McAfee MVISION Cloud for Box

McAfee® MVISION Cloud for Box helps organizations securely accelerate their business by providing total control over data and user activity in Box

Key Use Cases

Enforce sensitive data policies in Box

Prevent sensitive data that cannot be stored in the cloud from being uploaded to or created in Box.

Build sharing and collaboration guardrails

Prevent sharing of sensitive or regulated data in Box with unauthorized parties in real-time.

Limit download/sync to unmanaged devices

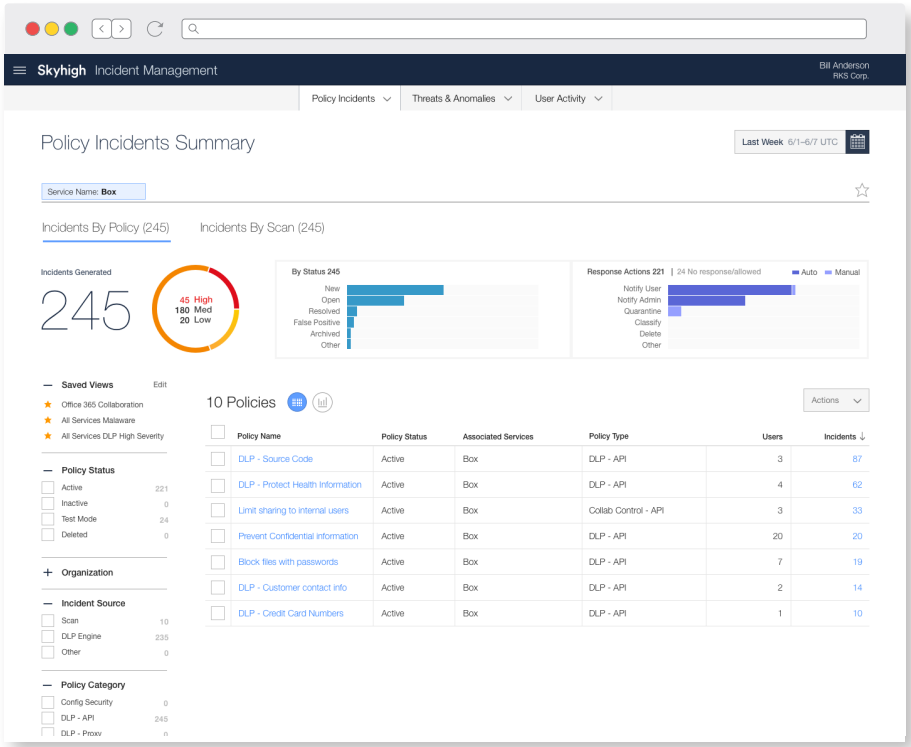
Gain total control over user access to Box by enforcing context-specific policies limiting end-user actions.

Perform forensic investigations with full context

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

Detect and correct user threats and malware

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



Connect With Us

Data Loss Prevention (DLP)

Prevent regulated data from being stored in Box. Leverage McAfee's content analytics engine to discover sensitive data created in or uploaded to Box based on:

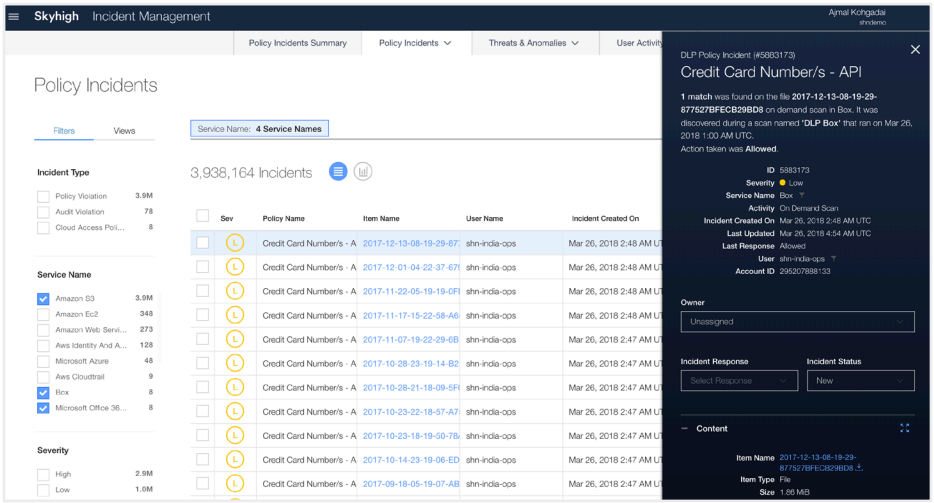
- Keywords and phrases indicative of sensitive or regulated information
- Pre-defined alpha-numeric patterns with validation (e.g. credit card numbers)
- Regular expressions to detect custom alpha-numeric patterns (e.g. part numbers)
- File metadata such as file name, size, and file type
- Fingerprints 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)

"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

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 Box file and folder collaboration.

McAfee can 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

"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

Common collaboration policies McAfee can enforce:

- 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

Remediate collaboration policy violations through:

- Revoking a shared link
- Downgrading permissions to view/edit
- Removing access permissions
- Notifying the end user in Box

Access Control

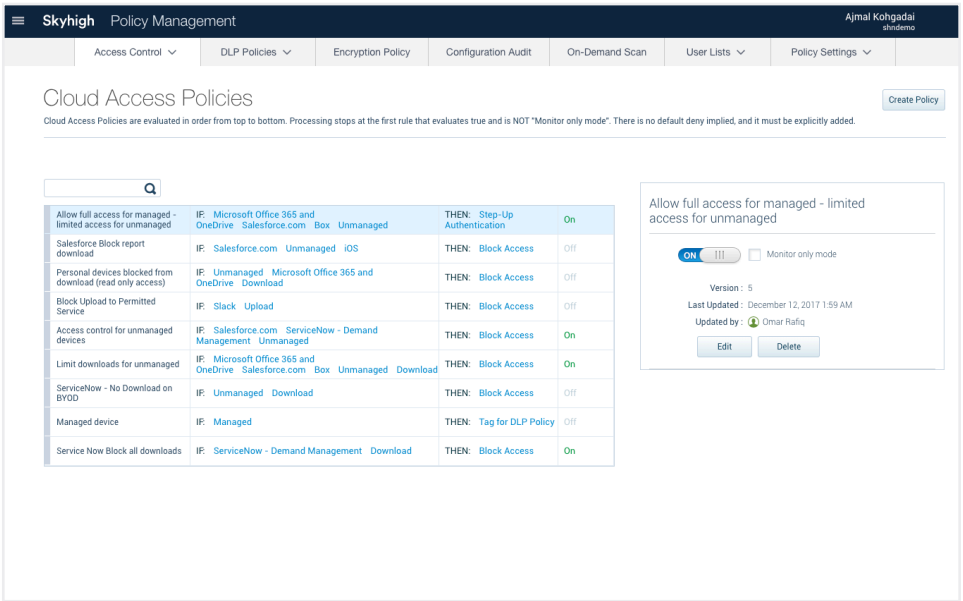
Protect corporate data from unauthorized access by enforcing granular, context-aware access policies such as preventing download from Box to unmanaged devices.

Control access to Box 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 policies such as:

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



> "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

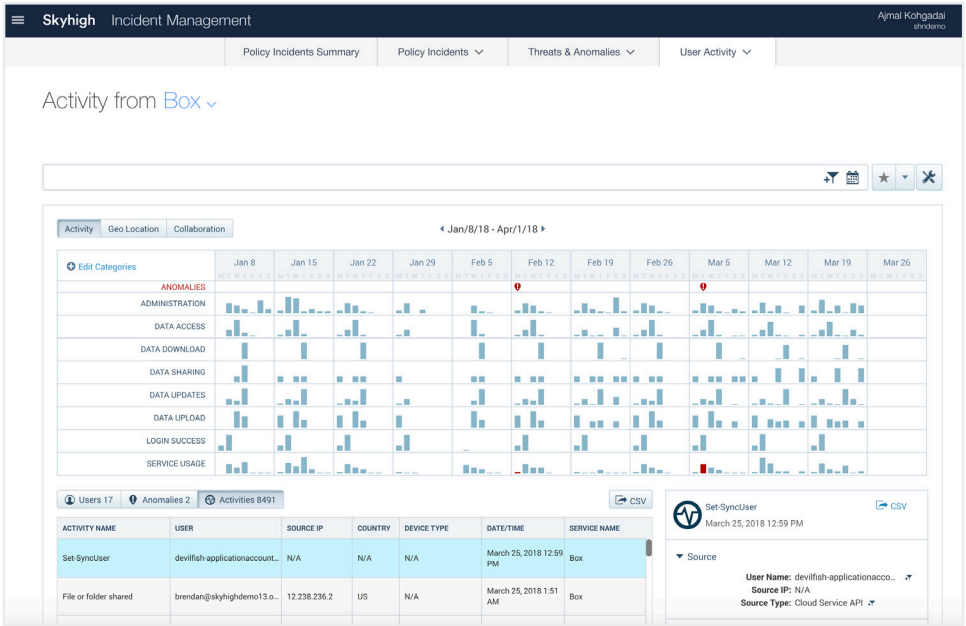
Activity Monitoring

Gain visibility into Box usage 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 14 categories for streamlined navigation. With McAfee, organizations can monitor:

- Who is accessing Box, 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



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.

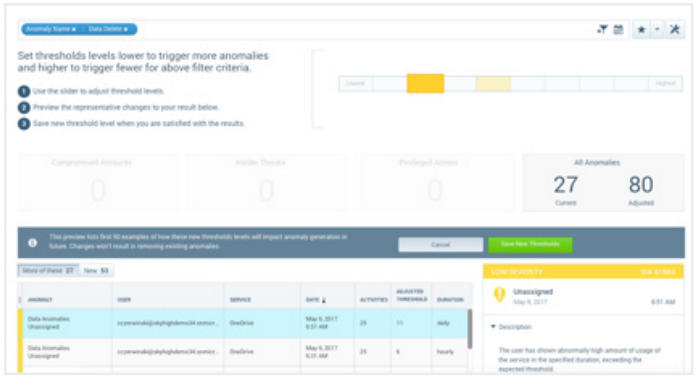
- **Insider threats:** Detect anomalous behavior across multiple dimensions including the amount of data uploaded/downloaded, volume of user action, access count, and frequency across time and cloud services.
- **Compromised accounts:** Analyze access attempts to identify impossible cross-region access,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

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

Rapidly operationalize Box 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.

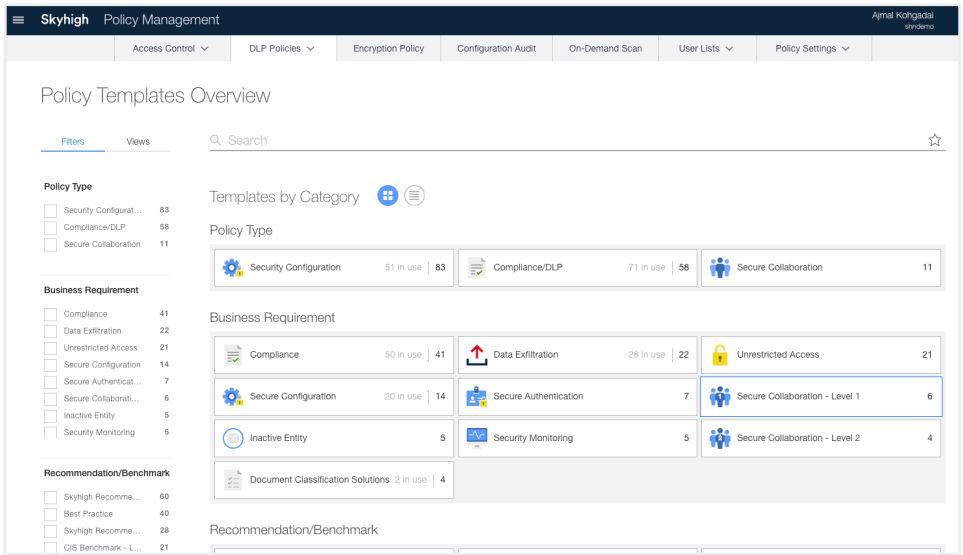
Policy creation wizard

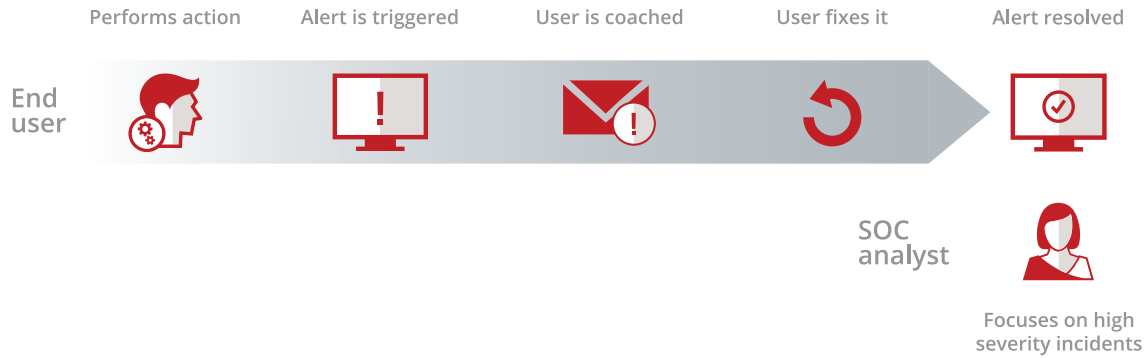
Create a custom policy with Boolean logic to conform to any corporate or regulatory requirement.

- 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
- 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:

- 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 Gateway

Enforces policies inline for data in motion in real-time.

Universal mode

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

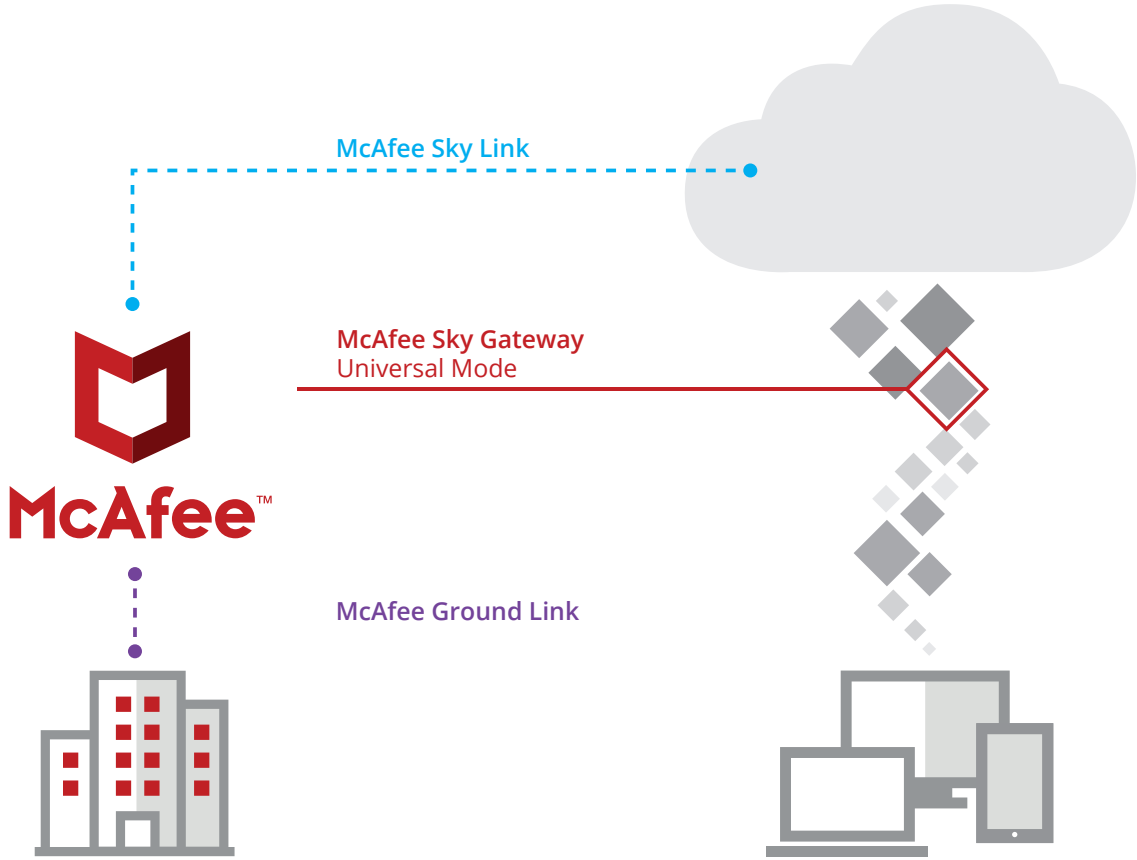
McAfee Sky Link

Connects to Box 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