SOLUTION BRIEF

McAfee Unified Cloud Edge

Protect data from device to cloud, and prevent cloud-native threats invisible to the corporate network

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 McAfee® Unified Cloud Edge.

Connect With Us

McAfee Unified Cloud Edge

McAfee Unified Cloud Edge is part of McAfee® MVISION, the cloud-native security platform from McAfee. McAfee Unified Cloud Edge enables consistent data and threat protection controls from device to cloud. It begins with three core technologies converged into a single solution:

1. **Cloud access security broker (CASB):** Direct API and reverse proxy-based visibility and control for cloud services
2. **Secure web gateway (SWG):** Proxy-based visibility and control over web traffic and unsanctioned cloud services
3. **Data loss prevention (DLP):** Agent- and network-based visibility and control over sensitive data

These technologies work together to protect data from device to cloud and to 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 McAfee Unified Cloud Edge.

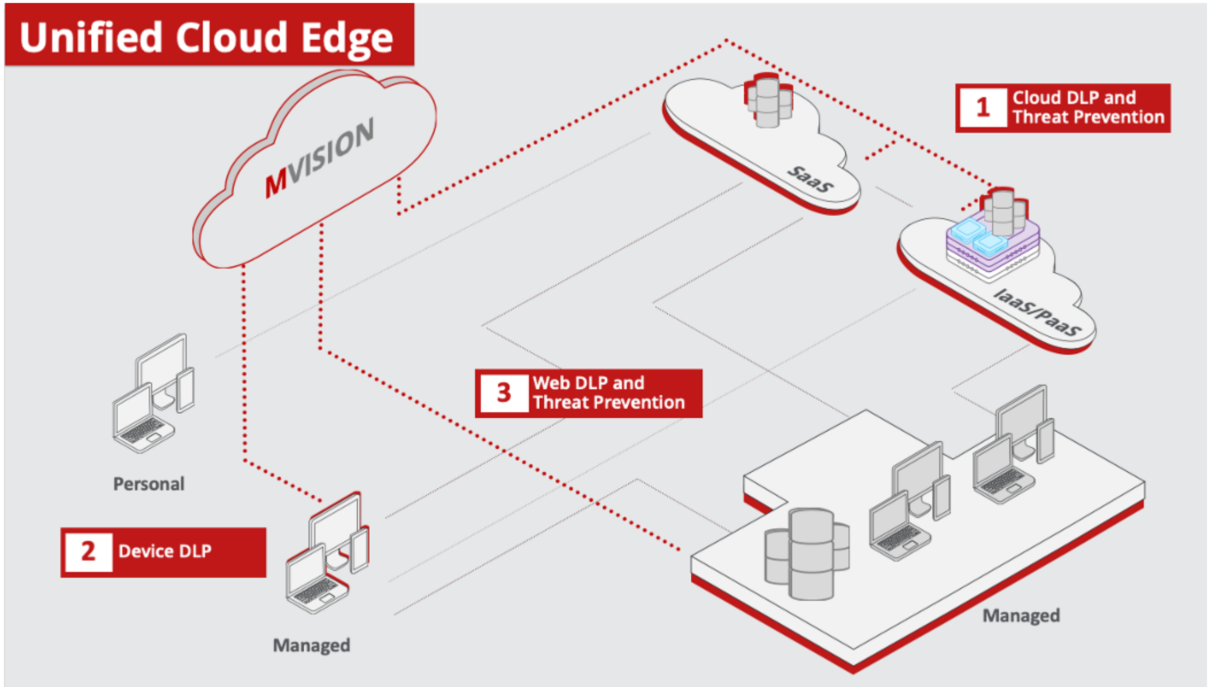


Figure 1. Simplified architecture for McAfee Unified Cloud Edge.

Convergence Delivers Simplicity and Business Speed

Adoption of these technologies individually creates a complex management challenge. All three utilize DLP—whether at the endpoint, network, or cloud—which, when managed separately, creates significant overhead. 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. Control over cloud service access is split inefficiently between web proxies and cloud access security brokers, with individual policies for access. Current architectures are grounded in hardware, with network costs and capacity limits holding back the potential of the cloud.

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 the cloud and web
- Cloud-native and direct-to-cloud architecture with enterprise scale and resilience

The way we work is shifting beyond the network to a new cloud edge. With McAfee 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.

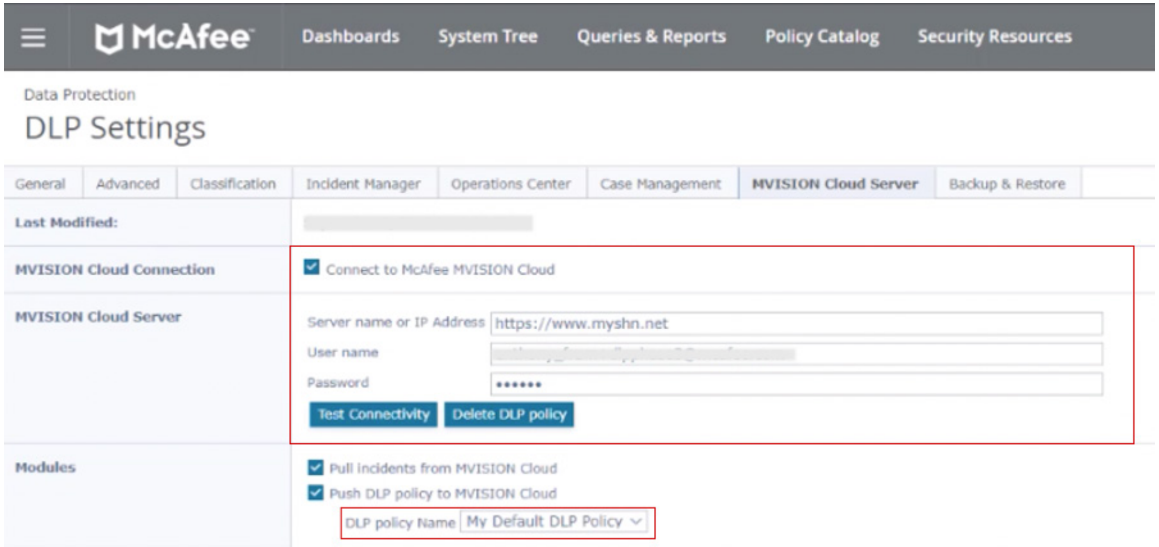
Consistent Visibility and Control Over Data from Device to Cloud

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 web traffic in the network remaining as a useful method to control unsanctioned cloud services, prevent malware, and manage general internet access.

Many companies have a well-established DLP practice on premises, where significant time has been invested 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® ePolicy Orchestrator® (McAfee ePO™) software as the starting point for creating and managing classifications, you can then synchronize your classifications between on-premises DLP and CASB, applying 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, can all be protected by the same DLP rules.



Data Protection

DLP Settings

Last Modified: [redacted]

MVISION Cloud Connection: ☑ Connect to McAfee MVISION Cloud

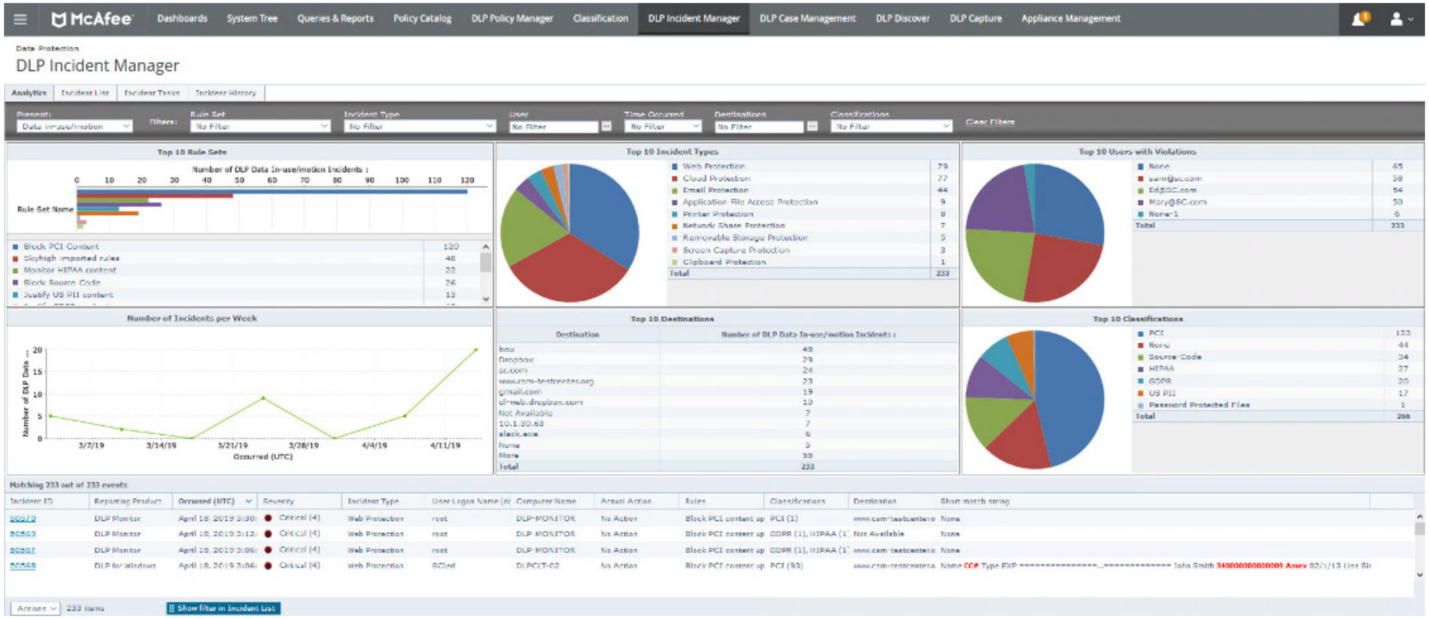
MVISION Cloud Server:
Server name or IP Address: https://www.myshn.net
User name: [redacted]
Password: ••••••

Modules:
☑ Pull incidents from MVISION Cloud
☑ Push DLP policy to MVISION Cloud
DLP policy Name: My Default DLP Policy

Figure 2. DLP classification push from McAfee ePO software to CASB.

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.



DLP Incident Manager

Present: Data in-use/motion
Filters:
Rule Set: No Filter
Incident Type: No Filter
User: No Filter
Time Occurred: No Filter
Destinations: No Filter
Classifications: No Filter

Top 10 Rule Sets

🟦 Block PCI Content	120
🟥 Skyhigh imported rules	48
🟩 Monitor HIPAA content	22
🟪 Block Source Code	26
🟦 Justify US PII content	13

Top 10 Incident Types

🟦 Web Protection	79
🟥 Cloud Protection	77
🟩 Email Protection	44
🟪 Application File Access Protection	9
🟦 Printer Protection	8
🟧 Network Share Protection	7
🟦 Removable Storage Protection	5
🟥 Screen Capture Protection	3
🟩 Clipboard Protection	1
Total	233

Top 10 Users with Violations

🟦 None	65
🟥 sam@sc.com	58
🟩 Ed@SC.com	54
🟪 Mary@SC.com	50
🟦 None-1	6
Total	233

Number of Incidents per Week

Top 10 Destinations

Destination	Number of DLP Data In-use/motion Incidents ↕
box	40
Dropbox	29
sc.com	24
www.csm-testcenter.org	23
gmail.com	19
dl-web.dropbox.com	10
Not Available	7
10.1.30.63	7
slack.exe	6
None	5
More	55
Total	233

Top 10 Classifications

🟦 PCI	123
🟥 None	44
🟩 Source Code	34
🟪 HIPAA	27
🟦 GDPR	20
🟧 US PII	17
🟦 Password Protected Files	1
Total	266

Matching 233 out of 233 events

Incident ID	Reporting Product	Occurred (UTC)	Severity	Incident Type	User Logon Name (dc	Computer Name	Actual Action	Rules	Classifications	Destination	Short match string
50570	DLP Monitor	April 18, 2019 3:30:	● Critical (4)	Web Protection	root	DLP-MONITOR	No Action	Block PCI content up	PCI (1)	www.csm-testcenter.o	None
50569	DLP Monitor	April 18, 2019 3:12:	● Critical (4)	Web Protection	root	DLP-MONITOR	No Action	Block PCI content up	GDPR (1), HIPAA (1	Not Available	None
50567	DLP Monitor	April 18, 2019 3:06:	● Critical (4)	Web Protection	root	DLP-MONITOR	No Action	Block PCI content up	GDPR (1), HIPAA (1	www.csm-testcenter.o	None
50568	DLP for Windows	April 18, 2019 3:06:	● Critical (4)	Web Protection	SC\ed	DLPCLT-02	No Action	Block PCI content up	PCI (93)	www.csm-testcenter.o	Name CC# Type EXP ===============..============= John Smith 340000000000009 Amex 02/1/13 Lisa Sh

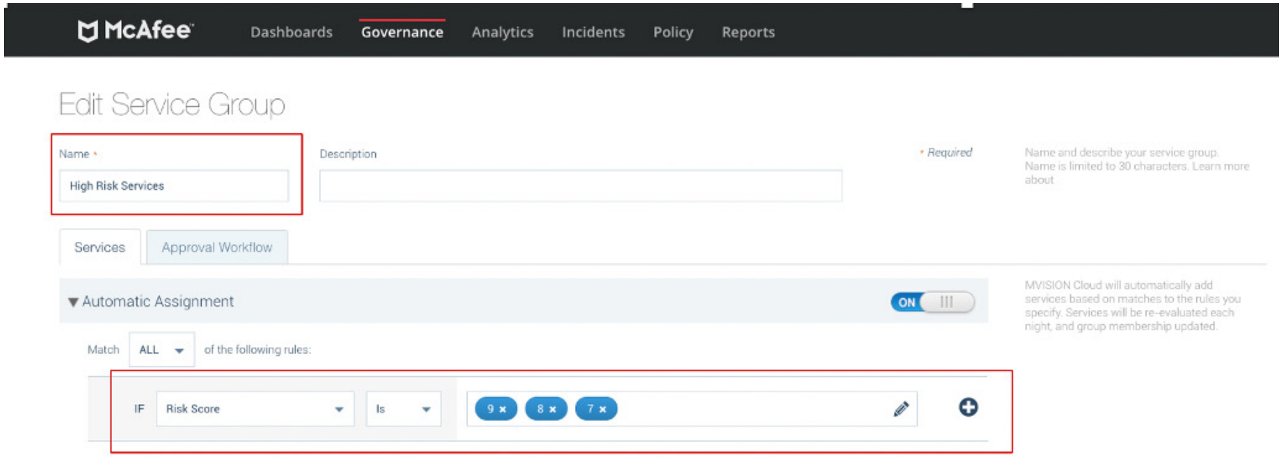
Figure 3. Unified DLP reporting for device, network, and cloud in McAfee ePO software.

Converging DLP management to one location saves time by enabling faster investigations and faster report creation, eliminating 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.

Unified Access Control and Threat Protection for the Cloud and Web

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 application programming interfaces (APIs), which allow CASBs to connect directly for visibility and control over data that enters the service, data created in the cloud, data shared cloud to cloud, or anywhere externally. Cloud-native threats that occur within these services can be detected by user and entity behavioral analytics (UEBA) that correlate activity across all of the cloud services you use. 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 that 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.



Edit Service Group

Name * High Risk Services

Description

* Required

Name and describe your service group. Name is limited to 30 characters. Learn more about

▼ Automatic Assignment ON

MVISION Cloud will automatically add services based on matches to the rules you specify. Services will be re-evaluated each night, and group membership updated.

Match ALL of the following rules:

IF Risk Score Is 9 × 8 × 7 ×

Figure 4. Converged cloud and web policy blocking all high-risk cloud services from web access.

McAfee Unified Cloud Edge allows you to control access to all cloud services and protect against threats that occur within them from a single console. From this console, you have access to the McAfee CASB and cloud-native SWG which can be combined into policies that deliver unprecedented cloud control. In Figure 4, we have a policy example that creates a grouping of all high-risk cloud services, current and future, that can be used as a restriction for web access. The result is that any high-risk cloud service will be blocked by the cloud-native SWG, preventing users from accessing these services to keep them safe from accidental data loss or malware.

Additional controls from the convergence of CASB and SWG within McAfee Unified Cloud Edge include:

- **Zero-day malware prevention:** Zero-day malware from any cloud service or website is detected and removed by our high-efficacy machine-learning based engine.
- **Remote browser isolation:** Ensure complete protection from any element of a web page reaching an endpoint by isolating browser sessions in a remote virtual environment.
- **Cloud application controls:** Control features of individual cloud services, like the ability to post or upload documents.
- **Tenant restrictions:** Differentiate between personal and corporate accounts of cloud services like Office 365, blocking personal accounts and guiding to the corporate account under your visibility and control.

McAfee Unified Cloud Edge uses a CASB to perform its sanctioned cloud service visibility and control via API and reverse proxy. For unsanctioned cloud services and the web, it uses a cloud-native SWG to enforce its policy via forward proxy. Control over cloud access and threats is converged to a single, cloud-native user interface.

Cloud-Native and Direct-to-Cloud Architecture with Enterprise Scale and Resilience

The network-centric model for security no longer provides adequate visibility and control over devices that can be anywhere, and cloud services that aren't operated by the enterprise. Access from devices to the cloud runs over web protocols, providing a layer of control for web proxies to enforce unsanctioned services policy, scan for sensitive data in motion, and block malware. Many enterprises today use hardware appliance proxies in their data center that capture traffic from remote sites over wide-area network techniques, including multiprotocol label switching (MPLS). Both the hardware and MPLS network carry cost and capacity limits. With a cloud-native architecture, the cost of hardware and MPLS routing can be eliminated, and capacity restraints replaced with the scale of the cloud.

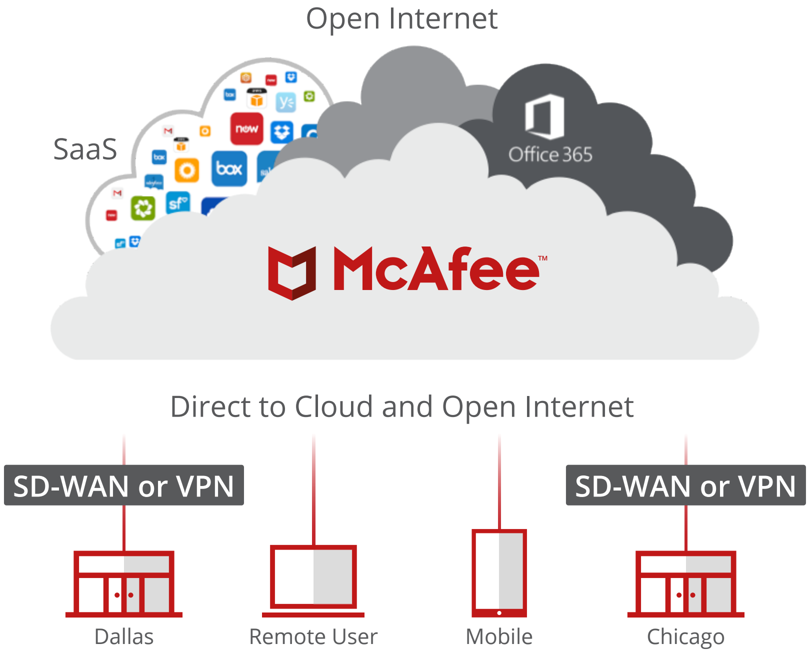


Figure 5. Simplified cloud-native architecture for web and cloud security.

Now, any device or physical site can connect directly to the cloud and open internet with increased levels of control over data and threats through McAfee Unified Cloud Edge. MPLS networks are no longer needed, with software-defined WAN (SD-WAN) or VPN technologies instead routing traffic from physical sites to the cloud. Other cloud-native proxies lack the converged contextual control of a CASB and cause significant disruption with service outages that cut off internet access. McAfee Unified Cloud Edge has a service availability of 99.999%, meaning minimal downtime for your organization. Your architecture is cost-effective, resilient, and upgraded to protect data and prevent threats in our cloud-first world.

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.

- 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 (2020) Enterprise Supernova: The Data Dispersion Cloud Adoption and Risk Report
3. McAfee (2018) Cloud Adoption and Risk Report
4. McAfee (2019) Cloud Adoption and Risk Report: Business Growth Edition

McAfee™

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

McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Learn more at mcafee.com. No online connected systems can be absolutely secure.

4422_0220
FEBRUARY 2020