DATA SHEET

# Skyhigh Security Cloud Access Security Broker (CASB)

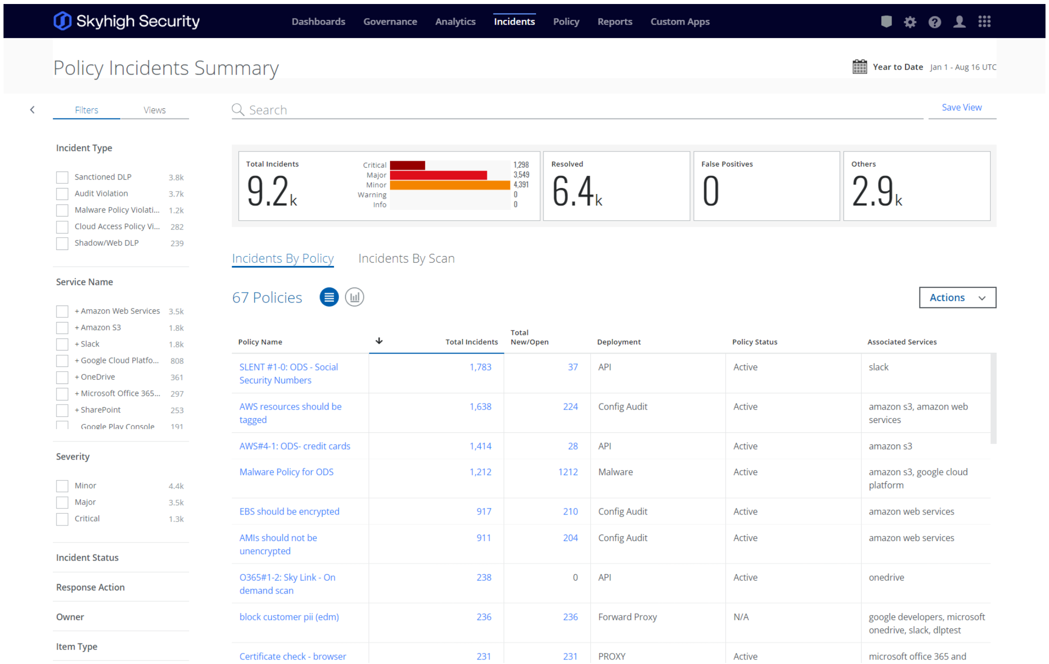
### KEY USE CASES

- 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.



Policy Incidents Summary

Year to Date Jan 1 - Aug 16 UTC

Incident Type

- □ Sanctioned DLP 3.8k
- □ Audit Violation 3.7k
- □ Malware Policy Violati... 1.2k
- □ Cloud Access Policy Vi... 282
- □ Shadow/Web DLP 239

Service Name

- □ + Amazon Web Services 3.5k
- □ + Amazon S3 1.8k
- □ + Slack 1.8k
- □ + Google Cloud Platfo... 808
- □ + OneDrive 361
- □ + Microsoft Office 365... 297
- □ + SharePoint 253
- □ Google Play Console 191

Severity

- □ Minor 4.4k
- □ Major 3.5k
- □ Critical 1.3k

Incident Status

Response Action

Owner

Item Type

| Total Incidents | | | Resolved | False Positives | Others |
|---|---|---|---|---|---|
| 9.2k | Critical | 1,298 | 6.4k | 0 | 2.9k |
| | Major | 3,549 | | | |
| | Minor | 4,391 | | | |
| | Warning | 0 | | | |
| | Info | 0 | | | |

67 Policies

| Policy Name | Total Incidents | Total New/Open | Deployment | Policy Status | Associated Services |
|---|---|---|---|---|---|
| SLENT #1-0: ODS - Social Security Numbers | 1,783 | 37 | API | Active | slack |
| AWS resources should be tagged | 1,638 | 224 | Config Audit | Active | amazon s3, amazon web services |
| AWS#4-1: ODS- credit cards | 1,414 | 28 | API | Active | amazon s3 |
| Malware Policy for ODS | 1,212 | 1212 | Malware | Active | amazon s3, google cloud platform |
| EBS should be encrypted | 917 | 210 | Config Audit | Active | amazon web services |
| AMIs should not be unencrypted | 911 | 204 | Config Audit | Active | amazon web services |
| O365#1-2: Sky Link - On demand scan | 238 | 0 | API | Active | onedrive |
| block customer pii (edm) | 236 | 236 | Forward Proxy | N/A | google developers, microsoft onedrive, slack, dlptest |
| Certificate check - browser | 231 | 231 | PROXY | Active | microsoft office 365 and |

## Our Skyhigh Security Cloud Platform

### Unified Policy Engine

Applies unified policies to all cloud services across datavat 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 thirdparty 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

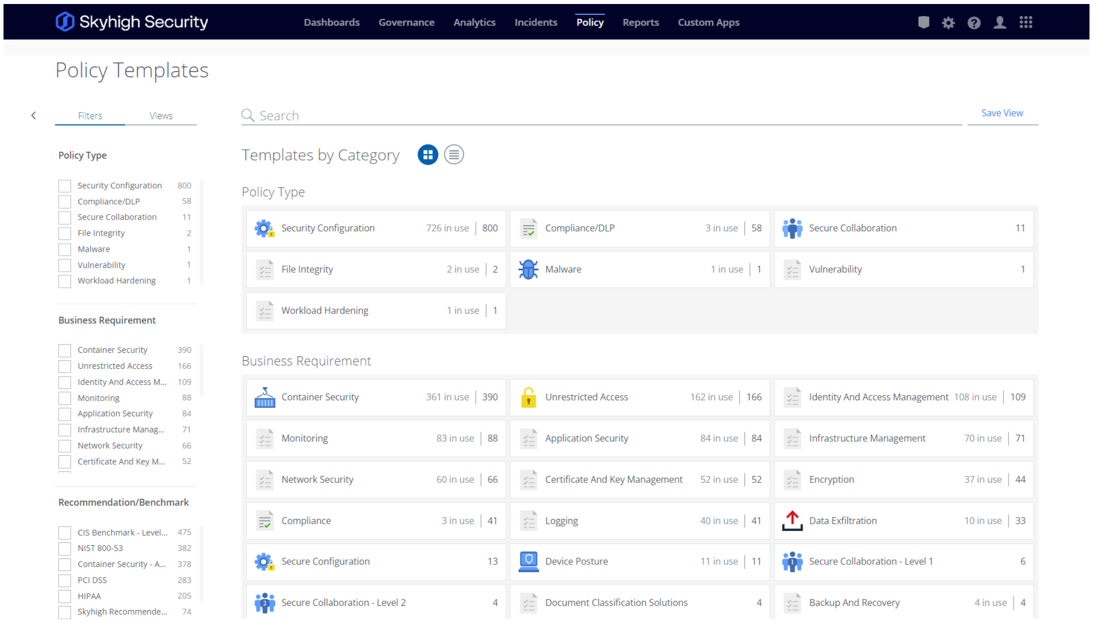
Coaches users to correct policy incidents, and once corrected, automatically resolves incident alerts to reduce manual review of incidents.

### 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.



Policy Templates

Policy Type

| | | |
|---|---|---|
| □ | Security Configuration | 800 |
| □ | Compliance/DLP | 58 |
| □ | Secure Collaboration | 11 |
| □ | File Integrity | 2 |
| □ | Malware | 1 |
| □ | Vulnerability | 1 |
| □ | Workload Hardening | 1 |

Business Requirement

| | | |
|---|---|---|
| □ | Container Security | 390 |
| □ | Unrestricted Access | 166 |
| □ | Identity And Access M... | 109 |
| □ | Monitoring | 88 |
| □ | Application Security | 84 |
| □ | Infrastructure Manag... | 71 |
| □ | Network Security | 66 |
| □ | Certificate And Key M... | 52 |

Recommendation/Benchmark

| | | |
|---|---|---|
| □ | CIS Benchmark - Level... | 475 |
| □ | NIST 800-53 | 382 |
| □ | Container Security - A... | 378 |
| □ | PCI DSS | 283 |
| □ | HIPAA | 205 |
| □ | Skyhigh Recommende... | 74 |

Templates by Category

Policy Type

| | | |
|---|---|---|
| Security Configuration 726 in use \| 800 | Compliance/DLP 3 in use \| 58 | Secure Collaboration 11 |
| File Integrity 2 in use \| 2 | Malware 1 in use \| 1 | Vulnerability 1 |
| Workload Hardening 1 in use \| 1 | | |

Business Requirement

| | | |
|---|---|---|
| Container Security 361 in use \| 390 | Unrestricted Access 162 in use \| 166 | Identity And Access Management 108 in use \| 109 |
| Monitoring 83 in use \| 88 | Application Security 84 in use \| 84 | Infrastructure Management 70 in use \| 71 |
| Network Security 60 in use \| 66 | Certificate And Key Management 52 in use \| 52 | Encryption 37 in use \| 44 |
| Compliance 3 in use \| 41 | Logging 40 in use \| 41 | Data Exfiltration 10 in use \| 33 |
| Secure Configuration 13 | Device Posture 11 in use \| 11 | Secure Collaboration - Level 1 6 |
| Secure Collaboration - Level 2 4 | Document Classification Solutions 4 | Backup And Recovery 4 in use \| 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

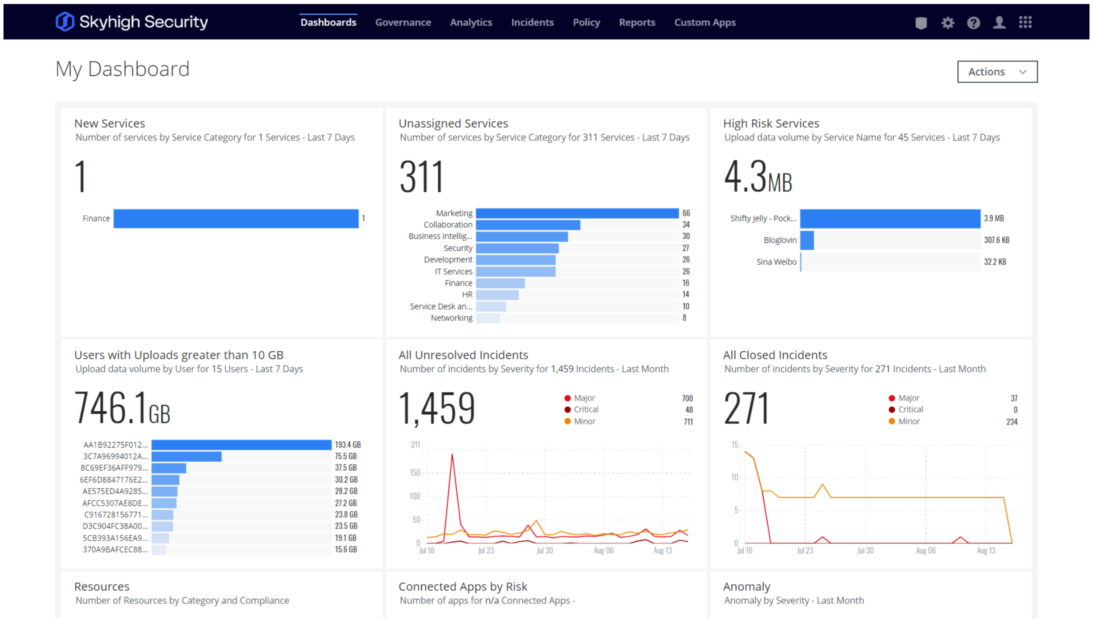
Understands access context including device operating system, device management status, location, and corporate/personal accounts.

### 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

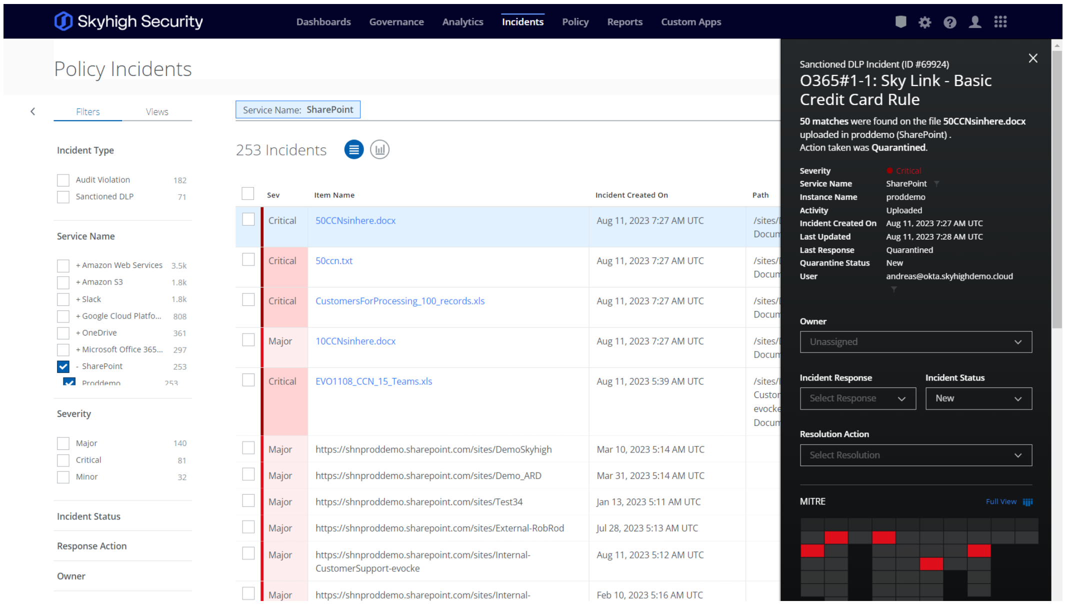
Enforces DLP policies for data uploaded to the cloud, created in the cloud, shared with collaborators, shared cloud-to-cloud from one service to another, and downloaded from the cloud.

### 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.



Policy Incidents

Service Name: SharePoint

Incident Type

| | |
|---|---|
| □ Audit Violation | 182 |
| □ Sanctioned DLP | 71 |

Service Name

| | |
|---|---|
| □ + Amazon Web Services | 3.5k |
| □ + Amazon S3 | 1.8k |
| □ + Slack | 1.8k |
| □ + Google Cloud Platfo... | 808 |
| □ + OneDrive | 361 |
| □ + Microsoft Office 365... | 297 |
| ☑ - SharePoint | 253 |
| ☑ Proddemo | 253 |

Severity

| | |
|---|---|
| □ Major | 140 |
| □ Critical | 81 |
| □ Minor | 32 |

Incident Status

Response Action

Owner

253 Incidents

| □ | Sev | Item Name | Incident Created On | Path |
|---|---|---|---|---|
| □ | Critical | 50CCNsinhere.docx | Aug 11, 2023 7:27 AM UTC | /sites/<br>Docum |
| □ | Critical | 50ccn.txt | Aug 11, 2023 7:27 AM UTC | /sites/<br>Docum |
| □ | Critical | CustomersForProcessing_100_records.xls | Aug 11, 2023 7:27 AM UTC | /sites/<br>Docum |
| □ | Major | 10CCNsinhere.docx | Aug 11, 2023 7:27 AM UTC | /sites/<br>Docum |
| □ | Critical | EVO1108_CCN_15_Teams.xls | Aug 11, 2023 5:39 AM UTC | /sites/<br>Custor<br>evocke<br>Docum |
| □ | Major | https://shnproddemo.sharepoint.com/sites/DemoSkyhigh | Mar 10, 2023 5:14 AM UTC | |
| □ | Major | https://shnproddemo.sharepoint.com/sites/Demo_ARD | Mar 31, 2023 5:14 AM UTC | |
| □ | Major | https://shnproddemo.sharepoint.com/sites/Test34 | Jan 13, 2023 5:11 AM UTC | |
| □ | Major | https://shnproddemo.sharepoint.com/sites/External-RobRod | Jul 28, 2023 5:13 AM UTC | |
| □ | Major | https://shnproddemo.sharepoint.com/sites/Internal-CustomerSupport-evocke | Aug 11, 2023 5:12 AM UTC | |
| □ | Major | https://shnproddemo.sharepoint.com/sites/Internal- | Feb 10, 2023 5:16 AM UTC | |

Sanctioned DLP Incident (ID #69924)

O365#1-1: Sky Link - Basic Credit Card Rule

**50 matches** were found on the file **50CCNsinhere.docx** uploaded in proddemo (SharePoint) .
Action taken was **Quarantined**.

| | |
|---|---|
| **Severity** | ● Critical |
| **Service Name** | SharePoint |
| **Instance Name** | proddemo |
| **Activity** | Uploaded |
| **Incident Created On** | Aug 11, 2023 7:27 AM UTC |
| **Last Updated** | Aug 11, 2023 7:28 AM UTC |
| **Last Response** | Quarantined |
| **Quarantine Status** | New |
| **User** | andreas@okta.skyhighdemo.cloud |

**Owner**: Unassigned

**Incident Response**: Select Response

**Incident Status**: New

**Resolution Action**: Select Resolution

MITRE

Full View

### 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

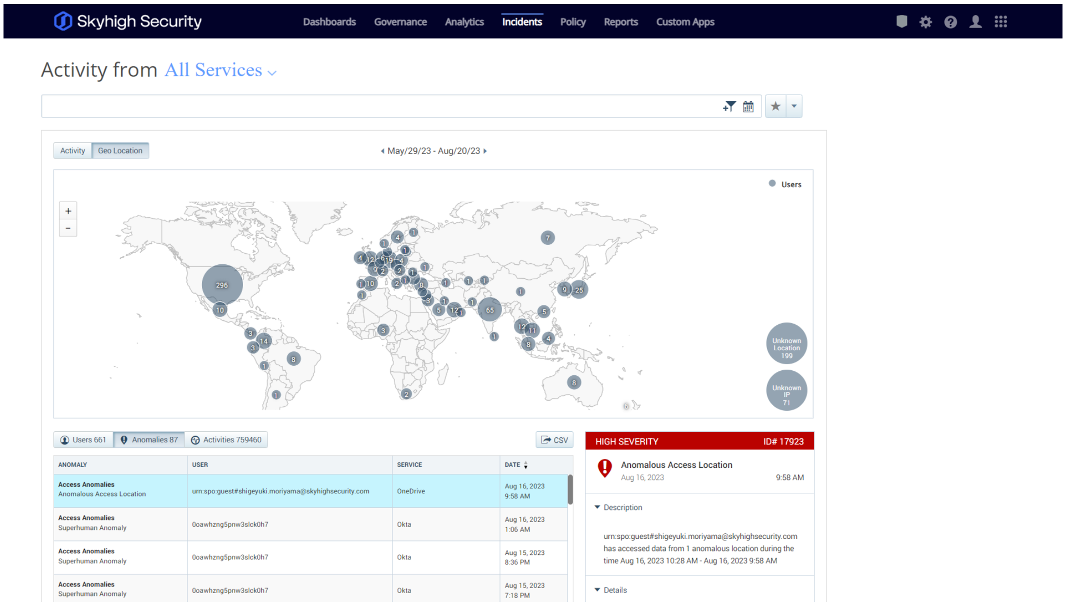
Enforces coarse allow/block access rules based on service level risk, device type, and granular activity-level controls to prevent upload and download of data.

### 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.



| ANOMALY | USER | SERVICE | DATE |
|---|---|---|---|
| **Access Anomalies**<br>Anomalous Access Location | urn:spo:guest#shigeyuki.moriyama@skyhighsecurity.com | OneDrive | Aug 16, 2023<br>9:58 AM |
| **Access Anomalies**<br>Superhuman Anomaly | 0oawhzng5pnw3slck0h7 | Okta | Aug 16, 2023<br>1:06 AM |
| **Access Anomalies**<br>Superhuman Anomaly | 0oawhzng5pnw3slck0h7 | Okta | Aug 15, 2023<br>8:36 PM |
| **Access Anomalies**<br>Superhuman Anomaly | 0oawhzng5pnw3slck0h7 | Okta | Aug 15, 2023<br>7:18 PM |

HIGH SEVERITY ID# 17923

Anomalous Access Location
Aug 16, 2023 9:58 AM

Description

urn:spo:guest#shigeyuki.moriyama@skyhighsecurity.com has accessed data from 1 anomalous location during the time Aug 16, 2023 10:28 AM - Aug 16, 2023 9:58 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.

### User and Entity Behavior Analytics (UEBA)

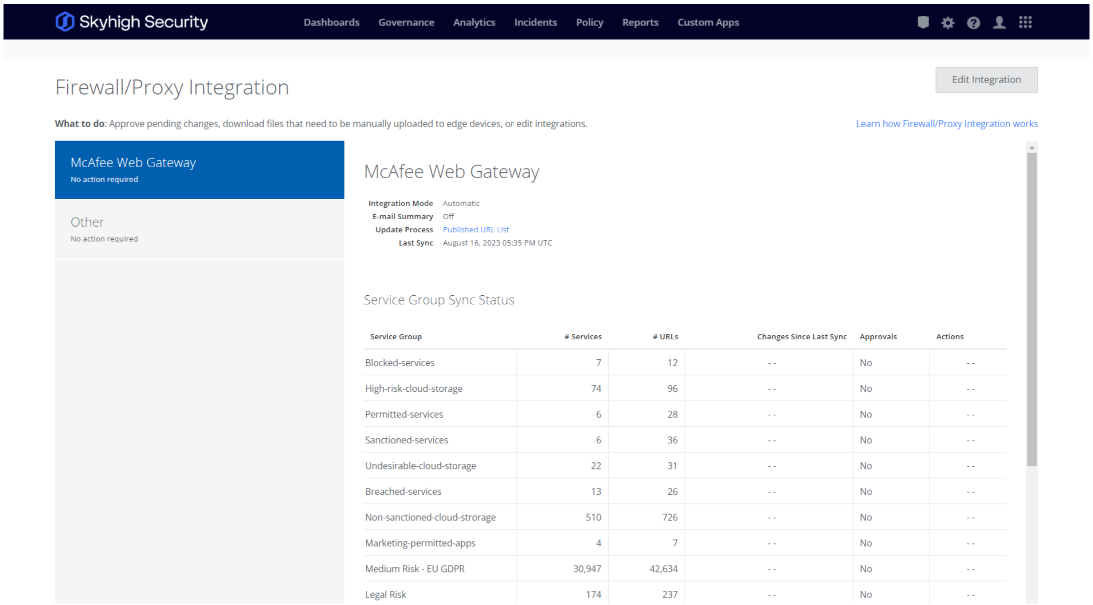
Automatically builds a self-learning model based on multiple heuristics and machine learning to identify patterns of activity indicative of user threats across multiple cloud services.

### 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.

### 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)



Firewall/Proxy Integration

**What to do**: Approve pending changes, download files that need to be manually uploaded to edge devices, or edit integrations.

McAfee Web Gateway
No action required

Other
No action required

McAfee Web Gateway

**Integration Mode** Automatic
**E-mail Summary** Off
**Update Process** Published URL List
**Last Sync** August 16, 2023 05:35 PM UTC

Service Group Sync Status

| Service Group | # Services | # URLs | Changes Since Last Sync | Approvals | Actions |
|---|---|---|---|---|---|
| Blocked-services | 7 | 12 | - - | No | - - |
| High-risk-cloud-storage | 74 | 96 | - - | No | - - |
| Permitted-services | 6 | 28 | - - | No | - - |
| Sanctioned-services | 6 | 36 | - - | No | - - |
| Undesirable-cloud-storage | 22 | 31 | - - | No | - - |
| Breached-services | 13 | 26 | - - | No | - - |
| Non-sanctioned-cloud-strorage | 510 | 726 | - - | No | - - |
| Marketing-permitted-apps | 4 | 7 | - - | No | - - |
| Medium Risk - EU GDPR | 30,947 | 42,634 | - - | No | - - |
| Legal Risk | 174 | 237 | - - | 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

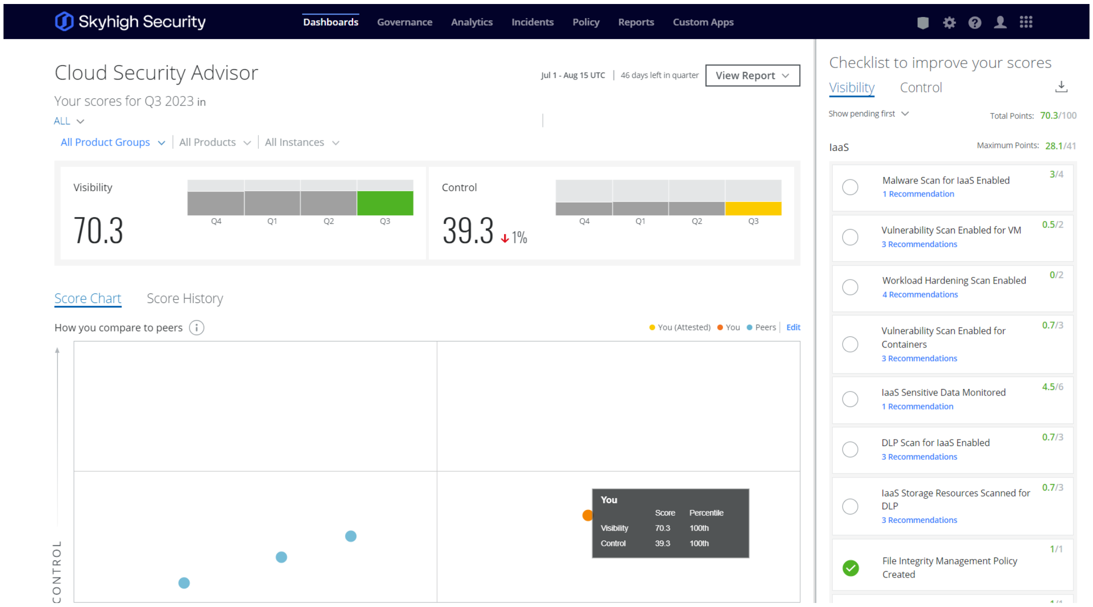
Leverages machine learning to detect activity signaling negligent and malicious behavior including insiders stealing sensitive data.

### 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.



Cloud Security Advisor

Jul 1 - Aug 15 UTC | 46 days left in quarter

Your scores for Q3 2023 in ALL

Visibility 70.3

Control 39.3 ↓1%

How you compare to peers

| You | Score | Percentile |
|---|---|---|
| Visibility | 70.3 | 100th |
| Control | 39.3 | 100th |

Checklist to improve your scores

Total Points: 70.3/100

IaaS — Maximum Points: 28.1/41

| | | |
|---|---|---|
| ○ | Malware Scan for IaaS Enabled<br>1 Recommendation | 3/4 |
| ○ | Vulnerability Scan Enabled for VM<br>3 Recommendations | 0.5/2 |
| ○ | Workload Hardening Scan Enabled<br>4 Recommendations | 0/2 |
| ○ | Vulnerability Scan Enabled for Containers<br>3 Recommendations | 0.7/3 |
| ○ | IaaS Sensitive Data Monitored<br>1 Recommendation | 4.5/6 |
| ○ | DLP Scan for IaaS Enabled<br>3 Recommendations | 0.7/3 |
| ○ | IaaS Storage Resources Scanned for DLP<br>3 Recommendations | 0.7/3 |
| ✓ | File Integrity Management Policy Created | 1/1 |

## 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**

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com