

McAfee Skyhigh Security Cloud for Citrix ShareFile®

McAfee® Skyhigh Security Cloud for Citrix ShareFile® helps organizations securely accelerate their business by providing industry-best Data Loss Prevention and Activity Monitoring visibility

Key Use Cases

Enforce sensitive data policies in Citrix ShareFile®

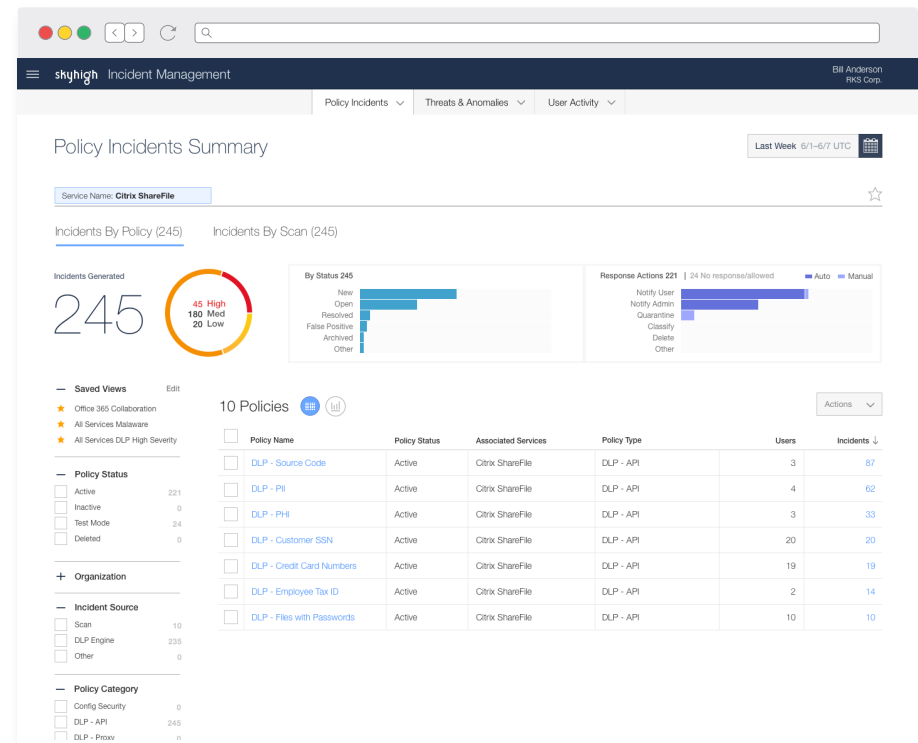
Enable Data Loss Prevention policies for deep inspection of data uploaded to the cloud.

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

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



Connect With Us



DATA SHEET

Data Loss Prevention (DLP)

Prevent regulated data from being stored in Citrix Sharefile®. Leverage McAfee's content analytics engine to discover sensitive data created in or uploaded to Citrix Sharefile® 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
- 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

The screenshot displays the McAfee Policy Incidents dashboard. The main table lists incidents with columns for Severity, Policy Name, User Name, Incident Created On, and Incident Response. A detailed view on the right shows the incident details for 'File names containing Password (ODS)', including its ID, severity, service name, instance name, creation and update timestamps, and the user who triggered it. The incident response is set to 'Suppressed'.

Sev	Policy Name	User Name	Incident Created On	Incident Response
H	File names containing Password (ODS)	o365mc@email2.microsoft.com	Jul 9, 2018 12:24 PM UTC	Allowed
H	-Social Security Numbers -API (Quarantine)	o365mc@email2.microsoft.com	Jul 9, 2018 12:24 PM UTC	Allowed
H	File names containing Password (ODS)	o365mc@email2.microsoft.com	Jul 9, 2018 12:24 PM UTC	Allowed
H	-Social Security Numbers -API (Quarantine)	o365mc@email2.microsoft.com	Jul 9, 2018 12:24 PM UTC	Allowed
H	File names containing Password (ODS)	o365mc@email2.microsoft.com	Jul 9, 2018 12:24 PM UTC	Allowed
H	-Social Security Numbers -API (Quarantine)	o365mc@email2.microsoft.com	Jul 9, 2018 12:24 PM UTC	Allowed

DLP Policy Incident (#10084780)
File names containing Password (ODS)
4 matches were found in the file named Passwords.docx in Citrix ShareFile.
Action taken was: Allowed.
ID: 10084780
Severity: High
Service Name: Citrix ShareFile
Instance Name: Default
Incident Created On: Jul 9, 2018 12:24 PM UTC
Last Updated: Jul 9, 2018 12:27 PM UTC
Last Response: Allowed
User: o365mc@email2.microsoft.com
Owner: Unassigned
Incident Response: Select Response
Incident Status: Suppressed
The same file triggered incidents for the following policies:
• File names containing Password (ODS)
• Social Security Numbers -API (Quarantine)

DATA SHEET

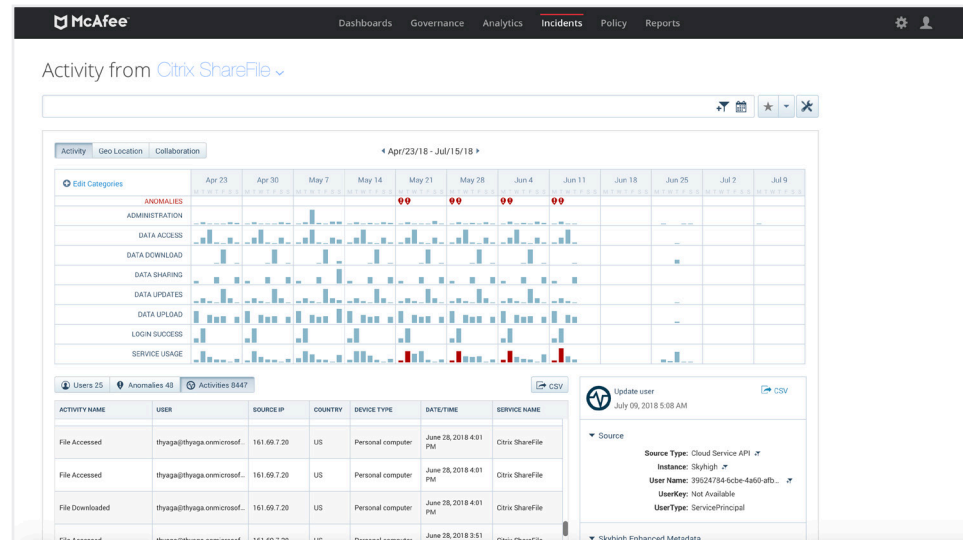
Activity Monitoring

Gain visibility into Citrix ShareFile® 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 Citrix Sharefile®, 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.

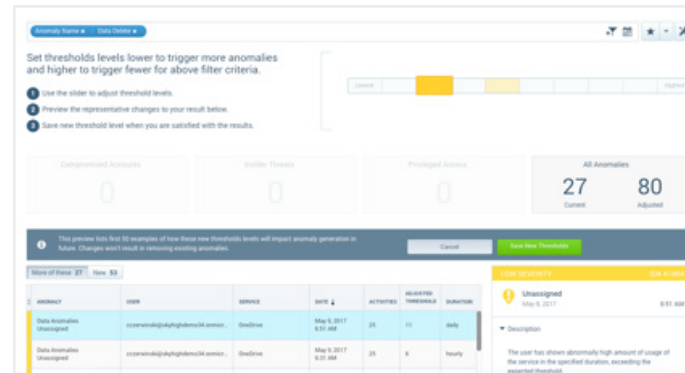
- **Insider threats:** Detect anomalous behavior across multiple dimensions including the amount of data uploaded/downloaded, volume of user action, access count, and frequency across time and cloud services.
- **Compromised accounts:** Analyze access attempts to identify impossible cross-region access,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

“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 Citrix Sharefile® 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

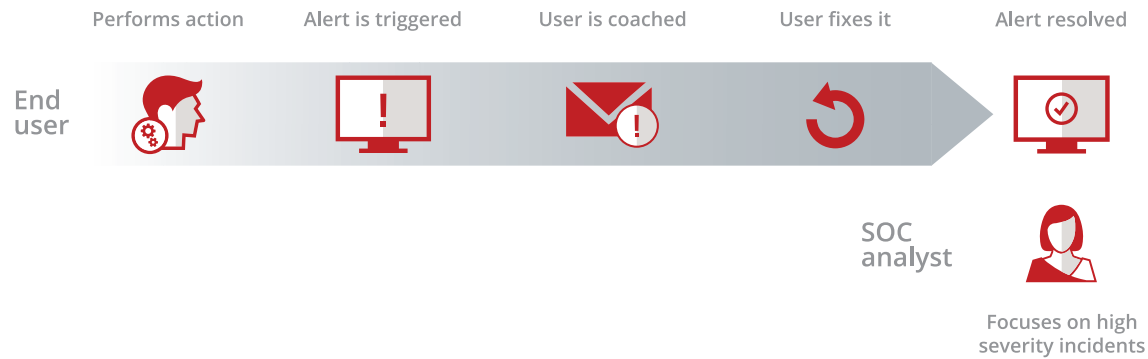
The screenshot displays the McAfee Skyhigh Policy Management interface. The top navigation bar includes 'Skyhigh Policy Management' and a user profile 'Ajmal Kohgadal'. Below the navigation bar are tabs for 'Access Control', 'DLP Policies', 'Encryption Policy', 'Configuration Audit', 'On-Demand Scan', '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 Configur... (83), Compliance/DLP (58), and Secure Collaboration (11). The 'Business Requirement' section lists various requirements with counts: 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 Link

Connects to Citrix ShareFile® APIs to gain visibility into data and user activity, and enforce policies across data uploaded data in near real-time.

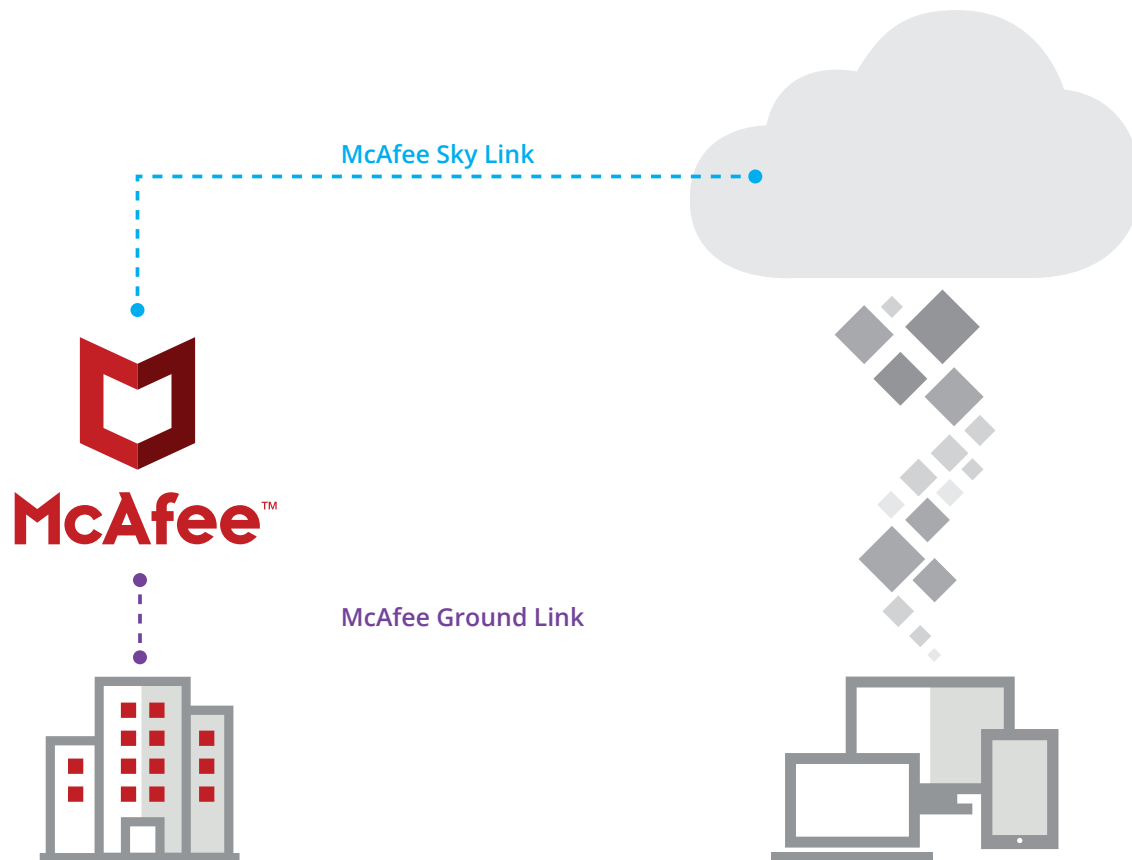
McAfee Ground Link

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

McAfee CASB Connect

Provides a simple API translation framework to rapidly deploy CASB services for customers using cloud applications. The CASB Connect Catalog contains all of McAfee Skyhigh Security Cloud CASB integrations.

Visit us at www.mcafee.com.



2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
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. 4089_0718
JULY 2018