

McAfee MVISION Cloud for Shadow IT

McAfee® MVISION Cloud for Shadow IT provides continuous visibility into all cloud services in use and their risk, compliance and governance policy enforcement, and threat protection

Key Use Cases

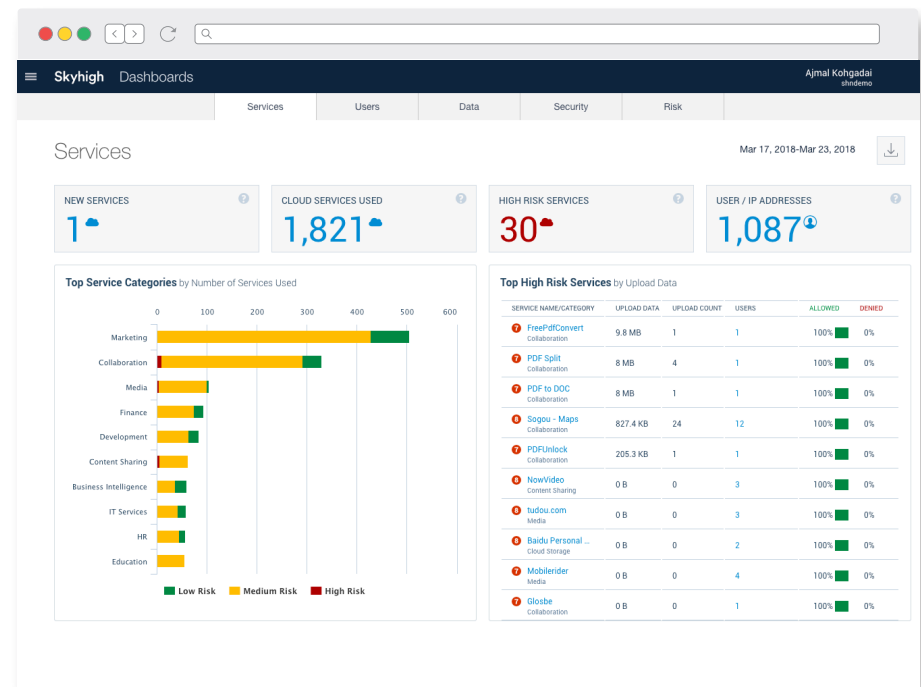
Discover all cloud services in use, their access count, security risks, and usage trends over time

Enforce acceptable-use cloud governance policies based on cloud service security risk

Expedite cloud service approval request workflow by accelerating the security assessment process

Detect and remediate policy enforcement gaps arising from proxy leakage

Gain granular visibility into user activity and block high-risk activities



Connect With Us



DATA SHEET

Key Features

Cloud Usage Discovery

Discovers all SaaS, PaaS, IaaS, and custom applications in use and visually summarizes traffic patterns, access count, and usage over time.

Cloud Registry

Provides the world's largest and most accurate registry of cloud services, including thousands of services uncategorized by firewalls and proxies.

CloudTrust Ratings

Assigns a risk rating for each service based on 50 attributes. Modify attribute and weights and add custom attributes to generate personalized ratings.

Cloud Service Governance

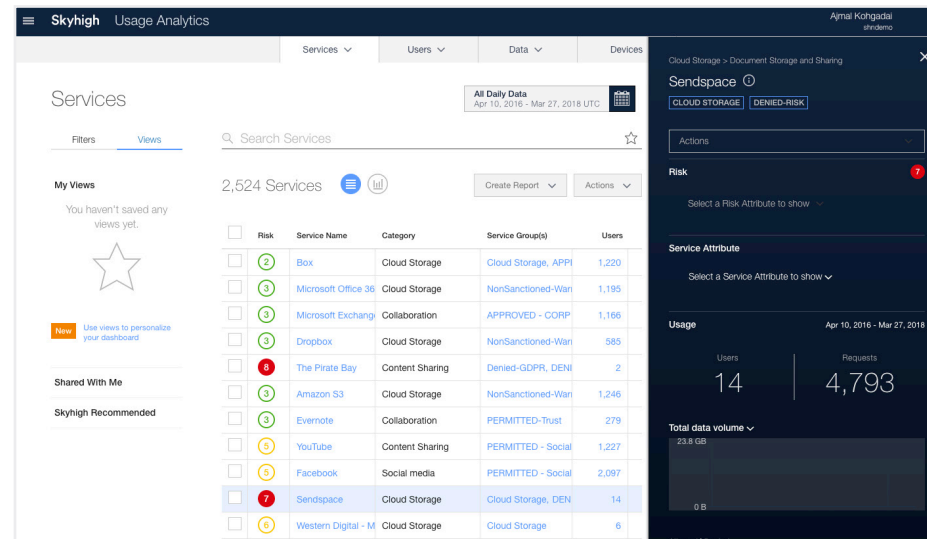
Provides a workflow to automatically or manually classify services based on risk criteria and enforces acceptable use policies through coaching and/or blocking.

Customizable Risk Scores

Provides the ability to customize and preview in real-time the risk scoring criteria for all services to match an organization's security priorities.

Cloud Enforcement Gap Analysis

Presents allowed and denied statistics and highlights gaps in cloud policy enforcement along with recommendations to close gaps.



Trend Analytics

Displays cloud service trends with 13+ months of data cross multiple categories and dimensions to identify usage patterns and facilitate governance policy creation.

“Cloud governance is about more than visibility. With McAfee, we’re creating and enforcing policies that work not only for our employees but also for IT.”

—Kevin Winter, Chief Information Officer, Booz Allen Hamilton

DATA SHEET

Cloud Service Comparison

Provides the ability to perform side-by-side comparison of cloud services across all risk attributes and usage statistics to accelerate cloud security assessment.

Customizable Views and Reports

Delivers pre-built reports and enables users to create custom views and reports, schedule periodic email reports, and download PDF, Excel, and CSV reports.

Activity Drilldown

Provides clickable drilldown to navigate from service-level upload statistics to granular user-level and event-level statistics with a complete activity feed for additional context.

Cloud SOC

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

User Behavior Analytics

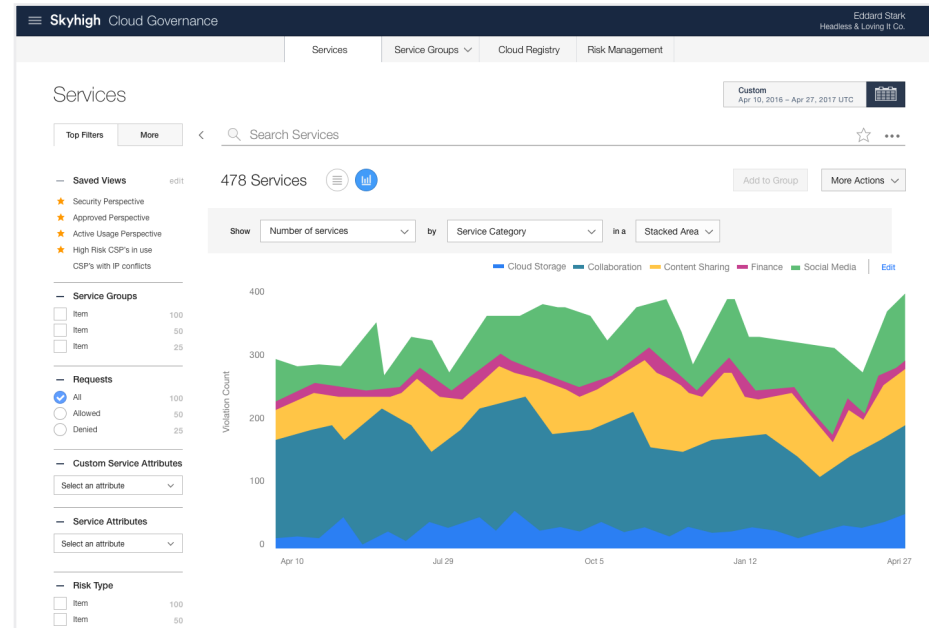
Automatically builds a self-learning model based on multiple heuristics and identifies patterns of activity indicative of user threats.

Insider Threat Detection

Leverages machine learning to detect activity signaling negligent and malicious behavior including insiders stealing sensitive data.

Threat Modeling

Correlates multiple anomalous events within a cloud service or across cloud services to accurately separate true threats from simple anomalies.



Cloud Activity Monitoring

Provides a comprehensive audit trail of all user and administrator activities to support post-incident investigations and forensics.

“When IT can bring the audit committee and executive members together and they are comfortable using the cloud, it is huge. McAfee is mitigating risk. It’s a fact.”

—Jeff Haskill, Chief Information Security Officer, AstraZeneca

DATA SHEET

Data Exfiltration Analytics

Leverages machine learning to identify traffic patterns indicative of malware or botnets exfiltrating data from on-premises systems via shadow IT cloud services.

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.

Unmatched IP Scanning

Analyzes outbound traffic to unknown destinations to identify malicious sites and services and enforces coarse-level governance policies.

Cloud Activity Control

Provides granular visibility into permitted shadow services and enforces activity control policies against high-risk activities.

Personal Account Control

Detects personal instances of sanctioned cloud services like Office 365 and AWS and enforces standardization on corporate variation of the service.

Privacy Guard

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

Role-Based Access Control

Delivers pre-defined roles with granular and customizable permissions to manage the data and product capabilities user can access within McAfee.

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)

The screenshot displays the Skyhigh Setup & Configuration interface. The top navigation bar includes 'Sanctioned Services', 'User Settings', 'Infrastructure', 'Integrations', and 'Audit Log'. The main content area is titled 'Firewall/Proxy Integration' and features an 'Edit Integration' button. Below the title, there is a 'What to do' section with instructions to approve pending changes and download files. A 'Learn how Firewall/Proxy Integration works' link is provided. The interface shows a list of integrations: Blue Coat (199 pending changes), McAfee Web Gateway (No action required), Zscaler (Sync Suspended, 60 pending changes), and Other (No action required). The Blue Coat integration details are expanded, showing 'Integration Mode: Automatic', 'E-mail Summary: Off', 'Update Process: Published URL List', and 'Last Sync: February 10, 2018 02:12 AM UTC'. A 'Approve pending changes' section for Blue Coat shows '199 Changes' and an 'Approve Changes' button. At the bottom, a 'Service Group Sync Status' table is visible.

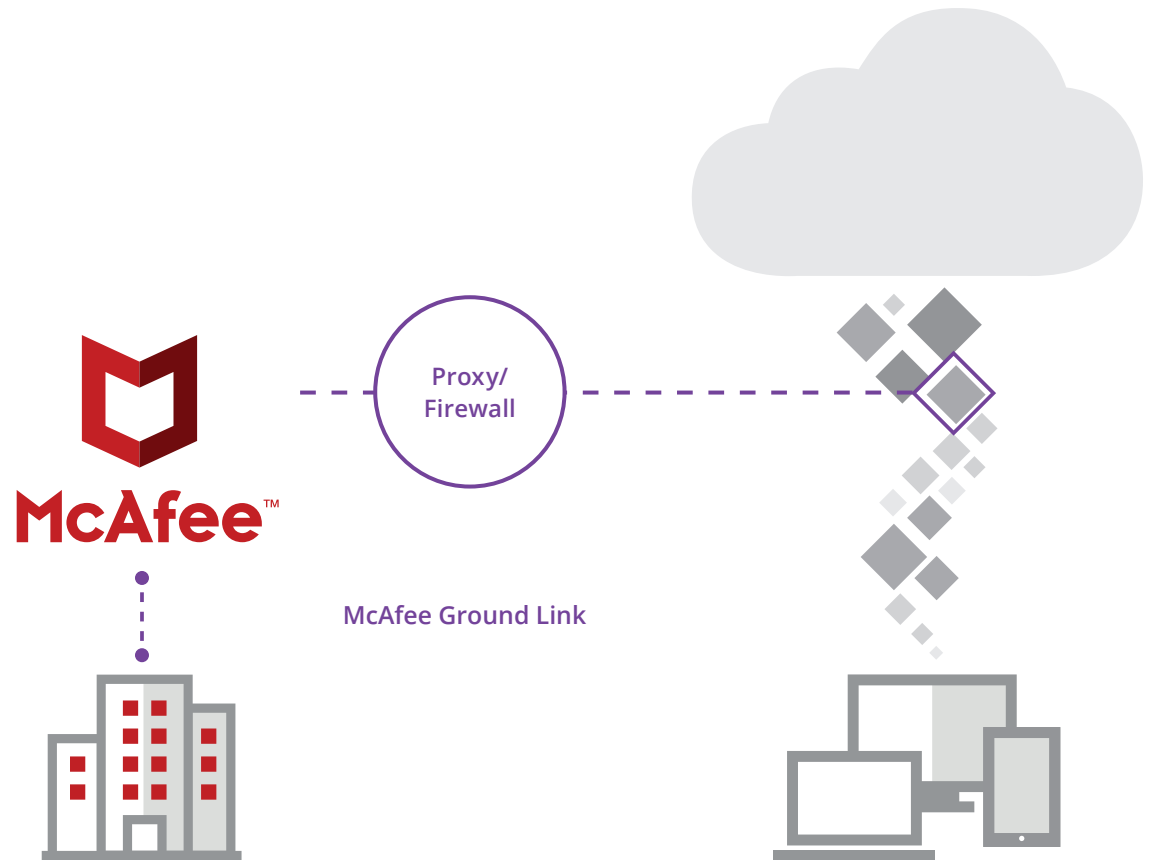
Service Group	# Services	# URLs	Changes Since Last Sync	Approvals	Actions
DENIED - Splash	5	11	--	No	--
Cloud Storage	158	176	199	Yes	Approve

DATA SHEET

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.



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. 3855_1018
OCTOBER 2018