

McAfee MVISION Cloud for Microsoft Teams

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

Key Use Cases

Enforce sensitive data policies in Microsoft Teams

Prevent sensitive data that cannot be stored in the cloud from being uploaded to Teams.

Build sharing and collaboration guardrails

Prevent sharing of sensitive or regulated data in Teams with unauthorized parties.

Limit Microsoft Teams activities for users on unmanaged devices and untrusted networks

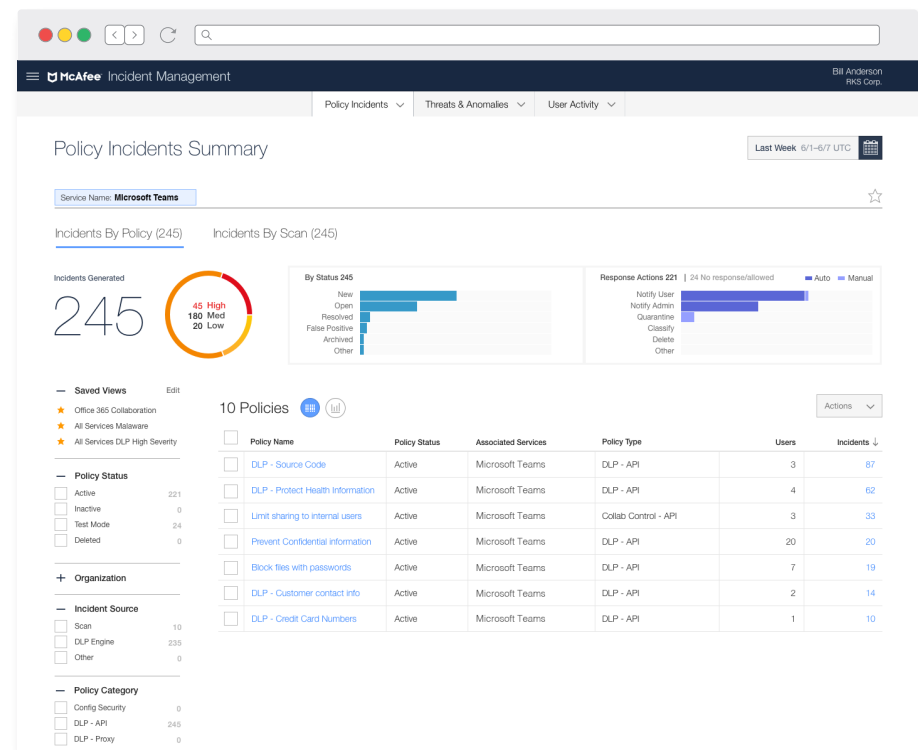
Gain total control over user access to Teams by enforcing context-specific policies limiting end-user actions.

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 Microsoft Teams. Leverage McAfee's content analytics engine to discover sensitive data uploaded to Microsoft Teams 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:

- Generate Incident
- Notify the end user
- Notify an administrator
- Quarantine the file
- Delete the message/file

The screenshot displays the McAfee Incident Management interface. The main view shows a table of Policy Incidents with columns for Severity, Policy Name, Item Name, User Name, and Incident Created On. A filter for 'Service Name: 4 Service Names' is applied, showing 3,950,461 incidents. The table lists several incidents related to Social Security Numbers and Credit Card Numbers. A detailed view of a specific incident is shown on the right, titled 'DLP Policy Incident (#5928924) -Social Security Numbers -API (Quarantine)'. The details include the incident ID (5928924), severity (High), service name (Microsoft Teams), incident created on (Mar 26, 2018 1:27 AM UTC), last updated (Mar 26, 2018 1:18 PM UTC), last response (Allowed), user (shn-india-ops), account ID (25650786133), S3 Bucket (au1005), owner (Unassigned), incident response (Select Response), and incident status (Suppressed). The content area shows 3 matches found on a file named '522462218264_us-west-2_20170922T0530Z_MAHJV1L8dYFytDnf.json.gz'.

Collaboration Control

Prevent sharing of sensitive data with unauthorized parties via Microsoft Teams channels and messages.

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, Executive Director of Security Innovation, Aetna

Common collaboration policies McAfee can enforce in Microsoft Teams:

- Prevent files and messages from being added to any Teams channel that contains external or non-approved users, user groups, business partners or personal email domains
- Prevent file/folder permissions that are open to the internet or the entire company
- Delete sensitive/confidential messages posted in channels with non-approved external users
- 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:

- Deleting sensitive messages shared with external users
- Revoking a shared link
- Downgrading permissions to view/edit
- Removing access permissions
- Notifying the end user in Teams

DATA SHEET

Access Control

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

Control access to Teams 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 Teams
- Allow/block specific Teams 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 shows the McAfee console interface for creating a new cloud access policy. The page title is "Create New Cloud Access Policy" with a "Required Fields" indicator. The "Name" field contains "Block downloads from unmanaged devices" and the "Description" field contains "Block downloads from unmanaged devices". A toggle switch is set to "ON" and "Monitor only mode" is unchecked. The "If the following conditions are met:" section lists three conditions: Service is Microsoft Office 365, Device is Unmanaged, and Activity is Download. The "Then take the following action:" section is set to "Block Access". The page includes "Save" and "Cancel" buttons at the bottom right.

DATA SHEET

Activity Monitoring

Gain visibility into Microsoft Teams usage and accelerate post-incident forensic investigations by capturing a comprehensive audit trail of all activity. McAfee MVISION Cloud captures hundreds of unique activity types and groups them into 14 categories for streamlined navigation. With MVISION Cloud organizations can monitor:

- Who is accessing Teams, 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

The screenshot displays the McAfee MVISION Cloud interface for monitoring Office365 activity. The top navigation bar includes 'Dashboards', 'Governance', 'Analytics', 'Incidents', 'Policy', and 'Reports'. The main content area is titled 'Activity from Office365' and features several filters: 'Service Name' (AzureAD, Microsoft-Teams) and 'Activity Name' (User Logged In - Failed, MemberAdded, TabAdded, TabUpdated, TeamCreated, TeamSettingChanged). Below the filters is a calendar view for the period Dec 24 to Mar 11, showing activity bars for categories like ANOMALIES, LOGIN FAILURE, and SERVICE USAGE. A table below the calendar lists activities with columns for Activity Name, User, Source IP, Country, Device Type, Date/Time, and Service Name. A right-hand pane provides detailed metadata for a selected 'User Logged In - Failed' event on February 21, 2019, at 4:34 PM, including source type (Cloud Service API), instance (Skyhigh Networks), source IP (49.207.53.62), user name (unknown), and enhanced metadata such as city (bangalore), region (ka), country (IN), ASN (24309), and IP organization (beam telecom pvt ltd).

ACTIVITY NAME	USER	SOURCE IP	COUNTRY	DEVICE TYPE	DATE/TIME	SERVICE NAME
User Logged In - Failed	admin@shnhydev03.onmi...	103.245.47.20	IN	N/A	February 20, 2019 4:09 PM	AzureAD
User Logged In - Failed	admin@shnhydev03.onmi...	103.245.47.20	IN	N/A	February 20, 2019 2:42 PM	AzureAD
TeamCreated	anuragteamstest2@shnhyd...	N/A	N/A	N/A	February 19, 2019 4:46 PM	Microsoft-Teams
TabUpdated	anuragteamstest2@shnhyd...	N/A	N/A	N/A	February 19, 2019 4:46 PM	Microsoft-Teams
TabAdded	anuragteamstest2@shnhyd...	N/A	N/A	N/A	February 19, 2019 4:46 PM	Microsoft-Teams
TabAdded	anuragteamstest2@shnhyd...	N/A	N/A	N/A	February 19, 2019 4:46 PM	Microsoft-Teams
MemberAdded	anuragteamstest2@shnhyd...	N/A	N/A	N/A	February 19, 2019 4:46 PM	Microsoft-Teams

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.

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

Operationalize Microsoft Teams 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

The screenshot displays the McAfee Policy Management dashboard. At the top, there are navigation 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 includes a search bar and filter options. The dashboard is organized into three main sections: Policy Type, Business Requirement, and Recommendation/Benchmark. Each section contains a grid of policy templates with their respective counts and usage statistics.

Policy Type	Count
Security Configurat...	83
Compliance/DLP	58
Secure Collaboration	11

Business Requirement	Count
Compliance	41
Data Exfiltration	22
Unrestricted Access	21
Secure Configuration	14
Secure Authentica...	7
Secure Collaborat...	6
Inactive Entity	5
Security Monitoring	5

Recommendation/Benchmark	Count
Document Classification Solutions	4

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

—Brian Lillie, Chief Information Officer, Equinix

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 MVISION Cloud 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)
- Identity Access Management (IAM)
- Information rights management (IRM)
- Enterprise mobility management (EMM/MDM)



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 © 2019 McAfee, LLC. 4249_0319 MARCH 2019