McAfee Unified Cloud Edge

Prevent data loss and threats where work gets done—in the cloud and on devices anywhere

More than 95% of companies today use cloud services, and 83% store sensitive data in the cloud.[1] Mobile devices and laptops allow for work to occur in and outside of the network, pushing the boundary for security to a new edge defined by the cloud. Yet only 30% of companies today can protect data with the same policies on their devices, network, and in the cloud. Only 36% can enforce data loss prevention (DLP) rules in the cloud at all. Sixty percent currently have no way to stop a personal, unsecured mobile device from downloading sensitive data from the cloud, completely invisible to IT.[2] Companies need a new way to secure their data in a consistent manner as it moves between devices to the cloud and from cloud to cloud. That is the McAfee® Unified Cloud Edge.

Connect With Us

Unified Cloud Edge

McAfee Unified Cloud Edge is a vision for cloud-native security that enables consistent data and threat protection controls from device to cloud. It consists of three core technologies that are converging into a single solution:

1. **Cloud Access Security Broker (McAfee® MVISION Cloud):** Direct API and reverse proxy-based visibility and control for cloud services
2. **Secure Web Gateway (McAfee® Web Protection):** Proxy-based visibility and control over web traffic and unsanctioned cloud services
3. **Data Loss Prevention (McAfee® DLP Endpoint and McAfee® DLP Network):** Agent- and network-based visibility and control over sensitive data

These technologies work together to protect data from device to cloud and prevent cloud-native breach attempts that are invisible to the corporate network. This creates a secure environment for the adoption of cloud services and enablement of access to the cloud from any device for ultimate workforce productivity. Companies can accelerate their business through faster adoption of transformative cloud services by protecting their data and assets with a Unified Cloud Edge.

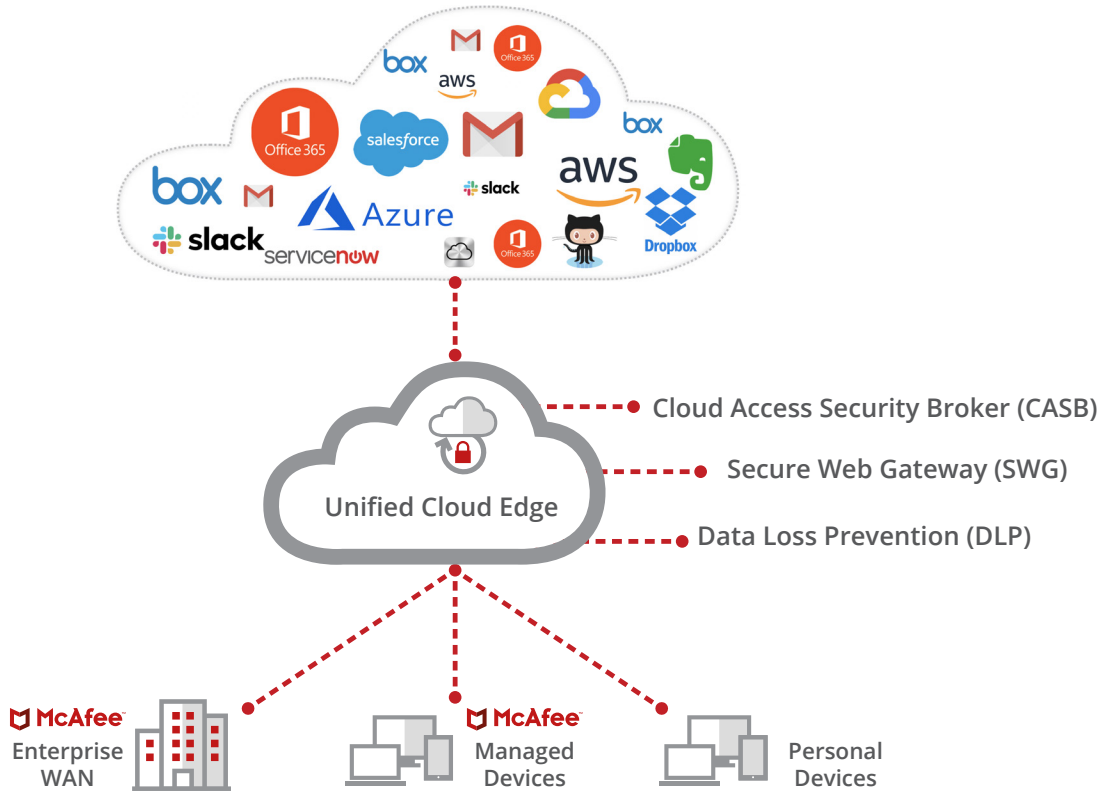

Figure 1. Simplified architecture for McAfee Unified Cloud Edge.

Convergence Delivers Simplicity and Business Speed

Adoption of these technologies individually creates a complex management challenge. All three utilize DLP at the endpoint, network, or cloud, which, when managed separately, creates significant overhead. Control over cloud service access is split inefficiently between web proxies and cloud access security brokers, with individual policies for access. Investigating any security event across this spectrum requires manually stitching together reports from individual products and repositories just to discover the path of data from a device to the cloud and often out to an external location.

Convergence creates simplicity. With McAfee Unified Cloud Edge, you can achieve:

- Consistent visibility and control over data from device to cloud
- Unified access control and threat protection for cloud services
- A single location for incident management, investigation workflows, and reporting across device, network, and cloud data protection

The way we work is shifting beyond the network to a new cloud edge. With a Unified Cloud Edge, you can enable your workforce to operate with maximum productivity while creating an efficient and consistent security management experience that keeps you running at the speed of the cloud.

Consistent Visibility and Control Over Data from Device to Cloud

As cloud adoption continues to shift data from the network perimeter to cloud provider environments, the primary control points for data protection shift. Devices can access cloud data from anywhere, and data can be created in the cloud and shared cloud to cloud without ever residing on a device. This makes the device and cloud focal points for data protection, with the network functioning primarily as a way to secure on-premises data stores.

Many companies have a well-established DLP practice on premises, where the majority of time invested has been in defining classifications for what data is sensitive to their organization, working with legal, marketing, customer support, and nearly every other department to gather data protection requirements.

Implementing DLP in the cloud used to require rebuilding these DLP classifications again in the cloud. 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.

McAfee Unified Cloud Edge streamlines the implementation of DLP in the cloud by sharing data classifications and DLP engines between all enforcement points: the device, network, and cloud. With McAfee® ePO™ software as the starting point for creating and managing classifications, you can then synchronize your classifications between on-premises DLP and MVISION Cloud, allowing you to apply them to policy for any cloud service and cloud-to-cloud traffic that would otherwise bypass your network. All devices, whether in or out of your managed network, and accessing any cloud service, can all be protected by the same DLP policies.

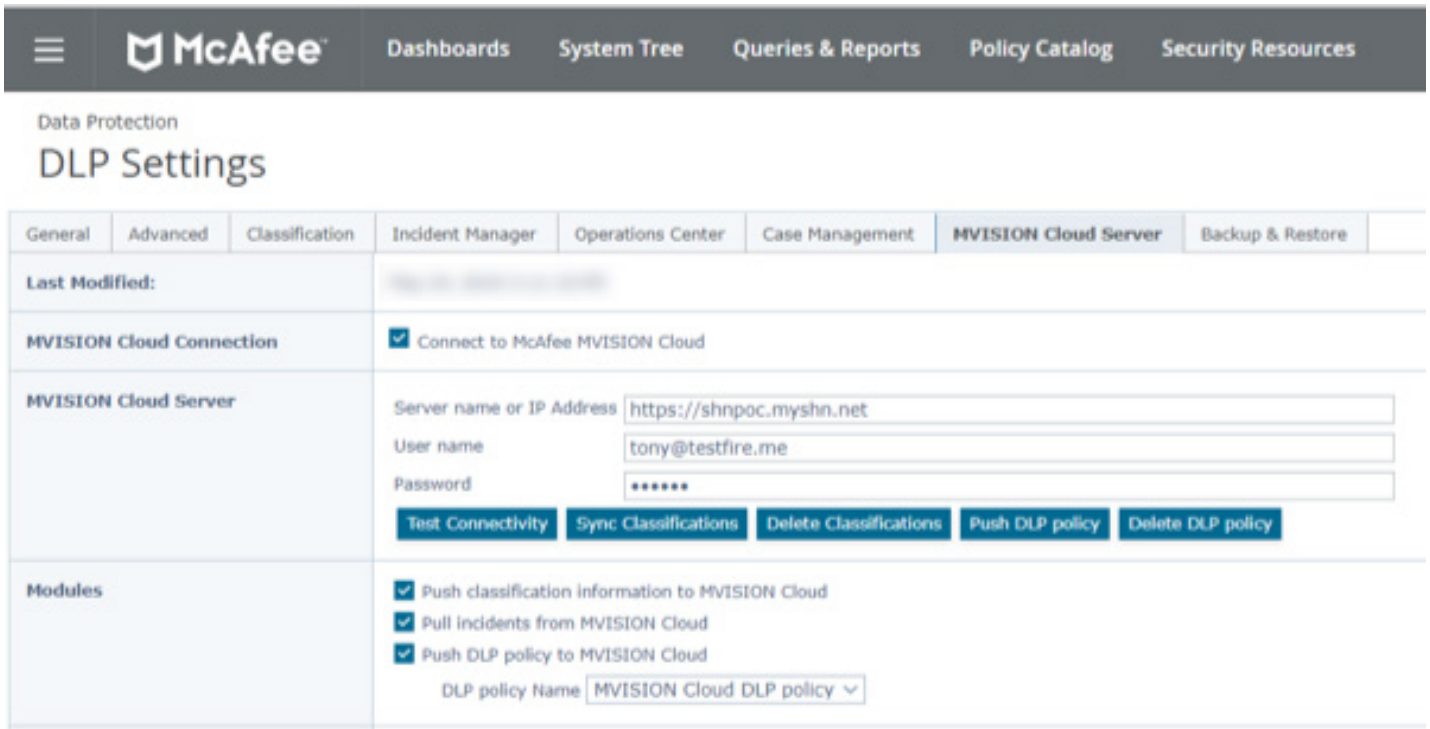

Figure 2. DLP policy push from McAfee ePO software to MVISION Cloud.

Unified Access Control and Threat Protection for Cloud Services

Cloud services come at multiple levels of risk and can be accessed by both managed and personal devices. Enterprise cloud services like Microsoft Office 365 have published APIs which allow cloud access security brokers (CASBs) to connect directly for visibility and control over data that enters the service, data created in the cloud, and data shared cloud to cloud, or anywhere externally. Personal devices can attempt to access corporate instances of Office 365, for example, and be blocked from downloading data by the CASB.

Most organizations think they use about 35 cloud services, but in reality, they use closer to 2,000.[3] That is a wide range of services to protect. However, 90% of data lives in the enterprise services IT sanctions, with 42% living in collaboration services like Office 365 alone. The remaining 10% of data lives in unsanctioned services, which are often referred to as "Shadow IT."[4] Despite holding a fraction of sensitive data, they are generally higher risk, meaning they don't meet security requirements like encrypting data at rest or achieving compliance certifications.

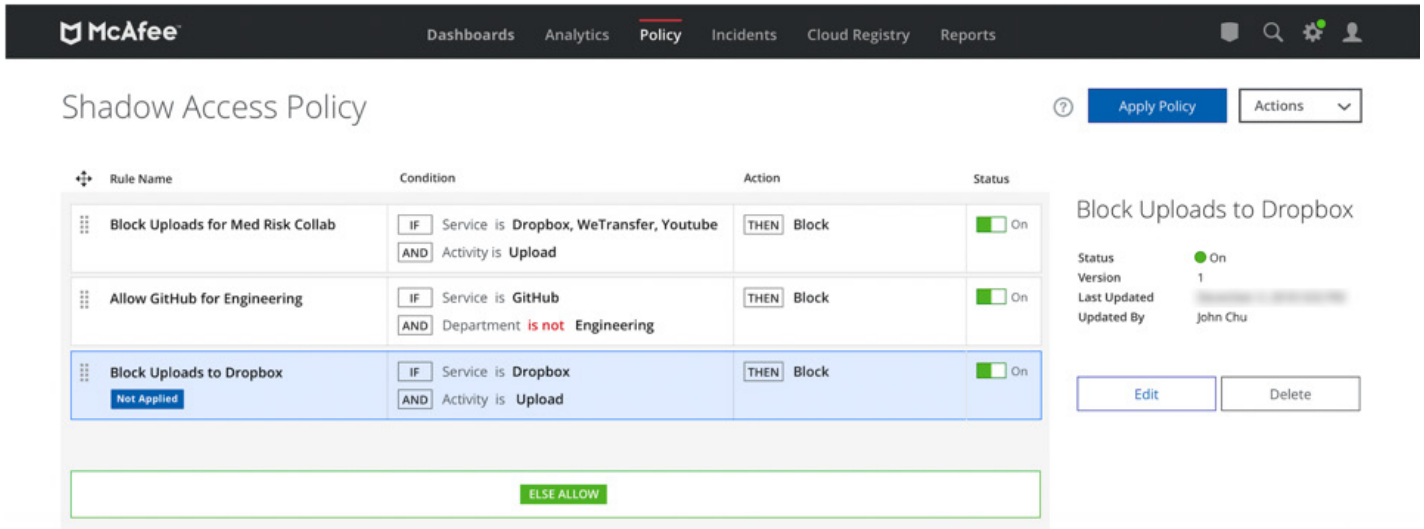

Figure 3. Shadow Access Policy in MVISION Cloud, using the McAfee Web Gateway Cloud Service to enforce the policy.

Unified Cloud Edge allows you to control access to all cloud services and protect against threats that occur within them from a single location. MVISION Cloud is the starting point, which sets access policy and detects threats within all the sanctioned services, like Office 365, that you connect to it. Zero-day malware within these services is detected and removed by a high-efficacy machine-learning based engine. From MVISION Cloud, you can also control access to unsanctioned, "Shadow IT" services, differentiating between personal and corporate accounts, and block features like the ability to upload documents.

MVISION Cloud performs its sanctioned cloud service visibility and control via API and reverse proxy. For unsanctioned cloud services, it uses the cloud-native McAfee® Web Gateway Cloud Service seamlessly from the same management console. Control over cloud access and threats is converged to a single, cloud-native user interface.

A Single Location for Incident Management, Investigation Workflows, and Reporting for Device, Network, and Cloud Data Protection

Companies that manage data protection for endpoint, network, and cloud separately have a complex setup to manage, with individual locations for daily tasks, like incident management, investigation, and reporting. Stitching these together for a comprehensive view from device to cloud is time-consuming. It's also difficult to maintain accuracy. And it's often not possible to follow breach events from start to finish as they leave different forms of evidence from each control point.

McAfee Unified Cloud Edge eliminates this challenge with a single location for incident management, investigation workflows, and reporting. All three enforcement points—device, network, and cloud—feed their event data to the same place while also sharing the same DLP engines and classifications. McAfee ePO software acts as this single location, bringing together both the creation of data classifications and the results of their policy implementation.

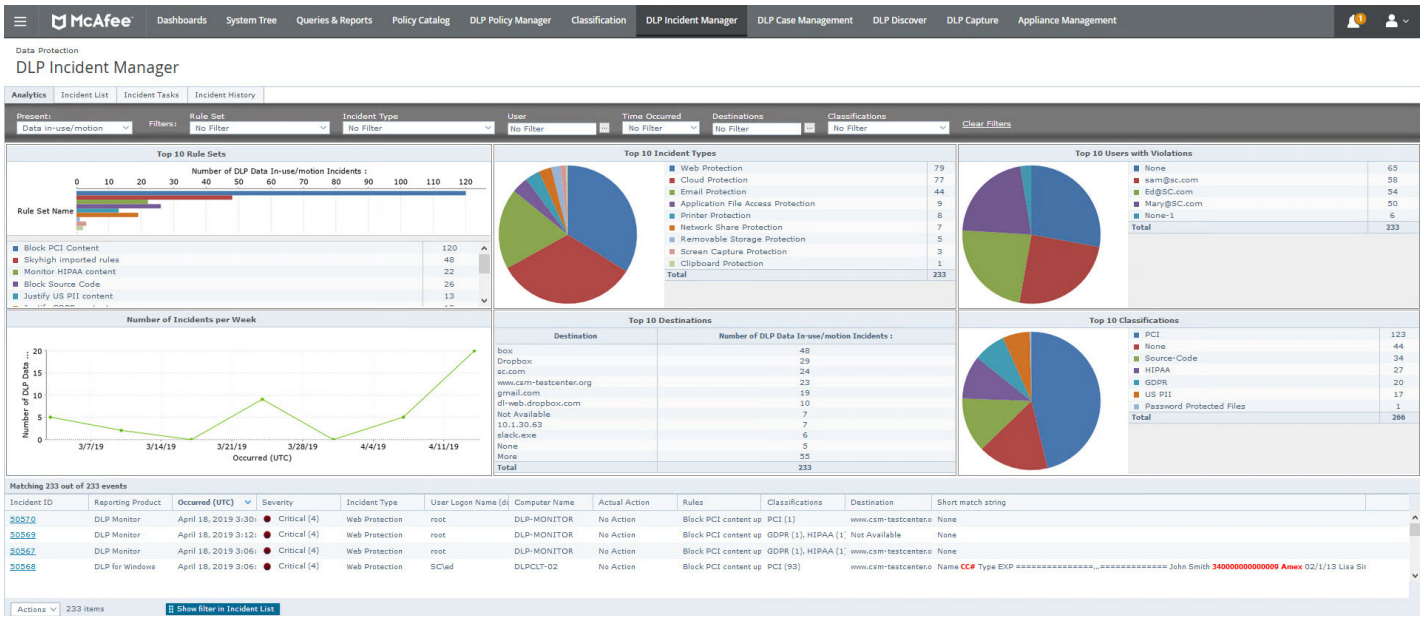

Figure 4. Unified DLP reporting for device, network, and cloud in McAfee ePO software.

Converging DLP management to one location saves time by enabling faster investigations and faster report creation. It eliminates the need to combine multiple data sources. Investigations and reports are more accurate, with fewer opportunities for mistakes made from manually combining data. Instead, data is combined automatically by McAfee ePO software. Incident data is all-encompassing and consistent, using the same DLP engines and classifications across each enforcement point and combining their event data.

Next Steps

McAfee Unified Cloud Edge can deliver consistent data and threat controls from device to cloud, allowing your organization to accelerate at the speed of the cloud while maintaining visibility and control. Reach out to McAfee to speak about how to implement McAfee Unified Cloud Edge at your organization.

If you are interested in testing individual components of the McAfee Unified Cloud Edge, visit the following:

McAfee MVISION Cloud

- Contact us for a demo
- Product details

McAfee Web Protection

- Free trial
- Product details

McAfee Data Loss Prevention

- Contact us for a demo
- Product details

Learn More

For more information visit us at **www.mcafee.com**.

1. McAfee (2018) Cloud Adoption and Risk Report
2. McAfee (2019) Cloud Adoption and Risk Report: Business Growth Edition
3. McAfee (2018) Cloud Adoption and Risk Report
4. McAfee (2019) Cloud Adoption and Risk Report: Business Growth Edition

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