

McAfee MVISION Cloud for Salesforce

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

Key Use Cases

Protect regulated and sensitive data using your own encryption keys unavailable to Salesforce

Block the download of Salesforce reports and attachments to unmanaged devices

Prevent sensitive data from being added to fields, chatter posts, or uploaded as an attachment

Detect and remediate insider threats, compromised accounts, and privileged user misuse

Capture a complete audit trail of all user and administrator activity for forensic investigations

Apply rights management protection to files and attachments to protect data anywhere

							RKS Cor
		Policy Incident	s v Threats	& Anomalies V User A	Activity 🗸		
Dolloy Incidente	Cummer					Last Week 6/1-	6/7 UTC
Policy Incidents	Summar	У				Last Week 6/1-	W/ UIC
Service Name: Salesforce							ź
Cervice Neime: Salestorce							L
Incidents By Policy (245)	Incidents	s By Scan (245)					
Incidents Generated		By Status 245			Response Actions 221 24 No res	sponse/allowed A	uto 💻 Manual
$\cap I = [$		New Open			Notify User Notify Admin		
	45 High						
240	45 High 180 Med 20 Low	Resolved False Positive			Quarantine		
240	180 Med	Resolved			Quarantine		
245	180 Med	Resolved False Positive Archived			Quarantine Classify Delete		
- Saved Views Edit	180 Med	Resolved False Positive Archived			Quarantine Classify Delete		
- Saved Views Edit Collaboration	180 Med 20 Low	Resolved False Positive Archived			Quarantine Classify Delete		Actions 🗸
 ★ Office 365 Collaboration ★ All Services Malaware 	180 Med 20 Low 10 Po	Presolved False Postive Archived Other			Ouarantine Classify Delete Other	(
★ Office 365 Collaboration	180 Med 20 Low 10 Po	Resolved False Positive Archived Other	Policy Status	Associated Services	Quarantine Classify Delete	Users	Actions V
Office 365 Collaboration All Services Malaware All Services DLP High Severity	180 Med 20 Low 10 Po	Presolved False Postive Archived Other	Policy Status Active	Associated Services Salesforce	Ouarantine Classify Delete Other	Users 3	
 ★ Office 365 Collaboration ★ All Services Malaware 	100 Med 20 Low	Resolved False Positive Archived Other			Ouarantine Classify Delete Other		Incidents
Office 365 Collaboration All Services Malaware All Services DLP High Severity Policy Status Active 221 Inactive 0	10 Po	Resolved False Positive Archived Other Olicies (III) olicy Name	Active	Salesforce	Outrantino Delte Other Policy Type DLP - API	3	Incidents 87
Office 365 Collaboration All Services Malaware All Services DLP High Severity Office 354 All Services DLP High Severity Active 221	10 Po	Perconder Pate Poster Actived Other Actived Other Actived Other Actived Actived Other Actived	Active Active	Salesforce Salesforce	Outrantino Delto Other Delto Other Delto Other Delto Delto Other	3	Incidents 4 87 62
Office 365 Collaboration Al Services Malaware Al Services DLP High Severity Policy Status Active 221 Inactive 00 Test Mode 24	10 Po	Alicies (2) (a) step Name K.P Source Code K.P Protect Health Information K.P Encycyt SSN NaKa Nevent Confidential Information	Active Active Active Active	Salesforce Salesforce Salesforce Salesforce	Outstation Outstation Deleta Other Other Other DLP - API DLP - API DLP - API DLP - API DLP - API DLP - API	3 4 3 20	Incidents 4 87 62 33 20
Office 365 Collaboration Al Services Malaware Al Services DLP High Severity Policy Status Active 221 Inactive 00 Test Mode 24	100 Med 20 Low 10 Po p 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Areoload Areolo	Active Active Active Active Active	Salesforce Salesforce Salesforce Salesforce Salesforce	Policy Type DLP - API	3 4 3 20 7	Incidents 4 87 62 33 20 19
Office 365 Collaboration Al Services Malavare Al Services DLP High Severity Policy Status Active 221 Inactive 0 Test Mode 28 Deleted 0	100 Med 20 Low 10 Po 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Alicies (2) (a) step Name K.P Source Code K.P Protect Health Information K.P Encycyt SSN NaKa Nevent Confidential Information	Active Active Active Active	Salesforce Salesforce Salesforce Salesforce	Outstation Outstation Deleta Other Other Other DLP - API DLP - API DLP - API DLP - API DLP - API DLP - API	3 4 3 20	Incidents 4 87 62 33 20

Connect With Us



Key Features

Unified Policy Engine

Applies unified policies to Salesforce and all cloud services across data at rest and in transit. Leverage policy templates, import policies from existing solutions, or create new ones.

Policy Creation Wizard

Defines customized policies using rules connected by Boolean logic, exceptions, and multi-tier remediation based on incident severity.

Pre-Built Policy Templates

Delivers out-of-the-box policy templates based on business requirement, compliance regulation, industry, cloud service, and third-party benchmark.

Privacy Guard

Leverages an irreversible one-way process to tokenize user identifying information on premises and obfuscate enterprise identity.

Usage Analytics

Identifies all users and groups accessing Salesforce and reveals which users are accessing sensitive data.

User Groups

Discovers and groups users from directory services and Salesforce. User groups can be leverage for analytics and policy enforcement.

Salesforce SOC

Delivers a threat dashboard and incident-response workflow to review and remediate insider threats, privileged user misuse, and compromised accounts.

Cloud Activity Monitoring

Provides a complete audit trail of all user and admin activities to enable post-incident forensic investigations.

=	Skyhigh	Incident M	Manage	ement										,	Ajmal Kohç shr	gadai ndemo
				Policy In	cidents Sumr	nary P	olicy Incident	s ∨	Threats &	Anomalies 🗸	Use	er Activity 🗸				
	Activity from Salesforce ~															
ず 値									* •	×						
	Activity	Geo Location	Collaborat	ion			;ل∢	an/8/18 -	Apr/1/18 🕨							
	O Edit Ca	tegories		Jan 8 M T W T F S S	Jan 15	Jan 22	Jan 29	Feb 5	Feb 12	Feb 19	Feb 26	Mar 5	Mar 12	Mar 19	Mar 26	
		AN	OMALIES						9			9				
		ADMINIS	STRATION	the la	<u>. </u>	dia.	- 1 - E	il	- In-	and a	-11	- Barres	din a	dia an	-	
		DAT	A ACCESS	de.	ala 👘	al.		1.	a de la compañía de l	and the	al.		و بداد	all and	_	
	DATA DOWNLOAD										1					
	DATA SHARING DATA UPDATES													_		
							. I.		1.1.1			1.1	La La			
	DATA UPLOAD					ΞĒ.	1.1.		i h	t la s						
	LOGIN SUCCESS								1.1	1				1.1.1.1		
								-					n In an			
	SERVICE USAGE															
🕲 Users 17 9 Anomalies 2 🛞 Activities 8640							🖙 csv									
	ACTIVITY NA	ME	USER		SOURCE IP	COUNTRY	DEVICE TYPE	DA	ATE/TIME	SERVICE NAME	C	March 26, 2	018 9:02 PM			
	User Logge	d in	thyaga@th	yaga.onmicrosof.	. 24.7.23.17	US	N/A	M. Ph	arch 26, 2018 9:02 M	Salesforce	•	Source	urce Type: Cir	ud Sanica API		
	User Logged in thyaga@thyaga.onmicrosof 24.7.23.17 US N/A				N/A		March 26, 2018 8:22 PM Salesforce Salesforce Source Type: Cloud Service AP Source Type: Cloud Service AP Instance: Skyhigh .r Source Direct Skyhigh .r Source Direct Skyhigh .r				yhigh 🖛 .7.23.17 🖛					
	User Logge	d in	thyaga@th	yaga.onmicrosof.	. 24.7.23.17	US	N/A	M Ph	arch 26, 2018 7:08 M	Salesforce				03BFFDA69F9F		
								M	arch 26, 2018 7:00							

DATA SHEET

User Behavior Analytics

Automatically builds a self-learning model based on multiple heuristics and identifies patterns of activity indicative of user threats.

Account Compromise Analytics

Analyzes login attempts to identify impossible crossregion access, brute-force attacks, and untrusted locations indicative of compromised accounts.

Privileged User Analytics

Identifies excessive user permissions, inactive accounts, inappropriate access, and unwarranted escalation of privileges and user provisioning.

Guided Learning

Provides human input to machine learning models with real-time preview showing the impact of a sensitivity change on anomalies detected by the system.

Cloud Data Loss Prevention

Enforces DLP policies based on data identifiers, keywords, and structured/unstructured fingerprints across standard/custom fields, files, and Chatter posts.

Multi-Tier Remediation

Provides coach user, notify administrator, block, apply rights management, quarantine, tombstone, and delete options and enables tiered response based on severity.

Policy Violations Management

Offers a unified interface to review DLP violations, including content that triggered the violation, with remediation workflow.

Match Highlighting

Displays an excerpt with content that triggered a violation. Enterprises, not McAfee, store excerpts, meeting stringent privacy requirements.

Structured Data Fingerprinting

Fingerprints billions of unique values stored in enterprise databases and systems of record and supports exact match detection of each value.

Unstructured Data Fingerprinting

Fingerprints sensitive files and detects exact match and partial or derivative matches with a policy-defined threshold for percentage similarity to the original.

Skyhigh Incident Manag	ement			Ajmal Kohgadal shndamo	
	Policy Incidents Summary	Policy Incidents V	hreats & Anomalies V User A	DLP Policy Incident (#6878965)	
Deliev Incidente				Social Security Numbers -API	
Policy Incidents				(Quarantine)	
Filters Views	Q. Search		1 match was found on the file file99937.json on demand scan		
Filters Views	C Search			in Salesforce. It was discovered during a scan named 'Demo DLP Scan' that ran on Mar 31, 2018 1:00 AM UTC.	
Incident Type	4.893.077 Incidents			Action taken was Allowed.	
	4,050,077 Incluents			ID 6878965 Severity 📕 High	
Policy Violation 4.9M Audit Violation 927				Service Name Salesforce	
Cloud Access Poli 8	Sev Policy Name	Item Name User Nar	ne Incident Created On	Activity On Demand Scan Incident Created On Mar 31, 2018 1:20 AM UTC	
	World Readable S3 Bi	u himanshu-matchhighlig N/A	Mar 31, 2018 3:27 AM U	Last Updated Apr 2, 2018 12:35 PM UTC Last Response Allowed	
Service Name	Unrestricted Access to	himanshu-matchhighlig N/A	Mar 31, 2018 3:27 AM U	User shn-india-ops	
Amazon S3 4.9M	Unencrypted S3 Buck	e himanshu-matchhighlig N/A	Mar 31, 2018 3:27 AM U	Account ID 295207888133	
Amazon Ec2 358	M Unencrypted S3 Buck	e dinesh-skyhigh-new-te N/A	Mar 31, 2018 3:27 AM L	Owner	
Amazon Web Servi 283 Aws Identity And A 134	MFA Enabled for IAM	L proddemo N/A	Mar 31, 2018 3:27 AM U	Unassigned V	
Microsoft Azure 53	MFA Enabled for Delet	i dineshtest N/A	Mar 31, 2018 3;27 AM L		
Aws Cloudtrail 13	L IAM Policies Attached		Mar 31, 2018 3:27 AM U	Incident Response Incident Status	
Box 10 Microsoft Office 36 8				Select Response V New V	
Mercular once but	CloudTrail Logs Encry		Mar 31, 2018 3:27 AM U		
Severity	CloudTrail Integration	A dineshtest N/A	Mar 31, 2018 3:27 AM U	- Content	
	Access Logging Enab	e dineshtest N/A	Mar 31, 2018 3:27 AM U	Item Name file99937.json 📩	
High 3.6M Low 1.3M	-Social Security Numb	6 522462218264_Cloud shn-indi	a-ops Mar 31, 2018 2:29 AM U	Item Type Fie Size 106 B	
Medium 933	-Social Security Numb	e 295207888133_Cloud shn-indi	a-ops Mar 31, 2018 2:03 AM U	Created On Sep 4, 2017 3:46 AM UTC	
	-Social Security Numb	e 295207888133_Cloud shn-indi	a-ops Mar 31, 2018 1:59 AM L		
Incident Status	-Social Security Numb	e 295207888133 Cloud shn-Indi	a-ops Mar 31, 2018 1:49 AM L	1 Content Match Found	

"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

Closed-Loop Policy Enforcement

Optionally leverages policies in on-premises DLP systems, enforces policies, and registers enforcement actions in the DLP system where the policy is managed.

Contextual Access Control

Enforces policies based on user, managed and unmanaged device, and geography with coarse and activity-level enforcement.

Contextual Authentication

Forces additional authentication steps in real-time via integration with identity management solutions based on pre-defined access control polices.

Encryption

Delivers peer-reviewed, function-preserving encryption schemes using enterprise-controlled keys for structured and unstructured data.

Encryption Key Brokering

Integrates with enterprise key management solutions to broker the management and rotation of enterprise encryption keys across multiple Salesforce instances.

Information Rights Management

Applies rights management protection to files uploaded to or downloaded from Salesforce, ensuring sensitive data is protected anywhere.

•	Skyhigh						Ajmal Kohgadal shndemo
	Encryption Policy Encryption Policy 1 Overview <u>Schema</u> H	for Salesforce ^{tistory}					Deploy
	40 Objects	Actions \checkmark	Recommendations				
	Standard Object O Custom Obje Account	Pending Deployment					Best Practices Fields such as amounts, quantities, and percentages don't generally mean arything without the context of an account name, a contact name, or an opportunity description.
	Field Name	API Name	Field Type	Identifier	Encryption Type		Therefore, they should not be encrypted.
	Account Name	Account.Name	Standard	31	Searchable Encryption - Length Prese	rving	Learn More
	Phone	Account.Phone	Standard	6	Format Preserving Encryption - Phone	•	
	Fax	Account.Fax	Standard	4	Unencrypted		Add Custom Objects
	Web site	Account.Website	Standard	5	Unencrypted		
	Billing Street	Account.BillingStreet	Standard	4	Searchable Encryption - Length Prese	rving	Add Missing Field Identifiers
	Shipping Street	Account.ShippingStreet	Standard	3	Searchable Encryption - Length Prese	rving	
	Billing City	Account.BillingCity	Standard	4	Searchable Encryption - Length Prese	rving	
	Shipping City	Account.ShippingCity	Standard	3	Searchable Encryption - Length Prese	rving	
	Billing State_Province	Account.BillingState	Standard	5	Searchable Encryption - Length Prese	rving	
	Shipping State_Province	Account.ShippingState	Standard	3	Searchable Encryption - Length Prese	rving	
	Billing Zlp_Postal Code	Account.BillingPostalCode	Standard	4	Searchable Encryption - Length Prese	rving	
	Shipping Zip_Postal Code	Account.ShippingPostalCode	Standard	3	Searchable Encryption - Length Prese	rving	

Integration

=

- Data loss prevention (DLP)
- Security information and event management (SIEM)
- Secure web gateway (SWG)
- Next generation firewall (NGFW)
- Key management service (KMS)
- Access management (IDaaS)
- Information rights management (IRM)
- Enterprise mobility management (EMM/MDM)
- Directory services (LDAP)

DATA SHEET

McAfee Sky Gateway

Enforces policies inline for data in motion in real-time.

Universal mode

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

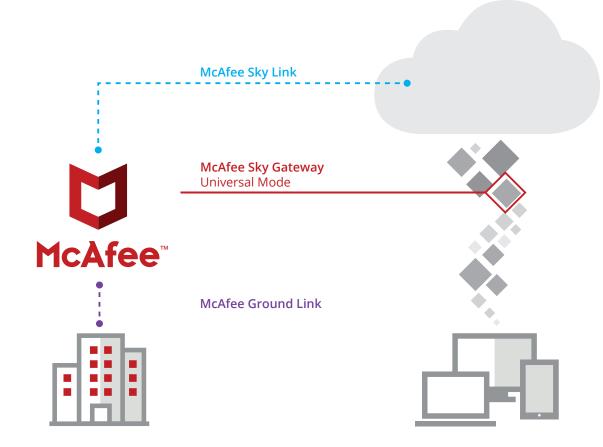
McAfee Sky Link

Connects to Salesforce 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. 3856_1018 OCTOBER 2018