SOLUTION BRIEF

McAfee MVISION Unified Cloud Edge

The SASE security service empowering cloud and network transformation

McAfee® MVISION™ Unified Cloud Edge is the security fabric between your workforce and their resources that enables fast direct-to-internet access by eliminating the need to route traffic through your data center for security. Data and threat protection are performed at every control point in a single pass to reduce the cost of security and simplify your management.

Connect With Us

Is Your Digital Transformation as Fast and Secure as It Should Be?

We are in the midst of digital transformation that is reaping tremendous benefits, but also presenting several substantial challenges.

- As the workforce adopts a "Work from Anywhere" model, traditional VPN and MPLS-connected branch users are only able to access their critical web and cloud resources by routing back through their traditional network infrastructure, which is increasingly congested and slow.
- Opening access to corporate resources through unmanaged mobile devices means that data is being accessed in new ways that are missed by perimeter security.
- Traditional security tools are not able to cope with the 630% spike in advanced cloud-based and web-based threats.[1]

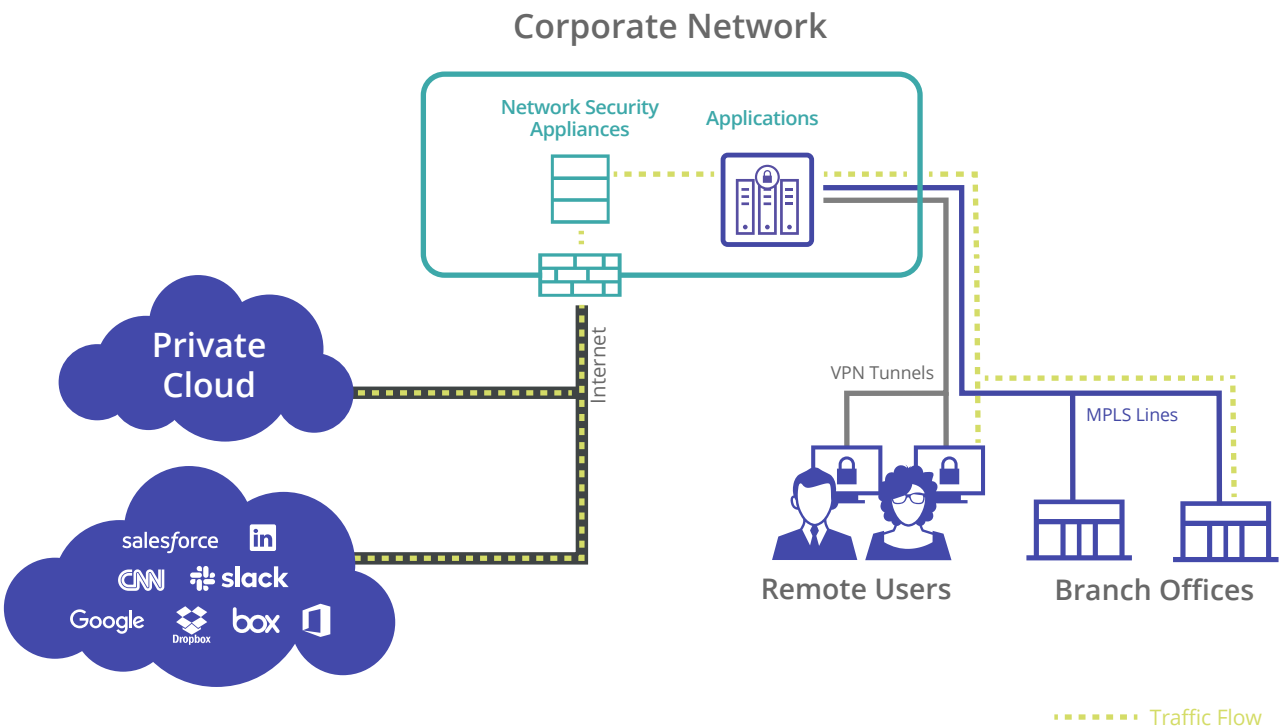


Figure 1. Traditional network architecture

1. McAfee: "Cloud Adoption and Risk Report: Work from Home"

Take the Fastest Route to SASE with MVISION Unified Cloud Edge

MVISION Unified Cloud Edge is the SASE security fabric that delivers data and threat protection to any location, so you can enable fast and secure direct-to-internet access for your distributed workforce.

As digital transformation creates a shift for organizations to "Work from Anywhere," enabling fast and secure access for your remote workers to your internal apps and data is crucial. With access delivered from a secure service edge, you can protect users and data in new ways; from full visibility over remote worker traffic, to unmanaged device control, and cloud-native activity monitoring.

Unlock direct internet access by seamlessly routing office locations and remote users through McAfee's cloud-native Hyperscale Service Edge—which processes your traffic for unauthorized access, data risk, and threats from anywhere in the world—and then directly to the cloud, eliminating the need to route traffic through your data center and back out.

- By transforming to a cloud-delivered SASE that converges connectivity and security, organizations are then able to reduce cost and complexity while increasing the speed and agility of the workforce.
- A SASE architecture delivers complete visibility and control over data at every policy decision point, whether it be at the endpoint, through the web, or in the cloud.
- Threat protection controls that adapt to changes in risk and context allow for protection against even the most sophisticated cyberattacks and data loss.

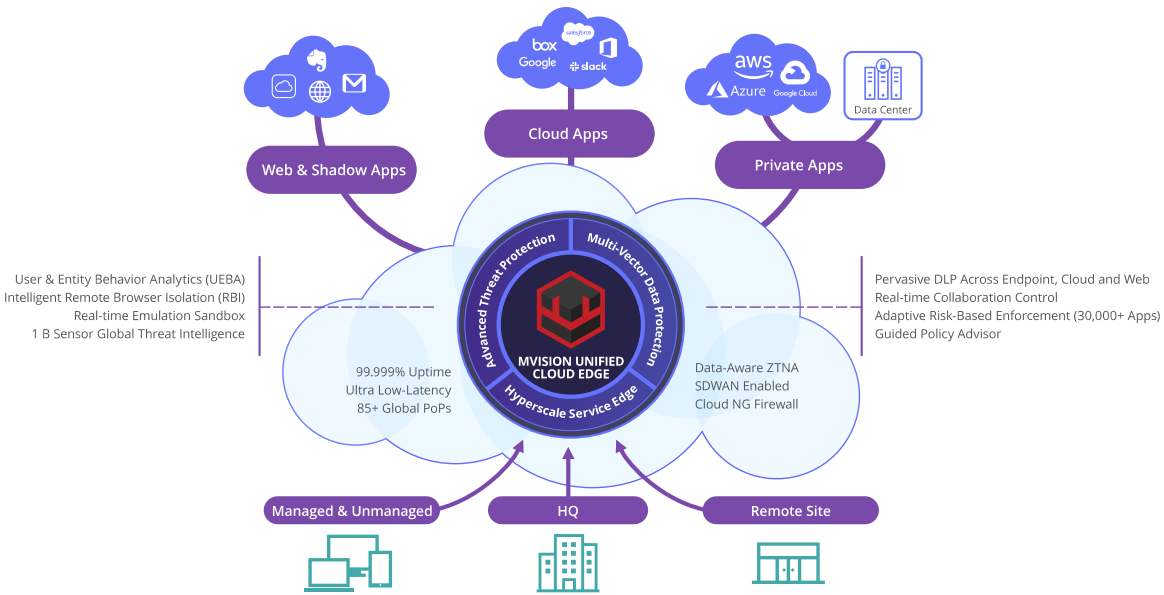


Figure 2. MVISION Unified Cloud Edge

SASE

Secure Access Service Edge (SASE)—defined by Gartner[2]—is a security framework for enabling secure and fast cloud adoption and helping ensure both users and devices have secure cloud access to applications, data, and services anywhere, any time. SASE converges networking and network security into a single, cloud-delivered offering to support the needs of digital business transformation, edge computing, and workforce mobility, while minimizing the impact on security, performance, complexity, and cost.

To learn more about SASE, click here.

2. Gartner: "2021 Strategic Roadmap for SASE Convergence"

Deliver SASE with MVISION Unified Cloud Edge Hyperscale Service Edge and SD-WAN

SD-WAN can transform your network with greater simplicity, cost effectiveness, and user productivity by simplifying and accelerating the connections between users and cloud resources. However, unless it is coupled with a ubiquitous cloud security platform, traffic must still be forced back to your data center. But doing this slows down productivity and doubles down on an already outdated architectural model.

McAfee's Hyperscale Service Edge is the cloud-native security fabric between your workforce, WAN infrastructure, cloud services, and the web. Additional capabilities of our service edge include:

- Over 60 Points of Presence (PoPs) peered with content providers at global Internet Exchange Points (IXPs).
- The capability to provide the fastest access to cloud applications possible, often outperforming direct-to-cloud access.
- A simplified architecture that empowers you to enable the access patterns of your workforce—anywhere, any application, and from any device.
- Operates at 99.999% uptime to keep your workforce connected without disruption.

Converge SD-WAN and ZTNA with our cloud-delivered service edge to simplify your technology stack so you have less to manage. Enjoy low latency and unlimited scalability with a global cloud footprint and cloud-native architecture. By bringing together MVISION Unified Cloud Edge with SD-WAN in a seamlessly integrated SASE solution, organizations can reduce complexity and costs while delivering a blazing fast user experience.

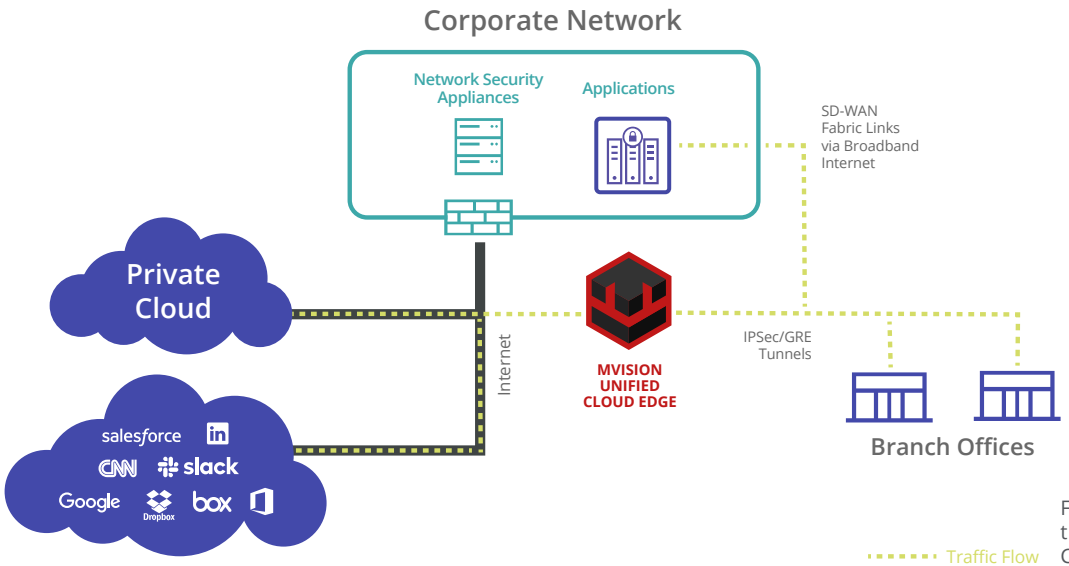


Figure 3. SASE direct-to-cloud transformation with MVISION Unified Cloud Edge and SD-WAN integration

Multi-Vector Data Protection: Data Awareness at Every Access Point

Cloud transformation has meant that a large portion of enterprise data now resides and is being accessed outside of the network perimeter and beyond the reach of traditional data security controls. Collaboration from the cloud to third parties, between cloud services, access by unmanaged devices, and devices at home connected to peripherals have created new blind spots that typically require multiple fragmented data protection solutions.

McAfee multi-vector data protection provides full-scope data protection for your workforce and eliminates data visibility gaps. Each control point works as part of a whole solution.

- Data classifications can be set once and applied across policies protecting the endpoint, network, web, and cloud.
- Shared data protection policies are enforced at every control point, allowing you to easily decide who can see your data and what they can do with it.
- Unified incident management between control points with no increase in operational overhead.

MVISION Unified Cloud Edge draws incident event information from all control points into one management console for a single view of your data protection environment. The unified data classification and management view delivers consistent detection results and prevents the data loss prevention (DLP) security gaps that occur when using multiple tools with disjointed policies and reporting. MVISION Unified Cloud Edge enables the correlation of data incidents across all vectors, enabling administrators to identify signs of potentially serious attacks.

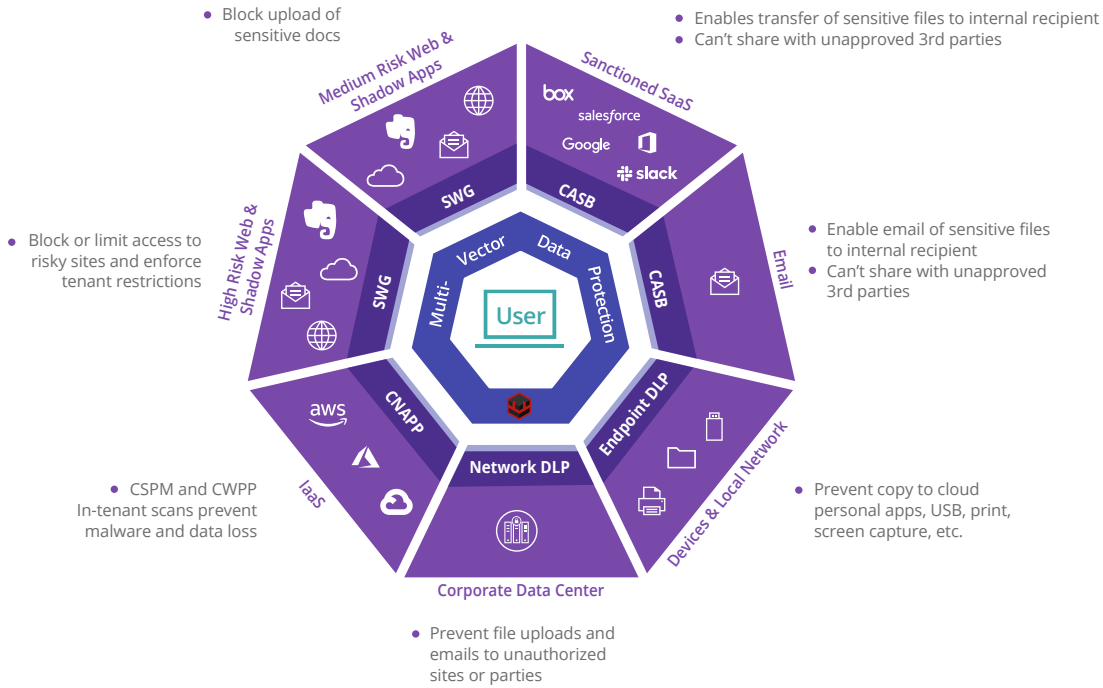


Figure 4. MVISION Unified Cloud Edge multi-vector data protection use cases

Defense Against Cloud-Native Threats and Advanced Malware

As valuable resources have shifted to the cloud, threat actors have followed. New methods of attack are emerging that leverage the features of cloud providers to fly under the radar while searching for and stealing information. Additionally, the advanced malware and malicious code used in fileless attacks remain an evolving threat. New protection methods are needed to detect and block these threats without impacting end-user productivity. MVISION Unified Cloud Edge defends against cloud-native threats, advanced malware, and fileless attacks with an array of traditional and state-of-the-art threat protection capabilities. These defenses mitigate the risk of attack and data loss as your enterprise transforms its network and productivity tools into cloud-based services.

User and Entity Behavior Analytics (UEBA) finds threats that traditional technologies miss by monitoring cloud activity across all your cloud services and refining millions of events to identify anomalies and threats in your environment. These anomalies are correlated to DLP incidents, cloud configurations, and app vulnerabilities to create a pre-built view of cloud-native attacks using the MITRE ATT&CK framework.

Any malware that attempts to land on your endpoints meets a rigorous, line-speed inspection path that includes the industry's most accurate real-time emulation sandbox. In cases where attacks forego malware in favor of zero-day exploits or fileless attacks that leverage operating system commands or website code, users automatically enter a Remote Browser Isolation session, allowing for full use of the web with zero possible infection.

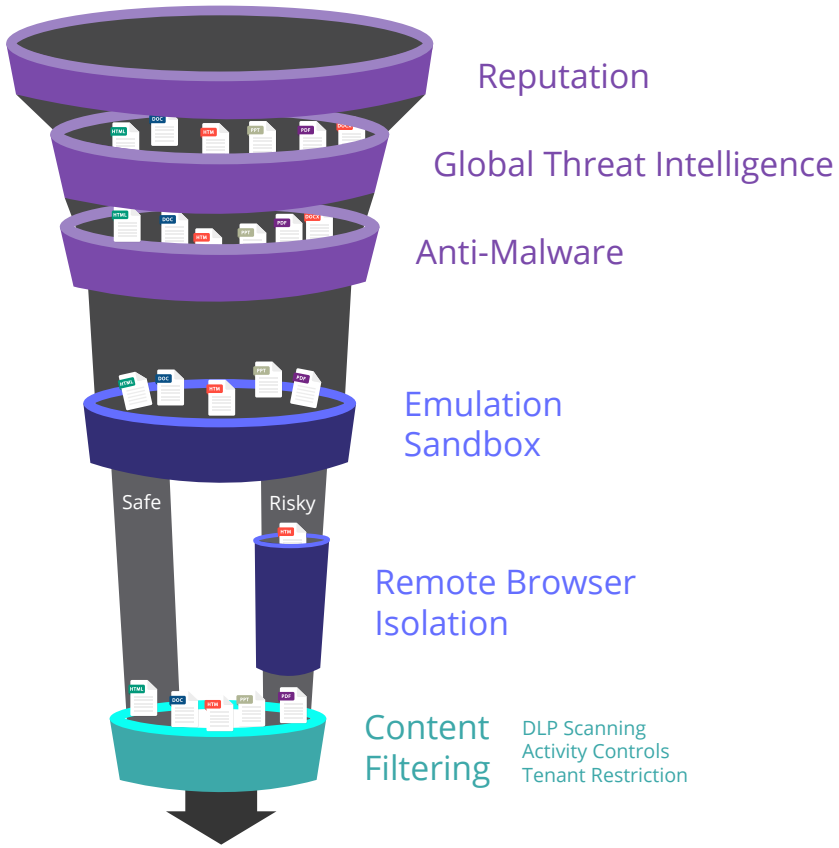


Figure 5. MVISION Unified Cloud Edge threat protection including Remote Browser Isolation

Additionally, all events from MVISION Unified Cloud Edge can be shared with MVISION XDR or third-party SIEM solutions to empower security operations teams.

MVISION Private Access—Industry's First Sensitive Data-Aware ZTNA

It's important for users to have access to internal-facing, private apps that often contain sensitive information. Virtual Private Networks (VPNs) have traditionally been used for this, but they suffer from performance and scalability issues, and make it difficult to enforce tight security controls. While traditional Zero Trust Network Access (ZTNA) solutions provide fast, direct access to private assets while employing granular dynamic access policies that prevent oversharing or lateral movement, they lack stringent data protection controls to secure the sensitive data hosted within those assets.

MVISION Private Access secures access to private applications from any location and device, and controls data collaboration with integrated data loss prevention (DLP). MVISION Private Access performs continuous risk assessment of the connecting devices by deriving enhanced posture information through McAfee endpoint security technology and provides blazing fast, "least privileged" access to private applications through a cloud-native hyperscale service edge.

MVISION Cloud Firewall—Secure All Non-Web Traffic for Remote Users and Sites

The proliferation of remote sites and users has challenged security practitioners to secure the non-web and non-cloud traffic. Backhauling every connection to centralized datacenters for security inspection leads to network latency and affects the user performance.

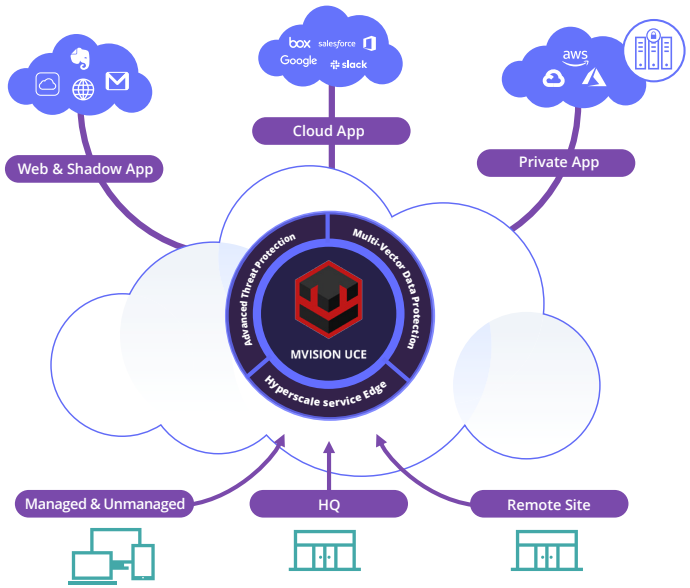
MVISION Cloud Firewall extends next-generation firewall (NGFW) capabilities to remote users through a cloud-delivered service model, securing local internet breakouts across all ports and protocols. The solution includes a sophisticated policy engine offering contextual awareness and a next-generation intrusion prevention system (IPS) with superior IPS efficacy, while offering end-to-end traffic visibility for troubleshooting and optimizing the network issues. The solution combines with MVISION Extended Threat Detection and Response (XDR) to block malware threats with a high degree of accuracy.

MVISION Private Access and MVISION Cloud Firewall converge with MVISION Unified Cloud Edge, offering organizations an all-encompassing, cloud-delivered Secure Access Service Edge (SASE) solution for accelerating their business transformation.

MVISION Unified Cloud Edge: The SASE Security Service Empowering Cloud and Network Transformation

Cloud Security Transformation

Mitigate risk in your distributed enterprise with a cloud-delivered service edge that provides fast and secure access to resources from anywhere in the world, performing threat and data protection in a single-pass to reduce cost and complexity.



Network Transformation

Unlock direct-to-internet access for your sites and remote users. Stop sending traffic back through your datacenter and instead connect to a hyperscale, cloud-delivered service edge from anywhere in the world.

Learn More

To learn more, visit www.mcafee.com/unifiedcloudedge

McAfee

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com