McAfee
Together is power.

McAfee MVISION Cloud for Custom Applications

McAfee® MVISION Cloud for Custom Applications helps organizations securely accelerate their business by providing total control over data and user activity in custom-built cloud services

Key Use Cases

Enforce sensitive data policies in custom applications

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

Limit download/sync to unmanaged devices

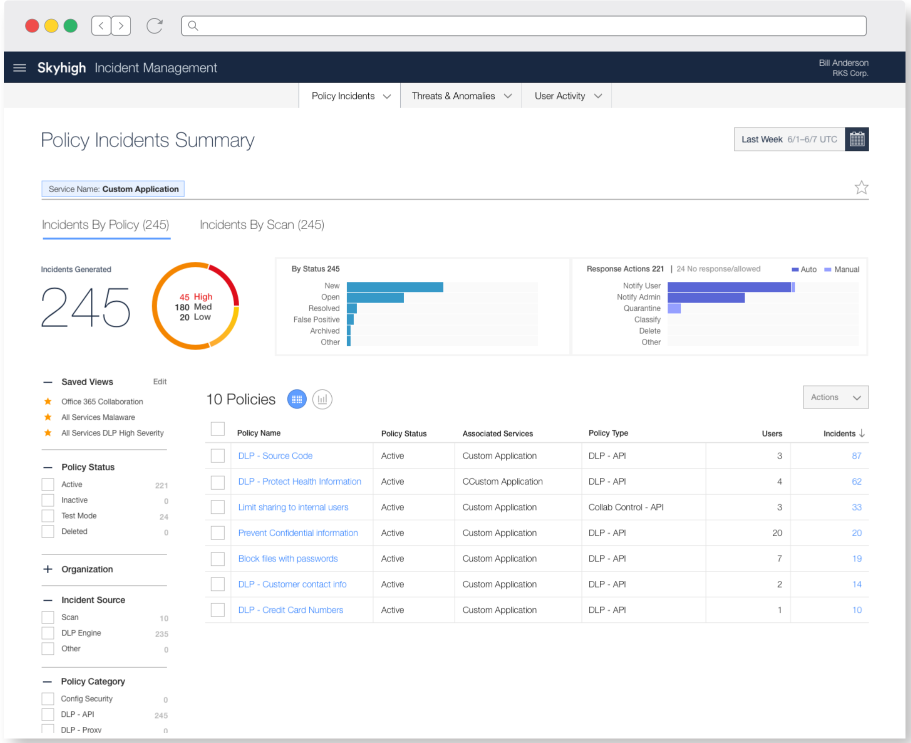
Gain total control over user access to custom applications by enforcing context-specific policies limiting specific end-user actions.

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.



Policy Incidents Summary

Last Week 6/1–6/7 UTC

Service Name: **Custom Application**

245

Saved Views — Edit
- Office 365 Collaboration
- All Services Malware
- All Services DLP High Severity

Policy Status
- □ Active 221
- □ Inactive 0
- □ Test Mode 24
- □ Deleted 0

Organization

Incident Source
- □ Scan 10
- □ DLP Engine 235
- □ Other 0

Policy Category
- □ Config Security 0
- □ DLP - API 245
- □ DLP - Proxy 0

10 Policies

□	Policy Name	Policy Status	Associated Services	Policy Type	Users	Incidents ↓
□	DLP - Source Code	Active	Custom Application	DLP - API	3	87
□	DLP - Protect Health Information	Active	CCustom Application	DLP - API	4	62
□	Limit sharing to internal users	Active	Custom Application	Collab Control - API	3	33
□	Prevent Confidential information	Active	Custom Application	DLP - API	20	20
□	Block files with passwords	Active	Custom Application	DLP - API	7	19
□	DLP - Customer contact info	Active	Custom Application	DLP - API	2	14
□	DLP - Credit Card Numbers	Active	Custom Application	DLP - API	1	10

Connect With Us

Data Loss Prevention (DLP)

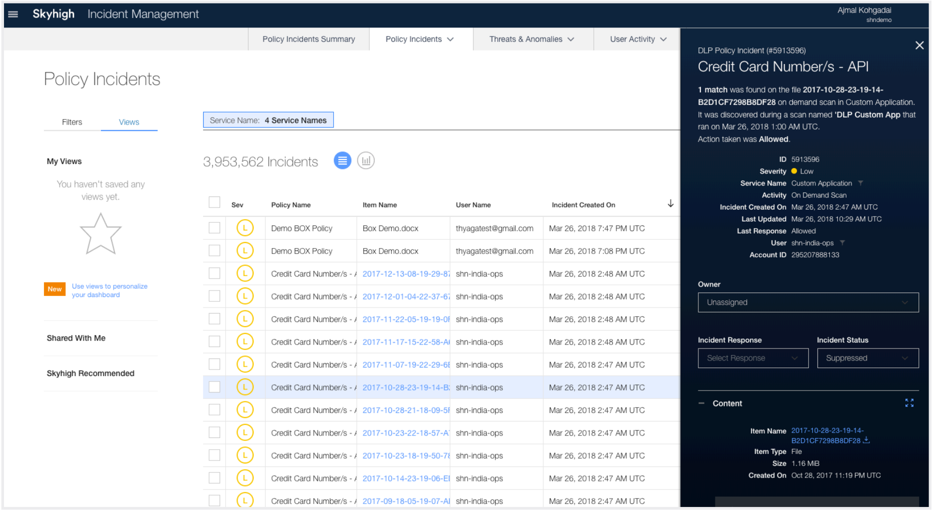
Prevent regulated data from being stored in custom applications. Leverage McAfee's content analytics engine to discover sensitive data uploaded to a custom application based on:

- 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



Policy Incidents

My Views

You haven't saved any views yet.

Shared With Me

Skyhigh Recommended

Service Name: **4 Service Names**

3,953,562 Incidents

□	Sev	Policy Name	Item Name	User Name	Incident Created On
□	L	Demo BOX Policy	Box Demo.docx	thyagatest@gmail.com	Mar 26, 2018 7:47 PM UTC
□	L	Demo BOX Policy	Box Demo.docx	thyagatest@gmail.com	Mar 26, 2018 7:08 PM UTC
□	L	Credit Card Number/s - A	2017-12-13-08-19-29-87	shn-india-ops	Mar 26, 2018 2:48 AM UTC
□	L	Credit Card Number/s - A	2017-12-01-04-22-37-67	shn-india-ops	Mar 26, 2018 2:48 AM UTC
□	L	Credit Card Number/s - A	2017-11-22-05-19-19-0F	shn-india-ops	Mar 26, 2018 2:48 AM UTC
□	L	Credit Card Number/s - A	2017-11-17-15-22-58-A(	shn-india-ops	Mar 26, 2018 2:48 AM UTC
□	L	Credit Card Number/s - A	2017-11-07-19-22-29-6E	shn-india-ops	Mar 26, 2018 2:47 AM UTC
□	L	Credit Card Number/s - A	2017-10-28-23-19-14-B2	shn-india-ops	Mar 26, 2018 2:47 AM UTC
□	L	Credit Card Number/s - A	2017-10-28-21-18-09-5F	shn-india-ops	Mar 26, 2018 2:47 AM UTC
□	L	Credit Card Number/s - A	2017-10-23-22-18-57-A7	shn-india-ops	Mar 26, 2018 2:47 AM UTC
□	L	Credit Card Number/s - A	2017-10-23-18-19-50-78	shn-india-ops	Mar 26, 2018 2:47 AM UTC
□	L	Credit Card Number/s - A	2017-10-14-23-19-06-EI	shn-india-ops	Mar 26, 2018 2:47 AM UTC
□	L	Credit Card Number/s - A	2017-09-18-05-19-07-AI	shn-india-ops	Mar 26, 2018 2:47 AM UTC

DLP Policy Incident (#5913596)

Credit Card Number/s - API

1 match was found on the file **2017-10-28-23-19-14-B2D1CF7298B8DF28** on demand scan in Custom Application. It was discovered during a scan named **'DLP Custom App** that ran on Mar 26, 2018 1:00 AM UTC.
Action taken was **Allowed**.

ID	5913596
Severity	● Low
Service Name	Custom Application
Activity	On Demand Scan
Incident Created On	Mar 26, 2018 2:47 AM UTC
Last Updated	Mar 26, 2018 10:29 AM UTC
Last Response	Allowed
User	shn-india-ops
Account ID	295207888133

Owner: Unassigned

Incident Response: Select Response

Incident Status: Suppressed

Item Name	2017-10-28-23-19-14-B2D1CF7298B8DF28
Item Type	File
Size	1.16 MiB
Created On	Oct 28, 2017 11:19 PM UTC

Access Control

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

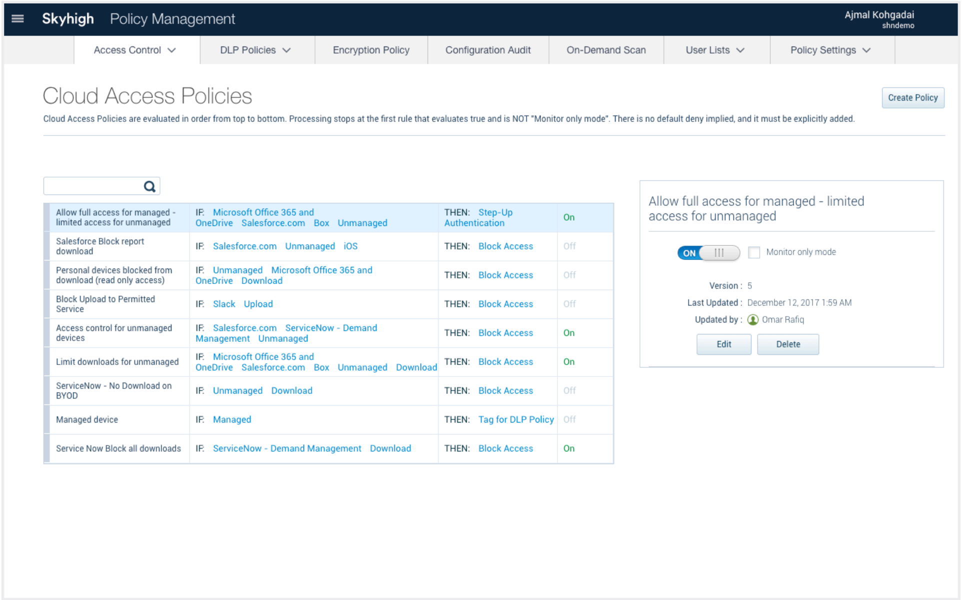
Control access to custom apps based on:

- 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 custom apps
- Allow/block specific custom apps 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



Cloud Access Policies

Cloud Access Policies are evaluated in order from top to bottom. Processing stops at the first rule that evaluates true and is NOT "Monitor only mode". There is no default deny implied, and it must be explicitly added.

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

Allow full access for managed - limited access for unmanaged

ON □ Monitor only mode

Version : 5

Last Updated : December 12, 2017 1:59 AM

Updated by : Omar Rafiq

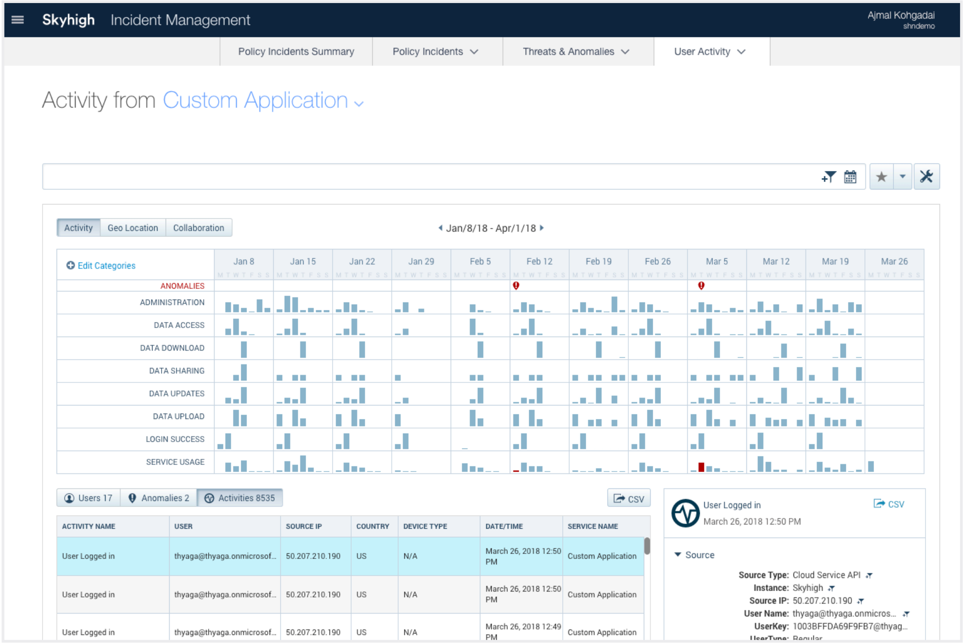
Activity Monitoring

Gain visibility into custom application 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 a custom app, 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



Activity from Custom Application

ACTIVITY NAME	USER	SOURCE IP	COUNTRY	DEVICE TYPE	DATE/TIME	SERVICE NAME
User Logged in	thyaga@thyaga.onmicrosof...	50.207.210.190	US	N/A	March 26, 2018 12:50 PM	Custom Application
User Logged in	thyaga@thyaga.onmicrosof...	50.207.210.190	US	N/A	March 26, 2018 12:50 PM	Custom Application
User Logged in	thyaga@thyaga.onmicrosof...	50.207.210.190	US	N/A	March 26, 2018 12:49 PM	Custom Application

User Logged in
March 26, 2018 12:50 PM

Source

Source Type: Cloud Service API
Instance: Skyhigh
Source IP: 50.207.210.190
User Name: thyaga@thyaga.onmicros...
UserKey: 1003BFFDA69F9FB7@thyag...
UserType: Regular

User Behavior Analytics and Malware Detection

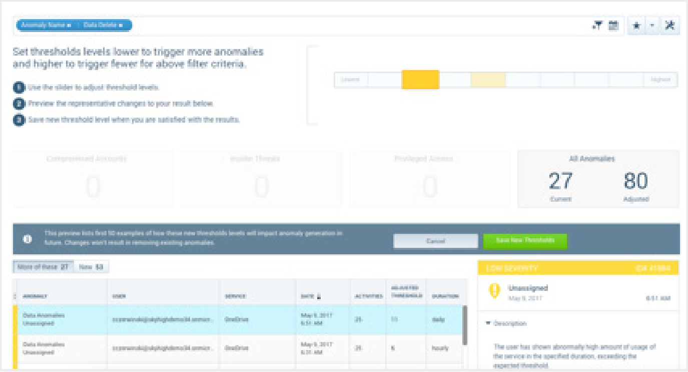
McAfee uses data science and machine learning to automatically build models of typical user behavior and identifies behavior that may be indicative of a threat.

- **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.



Set thresholds levels lower to trigger more anomalies and higher to trigger fewer for above filter criteria.

1 Use the slider to adjust threshold levels.
2 Preview the representative changes to your result below.
3 Save new threshold level when you are satisfied with the results.

Compromised Accounts 0
Insider Threats 0
Privileged Access 0
All Anomalies 27 Current 80 Adjusted

This preview lists first 50 examples of how these new thresholds levels will impact anomaly generation in future. Changes won't result in removing existing anomalies.

ANOMALY	USER	SERVICE	DATE	ACTIVITIES	ADJUSTED THRESHOLD	DURATION
Data Anomalies Unassigned	ccorwinski@skyhighdemo34.onmicr...	OneDrive	May 9, 2017 6:51 AM	25	11	daily
Data Anomalies Unassigned	ccorwinski@skyhighdemo34.onmicr...	OneDrive	May 9, 2017 6:51 AM	25	6	hourly

LOW SEVERITY ID# 41988

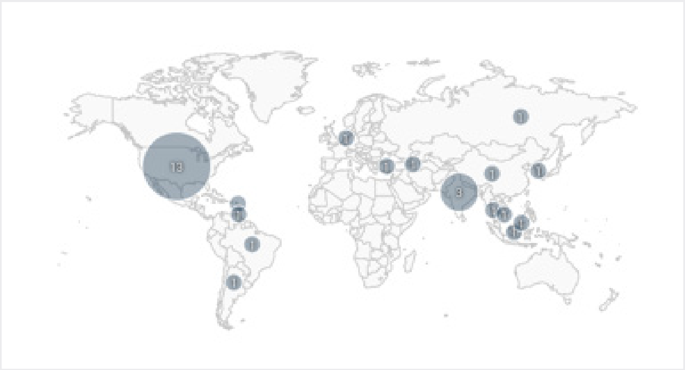
Unassigned
May 9, 2017 6:51 AM

Description

The user has shown abnormally high amount of usage of the service in the specified duration, exceeding the expected threshold.

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

Policy import

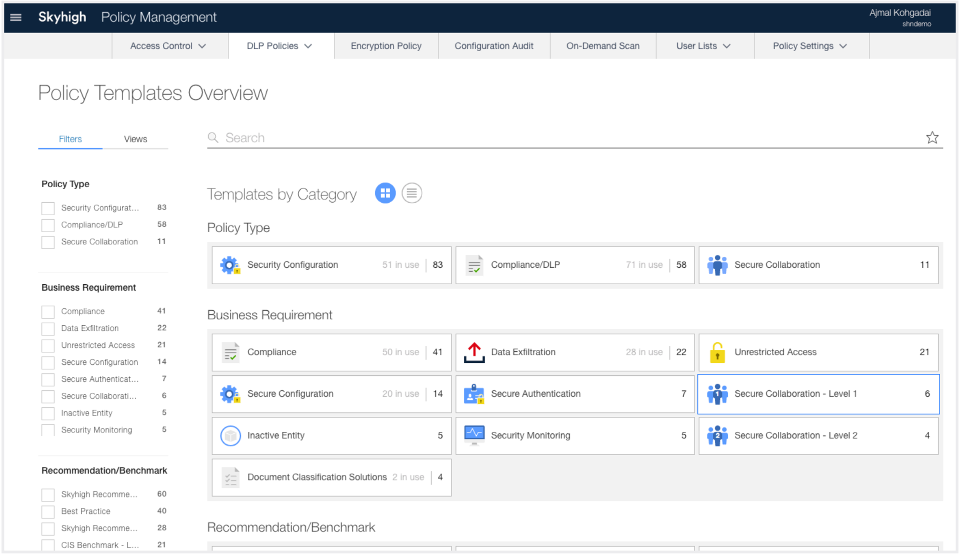
Import policies from existing security solutions or policies from other McAfee customers or partners.

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



Policy Templates Overview

Policy Type

□	Security Configurat...	83
□	Compliance/DLP	58
□	Secure Collaboration	11

Business Requirement

□	Compliance	41
□	Data Exfiltration	22
□	Unrestricted Access	21
□	Secure Configuration	14
□	Secure Authenticat...	7
□	Secure Collaborati...	6
□	Inactive Entity	5
□	Security Monitoring	5

Recommendation/Benchmark

□	Skyhigh Recomme...	60
□	Best Practice	40
□	Skyhigh Recomme...	28
□	CIS Benchmark - L...	21

Templates by Category

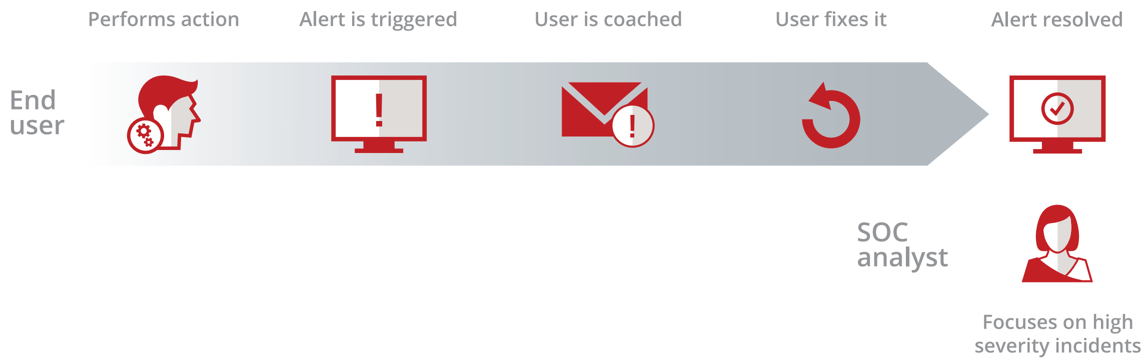
Policy Type

Security Configuration	51 in use	83
Compliance/DLP	71 in use	58
Secure Collaboration		11

Business Requirement

Compliance	50 in use	41
Data Exfiltration	28 in use	22
Unrestricted Access		21
Secure Configuration	20 in use	14
Secure Authentication		7
Secure Collaboration - Level 1		6
Inactive Entity		5
Security Monitoring		5
Secure Collaboration - Level 2		4
Document Classification Solutions	2 in use	4

Recommendation/Benchmark



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.

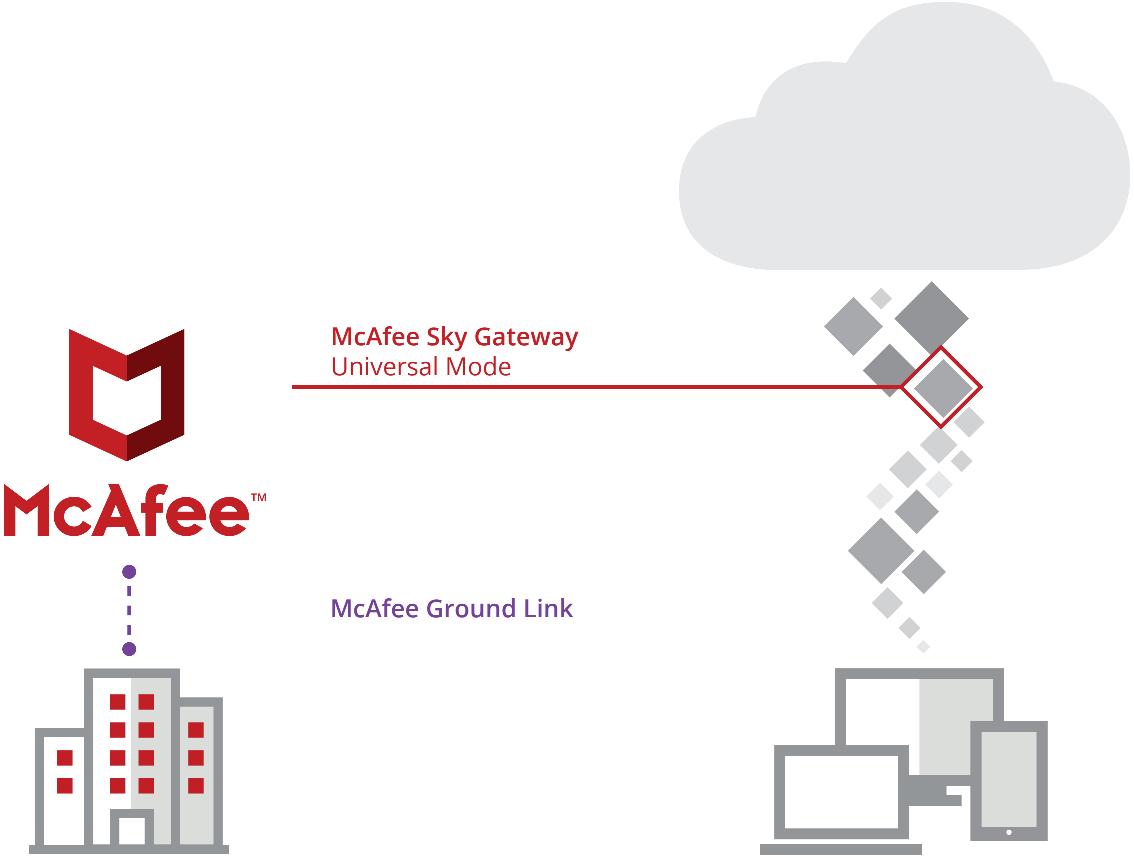
Universal mode

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

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