

# 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

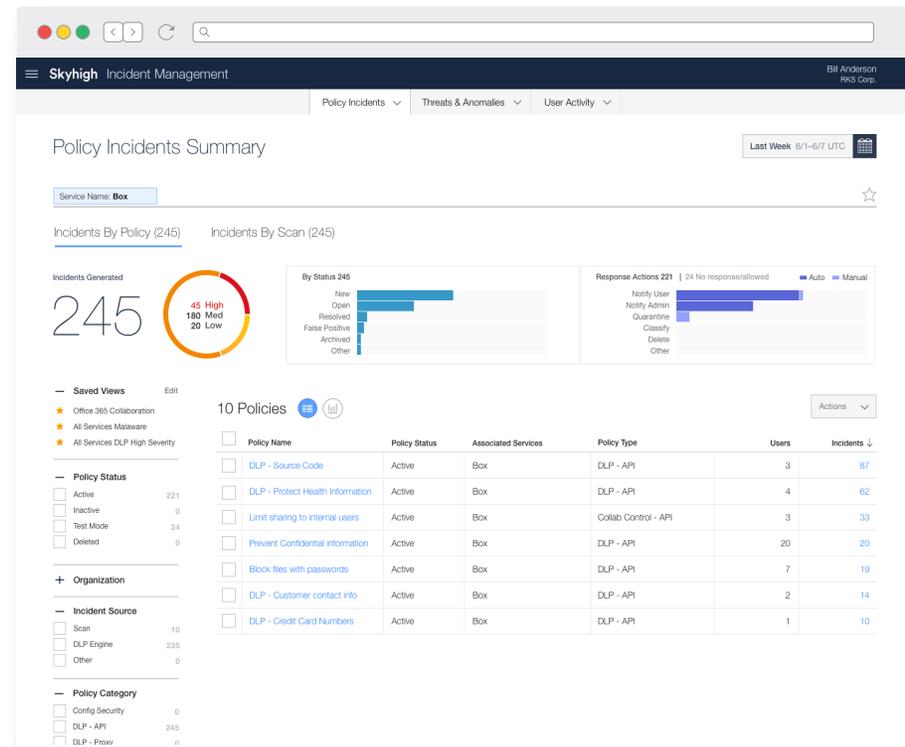
Gain total control over user access to Box by enforcing context-specific policies limiting end-user actions.

### 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 SHEET

### 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)

### DLP remediation options:

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

The screenshot displays the Skyhigh Incident Management dashboard. The main view shows a table of Policy Incidents with columns for Severity, Policy Name, Item Name, User Name, and Incident Created On. A sidebar on the left allows filtering by Incident Type, Service Name, and Severity. A detailed view of a specific incident is shown on the right, including the incident ID, severity, service name, activity, and incident response options.

Sev	Policy Name	Item Name	User Name	Incident Created On
Low	Credit Card Number/s - A	2017-12-13-08-19-23-87	shn-india-ops	Mar 26, 2018 2:48 AM UTC
Low	Credit Card Number/s - A	2017-12-01-04-22-37-671	shn-india-ops	Mar 26, 2018 2:48 AM UTC
Low	Credit Card Number/s - A	2017-11-22-05-19-19-0F1	shn-india-ops	Mar 26, 2018 2:48 AM UTC
Low	Credit Card Number/s - A	2017-11-17-15-22-58-A6	shn-india-ops	Mar 26, 2018 2:48 AM UTC
Low	Credit Card Number/s - A	2017-11-07-19-22-29-6B	shn-india-ops	Mar 26, 2018 2:47 AM UTC
Low	Credit Card Number/s - A	2017-10-28-23-19-14-82	shn-india-ops	Mar 26, 2018 2:47 AM UTC
Low	Credit Card Number/s - A	2017-10-28-21-18-09-5F4	shn-india-ops	Mar 26, 2018 2:47 AM UTC
Low	Credit Card Number/s - A	2017-10-23-22-18-57-A7	shn-india-ops	Mar 26, 2018 2:47 AM UTC
Low	Credit Card Number/s - A	2017-10-23-18-19-50-79	shn-india-ops	Mar 26, 2018 2:47 AM UTC
Low	Credit Card Number/s - A	2017-10-14-23-19-06-ED	shn-india-ops	Mar 26, 2018 2:47 AM UTC
Low	Credit Card Number/s - A	2017-09-18-05-19-07-AB	shn-india-ops	Mar 26, 2018 2:47 AM UTC

**DLP Policy Incident: #5883173**  
**Credit Card Number/s - API**  
1 match was found on the file 2017-12-13-08-19-23-877527BFECB29BD8 on demand scan in Box. It was discovered during a scan named "DLP Box" that ran on Mar 26, 2018 1:00 AM UTC.  
Action taken was Allowed.

ID: 5883173  
Severity: Low  
Service Name: Box  
Activity: On Demand Scan  
Incident Created On: Mar 26, 2018 2:48 AM UTC  
Last Updated: Mar 26, 2018 4:54 AM UTC  
Last Response: Allowed  
User: shn-india-ops  
Account ID: 295207888133

Owner: Unassigned  
Incident Response: Select Response  
Incident Status: New

Content: Item Name: 2017-12-13-08-19-23-877527BFECB29BD8...  
Item Type: File  
Size: 1.88 MB

“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

## Collaboration Control

Prevent sharing of sensitive data with unauthorized parties via Box file and folder collaboration.

### McAfee can enforce secure collaboration based on:

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

### Files/folders



---

“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

## DATA SHEET

### 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

---

The screenshot displays the Skyhigh Policy Management interface. The top navigation bar includes 'Access Control', 'DLP Policies', 'Encryption Policy', 'Configuration Audit', 'On-Demand Scan', 'User Lists', and 'Policy Settings'. The main content area is titled 'Cloud Access Policies' and features a search bar and a 'Create Policy' button. Below the search bar is a table of policies with columns for Name, IP, THEN, and On/Off status. A detailed view of a policy is shown on the right, including its name, version, last updated date, and update by user.

Name	IP	THEN	On/Off
Allow full access for managed - limited access for unmanaged	IP: Microsoft Office 365 and OneDrive Salesforce.com Box Unmanaged	THEN: Step-Up Authentication	On
Salesforce Block report download	IP: Salesforce.com Unmanaged IOS	THEN: Block Access	Off
Personal devices blocked from download (read only access)	IP: Unmanaged Microsoft Office 365 and OneDrive Download	THEN: Block Access	Off
Block Upload to Permitted Service	IP: Slack Upload	THEN: Block Access	Off
Access control for unmanaged devices	IP: Salesforce.com ServiceNow - Demand Management Unmanaged	THEN: Block Access	On
Limit downloads for unmanaged	IP: Microsoft Office 365 and OneDrive Salesforce.com Box Unmanaged Download	THEN: Block Access	On
ServiceNow - No Download on BYOD	IP: Unmanaged Download	THEN: Block Access	Off
Managed device	IP: Managed	THEN: Tag for DLP Policy	Off
Service Now Block all downloads	IP: ServiceNow - Demand Management Download	THEN: Block Access	On

Policy Name: Allow full access for managed - limited access for unmanaged  
Version: 5  
Last Updated: December 12, 2017 1:59 AM  
Updated by: Omar Rafiq  
Buttons: Edit, Delete

## DATA SHEET

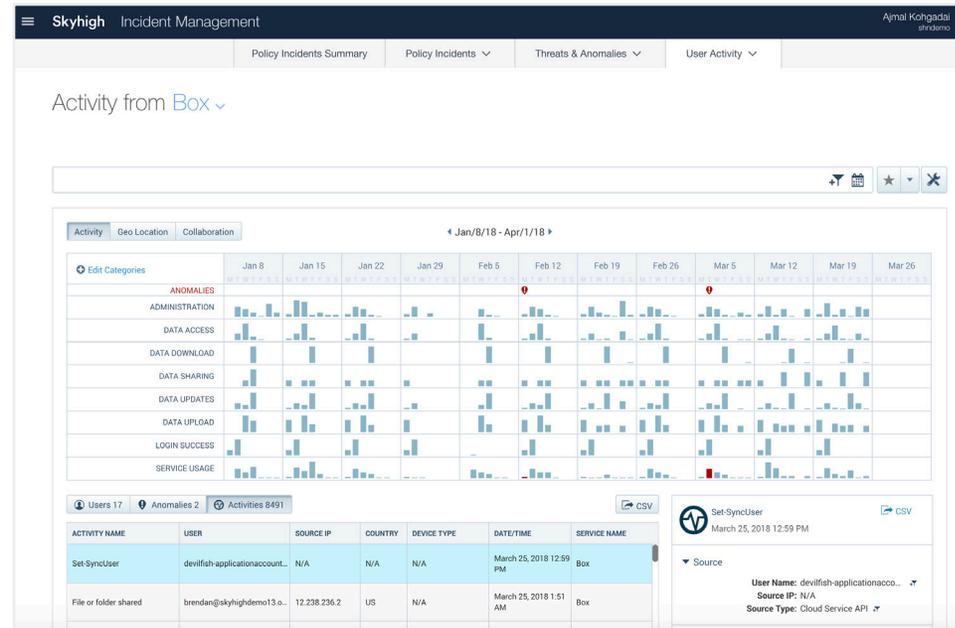
### Activity Monitoring

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



## DATA SHEET

### 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.

---

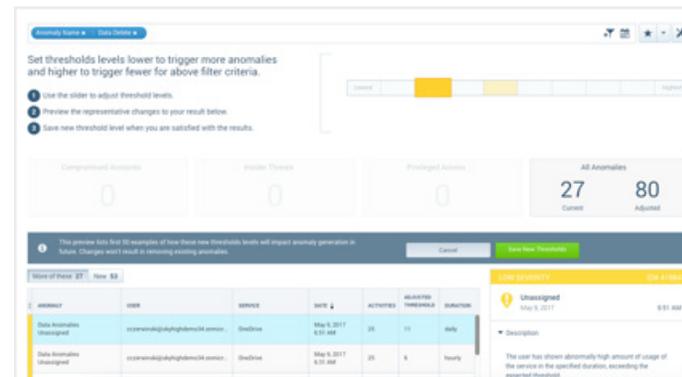
“In an environment with millions of unique events each day, McAfee does a nice job of cutting through the noise and directing us to the areas of greatest security concern.”

—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 SHEET

### 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

---

The screenshot displays the Skyhigh Policy Management interface. The top navigation bar includes 'Skyhigh Policy Management' and a user profile 'Ajmal Kohgadal'. Below the navigation are tabs for 'Access Control', 'DLP Policies', 'Encryption Policy', 'Configuration Audit', 'On-Demand Scan', 'User Lists', and 'Policy Settings'. The main content area is titled 'Policy Templates Overview' and features a search bar and a 'Filters' section. The 'Policy Type' section lists categories with counts: Security Configurat... (83), Compliance/DLP (58), and Secure Collaboration (11). The 'Business Requirement' section lists: Compliance (41), Data Exfiltration (22), Unrestricted Access (21), Secure Configuration (14), Secure Authentica... (7), Secure Collaborat... (6), Inactive Entity (5), and Security Monitoring (5). The 'Recommendation/Benchmark' section lists: Skyhigh Recomme... (60), Best Practice (40), Skyhigh Recomme... (28), and CIS Benchmark - L... (21). The 'Templates by Category' section shows a grid of policy templates with their respective counts and 'in use' status.

Policy Type	In Use	Total
Security Configuration	51	83
Compliance/DLP	71	58
Secure Collaboration		11

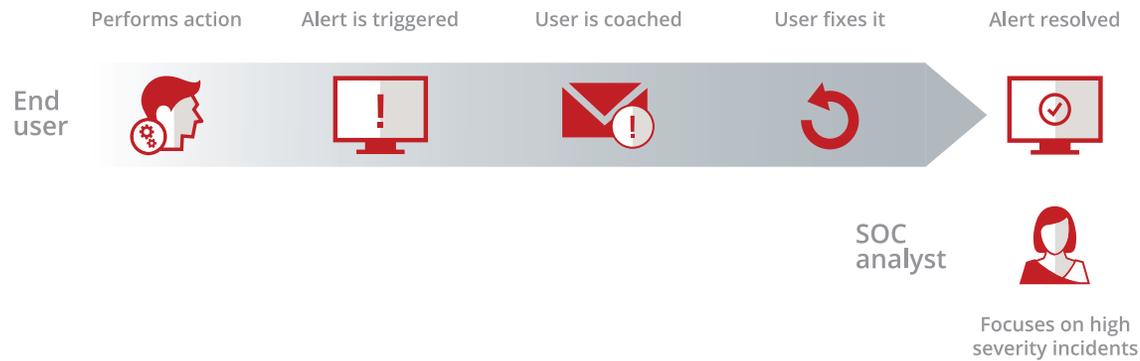
  

Business Requirement	In Use	Total
Compliance	50	41
Data Exfiltration	28	22
Unrestricted Access		21
Secure Configuration	20	14
Secure Authentication		7
Inactive Entity		5
Security Monitoring		5

Recommendation/Benchmark	In Use	Total
Document Classification Solutions	2	4

## DATA SHEET



### 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)

## DATA SHEET

### 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.

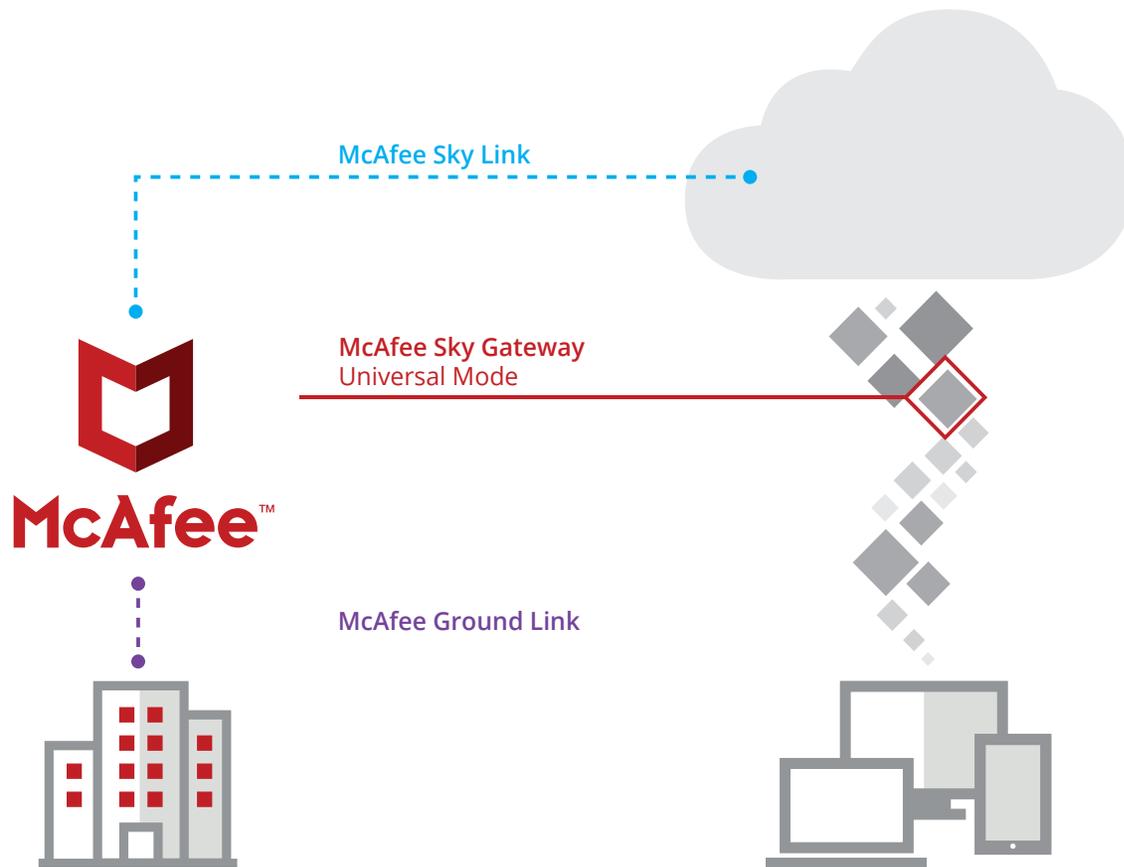
### McAfee Sky Link

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](http://www.mcafee.com).



2821 Mission College Blvd.  
Santa Clara, CA 95054  
888.847.8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC. 3857\_1018  
OCTOBER 2018