McAfee MVISION Cloud

Cloud Security that Accelerates Business

McAfee® MVISION Cloud protects data and stops threats in the cloud across SaaS, PaaS, and IaaS from a single, cloud-native enforcement point.

Visibility

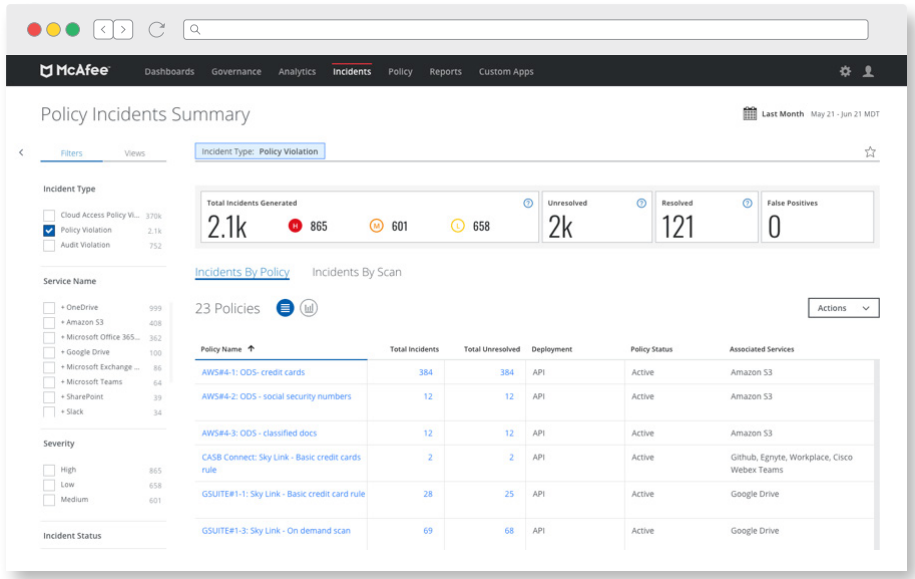
Gain visibility into all cloud use and data.

Control

Take control over data and cloud activity from any source.

Protection

Protect against cloud threats and misconfiguration.



Key Use Cases

- Enforce data loss prevention (DLP) policies on data in the cloud, in sync with your endpoint DLP.
- Prevent unauthorized sharing of sensitive data to the wrong people.
- Block sync/download of corporate data to personal devices.
- Detect compromised accounts, insider threats, and malware.
- Gain visibility into unsanctioned applications and control their functionality.
- Audit for misconfiguration against industry benchmarks and automatically change settings.
- Container optimized strategies for securing dynamic and ever-changing container workloads and the infrastructure on which they depend.

Connect With Us

The MVISION Cloud Platform

Unified Policy Engine

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

Pre-Built Policy Templates

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

Policy Creation Wizard

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

Policy Incident Management

A unified interface to review incidents, take manual action, and rollback automatic remediation actions to restore files and permissions.

Cloud Registry

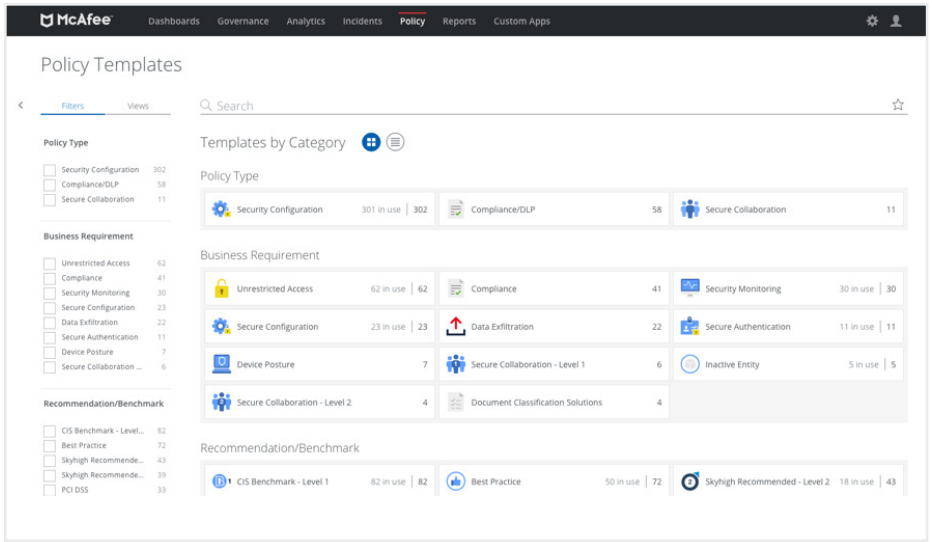
Provides the world's largest and most accurate registry of cloud services with a 1-10 CloudTrust Rating based on a 261-point risk assessment.

Privacy Guard

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

Autonomous Remediation

Coaches users to correct policy incidents, and once corrected, automatically resolves incident alerts to reduce manual review of incidents.



In-App Coaching

Coaches users in real-time within the native email, messaging, and collaboration application where the incident occurred.

AI-Driven Activity Mapper

Leverages artificial intelligence to understand apps and map user actions to a uniform set of activities, enabling standardized monitoring and controls across apps.

Multi-Cloud Protection

Enforce a uniform set of security policies across all cloud services, with the ability to associate policy violations and investigate activities, anomalies, and threats at individual services.

Visibility Into All Cloud Use and Data

Content Analytics

Leverages keywords, pre-defined alphanumeric patterns, regular expressions, file metadata, document fingerprints, and database fingerprints to identify sensitive data in cloud services.

Collaboration Analytics

Detects granular viewer, editor, and owner permissions on files and folders shared to individual users, everyone in the organization, or anyone with a link.

Access Analytics

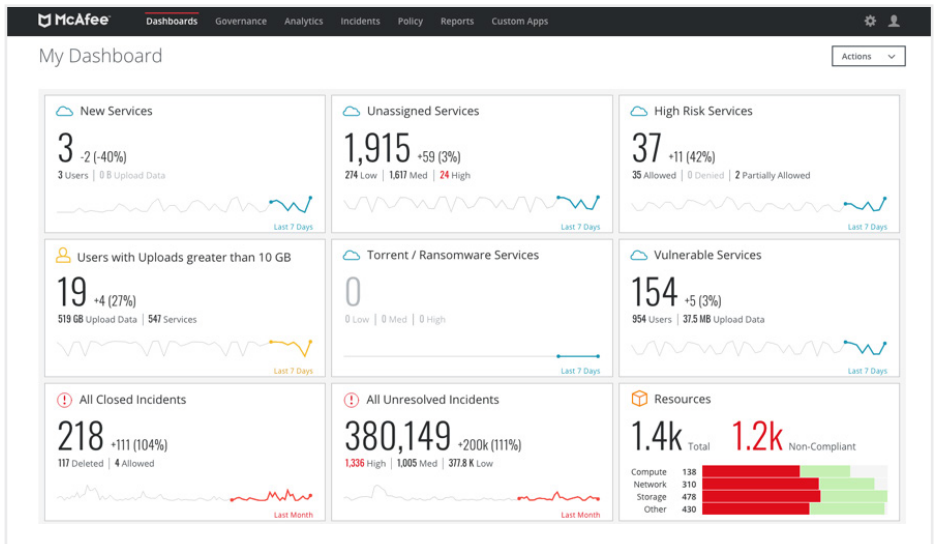
Understands access context including device operating system, device management status, location, and corporate/personal accounts.

Cloud Usage Analytics

Summarizes cloud usage including cloud services in use by a user, data volumes, upload count, access count, and allowed/denied activity over time.

Cloud Activity Monitoring

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



Control Over Data and Activity in the Cloud

Cloud Data Loss Prevention (DLP)

Enforces policies based on your own content rules to prevent data loss in cloud applications and infrastructure, across file, structured, and unstructured data. On-premises McAfee® Data Loss Prevention (DLP) content rules and policies can be synced with MVISION Cloud and applied to cloud services.

Multi-Source Control

Enforces DLP policies for data uploaded to the cloud, created in the cloud, shared with collaborators, shared cloud-to-cloud from one service to another, and downloaded from the cloud.

Multi-Tier Response

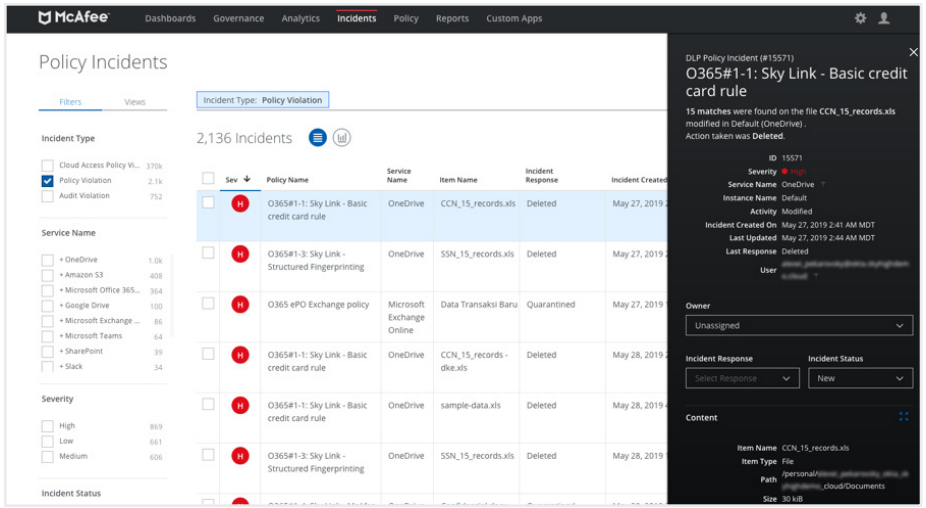
Defines policies with multiple levels of severity and enforces distinct response actions based on the severity level of the incident. Response actions, such as a DLP scan in real time, can be automatically triggered by a misconfiguration found in an audit.

Quarantine

Isolates files that trigger policies in a secure administrative location within the cloud service where it was found. McAfee never stores quarantined files.

Encryption

Protects sensitive data with peer-reviewed, function preserving encryption schemes using customer-controlled keys for structured and unstructured data.



Information Rights Management

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

Collaboration Control

Downgrades file and folder permissions for specified users to editor or viewer, removes permissions, and revokes shared links. Permissions can be based on sensitivity of data.

Connected Apps

Provides visibility into third-party applications connected to sanctioned cloud services, such as marketplace apps. Take policy-driven control over third-party apps based on specific users, applications, or access permissions.

Removal

Permanently removes data from cloud services that violate policy, to comply with compliance regulations.

Contextual Access Control

Enforces coarse allow/block access rules based on service level risk, device type, and granular activity-level controls to prevent upload and download of data.

Adaptive Authentication

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

Cloud Application Control

Granular policy for unsanctioned cloud services including the ability to allow or block activities and control access to unsanctioned tenants all from the MVISION Cloud console.

Protection Against Cloud Threats and Misconfiguration

Security Configuration Audit

Discovers current cloud application or infrastructure security settings and suggests modifications to improve security based on industry standards such as the Center for Internet Security (CIS) benchmarks. Audits can be run prior to deployment of code into infrastructure-as-a-service (IaaS) to pre-emptively mitigate risk.

Automated Configuration Remediation

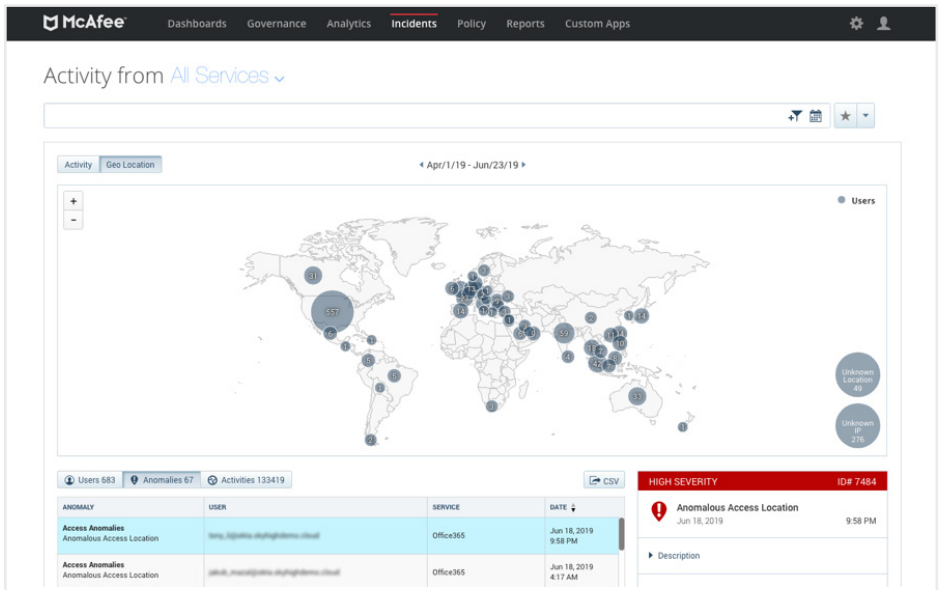
Enables a policy-based response to misconfiguration discovered in an audit to automatically change the setting, such as disabling public access for an IaaS storage bucket.

User and Entity Behavior Analytics (UEBA)

Automatically builds a self-learning model based on multiple heuristics and machine learning to identify patterns of activity indicative of user threats across multiple 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.



Account Compromise Detection

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

Insider Threat Detection

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

Privileged User Analytics

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

Malware Detection

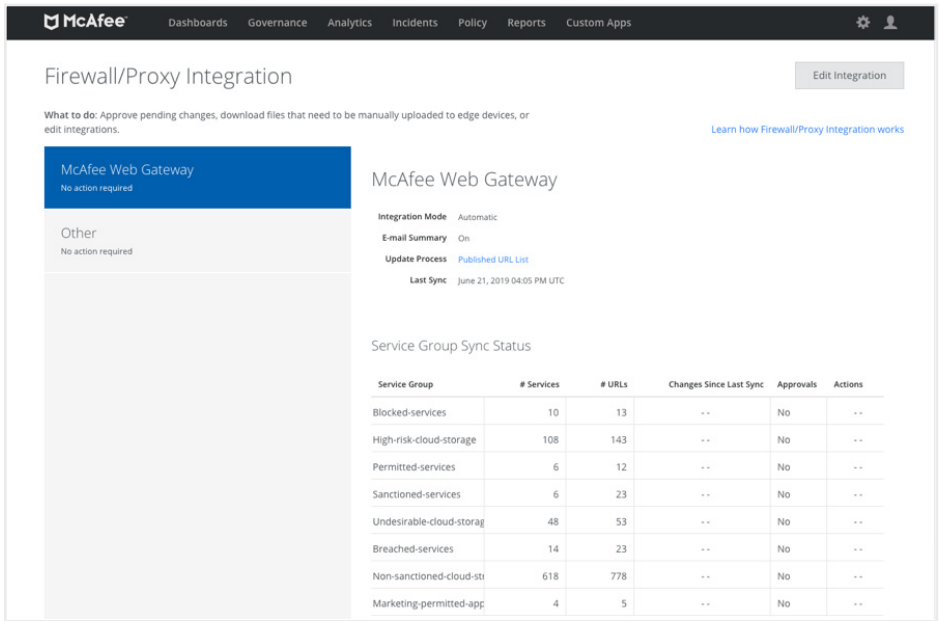
Identifies malware and detects behavior indicative of malware exfiltrating data from cloud services. Cloud services can be scanned on-demand for historical compromise and in real-time.

Malware Removal

Eliminates advanced threats by permanently neutralizing and removing malware.

Enterprise Technology Integrations

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



Deployment Modes

McAfee Sky Link

Connects to cloud service 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 Lightning Link

Establishes a direct out-of-band connection to cloud services to enforce policies in real-time with comprehensive data, user, and device coverage.

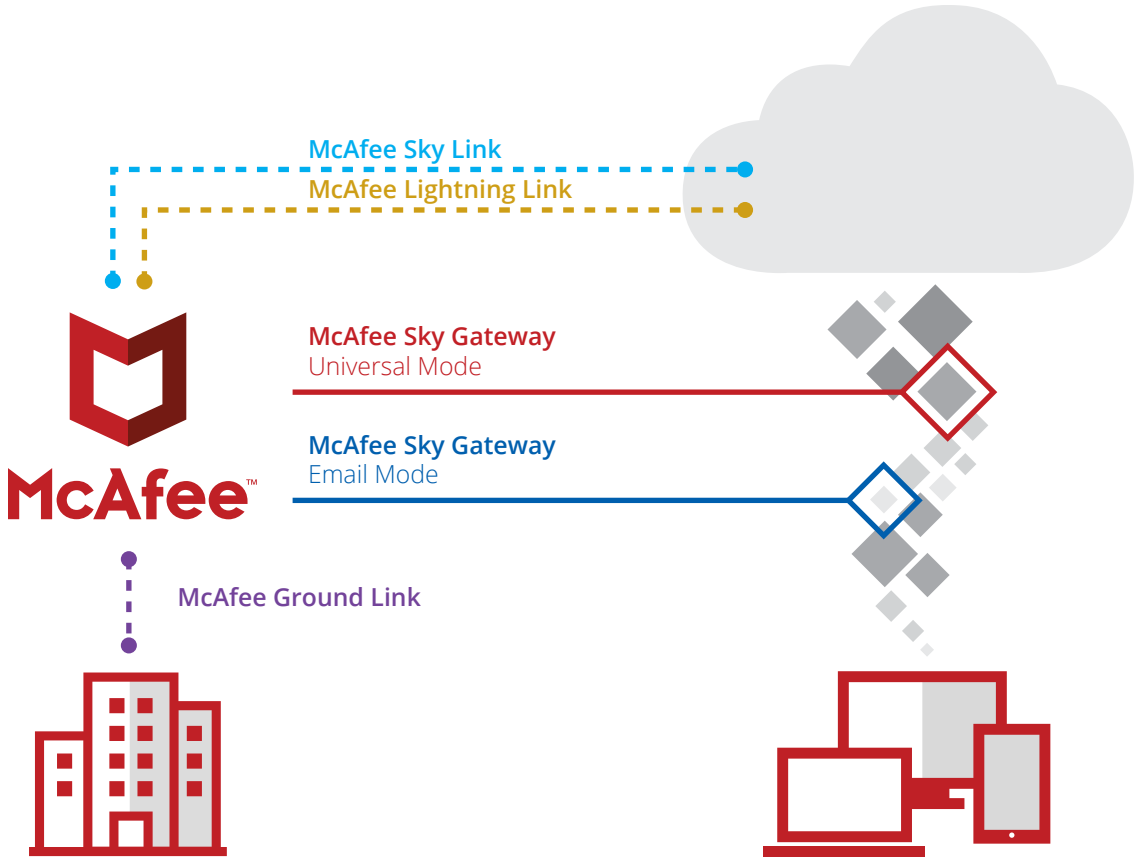
McAfee Ground Link

Brokers the connection between McAfee and on-premises LDAP directory services, DLP solutions, proxies, firewalls, and key management services.

McAfee Sky Gateway

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

- **Email mode:** Leverages native mail flow to enforce policies across all messages sent by Exchange Online inline or in passive monitoring mode.
- **Universal mode:** Sits inline between the user and cloud service and steers traffic after authentication to cover all users and all devices, without agents.

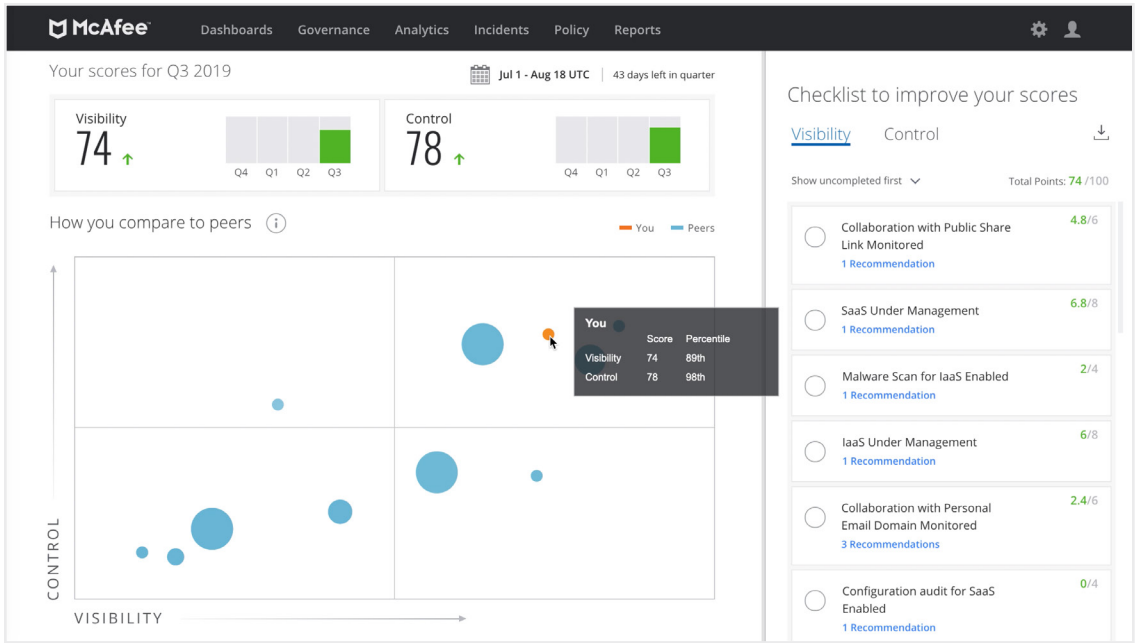


Cloud Security Advisor

The Cloud Security Advisor is a portal in the MVISION Cloud Security platform to enable customers to track their cloud security progress. It provides unique recommendations to enterprises on how to prioritize efforts to implement cloud security controls.

The Cloud Security Advisor includes:

- **Cloud Security Report:** An overview of key usage statistics focusing on key security metrics, such as cloud footprint, incidents, data at risk, and number of users.
- **Cloud Security Advisor Scores and Quadrant:** Provides scores for visibility and control, each on a scale of 100. These are based on cloud security metrics and implementation progress and compared with industry peers (of similar size).
- **Cloud Security Recommendations:** Provides enterprises with a unique set of prescriptive recommendations in a prioritized order to improve cloud security. Recommendations are weighted with points, based on their potential impact.

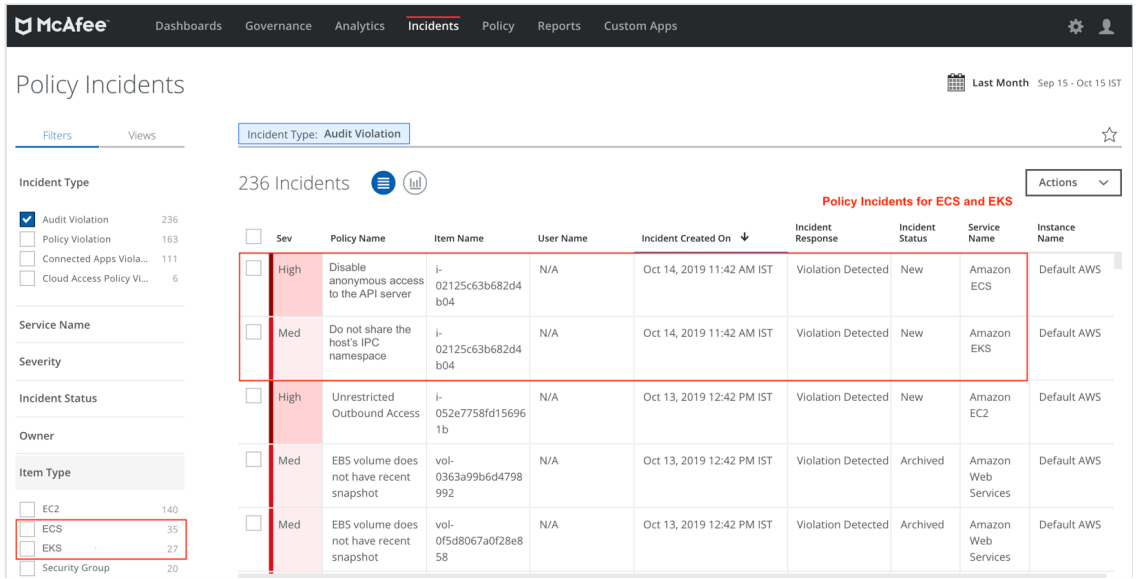


MVISION Cloud for Containers

Container workloads are the natural progression of virtualization and are optimized to take full advantage of the benefits of the cloud. MVISION Cloud Container Security provides a unified cloud security platform with container optimized strategies for securing dynamic and ever-changing container workloads and the infrastructure on which they depend.

The MVISION Cloud for Containers provides:

- **Vulnerability Assessment** for container components
  - Evaluate the code embedded in containers at build time and periodically to ensure that known risks are exposed or mitigated to reduce the opportunities malicious actors have to land in a container workload
- **Cloud Security Posture Management** for container infrastructure and orchestration systems such as Kubernetes
  - Ensure that the environment's configuration is not a source of risk
  - Ensure that the configuration of the environment does not drift over time, exposing unintentional risk
- **NanoSegmentation** for inter-container communication
  - Zero Trust: Always Verify Never Trust. Discover and monitor the behavior of network communications between container processes in a way that can deal with the ephemeral nature of containers and not reliant on external factors such as an IP address



  - Detect abnormal communications and notify or block based on user preference
  - Detect changes in communication patterns between versions of containers as the application evolves over time
  - Leverage known good configurations as a way to secure workloads, as opposed to keeping up with known bad

Learn More

To learn more about McAfee® Endpoint Security, visit us here.

To learn more about how McAfee Endpoint Security complements the McAfee product portfolio, visit:

- McAfee® MVISION Endpoint
- McAfee® MVISION product family
- McAfee® Threat Intelligence Exchange
- McAfee® MVISION Endpoint Detection and Response (MVISION EDR)
- McAfee® ePolicy Orchestrator® (McAfee® ePO™)

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com

McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO 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 © 2020 McAfee, LLC. 4482_0520
MAY 2020