McAfee Cloud Visibility—Community Edition

Gain visibility into cloud application usage, associated risk, sensitive data flow, and endpoint health (Available to McAfee DLP, Encryption, or Web Protection customers)

Key Advantages

- Available to McAfee DLP, Encryption, or Web Protection customers.
- Free service.
- Get visibility into shadow IT.
- Discover 5000+ cloud services.
- Analyze risks.
- Common risk database across web and data protection.
- Monitor sensitive data flow.
- Track endpoint health.
- Easy to activate and use.
- Leverage McAfee ePO software.
- Integrates with endpoint, web, and data protection.

Enterprise staff and in-house developers increasingly turn to cloud services—from Microsoft Office 365 (O365), Box, and Amazon Web Services (AWS)—for their productivity and collaboration benefits. As a result, unauthorized use of these cloud-based services has become so widespread that the phenomenon now has its own name—Shadow IT. However, even if select cloud services are allowed, IT and security administrators still have little to no visibility into how these services are being used, who's using them, and most importantly—what data is being uploaded and stored in them. Access to data stored in cloud services by unauthorized personnel could result in data breaches, compliance violations, and damage to the reputation of the business. To reduce risk, organizations need a way to both monitor cloud access and track sensitive data going to, coming from, and being used within cloud applications. McAfee® Cloud Visibility—Community Edition addresses this need.

Available to McAfee DLP, Encryption, or Web Protection customers, McAfee Cloud Visibility—Community Edition is a free service that provides a centralized dashboard view into cloud applications being used. With this service you can:

- Discover authorized and unauthorized cloud applications used by employees.
- Identify risk associated with cloud applications based on risk indicators.
- Monitor sensitive data flowing between users and cloud applications.
- Track endpoint health around threats, data leakage, and theft.

Why is McAfee Cloud Visibility—Community Edition Unique?

McAfee Cloud Visibility—Community Edition leverages a common risk database across web protection and data protection along with visibility into cloud application usage, associated risk, sensitive data flow, and endpoint health. It provides a true single-pane-of-glass experience with an endpoint-to-cloud view.

intel Security

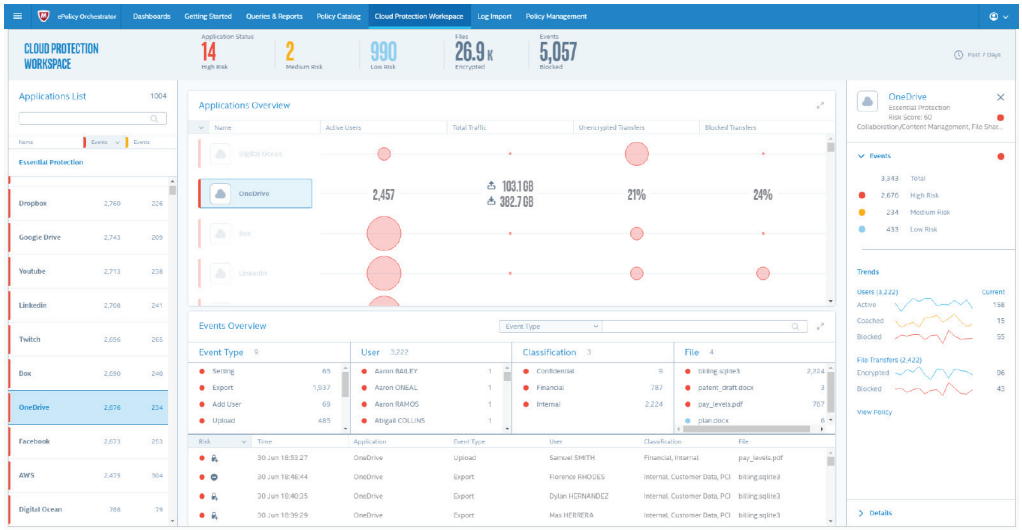

Figure 1. Cloud protection workspace.

Discover Authorized and Unauthorized Cloud Applications Used by Employees

McAfee Cloud Visibility—Community Edition can be accessed using McAfee ePolicy Orchestator® (McAfee ePO™) Cloud software that seamlessly integrates with other McAfee solutions. It comes with McAfee Cloud Protection Workspace—a key feature that provides a quick snapshot of cloud application usage. It offers a new-user experience that makes it easy for an administrator to navigate between different details against cloud applications that are used in the organization, finds the number of active users, total traffic, and encrypted and blocked file transfers against a list of cloud applications. It also provides a searchable-events overview to further investigate into certain event types (such as export, upload, and share), users, classifications, or files.

Identify Risk Associated with Cloud Applications Based on Risk Indicators

McAfee Cloud Visibility—Community Edition offers risk level based on multiple parameters such as:

- Cloud application company profile.
- Legal considerations such as end user license agreement (EULA), terms of service, and privacy policies.
- Compliance—whether or not the cloud application complies with national or international data requirements.
- Intel® Security measurements.
- Authentication and access control.
- Service reliability and security.
- User activity.

This level of visibility provides risk-assessment capability to help block threats. Cloud applications are identified and stack-ranked by their risk scores, allowing administrators to prioritize actions and identify and understand risks that they may not have been aware of previously.

Monitor Sensitive Data Flowing Between Users and Cloud Applications

Your administrator gets a 360-degree view from endpoint to cloud user activity. With details regarding how and where sensitive data is flowing, it becomes easy to plan necessary endpoint data loss-prevention policies for better control over sensitive data. The ability to monitor specific sensitive data flow (such as PCI and PII) between cloud applications and users, and correlating risk level with sensitive data-on-cloud applications is extremely useful.

Track Endpoint Health Around Threats, Data Leakage, and Theft

The constant ability to track endpoint health around presence of anti-malware, data loss prevention, and encryption technologies provides an opportunity to create a comprehensive threat defense plan. You can identify the endpoints that are protected against threats and that need anti-malware, track the endpoints that need encryption which is key to secure data in case of endpoint theft, and check which endpoints require data loss prevention technology.

Feature	Benefits
Cloud Application Discovery Valuable for McAfee Web Gateway and DLP customers.	• Granular visibility into cloud services usage such as O365, AWS, and Box. • Identify amount of data flowing to and from sanctioned and unsanctioned applications. • Observe which users are accessing what cloud applications.
Risk Assessment Valuable for Web Gateway and DLP customers.	• Leverage risk categories applied-based comprehensive logic that combines multiple factors. • High-risk, medium-risk, and low-risk categories makes monitoring easy. • Identify ways to manage risky users and devices.
Sensitive Data Distribution and Event Tracking Valuable for DLP customers.	• Avoid data loss by closely tracking endpoint activity. • Identify whether to block or allow certain activity.
Centralized Control and Monitoring with McAfee ePolicy Orchestrator Cloud	• Single-pane manageability through McAfee ePO Cloud for cloud-based SaaS applications as well as PaaS and IaaS cloud services. • Integrates with on-premises security technologies. • Centrally manage multiple user accounts across multiple cloud platforms. • Easily deploy and enforce cloud service policies to maintain regulatory and legal compliance.
Endpoint Health Check Valuable for endpoint customers.	• Identify which endpoints are protected against threats and which need anti-malware. • Track which endpoints need encryption which is key to secure data in case of endpoint theft. • Check which endpoints have data loss prevention technology.

To activate this free service visit: mcafee.com/cloudvisibility

Legal Notice:

- Customer data transferred to any McAfee Cloud Services may be stored outside the country of origin and is subject to the **Intel Security Cloud Terms of Service Agreements.**
- McAfee Cloud Visibility—Community Edition will follow **Intel Security Cloud Terms of Service Agreements**. Intel Security has sole discretion and may discontinue or modify McAfee Cloud Visibility—Community Edition at any time. For any help please refer to **www.community.mcafee.com**. Intel Security has no obligation to retain any customer data or other customer information. Refer to **Intel Security Cloud Terms of Service Agreements** Free Services section for the complete set of terms.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

Intel and the Intel and McAfee logos, ePolicy Orchestrator, and McAfee ePO are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 Intel Corporation. 2469_0217
FEBRUARY 2017