

McAfee MVISION Cloud for Amazon Web Services

McAfee[®] MVISION Cloud for Amazon Web Services (AWS) is a comprehensive monitoring, auditing, and remediation solution for your AWS environment

Key Use Cases

Security configuration and compliance audit

Audit the configuration of AWS 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 AWS storage services such as S3 buckets.

Unsanctioned AWS accounts discovery

Identify managed and unmanaged AWS accounts and enforce the same policies across all AWS accounts.

Policy Incid					& Anomalies V User Ac	tivity 🗸		
	ents S	ummary					Last Week 6/1-	-6/7 UTC
Service Name: AWS								Z
Incidents By Polic	(245)	Incidents By S	Scan (245)					
	y (2-40)	inoldonito by c	50011(240)					
Incidents Generated			By Status 245			Response Actions 221 24 No res	ponse/allowed	Auto 💻 Manual
\bigcirc $1 \square$		High	New Open			Notify User Notify Admin		
245	180	Med	Resolved False Positive			Quarantine		
			Archived			Delete		
			Archived Other			Delete Other		
 Saved Views 	Edit							
Saved Views Office 365 Collaborati		10 Policies	Other					Actions 🗸
Office 365 Collaborati All Services Malaware	on		Other			Other		
* Office 365 Collaborati	on	Policy Na	Other	Policy Status	Associated Services	Other Policy Type	Users	Incidents
Office 365 Collaborati All Services Malaware	on	Policy Na Unencry	Other	Active	Amazon Web Services	Other Policy Type Config Audit - API	0	Incidents J 87
Office 365 Collaborati All Services Malaware All Services DLP High Policy Status Active	Severity 221	Policy Na Unencry	Other			Other Policy Type		Incidents
Office 365 Collaborati All Services Malaware All Services DLP High Policy Status	Severity	Policy Na Unencry AM Polic	Other	Active	Amazon Web Services	Other Policy Type Config Audit - API	0	Incidents J 87
Office 365 Collaborat All Services Malaware All Services DLP High Policy Status Active Inactive	Severity 221 0	Policy Na Unencry Idate Policy Prevent 3	other	Active Active	Amazon Web Services Amazon Web Services	Ditter Policy Type Config Audit - API Config Audit - API	0	Incidents J 87 62
Office 365 Collaborat All Services Malaware All Services DLP High Policy Status Active Inactive Test Mode Deleted	221 24	Policy Na Unencry Interpretation IAM Polic Prevent 3 Unused	other	Active Active Active	Amazon Web Services Amazon Web Services Amazon Web Services	Other Policy Type Contig Audt - API Contig Audt - API DLP - API	0 0 3	Incidents J 87 62 33
Office 365 Collaborat All Services Matavare All Services DLP High Policy Status Active Inactive Test Mode	221 24	Policy Na Unencry IAM Poli Prevent : Unused VPC Flor	other S E (iii) (i	Active Active Active Active	Amazon Web Services Amazon Web Services Amazon Web Services Amazon Web Services	Other Potcy Type Contig Audit - API DLP - API Contigu Audit - API Contigu Audit - API	0 0 3 20	Incidents J 87 62 33 20
Office 345 Collaborat Al Services Matemare Al Services DurP High Policy Status Active Inactive Test Mode Deleted Incident Source Incident Source	221 24 0	Policy Na Unancry IAM Poli Prevent : Unused VPC Floi Publicab	other Control Contro Control Control Control Control Control Contr	Active Active Active Active Active Test Mode	Amazon Web Services Amazon Web Services Amazon Web Services Amazon Web Services Amazon Web Services Amazon Web Services		0 0 3 20 0	Incidents J 87 62 33 20 19 14
Mice 365 Collaborat Al Services Malavaer Al Services Malavaer Al Services Malavaer Al Services DLP High Policy Status Active Inactive Inactive Deleted Deleted Hogenization	221 24	Policy Na Unancry IAM Poli Prevent : Unused VPC Floi Publicab	other I S (B) (m) me ptrof Storage cy Volation Storing Confidential UAM users w Logs Enabled	Active Active Active Active Active	Amazon Web Services Amazon Web Services	Policy Type Contig Audt - API	0 0 3 20 0	Incidents J 87 62 33 20 19

Connect With Us



Security Configuration and Compliance Audit

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

Detect misconfigurations for:

- Elastic Compute Cloud (EC2) instances
- Amazon Machine Images (AMI)
- Storage services like S3 buckets, EBS, RDS
- Identity and access management (IAM)
- Logging and monitoring services like CloudTrail
- Network Security Groups and Virtual Private Cloud (VPC) networks

Correct misconfigured services using:

- McAfee recommended best practices derived from existing customers
- Center for Internet Security (CIS) benchmark recommendations levels 1 and 2
- Compliance recommendations for regulations such as HIPAA-HITECH, ISO, FedRAMP, ITAR, or internal compliance policies

Skyhigh Policy N	/lanage	ement							Ajmal Kohgadai shridemo
1	Access Co	antrol 🗸	DLP Policies \checkmark	Encryption Policy	Configuration	Audit On-Dema	Ind Scan User I		×
Security Cor	nfigur	ation A	Audit					Risk of unauthorize	Access to S3 Bucket ad access or loss of customer data increases ccess to S3 buckets.
Filters		Servic	e Name: Amazon Web Se	ervices				Policy Type	
								Policy Status	Active ~
Policy Status		67 P	olicies						
Active	96								
Inactive	1		Policy Name		Status	Service Name	Policy Category	- Schedule	
			Unrestricted Outbound Act	cess	 Active 	Amazon Web Service	Unrestricted Access	Runs every 24	
Service Name			World Readable S3 Bucker	ts	 Active 	Amazon Web Service	s Secure Config	- Permissions	
Amazon Web Servi Microsoft Azure	67 30		Use tags to organize AWS	resources (4)	 Active 	Amazon Web Service	s Secure Config	T en la succió	
			AWS Lambda (1)		 Active 	Amazon Web Service	s Secure Config	4 Required	I Permissions
Policy Type			Verify VPC Flow Logs		 Active 	Amazon Web Service	s Secure Config	s3:ListAIM	
Config Audit	97		Use tags to organize AWS	resources (2)	 Active 	Amazon Web Service	s Secure Config	s3:GetBuck s3:GetBuck	ketLogging
			Unrestricted Access to S3	Bucket	 Active 	Amazon Web Service	s Secure Config	s3:GetBuci	ketPolicy
Policy Category			Unencrypted S3 Buckets		 Active 	Amazon Web Service	s Secure Config		
Secure Config	31 19		Validate resources by Cost	Center	 Active 	Amazon Web Service	s Secure Config		
Security Center Re	17		Custom Policy using AWS	Lambda (Beta)	 Active 	Amazon Web Service	s Secure Config		
Secure Auth	7		Invalid Cost Center		 Active 	Amazon Web Service	s Secure Config		
Security Monitoring	5		Key rotation for customer of	created CMKs	 Active 	Amazon Web Service			
SQL Services	5		,						

"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

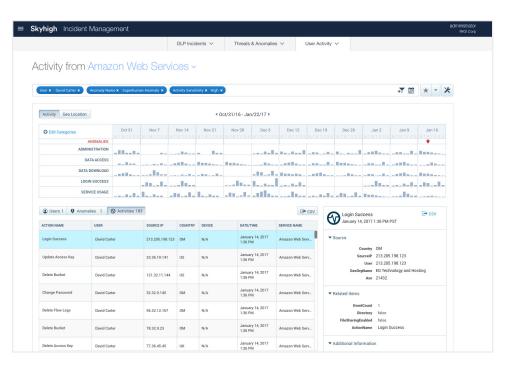
Activity Monitoring

Gain visibility into usage across managed and unmanaged AWS accounts 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 AWS accounts, 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 AWS 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



"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 and types 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.



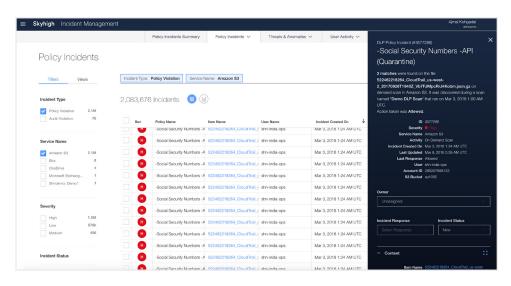
Data Loss Prevention (DLP)

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



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 AWS 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

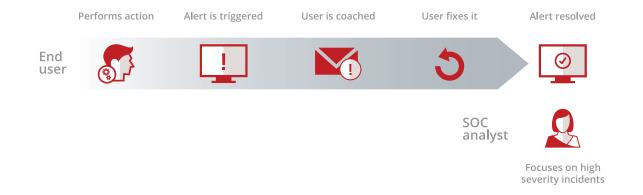
Create a custom policy with Boolean logic to conform to any corporate or regulatory requirement.

- 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

=	Skyhigh Policy Manag	ement						Ajmal Kohgadal shndemo
	Access Cont	trol V DLP Policies V	Encryption Policy	Configuration Audit	On-Demand Scan	User Lists 🗸	Policy Settings $ \smallsetminus $	
	Policy Templates	Overview						
	Filters Views	Q Search						☆
	Policy Type Templates by Category Security configurat 83 Compliance DLP 56 Security Configuration 11							
		Security Configuration	m 51 in use 83	Compliance/DL	P 71 in use	58 👬 Sec	ure Collaboration	11
	Business Requirement Compliance 41 Data Exfiitration 22	Business Requirement						
	Unrestricted Access 21 Secure Configuration 14	Compliance	50 in use 41	1 Data Exfiltration	a 28 in use	22 🔓 Unit	estricted Access	21
	Secure Authenticat 7 Secure Collaborati 6 Inactive Entity 5	Secure Configuration	a 20 in use 14	Secure Authent	Ication	7 🏟 Sec	ure Collaboration - Level 1	6
	Security Monitoring 5	Inactive Entity	5	Security Monito	ring	5 🏟 Sec	ure Collaboration - Level 2	4
	Recommendation/Benchmark Skyhigh Recomme 60	Document Classifica	tion Solutions 2 in use 4					
	Best Practice 40 Skyhigh Recomme 28 CIS Benchmark - L 21	Recommendation/Ber	ichmark					



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)

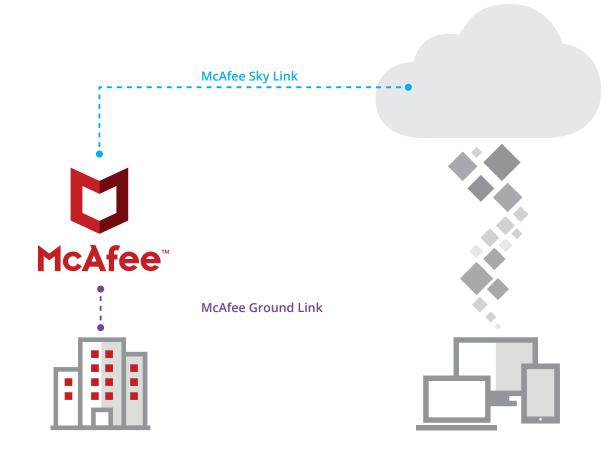
McAfee Sky Link

Connects to AWS APIs to gain visibility into AWS infrastructure and services, data and user activity, and enforces a unified set of policies across AWS services, data, and users.

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. 3776_1018 OCTOBER 2018