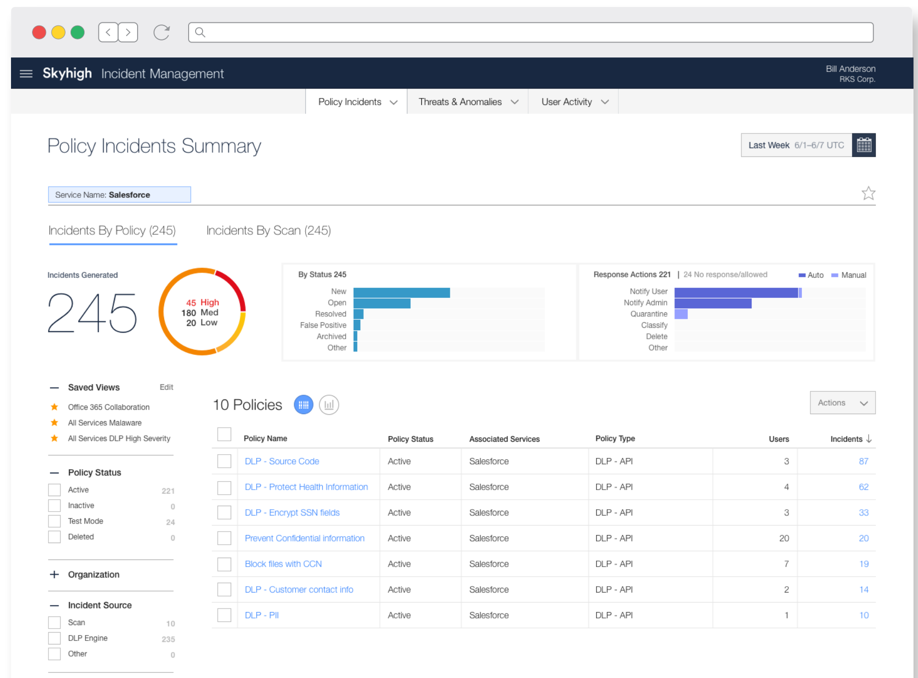
McAfee MVISION Cloud for Salesforce

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

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

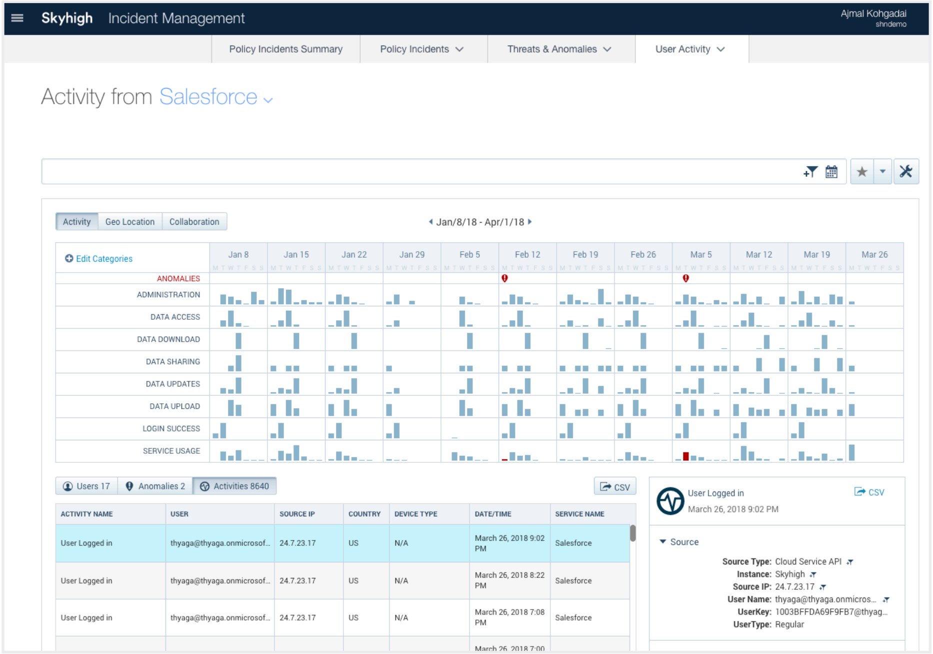
Discovers and groups users from directory services and Salesforce. User groups can be leverage for analytics and policy enforcement.

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.



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 cross-region 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.

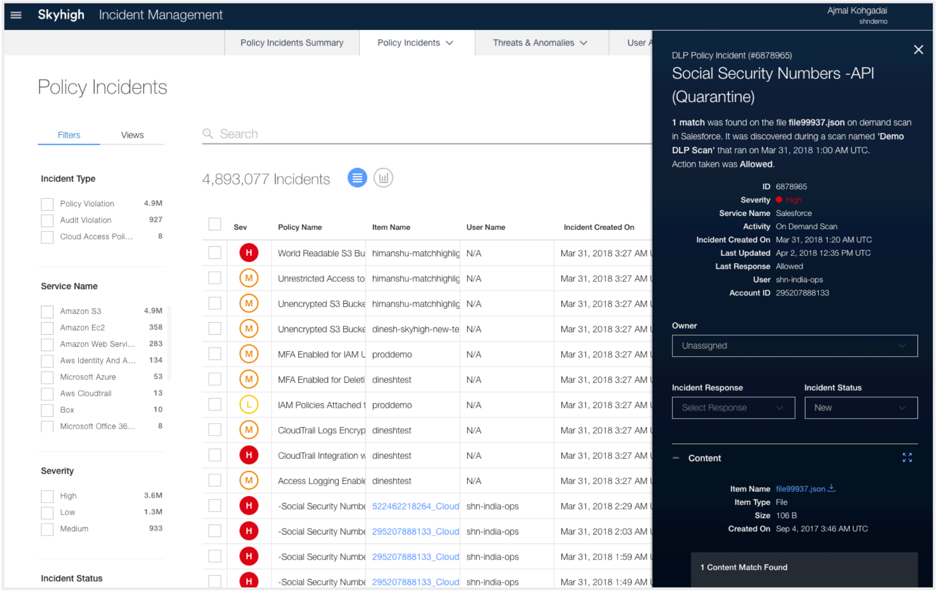
Multi-Tier Remediation
Provides coach user, notify administrator, block, apply rights management, quarantine, tombstone, and delete options and enables tiered response based on severity.

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.



> "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

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

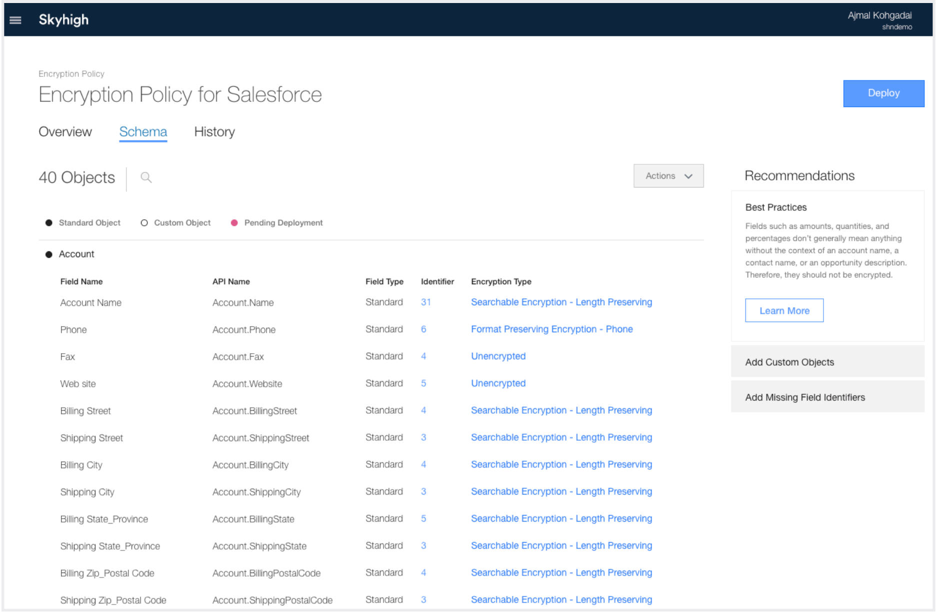
Delivers peer-reviewed, function-preserving encryption schemes using enterprise-controlled keys for structured and unstructured data.

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.



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)

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.

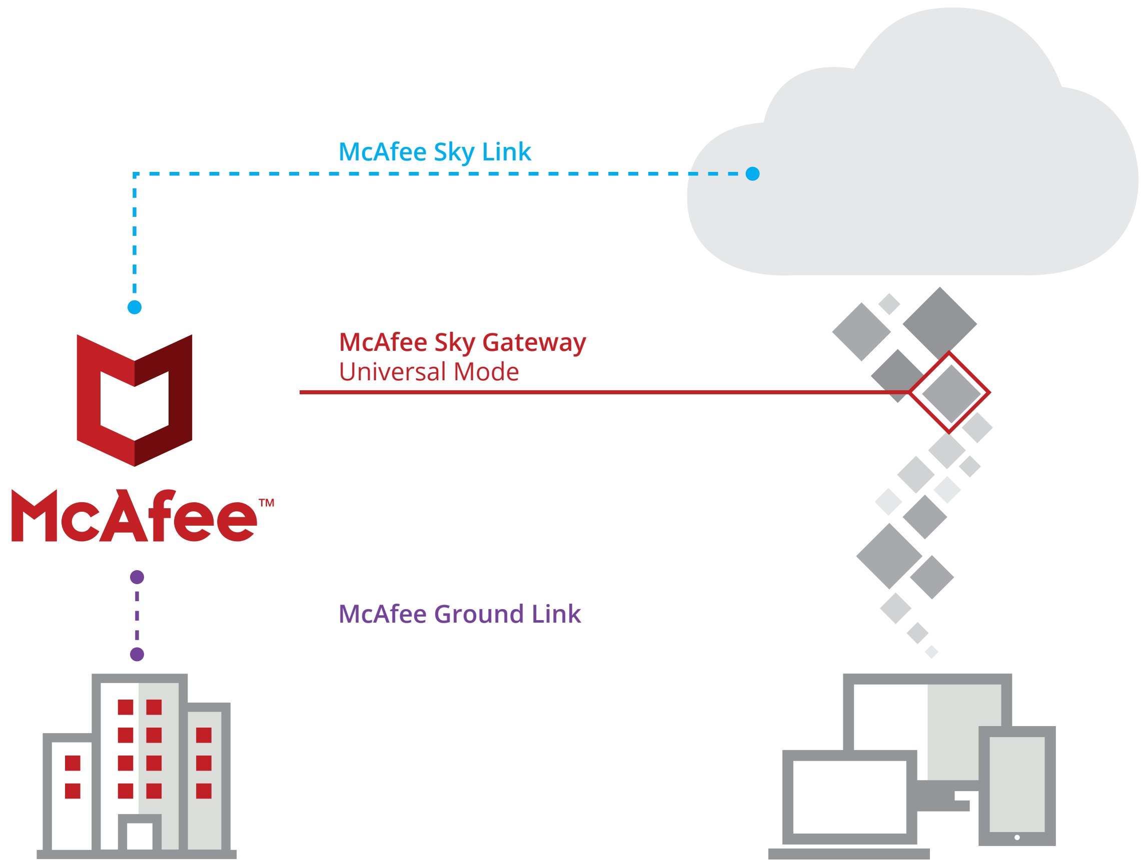
McAfee Sky Link

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 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