
Data Sharing	sallyburton@rks.com	OneDrive	Jul 22, 2016 6:13 AM
Data Access	sallyburton@rks.com	OneDrive	Jul 22, 2016 6:13 AM
Data Sharing	sallyburton@rks.com	OneDrive	Jul 22, 2016

LOW SEVERITY

Data Download
Jul 21, 2016 9:05 AM

Description

Details
User activity (12 weeks UTC)

Anomaly Category: Data Anomalies
Activity Name: File downloaded
No. of Activities: 114 Download CSV
Anomaly Threshold: 50

Cloud SOC: Unified dashboard for cloud-based threats

Information Rights Management

Applies rights management protection to files uploaded to or downloaded from cloud services, ensuring sensitive data is protected anywhere.

PLATFORM

Skyhigh Gateway

Enforces policies with an inline proxy and steers traffic via device agent, proxy chaining, and identity providers to cover all access scenarios.

Skyhigh Cloud Connector

Connects to cloud services via cloud provider APIs to provide visibility and enforce security and compliance policies for all users and cloud-to-cloud activity.

Skyhigh Enterprise Connector

Collects logs from firewalls, proxies, and SIEMs, integrates with directory services via LDAP, and tokenizes sensitive data before uploading to the cloud.

Privacy Guard

Leverages an irreversible one-way process to tokenize user identifying information on premises and obfuscate enterprise identity.

Role-Based Access Control

Delivers pre-defined roles with granular and customizable permissions to manage the data and product capabilities users can access within Skyhigh.

Integration with Firewalls / Proxies

Provides script, API, and ICAP-based integration allowing you to enforce access and security policies consistently across your existing firewalls and proxies.

Integration with On-Premises DLP

Provides integration and closed-loop remediation with existing on-premises DLP solutions such as Symantec, Intel McAfee, and Forcepoint.

Integration with SIEMs

Collects log files from SIEMs and provides the ability to report on incidents and events from Skyhigh in SIEM solutions via syslog and API integration.

Integration with Key Management Systems

Seamlessly integrates with your existing key management systems using KMIP to encrypt data with enterprise-controlled keys.

Integration with IDM

Leverages identity management (IDM) solutions for pervasive and seamless traffic steering through Skyhigh Gateway and contextual authentication.

Integration with IRM

Integrates with leading information rights management systems to enforce existing policies across sensitive data.

Integration with EMM/MDM

Integrates with enterprise mobility management solutions to enforce access control policies based on whitelisted devices and EMM certificates.

FEATURED PRODUCTS

- Skyhigh for Shadow IT
- Skyhigh for Office 365
- Skyhigh for Box
- Skyhigh for Salesforce
- Skyhigh for Slack
- Skyhigh for Google Drive
- Skyhigh for Amazon Web Services
- Skyhigh for Custom Applications
- Skyhigh for Microsoft Azure
- Skyhigh for Dropbox
- Skyhigh for ServiceNow
- Skyhigh for Google Cloud Platform

SKYHIGH IS THE #1 CASB

#1

Breadth of Functionality

Only CASB to provide DLP, threat protection, access control, and structured data encryption in one unified product.

#1

Breadth of Coverage

Only CASB to cover all cloud services (SaaS, PaaS & IaaS), all devices (managed and unmanaged) and from anywhere (on and off network)

#1

Platform Scalability

Only CASB that scales to support 2 billion cloud transactions per day at the world's largest global enterprises.

#1

Platform Security

Only CASB that is FedRAMP compliant, ISO 27001/27018 certified, and stores no sensitive customer data in our cloud.