McAfee
Together is power.

McAfee MVISION Cloud for Azure

McAfee® MVISION Cloud for Azure is a comprehensive monitoring, auditing, and remediation solution for your Azure environment

Key Use Cases

Security configuration and compliance audit

Audit the configuration of Azure services to identify settings that are insecure or non-compliant and recommend corrective measures.

Activity monitoring

Capture a complete audit trail of all user activity enriched with threat intelligence to facilitate post-incident forensic investigations.

Threat protection

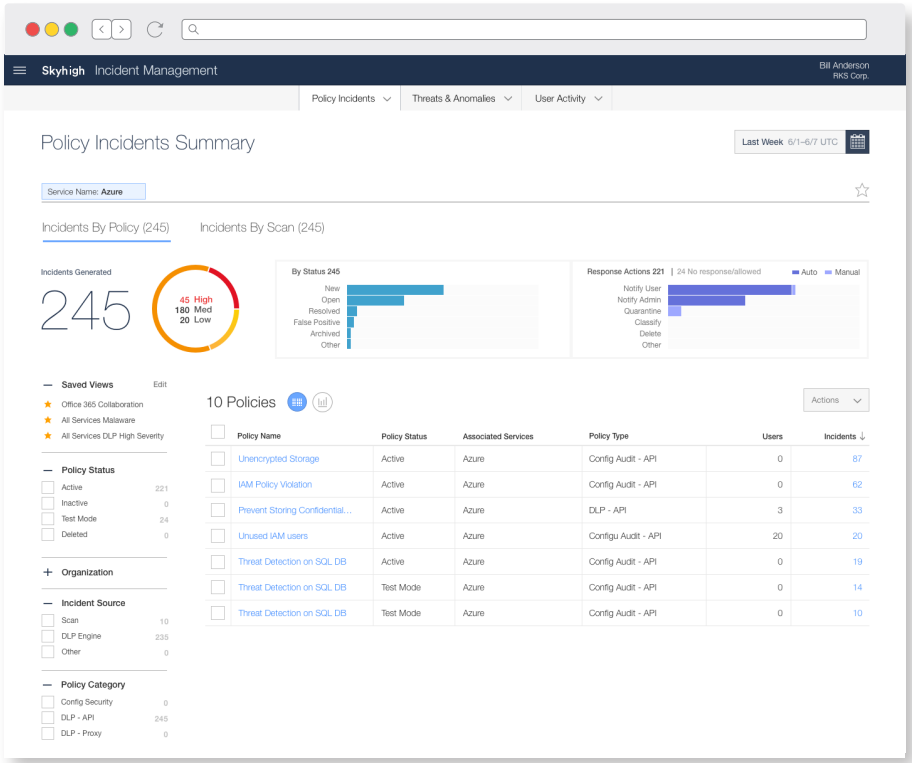
Detect threats from compromised accounts, insider threats, privileged access misuse, and malware infection.

Data loss prevention (DLP)

Enforce DLP policies for sensitive data stored in Azure Storage Containers and Blob Storage.

Unsanctioned Azure accounts discovery

Identify managed and unmanaged Azure subscriptions and enforce a uniform set of security policies across all Azure subscriptions.



Connect With Us

Security Configuration and Compliance Audit

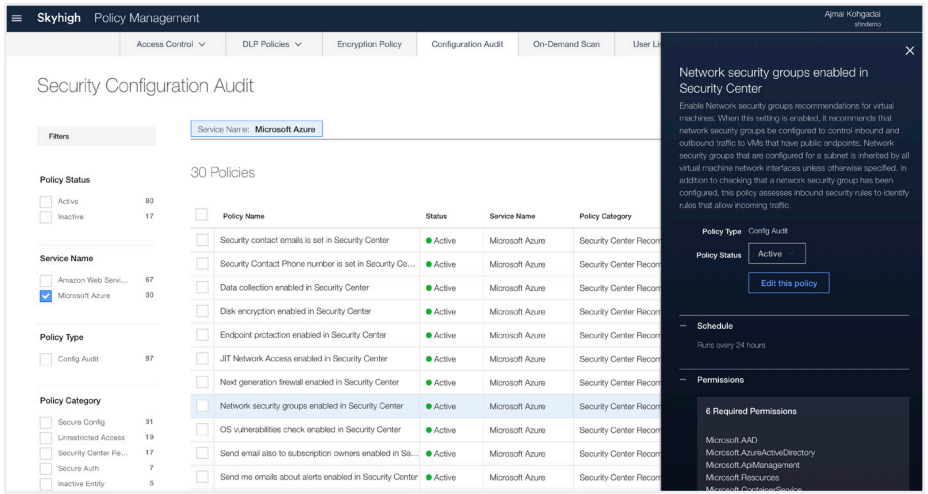
Audit and monitor the security configurations of all your Azure subscriptions to detect and correct misconfigurations to reduce risk and comply with internal and external policies.

Detect misconfigurations for:

- Virtual Machines (VMs)
- Storage services including Blobs, Files, Queue, and Table storage
- Identity and access management (IAM)
- SQL services
- Logging and monitoring services
- Network security groups

Correct misconfigured services using:

- McAfee recommended best practices derived from existing customers
- Center for Internet Security (CIS) benchmark recommendations for Azure
- Compliance recommendations for regulations such as HIPAA-HITECH, ISO, FedRAMP, ITAR, or internal compliance policies



"McAfee's expansion of its security controls beyond SaaS is a key way IT can empower the business to fully leverage custom applications running in public IaaS, as well as having the confidence in protecting the IaaS platforms themselves."

—David Smoley, Chief Information Officer, AstraZeneca

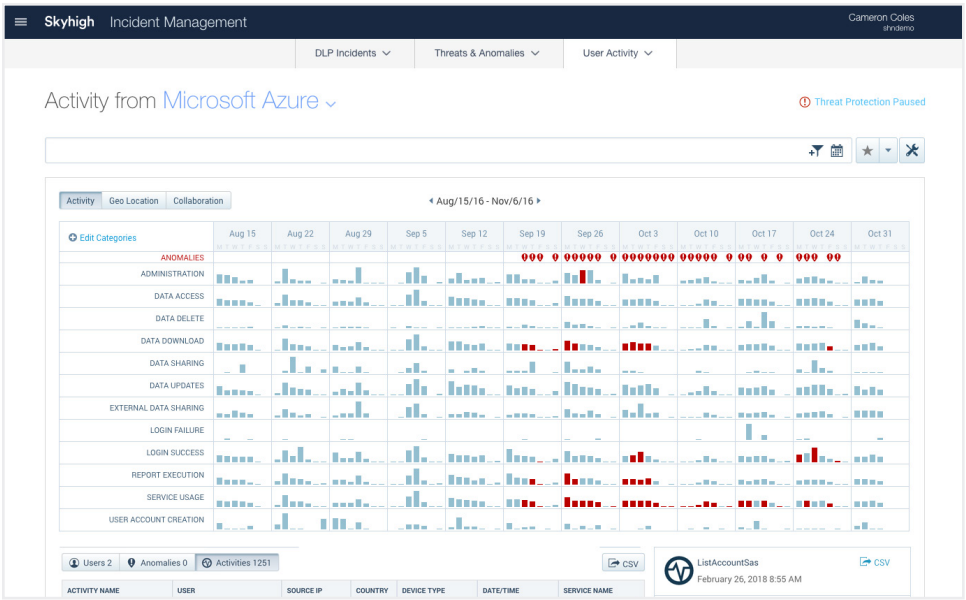
Activity Monitoring

Gain visibility into usage across managed and unmanaged Azure subscriptions and accelerate post-incident forensic investigations by capturing a comprehensive audit trail of all activity. McAfee captures hundreds of unique activity types and groups them into distinct categories for streamlined navigation. With McAfee, organizations can monitor:

- Usage of managed and unmanaged Azure subscriptions, who is accessing which services, the types of activities performed, their role, device type, geographic location, and IP address
- Inactive user accounts or former employees who retain access to Azure so their accounts can be deleted to reduce latent risk
- 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



"We now have the visibility and control we need to be able to allow access to the cloud-based tools our employees need to be competitive and efficient, without compromising our security standards."

—Rick Hopfer, Chief Information Officer, Molina Healthcare

User Behavior Analytics and Malware Detection

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

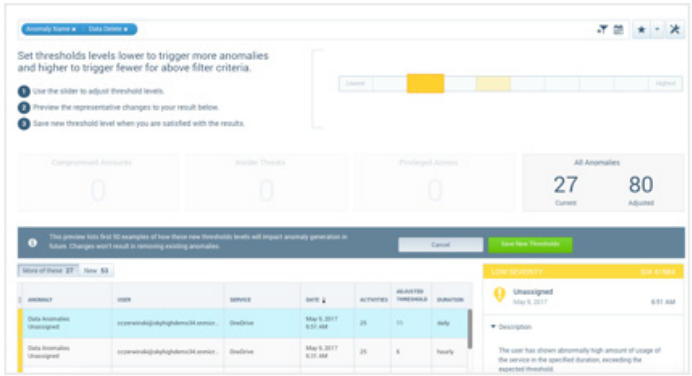
- **Insider threats:** Detect anomalous behavior across multiple dimensions including the amount of data uploaded/downloaded, volume of user action, access count, and frequency across time and cloud services.
- **Compromised accounts:** Analyze access attempts to identify impossible cross-region access, brute-force attacks, and suspicious locations indicative of a compromised account.
- **Privileged 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.

"In an environment with millions of unique events each day, McAfee does a nice job of cutting through the noise and directing us to the areas of greatest security concern."

—Ralph Loura, Chief Information Officer, HP

Supervised Machine Learning

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



Network Effects

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

Data Loss Prevention (DLP)

Prevent unauthorized regulated data from being stored in Azure storage services. Leverage McAfee's content analytics engine to discover sensitive data stored in Azure services based on:

- Keywords and phrases indicative of sensitive or regulated information
- Pre-defined alpha-numeric patterns with validation (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

"McAfee allows us to extend DLP outside the perimeter and into the cloud and the user experience is seamless."

—Mike Benson, Chief Information Officer, DirecTV

Unified Policy Engine

McAfee 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 templates

Operationalize Azure policy enforcement with pre-built templates based on industry, security use case, and benchmark.

Policy import

Import policies from existing security solutions or policies from other McAfee customers or partners.

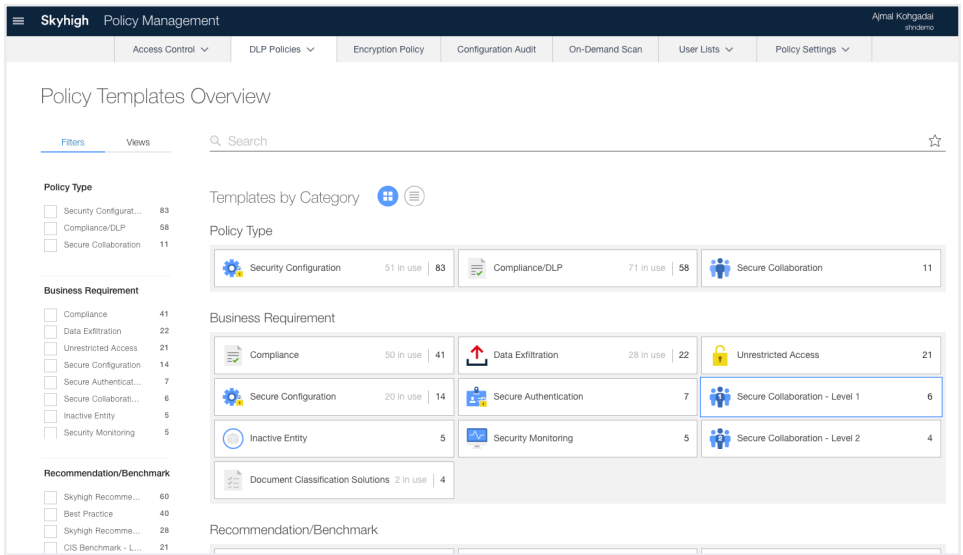
Policy creation wizard

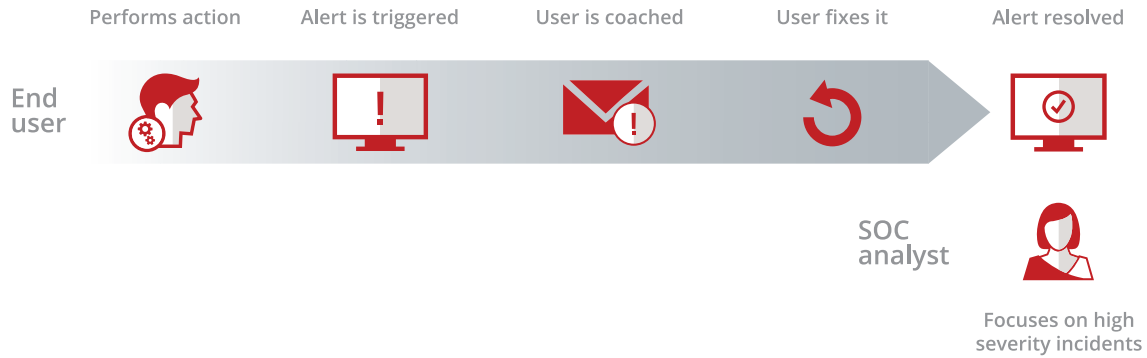
Create a custom policy with Boolean logic to conform to any corporate or regulatory requirement.

- 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

"With McAfee we were able to implement cloud security policies without impacting business user productivity."

—Brian Lillie, Chief Information Officer, Equinix





Incident Response Management

McAfee's incident response management console offers a unified interface to triage and resolve incidents. With McAfee, 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

McAfee 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%

Integrations

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

- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Secure web gateway (SWG)
- Next-generation firewall (NGFW)
- Access management (AM)
- Information rights management (IRM)
- Enterprise mobility management (EMM/MDM)

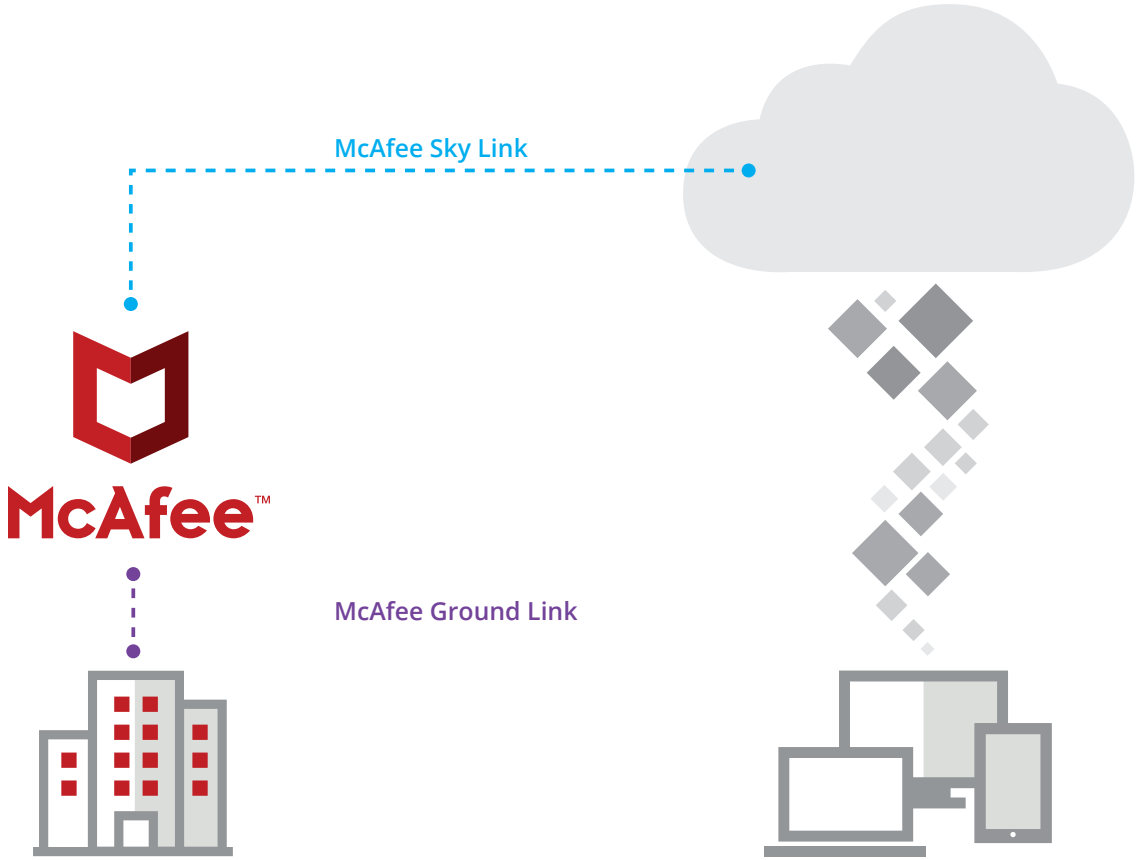
McAfee Sky Link

Connects to Azure 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 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