McAfee Skyhigh Security Cloud

Data Security for the Cloud Era

McAfee® Skyhigh Security Cloud protects data where it lives today, with a solution that was built natively in the cloud, for the cloud. It's cloud-native data security.

Detect

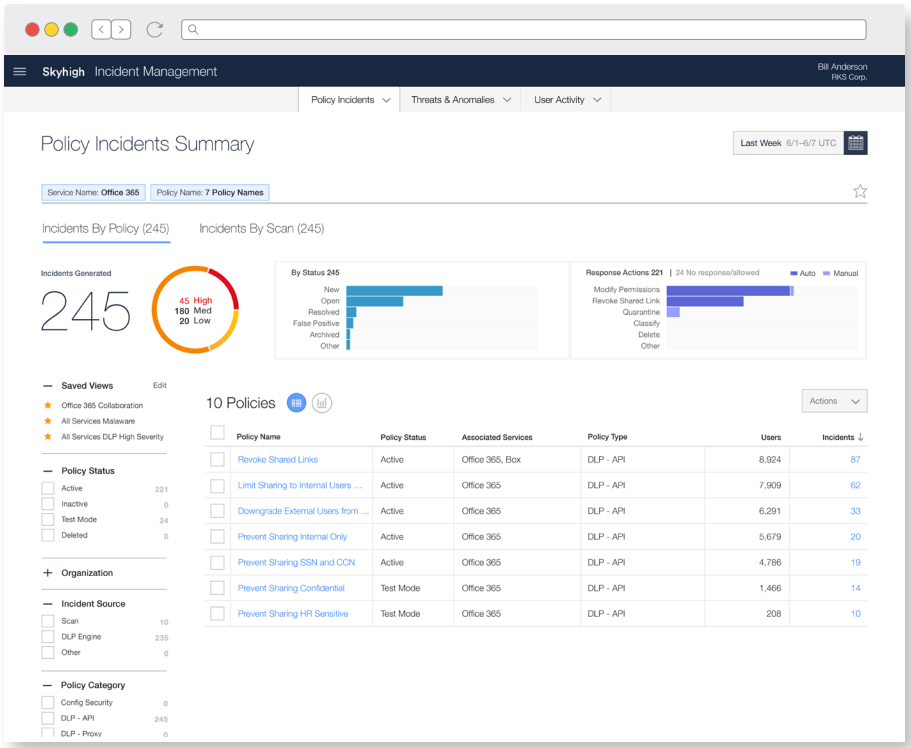
Gain complete visibility into data, context, and user behavior across all cloud services, users, and devices.

Protect

Take real-time action to enforce policies across cloud services and apply persistent data protection.

Correct

Remediate security threats by eliminating security misconfigurations and correcting high-risk user activities.



Key Use Cases

Enforce data loss prevention (DLP) policies across data in the cloud

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

Encrypt cloud data with keys that only you can access

Audit and tighten the security settings of cloud services

Connect With Us

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.

Policy Creation Wizard

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

Pre-Built Policy Templates

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

Cloud Registry

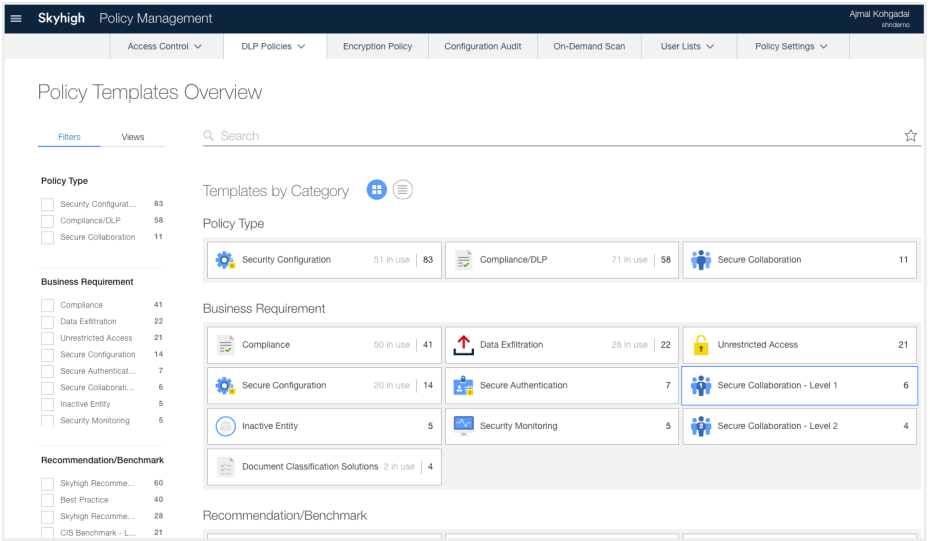
Provides the world's largest and most accurate registry of cloud services with a 1-10 CloudTrust Rating based on a 261-point risk assessment.

Privacy Guard

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

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.



User Behavior Analytics

Automatically builds a self-learning model based on multiple heuristics and identifies patterns of activity indicative of user threats.

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.

Detect

Content Analytics

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

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.

Security Configuration Audit

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

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.

Account Compromise Detection

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

Cloud Activity Monitoring

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

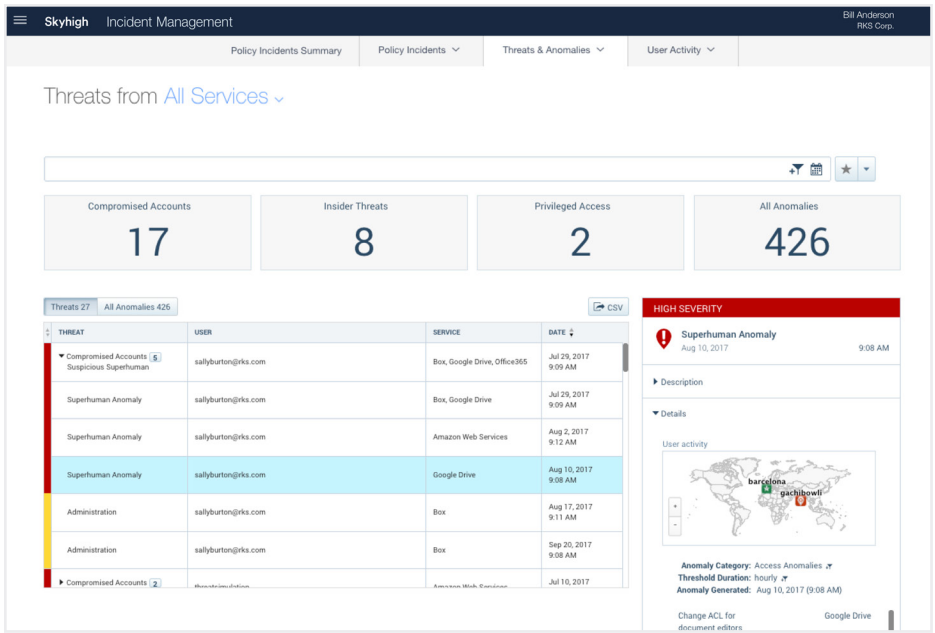
Insider Threat Detection

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.

> "We use McAfee to layer security controls like data loss prevention and access control so that the easy path to collaboration is also the secure path."
>
> —Tim Tompkins, Senior Director of Security Innovation, Aetna



Protect

Multi-Tier Response

Defines policies with multiple levels of severity and enforce distinct response actions based on the severity level of the incident.

Quarantine

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

Collaboration Control

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

Removal

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

Contextual Access Control

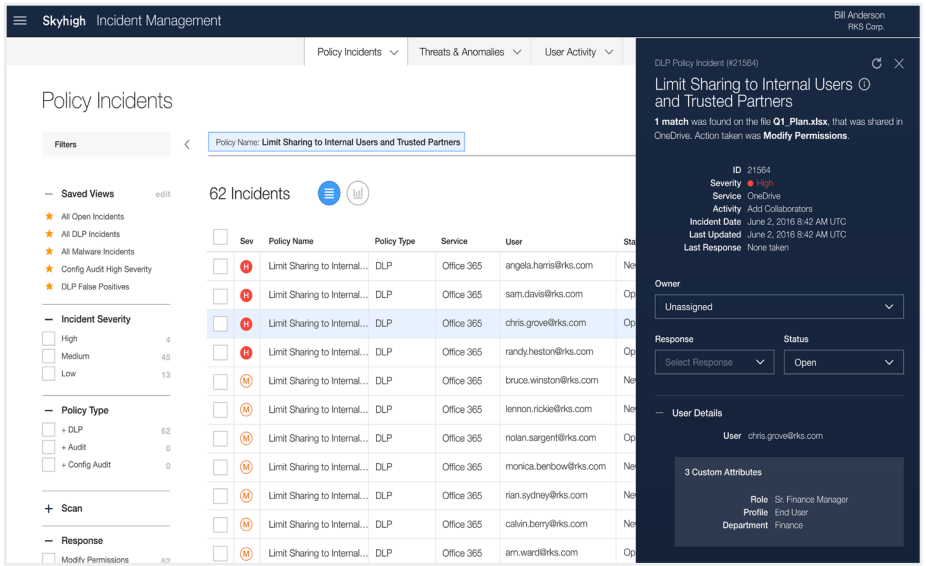
Enforces coarse allow/block access based on service-level risk and granular activity-level controls to prevent upload and download of data.

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.



Encryption

Protects sensitive data with peer-reviewed, function-preserving encryption schemes using enterprise-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.

Policy Incident Management

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

Correct

Adaptive Authentication

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

Closed-Loop Policy Enforcement

Integrates with existing firewall or web gateway to govern risky cloud service usage and activities.

Malware Detection

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

Malware Extermination

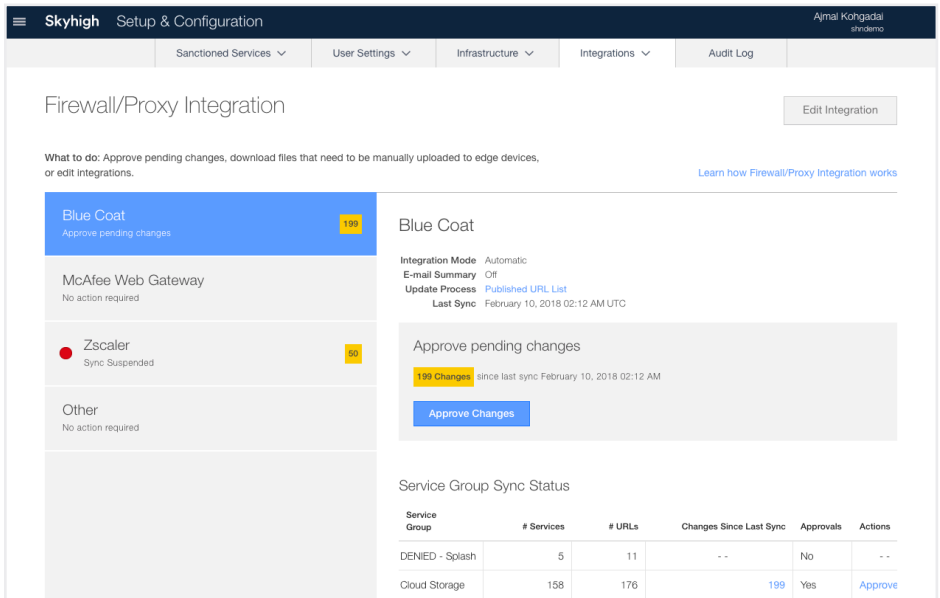
Terminates advanced threats by permanently neutralizing and removing malware.

"McAfee's Cloud-Native Data Security technology is helping Caesars Entertainment protect our valuable company data as we move from legacy applications to cloud applications."

—Les Ottolenghi, Executive Vice President and CIO, Caesars Entertainment

Integration

- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Secure web gateway (SWG)
- Next generation firewall (NGFW)
- Key management service (KMS)
- Access management (IDaaS)
- Information rights management (IRM)
- Enterprise mobility management (EMM/MDM)
- Directory services (LDAP)



McAfee Sky Gateway

Enforces policies inline for data in motion in real time.

Email mode

Leverages the native mail flow to enforce policies across all messages sent by Exchange Online inline or in passive monitoring mode.

Universal mode

Sits inline between the user and cloud service and steers traffic after authentication to cover all users and all devices, without agents.

McAfee Sky Link

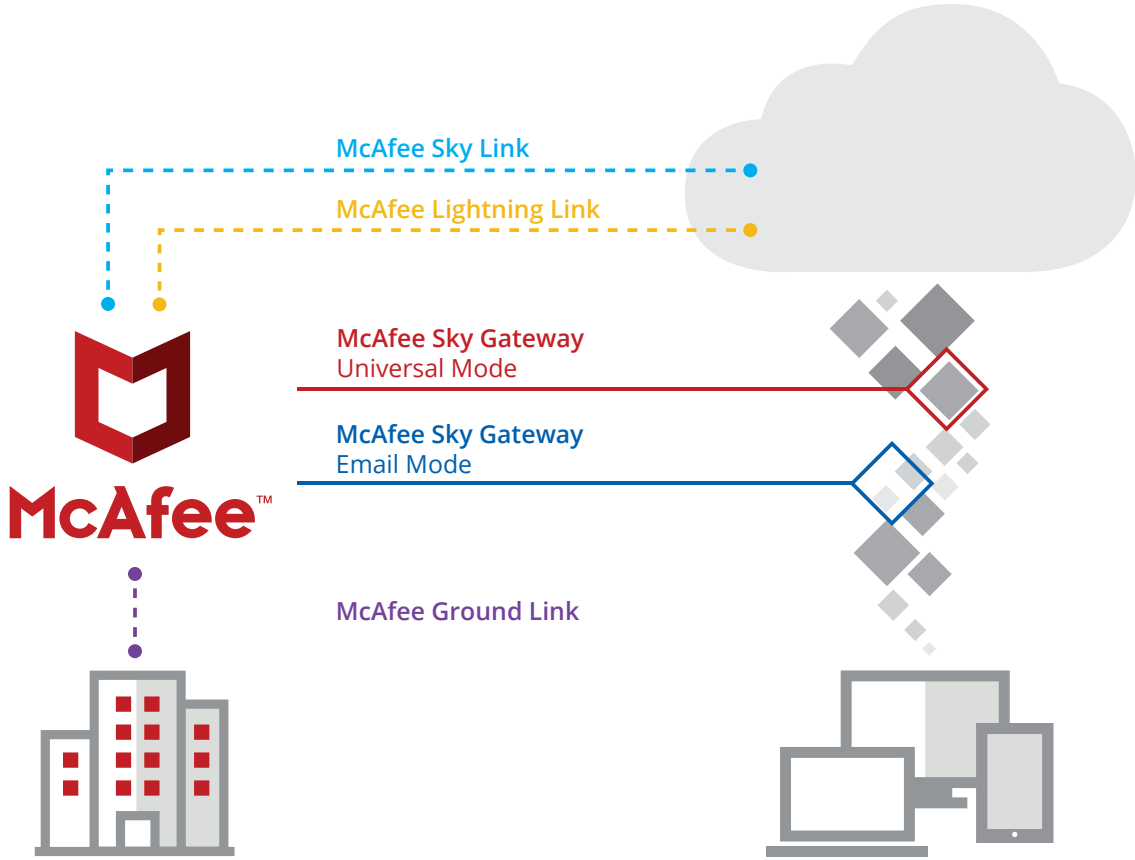
Connects to cloud service APIs to gain visibility into data and user activity, and enforce policies across data uploaded or shared in near real time and data at rest.

McAfee Lightning Link

Establishes a direct out-of-band connection to cloud services to enforce policies in real-time with comprehensive data, user, and device coverage.

McAfee Ground Link

Brokers the connection between McAfee and on-premises LDAP directory services, DLP solutions, proxies, firewalls, and key management services.



Visit us at **www.mcafee.com**.

McAfee
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com