

McAfee MVISION Cloud for Azure

McAfee[®] MVISION Cloud for Azure is a comprehensive monitoring, auditing, and remediation solution for your Azure environment

Key Use Cases

Security configuration and compliance audit

Audit the configuration of Azure services to identify settings that are insecure or non-compliant and recommend corrective measures.

Activity monitoring

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

Threat protection

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

Data loss prevention (DLP)

Enforce DLP policies for sensitive data stored in Azure Storage Containers and Blob Storage.

Unsanctioned Azure accounts discovery

Identify managed and unmanaged Azure subscriptions and enforce a uniform set of security policies across all Azure subscriptions.

•••	C C	٩						
Skyhiah	Incident Manac	iement						Bill Anderson
okymgn	inolaoni Manag	Jernerit						RKS Corp
			Policy Incider	nts 🗸 Threats a	& Anomalies V User A	ctivity 🗸		
Policy	Incidents S	Summ	ary				Last Week 6/	1-6/7 UTC
Service Nam	ne: Azure							N.
Incidents	By Policy (245)	Incide	nts By Scan (245)					
Incidents Gene	erated		By Status 245			Response Actions 221 24 No	response/allowed	Auto 💻 Manual
\frown	1		New			Notify User		
')/	h	45 High 80 Med	Open Resolved			Notify Admin Quarantine		
\angle^{-}	+ 🕖 🚺	20 Low	False Positive			Classify		
			Archived			Other		
- Saved	Views Edit	101	Delieiee 🔍 🕕					Actions
Saved Saved All Service	Views Edit 35 Collaboration ces Malaware	10 F	Policies 🛑 🔟					Actions 🗸
Saved Saved All Servic All Servic	Views Edit 35 Collaboration ces Malaware ces DLP High Severity	10 F	Policies 🔳 🔟	Policy Status	Associated Services	Policy Type	Users	Actions V
Saved 1 Office 38 All Servic All Servic Policy 5	Views Edit 35 Collaboration ces Malaware ces DLP High Severity Status	10 F	Policies III III	Policy Status Active	Associated Services Azure	Policy Type Config Audit - API	Users 0	Actions ↓ Incidents ↓ 87
Saved 1 Office 36 All Servic All Servic Policy 3 Active	Views Edit 35 Collaboration ces Malaware ces DLP High Severity Status 221	10 F	Policies Policy Name Unencrypted Storage IAM Policy Victation	Policy Status Active Active	Associated Services Azure Azure	Policy Type Config Audit - API Config Audit - API	Users 0 0	Actions ↓ Incidents ↓ 87 62
Saved 1 Saved 1 All Servic All Servic All Servic Policy S Active Inactive	Views Edit 55 Collaboration ces Malaware ces DLP High Seventy Status 221 0	10 F	Policies (a) (a) Policy Name Unencrypted Storage IAM Policy Violation Prevent Storag Contidential	Policy Status Active Active Active	Associated Services Azure Azure Azure	Policy Type Config Audit - API Config Audit - API Config Audit - API DLP - API	Users 0 0 3	Actions V Incidents J 87 62 33
Saved 1 Saved 1 All Service All Service Policy 3 Active Inactive Test Moc Defeted	Views Edit 55 Collaboration ces Malaware ces DLP High Seventy Status 221 0 de 24	10 F	Policies (III) Policy Name Unencrypted Storage UAM Policy Violation Prevent Storag Contidential	Policy Status Active Active Active Active Active Active	Associated Services	Policy Type Config Audit - API Config Audit - API DLP - API Configu Audit - API	Users 0 0 3 20	Actions ∨ Incidents ↓ 87 62 33 20
Saved 1 Office 36 All Servic All Servic All Servic All Servic Active Inactive Test Moc Deleted	Views Edit 55 Collaboration ces Malavare ces DLP High Severity Status 221 0 de 24 0	10 F	Policies (1) (1) Perceytent Storage UM Patry Valation Prevent Storage Confidential Unused Walations (2) (2) (2)	Policy Status Active Active Active Active Active Active	Associated Services Azuro Azuro Azuro Azuro Azuro Azuro Azuro	Policy Type Config Audt - API Config Audt - API DLP - API Config Audt - API Config Audt - API	Users 0 0 3 20	Actions ∨ Incidents ↓ 87 62 33 20
Saved 1 Office 36 All Servic All Servic All Servic All Servic Active Inactive Inactive Deleted + Organia	Views Edit 55 Collaboration		Policies (1) (1) Policy Name Unercrysted Storage PM Policy Vication Prevent Storag Confidential Unuard VM users Threat Detection on SQL DB	Policy Status Active Active Active Active Active Active Active	Associated Services Azure Azure Azure Azure Azure Azure	Policy Type Contig Audt - API Contig Audt - API DLP - API Contig Audt - API Contig Audt - API	Users 0 0 3 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Actions V Incidents J 87 62 33 20 19
Saved 1 Office 36 All Service All Service Policy 3 Active Inactive Test Moc Deleted + Organiz	Views Edit dis Cottaboration dis Cottaboration ces Matemate ces Matemate ces Matemate Status 221 0 de 24 0 zation to Secure		Policies (a) (a) Peter Name Unincrysted Storage PAM Policy Violation Prevent Storing Confidential Unuaed MM users Threat Detection on SQL DB	Policy Status Active Active Active Active Active Active Active Test Mode	Acsociated Services Azure Azure Azure Azure Azure Azure Azure	Policy Type Config Audit - API Config Audit - API DLP - API Config Audit - API	Uters 0 0 3 20 0 0	Actions V Incidents J 87 62 33 20 19 14
Saved 1 Office 36 All Servic All Servic Policy 3 Active Inactive Test Moc Deleted H Organiz Incidem Scan	Views Edit dis Cottaboration ces Matimarie cos DLP High Severity Status de 221 o de 24 o zation		Policies (a) (a) Policy Name Unincrycted Storage My Policy Videtion Prevent Storing Contidential Unueld My Lawrs Thread Editection on SCL DB Thread Editection on SCL B3	Policy Status Active Active Active Active Active Active Active Test Mode Test Mode	Associated Services Azuro Azuro Azuro Azuro Azuro Azuro Azuro Azuro	Policy Type Config Audit - API Config Audit - API DLP - API Config Audit - API	Uters 0 3 20 0 0 0	Actions ↓ Incidents ↓ 87 62 33 20 19 19 14
Saved 1 Office 36 All Servic All Servic Policy 5 Active Inactive Test Moc Deleted H Organiz Inciden Scan DLP Eng	Views Edit 55 Collaboration Ces Makiware ces DLP High Severity Status de 221 0 0 0 221 0 0 0 0 1 0 0 1 0 0 1 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1		Policies (a) (a) Poly Name Unercrysted Storage UM Poly Vidaton Prevent Storage Containstat Unual VM users Trivial Detection on SQL DB Trivial Detection on SQL DB	Policy Status Active Active Active Active Active Test Mode	Associated Services Azuro Azuro Azuro Azuro Azuro Azuro Azuro	Policy Type Contig Audit - API Contig Audit - API DLP - API Contig Audit - API	Users 0 0 3 20 0 0 0 0	Actions ✓ Incidents ↓ 62 33 20 19 14 14
Saved 1 Office 38 All Servic All Servic All Servic All Servic Active Inactive Inactive Test Moo Deleted Unciden Scan DLP Prog Other	Views Edit 55 Cottaboration Ees Matalows Cottaboration Statuse 221 0 0 24 0 25 0 25 0 25 0 25 0 25 0 25 0 25 0 25 0 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 25 10 10 10 10 10 10 10 10 10 10		Policies (a) (a) Peter Name Unercrysted Storage PAM Patey Volation Pervent Storing Considential Unused FMM users Threat Detection on SQL DB Threat Detection on SQL DB	Policy Status Active Active Active Active Active Active Active Test Mode	Associated Bervices Azure Azure Azure Azure Azure Azure Azure	Policy Type Contig Audit - API Contig Audit - API DLP - API Contig Audit - API Contig Audit - API Contig Audit - API Contig Audit - API	Uters 0 3 20 0 0 0 0	Actions V Incidents J 62 33 20 19 14 14
Saved 1 Office 38 All Servic All Servic All Servic Inactive Inactive Inactive Inactive Test Moc Deleted Crganiz Inciden Scan DLP Eng Other	Views Edit 55 Gollaboration		Policies (a) (a) Policy Name Unincrypted Storage M Policy Volation Prevent Storag Confidential Unued VM users Threat Detection on SQL DB Threat Detection on SQL DB	Policy Status Active Active Active Active Active Active Test Mode	Associated Services Azure Azure Azure Azure Azure Azure	Policy Type Config ALuit - API Config ALuit - API DLP - API Config ALuit - API Config ALuit - API Config ALuit - API Config ALuit - API	Uters 0 3 20 0 0 0	Actions ↓ Incident ↓ 87 62 33 20 19 14 10
Saved 1 Office 38 All Servic All Servic All Servic Inactive Inactive Inactive Inactive Inactive Inactive Inactive Inciden Scan DLP Eng Other Policy C	Views Edit 85 Gatbarans Cons Matemarie Status 2210 de 221 0 4 2210 0 24 0 24 0 24 0 24 0 24 0		Policies (a) (a) Poly Name Unercrypted Storage UM Poly Vidaton Prevent Storag Contactuat Unuted VM uses Trivial Defection on SOL DB Trivial Defection on SOL B3	Polcy Status Active Active Active Active Active Test Mode Test Mode	Associated Services Azure Azure Azure Azure Azure Azure	Policy Type Contig Audt - API Contig Audt - API DLP - API Contig Audt - API	Uters 0 3 20 0 0 0	Actions Incidents R7 02 33 20 19 14 10
Saved 1 Office 38 All Servic All Servic All Servic All Servic Active Inactive Test Moc Deleted Horganiz Inciden Scan DLP Eng Other Policy C Config S	Views Edit 45 Cottaboration Cost Matavare Status 2211 0 0 2 2 2 2 2 2 2 2 2 2 2 2 2		Policies (1) (1) Petrorysteed Storage Democrysteed Storage Petrory Votation Petrory Votation Prevent Storing Constituential Unuard MM users Threat Detection on SQL DB Threat Detection on SQL DB	Poley Status Active Active Active Active Active Active Test Mode	Associated Bervices Azure Azure Azure Azure Azure Azure Azure	Petry Type Contig Audit - API Contig Audit - API DLP - API Contig Audit - API Contig Audit - API Contig Audit - API Contig Audit - API	Uters 0 3 20 0 0 0 0	Actions ↓ Incidents ↓ 67 62 33 20 19 14 10
Saved 1 Office 38 All Servic All Servic All Servic All Servic Active Inactive Inactive Test Moc Detected Urganiz Inciden Scan DLP Eng Other Policy C Config S DLP - AF	Views Edit 35 Cottaburston Cost DLP High Severity de 24 24 de 24 24 de 24 24 25 24 24 25 24 25 25 25 25 25 25 25 25 25 25 25 25 25		Policies (a) (a) Policy Name Unincrypted Storage MM Policy Volation Prevent Storag Contidental Unued VM users Thread Detection on SQL DB Thread Detection on SQL DB	Policy Status Active Active Active Active Active Test Mode	Associated Services Azure Azure Azure Azure Azure Azure	Policy Type Config Audit - API Config Audit - API DLP - API Config Audit - API Config Audit - API Config Audit - API Config Audit - API	Uters 0 0 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Actions V Incidents J 62 333 20 19 14 14 10

Connect With Us



Security Configuration and Compliance Audit

Audit and monitor the security configurations of all your Azure subscriptions to detect and correct misconfigurations to reduce risk and comply with internal and external policies.

Detect misconfigurations for:

- Virtual Machines (VMs)
- Storage services including Blobs, Files, Queue, and Table storage
- Identity and access management (IAM)
- SQL services
- Logging and monitoring services
- Network security groups

Correct misconfigured services using:

- McAfee recommended best practices derived from existing customers
- Center for Internet Security (CIS) benchmark recommendations for Azure
- Compliance recommendations for regulations such as HIPAA-HITECH, ISO, FedRAMP, ITAR, or internal compliance policies

Skyhigh Policy N	Manage	ment					Ajmal Kohgadal shrdemo
	Access C	ontrol 🗸	DLP Policies V Encryption Policy	Configurat	ion Audit On-D	emand Scan User Lis	
Security Cor	nfigura	ation	Audit				Network security groups enabled in Security Center Enable Network security groups recommendations for virtual machines. When this setting is enabled, it recommends that
Filters Policy Status		Serv 30 F	ce Name: Microsoft Azure				network security groups be configured to control inbound and outbound traffic to VMe that have public andpoints. Network security groups that are configured for a subnet is inherined by a virtual machine network interfaces unless otherwise specified. In addition to chickling that a network security group has been
Active Inactive	80 17		Policy Name	Status	Service Name	Policy Category	configured, this policy assesses inbound security rules to identify rules that allow incoming traffic.
Canica Nama			Security contact emails is set in Security Center	 Active 	Microsoft Azure	Security Center Recom	Policy Type Config Audit Policy Status Active ~
Amazon Web Servi	67		Security Contact Phone number is set in Security Ce. Data collection enabled in Security Center	Active Active	Microsoft Azure Microsoft Azure	Security Center Recom	Edit this policy
Microsoft Azore	30		Disk encryption enabled in Security Center	 Active 	Microsoft Azure	Security Center Recom	
Policy Type			Endpoint protection enabled in Security Center	 Active 	Microsoft Azure	Security Center Record	
Config Audit	97		JIT Network Access enabled in Security Center	 Active 	Microsoft Azure	Security Center Recom	
			Next generation firewall enabled in Security Center	 Active 	Microsoft Azure	Security Center Recom	- Permissions
Policy Category			Network security groups enabled in Security Center	 Active 	Microsoft Azure	Security Center Recom	6 Required Permissions
Secure Config	31		OS vulnerabilities check enabled in Security Center	 Active 	Microsoft Azure	Security Center Recom	Microsoft A4D
Security Center Fe	17		Send email also to subscription owners enabled in Se	• Active	Microsoft Azure	Security Center Recorr	Microsoft AzureActiveDirectory
Secure Auth Inactive Entity	7		Send me emails about alerts enabled in Security Cent	er Active 	Microsoft Azure	Security Center Recorr	Microsoft Resources

"McAfee's expansion of its security controls beyond SaaS is a key way IT can empower the business to fully leverage custom applications running in public IaaS, as well as having the confidence in protecting the IaaS platforms themselves."

-David Smoley, Chief Information Officer, AstraZeneca

Activity Monitoring

Gain visibility into usage across managed and unmanaged Azure subscriptions 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 distinct categories for streamlined navigation. With McAfee, organizations can monitor:

- Usage of managed and unmanaged Azure subscriptions, who is accessing which services, the types of activities performed, their role, device type, geographic location, and IP address
- Inactive user accounts or former employees who retain access to Azure so their accounts can be deleted to reduce latent risk
- 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

Skyhigh Incident Manag	ement										Cameron Cole: shndem
		DLP Incidents	~ 1	"hreats & Anon	nalies 🗸	User Ac	tivity 🗸				
Activity from Micro	osoft Az	zure ~								() Threat	Protection Pau
										- ₹ 🗰	* • >
Activity Geo Location Collabora	tion		٩,	Aug/15/16 - No	w/6/16 ►						
O Edit Categories	Aug 15	Aug 22 Aug 29	Sep 5	Sep 12	Sep 19	Sep 26	Oct 3	Oct 10	Oct 17	Oct 24	Oct 31
ANOMALIES					000 0	00000 0	0000000	00000		000 00	
ADMINISTRATION	I Dave a	lass and	a da se	diam	II.	nH.	Inc. I		and a		diam'r.
DATA ACCESS						I.m.					
DATA DELETE											
DATA DOWNLOAD			-			Balles -			-		I to a
DATA DOWNLOAD	Inter -	litera terler				III III					
DATA SHARING	10 B	al a sur de la sur de	and a	a 1997		less and a second		-21		a dia s	
DATA UPDATES	fame -	line - seeles	desthes	http://	Internet and	Ilm	http://	see lies.	title -	all have	Info
EXTERNAL DATA SHARING	and the second	and the second	all.			Inc. Inc.	ada a			and the second	1111
LOGIN FAILURE											
LOGIN SUCCESS			1.1		1						
DEDORT EVECUTION		Illes Indias									
REPORT EXECUTION	Interaction of	Itters and a				Inter-					
SERVICE USAGE	1010a	laters and a				Inne					
USER ACCOUNT CREATION	Reason in	La THURS		diam'r	Care a	Sec. 2	12-		alle in		ALC: N
Users 2 Anomalies 0	Activities 1251						csv e		ountSas		E+ csv
ACTIVITY NAME USER		SOURCE IP COUN	TRY DEVICE TY	PE DATE/	TIME	SERVICE NAME		rebruar	y 20, 2018 8:00	PARA .	

"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

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 Loss Prevention (DLP)

Prevent unauthorized regulated data from being stored in Azure storage services. Leverage McAfee's content analytics engine to discover sensitive data stored in Azure services 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

"McAfee allows us to extend DLP outside the perimeter and into the cloud and the user experience is seamless."

---Mike Benson, Chief Information Officer, DirecTV

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

Operationalize Azure 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

\equiv Skyhigh	Policy Ma	anageme	ent						Ajmal Kohgadai shndemo
	Acces	ss Control 🚿	✓ DLP Policies ✓	Encryption Policy	Configuration Audit	On-Demand Scan	User Lists 🗸	Policy Settings 🗸	
Policy	/ Templa	ates C	verview						
Filters	Views		Q. Search						☆
Policy Type Securit Secure Secure	e ty Configurat lance/DLP a Collaboration	83 58 11	Templates by Categoria Cat	gory 🜐 (三) n 51 in use 83	Compliance/DL	P 71 in us	e 58 👬 Sec	ure Collaboration	11
Business F	Requirement								
Compli	iance	41	Business Requirement						
Unresti Secure	xtiltration ricted Access e Configuration	22 21 14	Compliance	50 in use 41	Data Exfiltration	a 28 in us	e 22	estricted Access	21
Secure Secure	e Authenticat e Collaborati e Entity	7 6 5	Secure Configuration	20 in use 14	Secure Authent	ication	7 🙀 Sec	ure Collaboration - Level 1	6
Securit	ty Monitoring	5	Inactive Entity	5	Security Monito	ring	5 🙀 Sec	ure Collaboration - Level 2	4
Recommen	ndation/Benchm	60	Document Classifica	tion Solutions 2 in use 4					
Best P Skyhig CIS Be	hactice h Recomme anchmark - L	40 28 21	Recommendation/Ber	chmark					

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
- Take manual action, such as quarantining a file
- 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:

- Data loss prevention (DLP)
- 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 Azure 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 onpremises LDAP directory services, DLP solutions, proxies, firewalls, and key management services.

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. 3752_1018 OCTOBER 2018