

Skyhigh Security Cloud Access Security Broker (CASB)

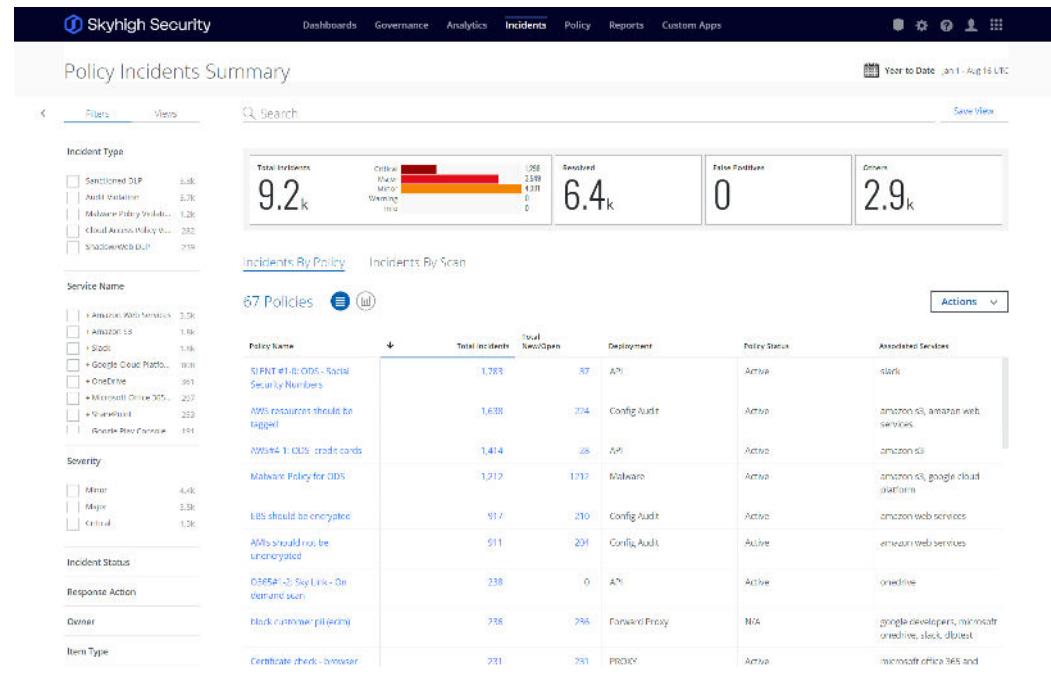
KEY USE CASES

- Enforce data loss prevention (DLP) policies on data in the cloud, in sync with your endpoint DLP.
- Prevent unauthorized sharing of sensitive data to the wrong people.
- Block sync/download of corporate data to personal devices.
- Detect compromised accounts, insider threats, and malware.
- Gain visibility into unsanctioned applications and control their functionality.
- Audit for misconfiguration against industry benchmarks and automatically change settings.
- Container optimized strategies for securing dynamic and ever-changing container workloads and the infrastructure on which they depend.

Cloud Security that Accelerates Business

A cloud access security broker that protects data and stops threats in the cloud across SaaS, PaaS, and IaaS from a single, cloud-native enforcement point.

- Visibility:** Gain visibility into all cloud use and data
- Control:** Take control over data and cloud activity from any source.
- Protection:** Protect against cloud threats and misconfiguration.





Our Skyhigh Security Cloud Platform

Unified Policy Engine

Applies unified policies to all cloud services across data at rest and in transit. Leverage policy templates, import policies from existing solutions, or create new ones.

Pre-Built Policy Templates

Delivers out-of-the-box policy templates based on business requirement, compliance regulation, industry, cloud service, and third-party benchmarks.

Policy Creation Wizard

Defines customized policies using rules connected by Boolean logic, exceptions, and multi-tier remediation based on incident severity.

Policy Incident Management

A unified interface to review incidents, take manual action, and rollback automatic remediation actions to restore files and permissions.

Cloud Registry

Provides the world's largest and most accurate registry of cloud services with a 1-10 CloudTrust Rating based on a 261-point risk assessment.

Privacy Guard

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

Autonomous Remediation

Coaches users to correct policy incidents, and once corrected, automatically resolves incident alerts to reduce manual review of incidents.

In-App Coaching

Coaches users in real-time within the native email, messaging, and collaboration application where the incident occurred. 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.

Multi-Cloud Protection

Enforce a uniform set of security policies across all cloud services, with the ability to associate policy violations and investigate activities, anomalies, and threats at individual services.

Category	Count In Use	Total Policies
Security Configuration	720	900
Compliance/DLP	3	50
Secure Collaboration	11	11
File Integrity	2	2
Malware	1	1
Vulnerability	1	1
Wildcard Hardening	1	1

Category	Count In Use	Total Policies
Container Security	361	390
Monitoring	83	89
Network Security	60	66
Certificate And Key Management	52	52
Compliance	0	41
Logging	40	41
Device Posture	11	11
Secure Collaboration - Level 1	6	6
Document Classification Solutions	4	4
Backup And Recovery	4	4



Visibility Into All Cloud Use and Data

Content Analytics

Leverages keywords, pre-defined alphanumeric patterns, regular expressions, file metadata, document fingerprints, and database fingerprints to identify sensitive data in cloud services.

Collaboration Analytics

Detects granular viewer, editor, and owner permissions on files and folders shared to individual users, everyone in the organization, or anyone with a link.

Access Analytics

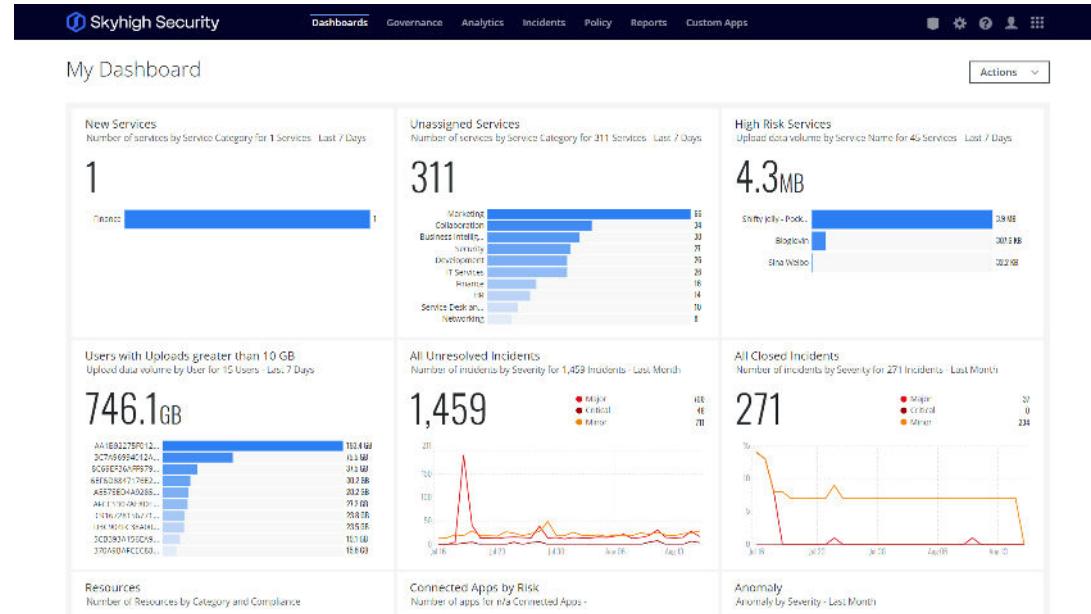
Understands access context including device operating system, device management status, location, and corporate/personal accounts.

Cloud Usage Analytics

Summarizes cloud usage including cloud services in use by a user, data volumes, upload count, access count, and allowed/denied activity over time.

Cloud Activity Monitoring

Captures a comprehensive audit trail of all user and administrator activities to support postincident investigations and forensics.





Control Over Data and Activity in the Cloud

Cloud Data Loss Prevention (DLP)

Enforces policies based on your own content rules to prevent data loss in cloud applications and infrastructure, across file, structured, and unstructured data. On premises Skyhigh Security Data Loss Prevention (DLP), powered by Trellix.

Multi-Source Control

Enforces DLP policies for data uploaded to the cloud, created in the cloud, shared with collaborators, shared cloud-to-cloud from one service to another, and downloaded from the cloud.

Multi-Tier Response

Defines policies with multiple levels of severity and enforces distinct response actions based on the severity level of the incident. Response actions, such as a DLP scan in real time, can be automatically triggered by a misconfiguration found in an audit.

Quarantine

Isolates files that trigger policies in a secure administrative location within the cloud service where it was found. Skyhigh Security never stores quarantined files.

The screenshot shows the Skyhigh Security interface with the following details:

- Service Name:** SharePoint
- Incident Type:** Audit Violation, Suspicious DLP
- Service Name (List):**
 - Amazon Web Services: 8,58
 - Amazon S3: 1,88
 - Facebook: 1,88
 - Google Cloud (Data): 870
 - OneDrive: 301
 - Microsoft Office 365: 297
 - Skyhigh: 253
 - SharePoint: 392
- Severity (List):** Major (140), Critical (81), Minor (52)
- Incident Status (List):** Quarantine, Investigate, Pending, Resolved
- Response Action (List):** Select Response, New
- Owner:** Unsigned
- Incident Response:** Select Resolution
- Resolution Action:** MITRE

Selected Incident Details:

O365#1-1: Sky Link - Basic Credit Card Rule
 Sanctioned DLP Incident (ID #69924)
Service Name: SharePoint
Instance Name: prod0001
Activity: Uploaded
Incident Created On: Aug 11, 2023 7:27 AM UTC
Last Updated: Aug 11, 2023 7:27 AM UTC
Last Response: Quarantine
Quarantine Status: New
User: unknown@skyhighcloud.com



Encryption

Protects sensitive data with peer-reviewed, function preserving encryption schemes using customer controlled keys for structured and unstructured data.

Information Rights Management

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

Collaboration Control

Downgrades file and folder permissions for specified users to editor or viewer, removes permissions, and revokes shared links.

Permissions can be based on sensitivity of data.

Connected Apps

Provides visibility into third-party applications connected to sanctioned cloud services, such as marketplace apps. Take policy-driven control over third-party apps based on specific users, applications, or access permissions.

Removal

Permanently removes data from cloud services that violate policy, to comply with compliance regulations.

Contextual Access Control

Enforces coarse allow/block access rules based on service level risk, device type, and granular activity-level controls to prevent upload and download of data.

Adaptive Authentication

Forces additional authentication steps in realtime via integration with identity management solutions based on access control policies.

Cloud Application Control

Granular policy for unsanctioned cloud services including the ability to allow or block activities and control access to unsanctioned tenants all from our console.

Skyhigh Security

Activity from All Services

Activity | Geo Location | May 26/23 - Aug 20/23 | Users

Legend:

- Unknown (199)
- Unknown (1)

Action	IP Address	Protocol	Date
Access Requests	109.111.111.111	OneDrive	Aug 12, 2023 8:00 AM
Access Requests	109.111.111.111	OneDrive	Aug 12, 2023 8:00 AM
Access Requests	Cloudflare (CloudFront)	OneDrive	Aug 12, 2023 8:00 AM
Access Requests	Cloudflare (CloudFront)	OneDrive	Aug 12, 2023 8:00 AM
Access Requests	Cloudflare (CloudFront)	OneDrive	Aug 12, 2023 8:00 AM

HIGH SEVERITY

ID# 17923

Anomalous Access Location

Aug 12, 2023 8:00 AM

Description

Aug 12, 2023 8:00 AM - Aug 12, 2023 8:00 AM

Details



Protection Against Cloud Threats and Misconfiguration

Security Configuration Audit

Discovers current cloud application or infrastructure security settings and suggests modifications to improve security based on industry standards such as the Center for Internet Security (CIS) benchmarks. Audits can be run prior to deployment of code into infrastructure-as-a-service (IaaS) to pre-emptively mitigate risk.

Automated Configuration Remediation

Enables a policy-based response to misconfiguration discovered in an audit to automatically change the setting, such as disabling public access for an IaaS storage bucket.

ENTERPRISE TECHNOLOGY INTEGRATIONS

- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Key management service (KMS)
- Identity and Access Management (IAM)
- Information rights management (IRM)
- Enterprise mobility management (EMM/MDM)
- Directory services (LDAP)

User and Entity Behavior Analytics (UEBA)

Automatically builds a self-learning model based on multiple heuristics and machine learning to identify patterns of activity indicative of user threats across multiple cloud services.

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.

The screenshot shows the Skyhigh Security platform interface. At the top, there's a navigation bar with links for Dashboards, Governance, Analytics, Incidents, Policy, Reports, and Custom Apps. On the far right of the header, there are icons for Edit Integration, Learn how Firewall/Proxy Integration works, and a search bar.

The main content area has two main sections:

- Firewall/Proxy Integration:** This section shows a summary for McAfee Web Gateway. It indicates "No entries reported" and provides details about integration mode (Automatic), email summary (On), update process (Published URL list), and last sync (August 19, 2022 02:29 PM UTC).
- Service Group Sync Status:** This section displays a table titled "Service Group Sync Status". The table has columns for Service Group, # Services, # URLs, Changes Since Last Sync, Approvals, and Actions. The data in the table is as follows:

Service Group	# Services	# URLs	Changes Since Last Sync	Approvals	Actions
Blocked services	7	12	No	No	
High-risk cloud storage	74	96	No	No	
Permitted services	6	28	No	No	
Sanctioned services	6	36	No	No	
Undesirable cloud storage	77	31	No	No	
Breach-as-a-service	18	26	No	No	
Non-sanctioned-cloud-storage	510	726	No	No	
Marketing/permited-spas	4	7	No	No	
Medium Risk - EU GDPR	30,917	42,634	No	No	
Legal Risk	174	227	No	No	



Account Compromise Detection

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

Insider Threat Detection

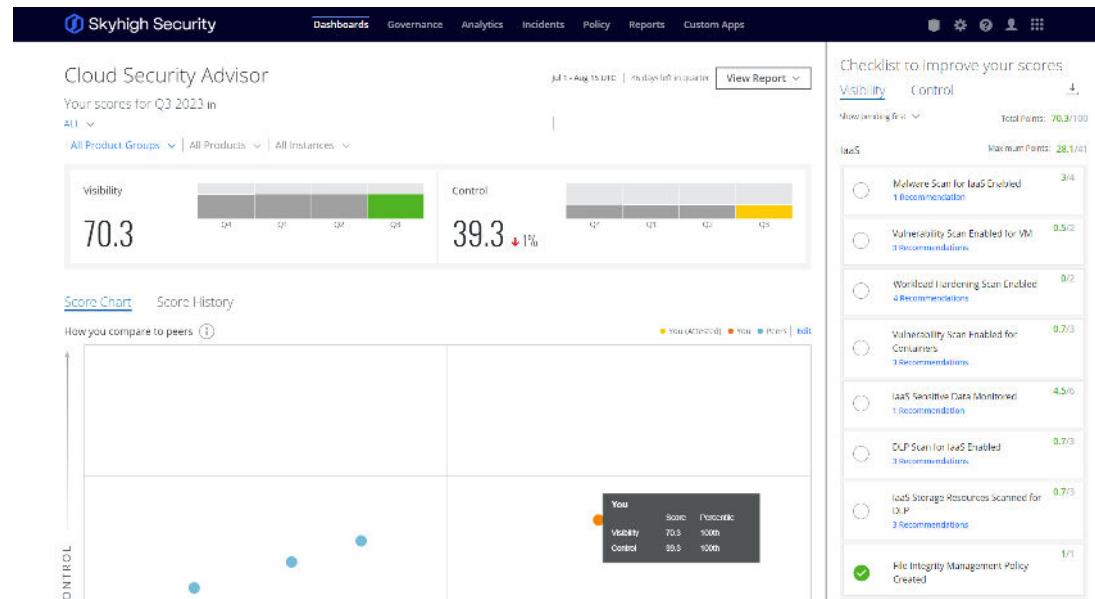
Leverages machine learning to detect activity signaling negligent and malicious behavior including insiders stealing sensitive data.

Privileged User Analytics

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

Malware Detection

Identifies malware and detects behavior indicative of malware exfiltrating data from cloud services. Cloud services can be scanned on-demand for historical compromise and in real-time.





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