McAfee Device-to-Cloud DLP

Unified data protection

Companies of all sizes are adopting cloud-based services such as Microsoft Office 365 to give their employees greater flexibility and easier access to core business applications. On-premises data protection solutions typically don't have visibility into data in cloud services like Office 365 and can't control collaboration or sharing within the cloud. Many organizations are considering adding a separate data protection solution for their cloud environment, but in doing so, they fragment their policies, reporting, and incident response. This results in increased operational overhead and inconsistent data protection across devices, networks, and cloud services.

McAfee® Device-to-Cloud DLP provides unified data protection across endpoints, networks, and the cloud by integrating two industry leading technologies: McAfee® Data Loss Prevention (McAfee DLP) and McAfee® MVISION Cloud. The integration provides organizations with a seamless, unified data protection experience, minimizing the risk of data loss while maximizing operational efficiency.

The Inefficiency of Fragmented Data Protection Solutions

Implementing DLP in the cloud used to require rebuilding the DLP rules you created for an on-premises context again in the cloud. On-premises DLP rules also lacked the context of cloud-native collaboration or sharing with third parties from cloud services. This resulted in excessive time spent replicating pre-existing work already completed for data on devices and in the network, with potentially inconsistent policy enforcement from different DLP engines. Data loss through collaboration or shared links in the cloud was invisible to on-premises DLP.

Easily Connect and Synchronize On-Premises DLP and Cloud DLP

McAfee® ePolicy Orchestrator® (McAfee ePO™) software makes it simple to enable device-to-cloud DLP. With MVISION Cloud and McAfee ePO software working together, you can protect data in any cloud service faster than ever before, with full context of cloud-native collaboration and sharing. Connecting the two solutions can be as easy as one click and as fast as one minute.[1]

Key Benefits

Seamless Integration

- Classify your data once in McAfee ePO software, and use the classifications for device, network, and cloud contexts.
- Connecting on premises and cloud DLP is as easy as one click and can be completed in under one minute.

Consistent data loss prevention

- A shared policy and classification engine works across multiple environments.
- There's no need to make changes in more than one console.

A single view for all incident management and reporting

- Rely on centralized management for incidents across multiple environments.
- There's no need to switch consoles to view incidents and reports.

Connect With Us

The DLP rules you build in McAfee ePO software for your devices and network are pushed to MVISION Cloud, where they can be applied to any cloud service and any cloud-native traffic that bypasses your network. Your data classifications are synchronized, ensuring consistent data loss prevention on endpoints and in the cloud. All incidents are sent to McAfee ePO software, giving you a single workflow for DLP from device to cloud.

How Enterprises Gain Operational Efficiency from Device-to-Cloud DLP

Customers using McAfee ePO software have taken advantage of this integration to make it as easy as possible to enforce DLP in cloud services and simplify their operations. For example, a large food services manufacturer using McAfee DLP on its endpoints and network file shares needed to discover where its data lived in the cloud and develop a strategy to protect it. The organization started with McAfee® Web Gateway, analyzing their web traffic to determine the top user destinations and where company data was held in the cloud. As a result, the organization discovered that the vast majority of its data was actually concentrated in Microsoft Office 365.

This company's requirements for protecting data in the cloud didn't change from on premises, but contextual differences like file sharing and collaboration in the cloud presented new challenges. For example, the company needed to scan its data in Office 365 on demand, similar to on premises scanning, while also enforcing DLP rules for data moving in and out of Office

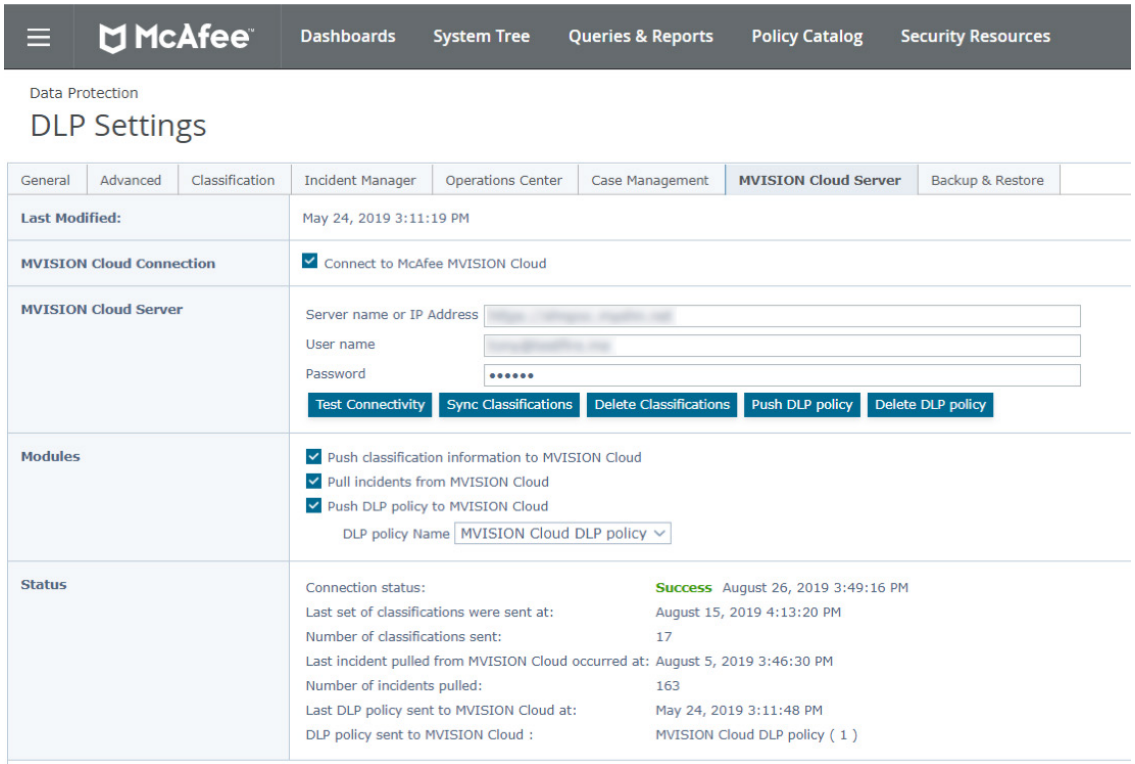

Figure 1. DLP policy synchronization to MVISION Cloud in McAfee ePO software.

365, unique to the cloud and outside of their network visibility. It was determined that a cloud access security broker (CASB) was the best solution to address these requirements and assessed multiple offerings in the market. Ultimately, the organization adopted MVISION Cloud because of the tight integration to its existing DLP rules in McAfee ePO software. From McAfee ePO software, the security team pushed on-premises data classifications to MVISION Cloud and then wrote policies

for Office 365 using those pre-built classifications. Now the organization has a single location for managing data classifications, DLP incidents from both device and cloud, along with web traffic reporting from McAfee Web Gateway—all in McAfee ePO software.

"We chose McAfee MVISION Cloud as our CASB because of the visibility it provides into where our data is going and who has access to it, as well as the ease in which we can understand the associated risk of a cloud service."

—CISO at a Global IoT Manufacturer

Centralized Incident Management and Reporting

With McAfee ePO software, you have a single-pane-of-glass experience when it comes to managing all DLP violations and reporting. There is no need to switch consoles to view incidents and generate reports, regardless of whether the DLP violations are coming from corporate devices or cloud applications. This centralized console also helps reduce complexity when it comes to auditing and regulatory compliance by providing visibility over sensitive data in multiple environments.

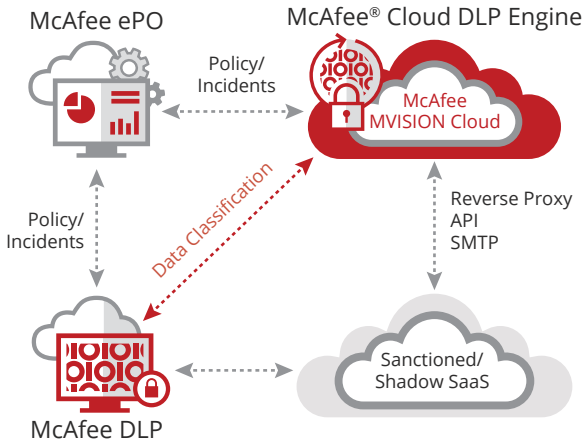

Figure 2. General architecture for McAfee Device-to-Cloud DLP incident management.

Summary

With more data being created in and sent to the cloud every day, it is more important than ever to have a set of consistent DLP policies that protect data from any leakage vectors—whether it's corporate endpoints, unmanaged devices, the network or cloud applications.

McAfee Device-to-Cloud DLP provides organizations with a seamless and unified data protection experience across multiple environments, saving time through operational efficiency and helping to minimize the risk of data loss.

Learn More

Find out more at
mcafee.com/dataprotection

1. Based on consistent McAfee internal lab testing.

McAfee
Together is power.

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