

Skyhigh Security Cloud Access Security Broker (CASB)

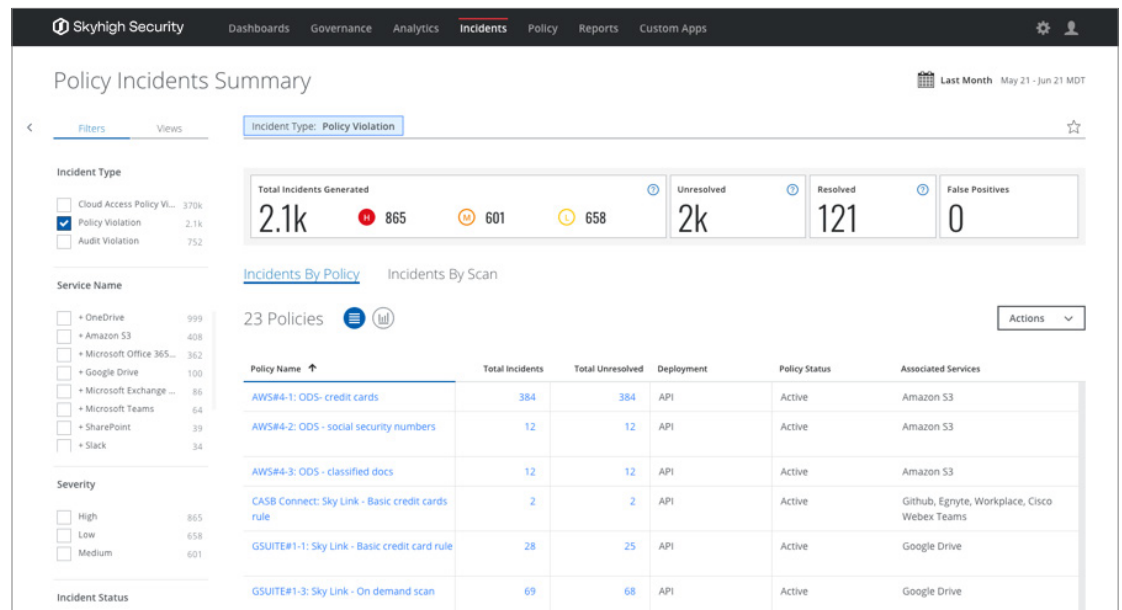
Cloud Security that Accelerates Business

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.

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

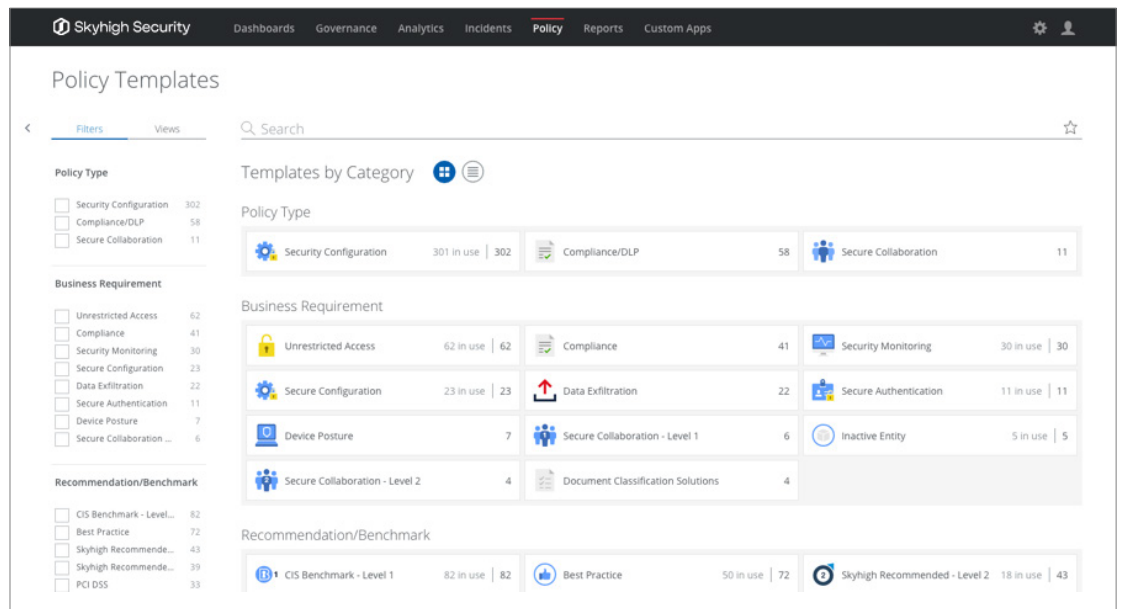
Coaches users in real-time within the native email, messaging, and collaboration application where the incident occurred.

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.





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

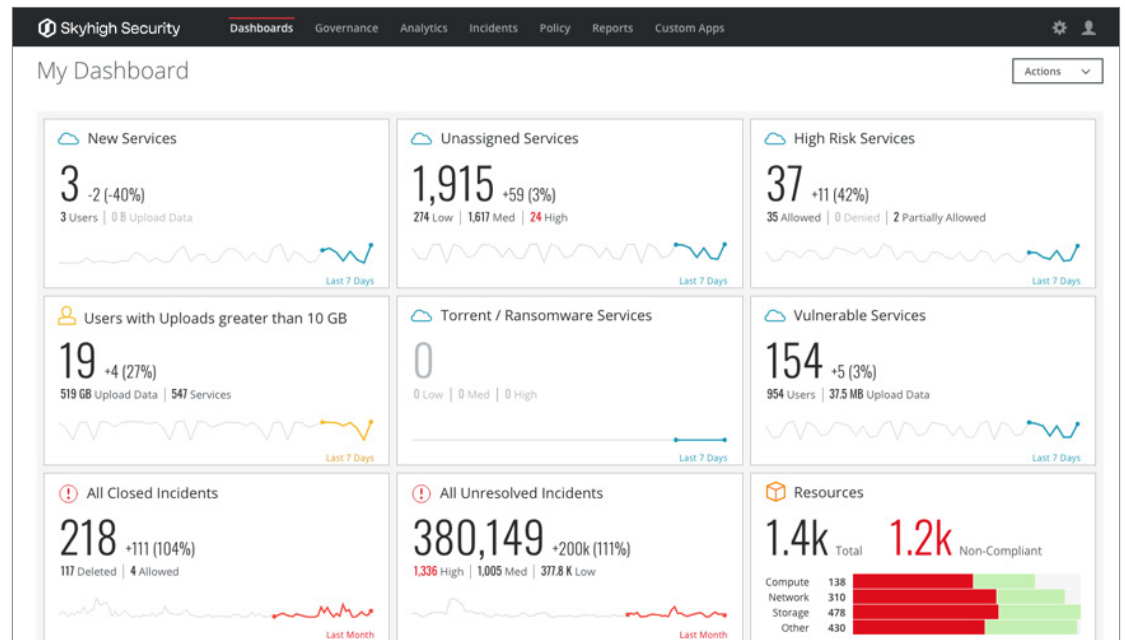
Understands access context including device operating system, device management status, location, and corporate/personal accounts.

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 post-incident 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

The screenshot displays the Skyhigh Security interface for Policy Incidents. The main view shows a table of 2,136 incidents, filtered by 'Policy Violation'. The table includes columns for Severity, Policy Name, Service Name, Item Name, Incident Response, and Incident Created. A detailed view of a specific incident is shown on the right, providing information such as ID, Severity (High), Service Name (OneDrive), Instance Name, Activity, Incident Created On, Last Updated, Last Response, Owner (Unassigned), Incident Response (New), and Content details (Item Name, Item Type, Path).

Sev	Policy Name	Service Name	Item Name	Incident Response	Incident Created
H	O365#1-1: Sky Link - Basic credit card rule	OneDrive	CCN_15_records.xls	Deleted	May 27, 2019
H	O365#1-3: Sky Link - Structured Fingerprinting	OneDrive	SSN_15_records.xls	Deleted	May 27, 2019
H	O365 ePO Exchange policy	Microsoft Exchange Online	Data Transaksi Baru	Quarantined	May 27, 2019
H	O365#1-1: Sky Link - Basic credit card rule	OneDrive	CCN_15_records - dke.xls	Deleted	May 28, 2019
H	O365#1-1: Sky Link - Basic credit card rule	OneDrive	sample-data.xls	Deleted	May 28, 2019
H	O365#1-3: Sky Link - Structured Fingerprinting	OneDrive	SSN_15_records.xls	Deleted	May 28, 2019



administrative location within the cloud service where it was found. Skyhigh Security never stores quarantined files.

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

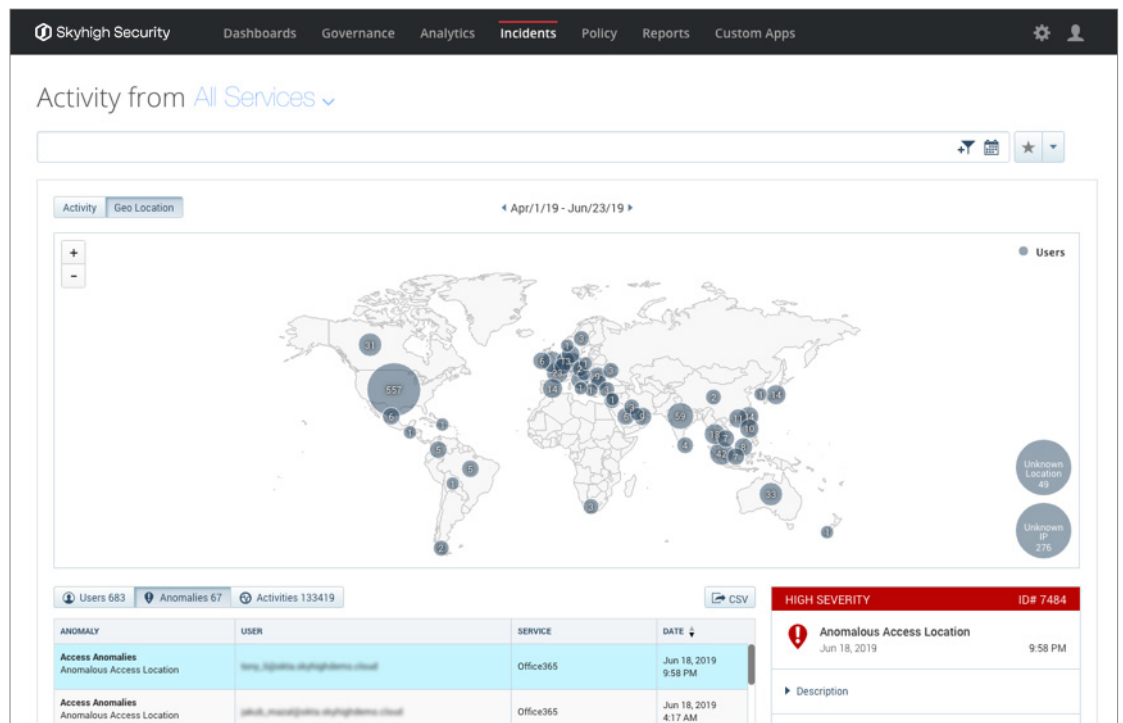
Enforces coarse allow/block access rules based on service level risk, device type, and granular activity-level controls to prevent upload and download of data.

Adaptive Authentication

Forces additional authentication steps in real-time 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.





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.

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

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)

The screenshot shows the 'Firewall/Proxy Integration' page in Skyhigh Security. It features a navigation bar with 'Dashboards', 'Governance', 'Analytics', 'Incidents', 'Policy', 'Reports', and 'Custom Apps'. The main content area is titled 'McAfee Web Gateway' and includes an 'Edit Integration' button. Below the title, there are instructions: 'What to do: Approve pending changes, download files that need to be manually uploaded to edge devices, or edit integrations.' and a link 'Learn how Firewall/Proxy Integration works'. The page displays integration details for McAfee Web Gateway, including 'Integration Mode: Automatic', 'E-mail Summary: On', 'Update Process: Published URL List', and 'Last Sync: June 21, 2019 04:05 PM UTC'. A 'Service Group Sync Status' table is also present, showing the number of services and URLs for various service groups.

Service Group	# Services	# URLs	Changes Since Last Sync	Approvals	Actions
Blocked-services	10	13	--	No	--
High-risk-cloud-storage	108	143	--	No	--
Permitted-services	6	12	--	No	--
Sanctioned-services	6	23	--	No	--
Undesirable-cloud-storag	48	53	--	No	--
Breached-services	14	23	--	No	--
Non-sanctioned-cloud-sti	618	778	--	No	--
Marketing-permitted-app	4	5	--	No	--



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.

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

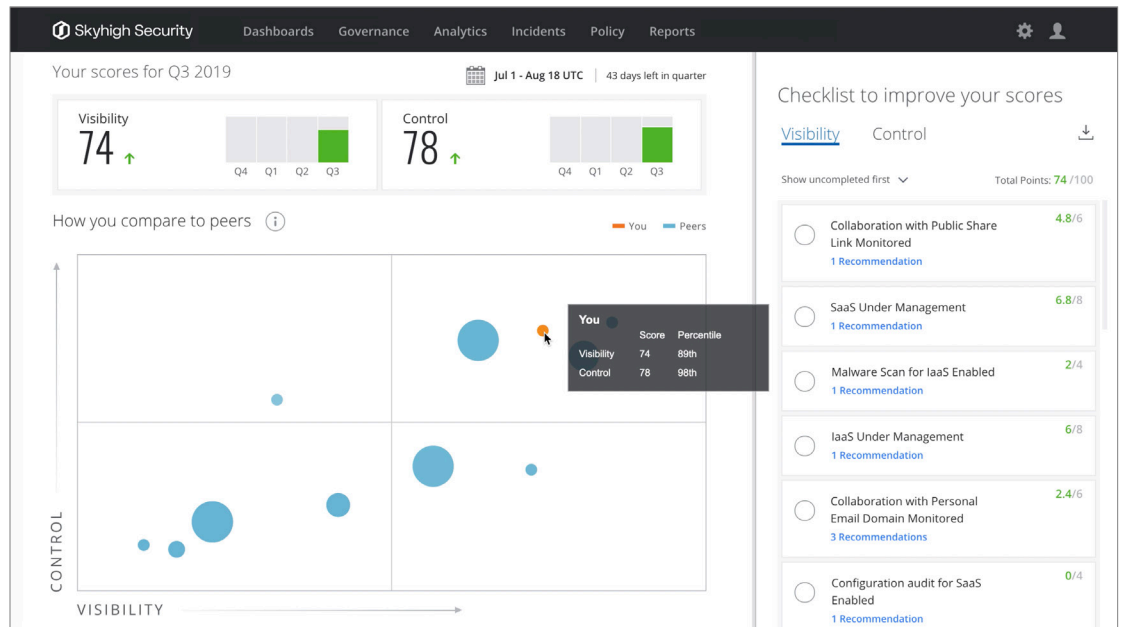
Leverages machine learning to detect activity signaling negligent and malicious behavior including insiders stealing sensitive data.

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





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.

Learn More

For more information visit us at skyhighsecurity.com



6220 America Center Drive
San Jose, CA 95002
888.847.8766
skyhighsecurity.com

Skyhigh Security is a registered trademark of Musarubra US LLC. Other names and brands are the property of these companies or may be claimed as the property of others. Copyright © 2022. March 2022