Skyhigh Security Cloud Access Security Broker (CASB) for Office 365

Helping organizations securely accelerate their business by providing total control over data and user activity in Office 365

Key Use Cases

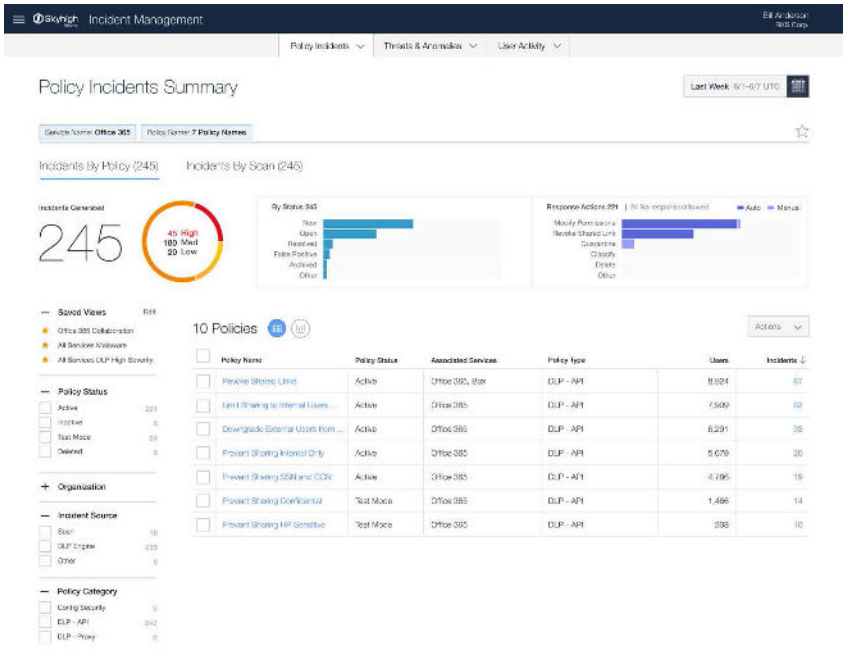
Enforce sensitive data policies across Office 365
Prevent sensitive data that cannot be stored in the cloud from being uploaded to or created in Office 365.

Build sharing and collaboration guardrails
Prevent sharing of sensitive or regulated data in Office 365 with unauthorized parties in real-time.

Limit download/sync to unmanaged devices
Gain total control over user access to Office 365 by enforcing context-specific policies limiting specific enduser actions.

Perform forensic investigations with full context
Capture a complete audit trail of all user activity enriched with threat intelligence to facilitate postincident forensic investigations.

Detect and correct user threats and malware
Detect threats from compromised accounts, insider threats, privileged access misuse, and malware infection.



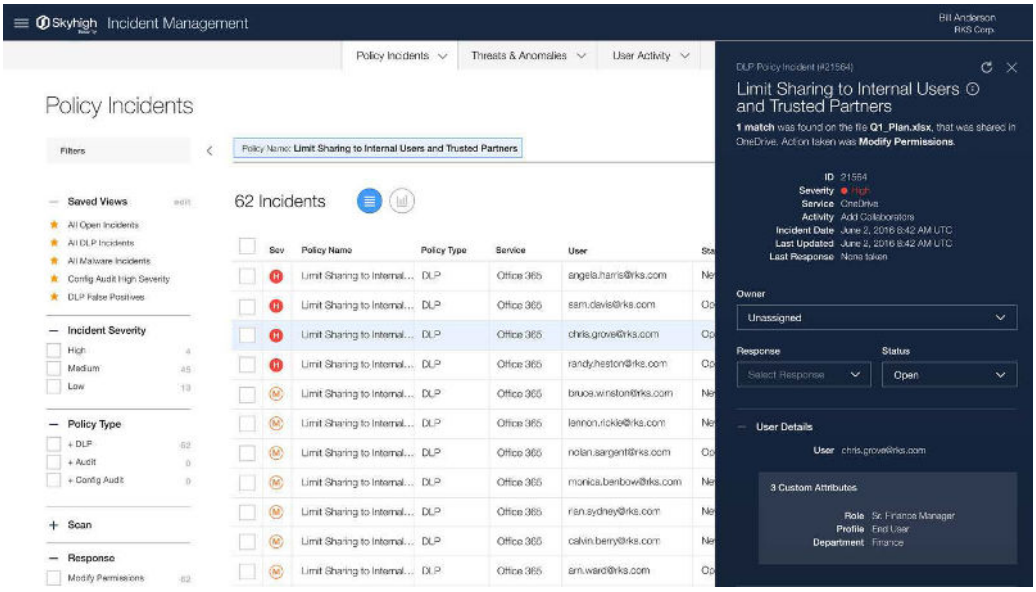
Data Loss Prevention (DLP)

Prevent regulated data from being stored in Office 365. Leverage Skyhigh Security's content analytics engine to discover sensitive data created in or uploaded to Office 365 based on:

- Keywords and phrases indicative of sensitive or regulated information
- Pre-defined alpha-numeric patterns with validtion (e.g. credit card numbers)
- Regular expressions to detect custom alpha-numeric patterns (e.g. part numbers)
- File metadata such as file name, size, and file type
- Fingerprints of unstructured files with exact and partial or derivative match
- Fingerprints of structured databases or other structured data files
- Keyword dictionaries of industry-specific terms (e.g. stock symbols)

DLP remediation options:

- Notify the end user
- Notify an administrator
- Quarantine the file
- Delete the file



Collaboration Control

Prevent sharing of sensitive data with unauthorized parties via OneDrive/SharePoint Online file and folder collaboration, as well as Exchange Online in real-time.

Enforce secure collaboration based on:

Files/folders

- Content
- Internal users/user groups
- Approved business partners
- Personal accounts (e.g. gmail.com)
- Links open to the internet
- Links accessible to internal users

Email

- Content
- Internal Users
- Approved business partners
- Personal accounts (e.g. gmail.com)

Common collaboration policies:

- Prevent file/folder permissions that are open to the internet or the entire company
- Revoke shared links that can be forwarded and accessed by anyone with the link
- Block file/folder sharing with personal email accounts
- Limit file/folder collaboration to internal users or whitelisted business partners
- Remove excessive owner/editor permissions of external users on corporate data
- Prevent sending sensitive data via email to external or unauthorized recipients

Remediate collaboration policy violations through:

- Revoking a shared link
- Downgrading permissions to view/edit
- Removing access permissions
- Blocking delivery of an email
- Notifying the end user in Office 365

Access Control

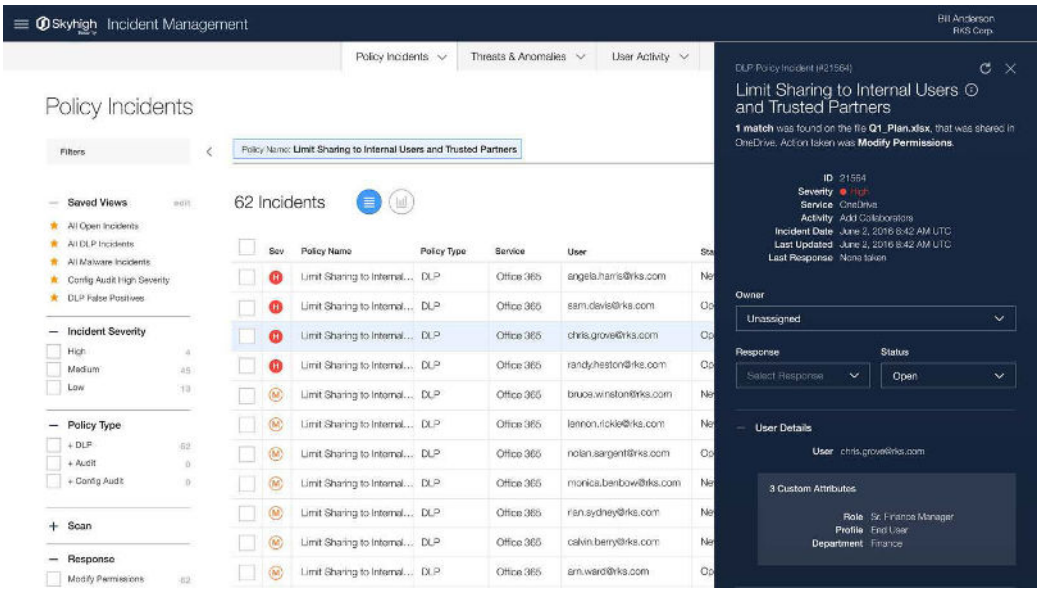
Protect corporate data from unauthorized access by enforcing granular, context-aware access policies such as preventing download of sensitive data from Office 365 to unmanaged devices.

Control access to Office 365 based on:

- Device type (e.g. managed, unmanaged)
- Activity type (e.g. download, upload)
- Specific user (e.g. David Carter)
- User attributes (e.g. role, department)
- IP address range (e.g. network, proxy)
- Geographic location (e.g. Ukraine)

Enforce granular access polices such as

- Allow/block access to Office 365
- Allow/block specific Office 365 user actions
- Force step-up authentication



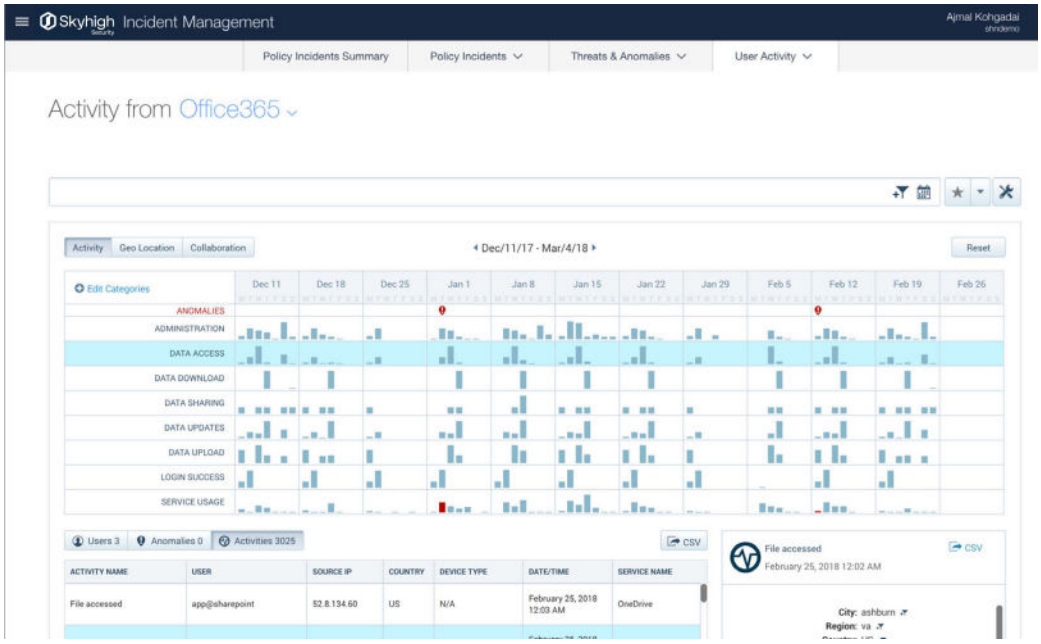
Activity Monitoring

Gain visibility into Office 365 usage and accelerate post-incident forensic investigations by capturing a comprehensive audit trail of all activity. Skyhigh Security captures hundreds of unique activity types and groups them into 14 categories for streamlined navigation. With our solution, organizations can monitor:

- Who is accessing Office 365, their role, device type, geographic location, and IP address
- How much data is being shared, accessed, created or updated, uploaded, downloaded, or deleted
- Successful/failed login attempts
- User account creation/deletion as well as updates to accounts by administrators

Drill down further into activity streams to investigate:

- A specific activity and all its associated users
- All activities generated by a single user
- All activities performed by users accessing via TOR or anonymizing proxy
- All activities generated by a specific source IP address or geographic location
- All access of and actions performed on a file containing sensitive data



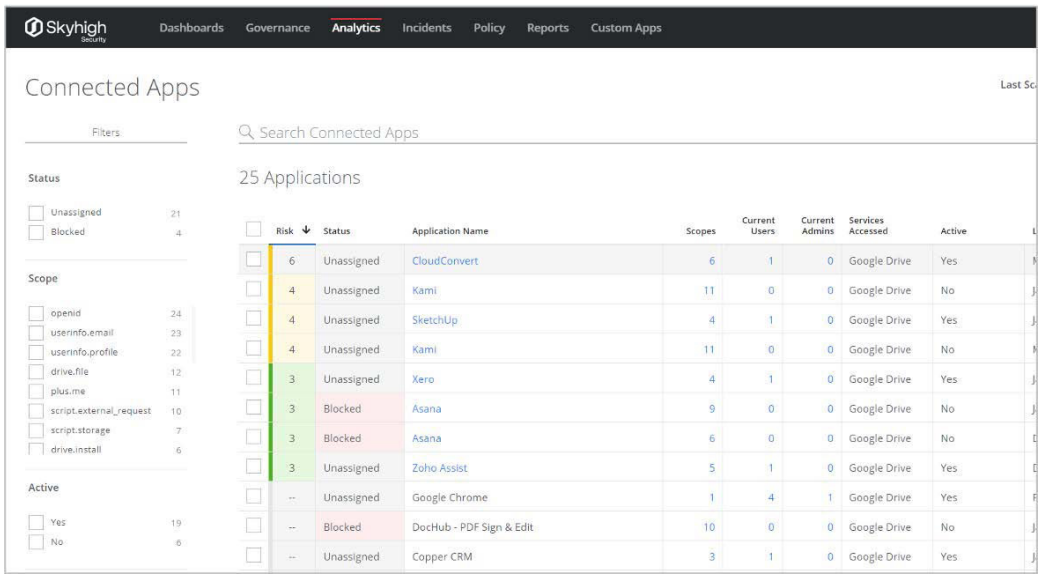
Connected Apps

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.

Connected Apps Protectopm Capabilities

- Visibility into 'shadow' apps connected via Oauth
- Risk score associated with the connected app
- Risk score sourced from the most comprehensive Cloud Registry with approximately 30K cloud services
- Usage analytics, such as user count and scopes
- Define policies to restrict access to apps that may be discovered in the future
- Policy parameters can be based on app name, scopes, and status
- Remediate actions include creation of incidents, notify users, and block apps
- Get a log of all events associated with a single app
- Activity data is enriched, allowing for categorization, searching, and filtering
- Seamless onboarding

- Visibility: Get visibility into user authorized connected apps
- Control: Apply implicit controls to Allow/Block/Restrict
- Policies: Define policies to secure from risky apps authorized in the future



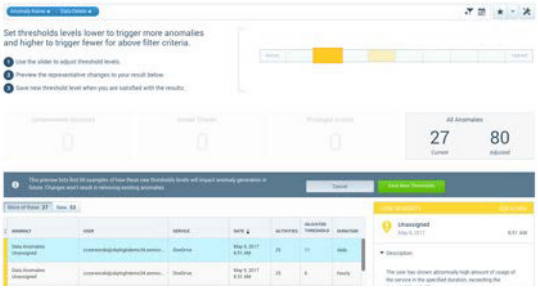
User Behavior Analytics and Malware Detection

Skyhigh Security uses data science and machine learning to automatically build models of typical user behavior and identifies behavior that may be indicative of a threat.

- **Insider Threats:** Detect anomalous behavior across multiple dimensions including the amount of data uploaded/downloaded, volume of user action, access count, and frequency across time and cloud services.
- **Compromised Accounts:** Analyze access attempts to identify impossible cross-region access, bruteforce attacks, and suspicious locations indicative of a compromised account.
- **Privleged user threats:** Identify inappropriate user permissions, dormant accounts, and unwarranted escalation of user privileges and provisioning.
- **Malware:** Block known malware signatures, sandbox suspicious files, and identify behavior indicative of malware data exfiltration or ransomware activity.

Supervised Machine Learning

Skyhigh Security incorporates security analyst input into machine learning models to improve accuracy. As analysts mark false positives and adjust detection sensitivity, tunes detection models.



Network Effects

With the largest installed base of any cloud security solution, Skyhigh Security leverages network effects other vendors cannot replicate. With more users, behavior models are able to more accurately detect threats.



Unified Policy Engine

Skyhigh Security leverages a central policy engine to apply consistent policies to all cloud services. There are three ways to define policies that can be enforced on new and pre-existing content, user activity, and malware threats.

Policy template

Operationalize Office 365 policy enforcement with prebuilt templates based on industry, security use case, and benchmark.

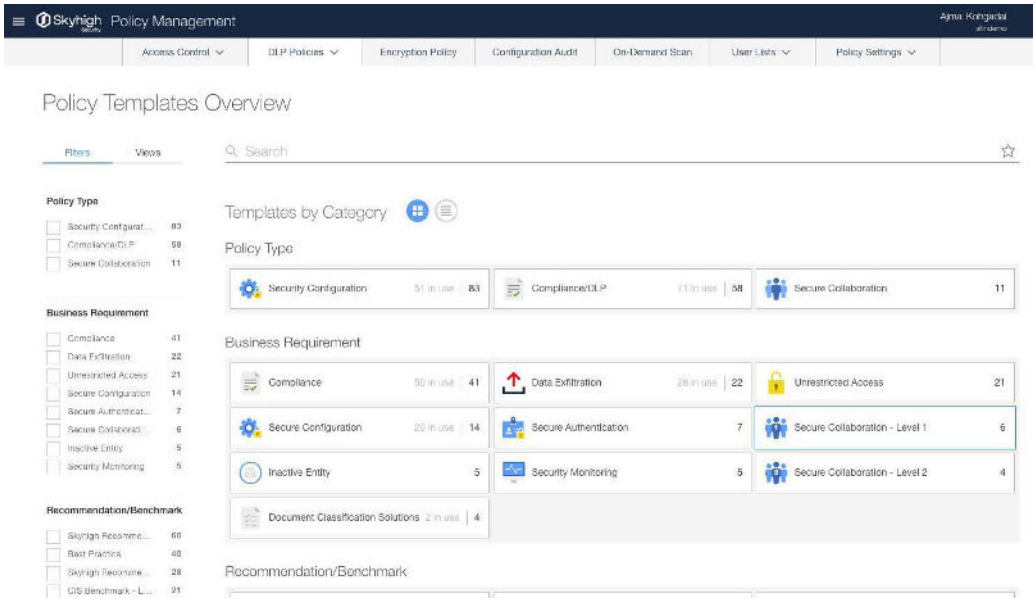
Policy Import

Import policies from existing security solutions or policies from other Skyhigh Security customers or partners.

Policy creation wizard

Create a custom policy with Boolean logic to conform to any corporate or regulatory requirement.

- Combine DLP, collaboration, and access rules to enforce granular policies
- Flexible policy framework leverages triggers and response actions
- Build policies using Boolean logic and nested rules and rule groups
- Enforce multi-tier remediation based on the severity of the incident
- Selectively target or exclude specific users and define exception rules



Incident Response Management

Skyhigh Security's incident response management console offers a unified interface to triage and resolve incidents. With Skyhigh Security, organizations can:

- Identify a single policy and all users violating it
- Analyze all policy violations by a single user
- Review the exact content that triggered a violation
- Take manual action, such as quarantining a file
- Rollback an automatic remediation action to restore a file and its permissions

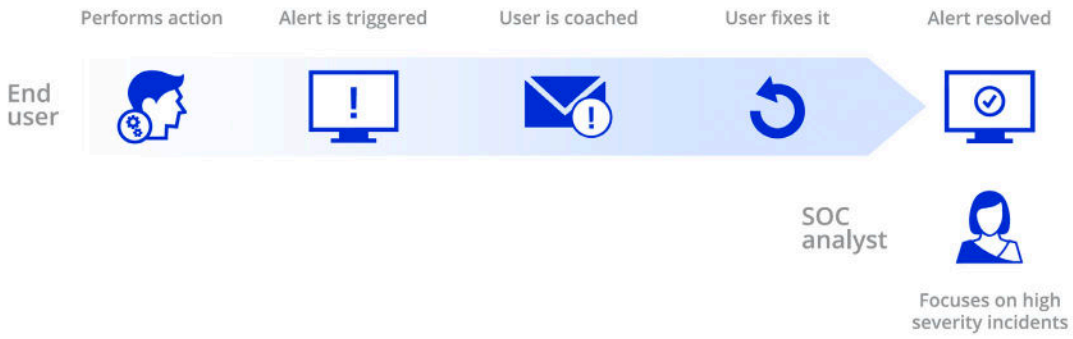
Our solution streamlines incident response through autonomous remediation that:

- Provides end-user coaching and in-app notifications of attempted policy violations
- Enables end users to self-correct the policy violation and resolve the incident alert
- Dramatically reduces manual incident review by security analysts by 97%

Integration

Skyhigh Security integrates with your existing security solutions including the leading vendors in:

- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Access management (AM)
- Information rights management (IRM)
- Enterprise mobility management (EMM/MDM)



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

Skyhigh Security

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