

McAfee Device-to-Cloud DLP

Lock your data down, not your business

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. Enabling such flexibility without considering the risks exposes gaps in traditional data security solutions. These gaps include a lack of visibility and control of sensitive data once it leaves the perimeter, inconsistent data loss detection across multiple environments (endpoints, networks, and the cloud), and the absence of centralized management for incident workflows and reporting, regardless where the violations occur. Many organizations have added or are considering adding a separate security solution to cover their cloud environment, but in doing so, these solutions become siloed and create additional maintenance overhead.

McAfee® device-to-cloud DLP provides universal data protection across endpoints, networks, and the cloud by integrating two industry leading technologies: McAfee® DLP and McAfee® MVISION Cloud. The integration provides organizations with a seamless, unified data protection experience, minimizing data loss risk while maximizing business agility.

Easily Connect and Synchronize On-premises DLP and Cloud DLP

McAfee® ePolicy Orchestrator® (McAfee ePO™) software makes it simple to enable device-to-cloud data loss prevention (DLP). By leveraging this centralized management and orchestration platform, organizations

can increase business efficiency and enable users to have a truly unified DLP experience. Existing DLP customers can easily extend current enterprise DLP policies to the cloud via the McAfee ePO console. Connecting the two solutions can be as easy as one click and as fast as under one minute.¹ In doing so, information from McAfee® DLP Endpoint is automatically shared with McAfee MVISION Cloud. For example, classification tags are synchronized and ensures consistent data loss detection and rule application on endpoints and in the cloud. This helps reduce the administrative burden by empowering data owners and getting them involved in corporate protection programs.

Key Benefits

Seamless upgrade

- No need to recreate policies
- Connecting on-premises and cloud DLP is as easy as one click and can happen in under one minute

Consistent data loss detection

- Common policy and classification engine across multiple environments
- No need to make changes in more than one console.

A single view for all incident management and reporting

- Centralized management for incidents across multiple environments
- No need to switch consoles to view incidents and reports

Connect With Us



Universal Device-to-Cloud Data Protection

All McAfee DLP components leverage a common policy engine across endpoints, networks, and the cloud. There's no need to recreate policies to protect the same piece of data in different environments or to make the same change in more than one console which can introduce more room for error. This common data protection policy capability is achieved via McAfee ePO software, one of the most open and proven orchestration consoles available, which currently supports approximately 47,000 organizations worldwide. An example of how a policy is created once and used universally is with Microsoft Exchange. When a data protection policy is created to protect email data in Microsoft Exchange and Exchange Online, it will be enforced on both corporate endpoints (using Microsoft Outlook) and unmanaged devices (using the Outlook web app).

Centralized Incident Management and Reporting

McAfee offers users a single-pane-of-glass experience when it comes to managing all DLP violations and reporting via McAfee ePO software. There is no need to switch consoles to view incidents and generate reports, regardless if 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.

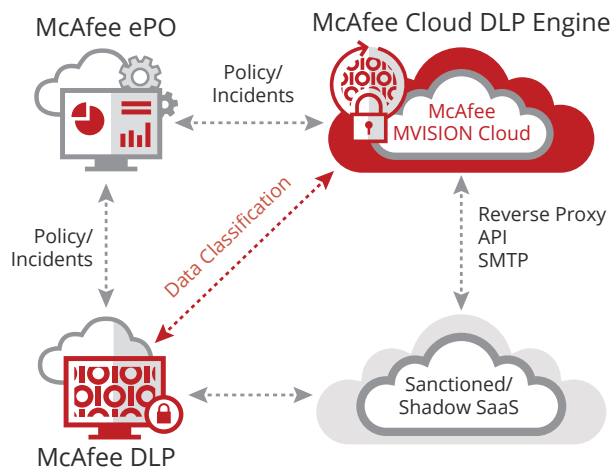


Figure 1. Device-to-cloud protection and security management.

Conclusion

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, on the network, or even in cloud applications.

McAfee device-to-cloud DLP provides organizations a seamless and universal data protection experience across multiple environments and helps minimize risk associated to data loss and maximize business agility.

1. Based on consistent McAfee internal lab testing.

Learn More

Find out more at <https://www.mcafee.com/dataprotection>



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

McAfee and 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 © 2018 McAfee, LLC. 4140_1018 OCTOBER 2018