McAfee MVISION Private Access

McAfee® MVISION™ Private Access is the industry's first data-aware Zero Trust Network Access solution that secures access to private applications from any location and device, and controls data collaboration with integrated data loss prevention (DLP). Private Access converges with MVISION Unified Cloud Edge to uniquely position McAfee with the best-in-class, integrated, and cloud-delivered security solution for accelerated Secure Access Service Edge (SASE) deployments.

Key Advantages of ZTNA

- Direct-to-app connectivity to private applications
- Explicit identity and context-based access
- Network micro-segmentation to prevent lateral movement of threats
- Least privileged access to specific, authorized applications
- Shielding private application from Internet-based exposure
- Cost reduction and performance improvement by replacing VPN and MPLS
- Consistent user experience for accessing SaaS and private applications

Connect With Us

The Need for Zero Trust Network Access

The current business transformation and remote workforce expansion have invalidated the concept of network perimeter security. With corporate resources moving out of enterprise boundaries to multiple distributed locations such as public clouds and private data centers, organizations are challenged with deploying security solutions to protect their sensitive data, while facilitating seamless access from any remote location and device.

Zero Trust Network Access (ZTNA) builds upon the "Zero Trust" security model to enforce identity-aware and context-aware policies for application access. This means that access to any resource is denied by default. Every user and device, whether internal or remote, is assumed to be unsecure and risky, and their identity and security posture must be verified before granting access to sensitive private resources. ZTNA moves away from fixed perimeter-based security architecture to a more logical, software-defined perimeter architecture that encompasses a set of users and applications. According to Gartner, by 2022, 80% of new digital business applications opened up to ecosystem partners will be accessed through zero-trust network access.[1]

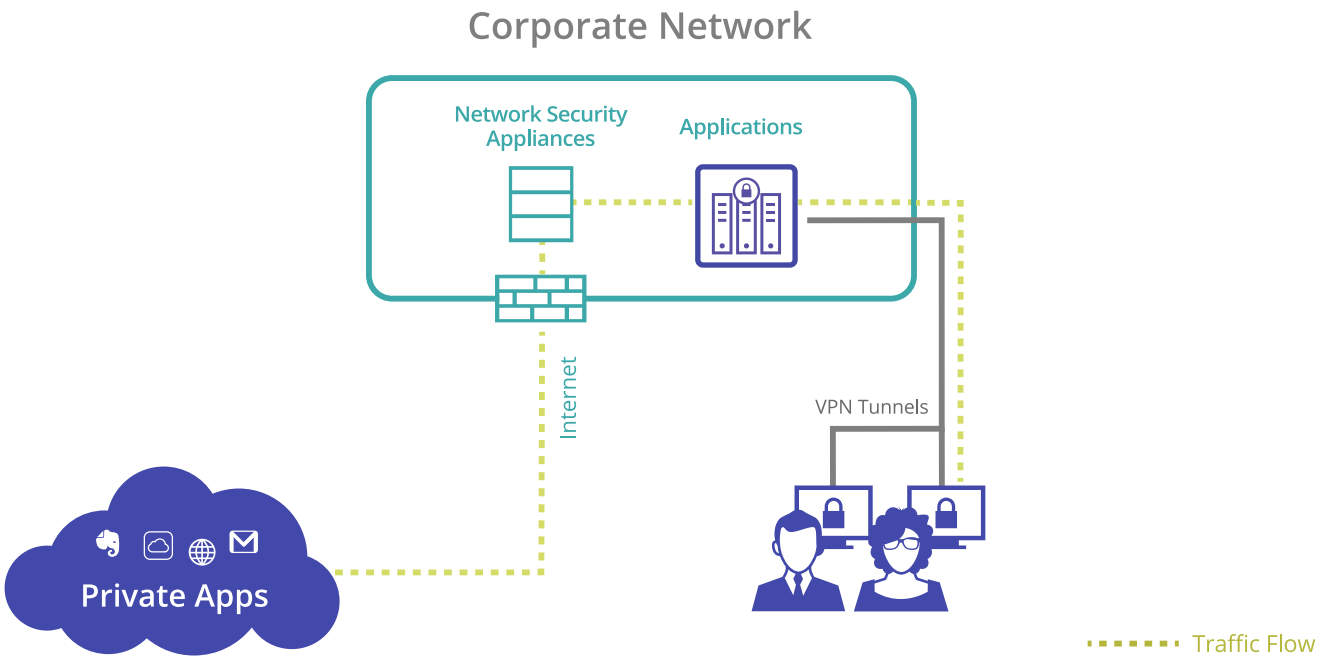

Figure 1. Traditional network architecture

1. https://www.gartner.com/en/documents/3986053/market-guide-for-zero-trust-network-access

Introducing MVISION Private Access

MVISION Private Access is the industry's first Zero Trust Network Access solution that comes with integrated Data Loss Prevention (DLP) and Remote Browser Isolation (RBI) capabilities. This allows organizations to enable granular "Zero Trust" access to private applications, apply policies to prevent loss of sensitive data during collaboration, and insulate private applications from potentially risky unmanaged devices through fully isolated web sessions.

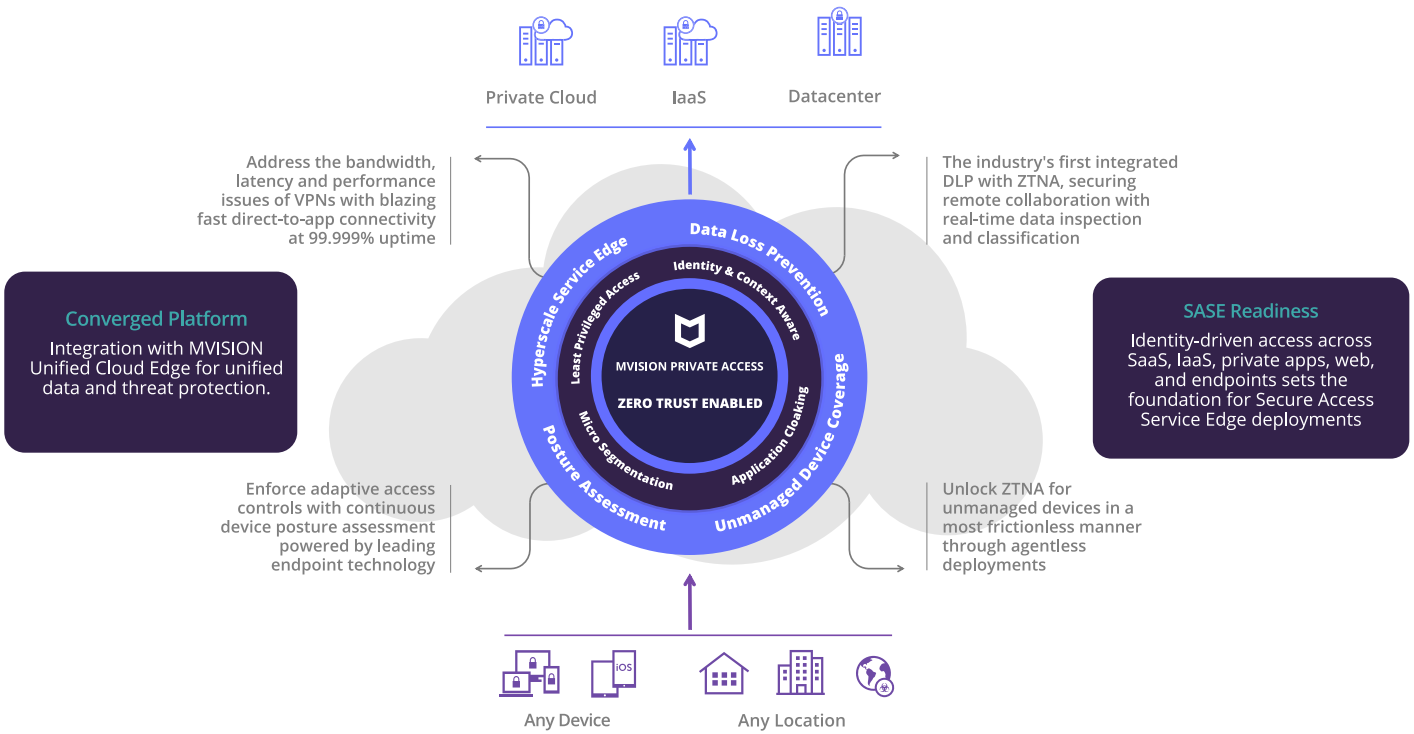

Figure 2. McAfee MVISION Private Access

Replacing VPN with Direct-to-App Connectivity

VPNs are not designed for a majority of the workforce connecting remotely to cloud-based deployments, leading to the following challenges:

- Corporate applications and data that users need to access are distributed across multiple locations. Hairpinning remote connections through centralized VPN hubs creates significant latency issues.
- The exponential increase in remote workforce traffic has throttled the network bandwidth and overtaxed the infrastructure capacity.
- An excessive implicit trust model permits full private network access to any user with valid login keys, increasing the risk of data exposure and lateral movement of threats.

McAfee Solution

MVISION Private Access utilizes the Hyperscale Service Edge to enable secure, direct-to-app access to private applications. The ubiquitous connectivity reduces network latency and allows a consistent and seamless user experience while accessing both SaaS and private applications.

Benefits

- The Hyperscale Service Edge runs at 99.999% uptime, providing uninterrupted access to corporate resources.
- Unlike VPNs, that allow full network access to authenticated users, Private Access micro-segments the networks and allows "least privilege" access to specific, authorized applications, and not the entire underlying network.

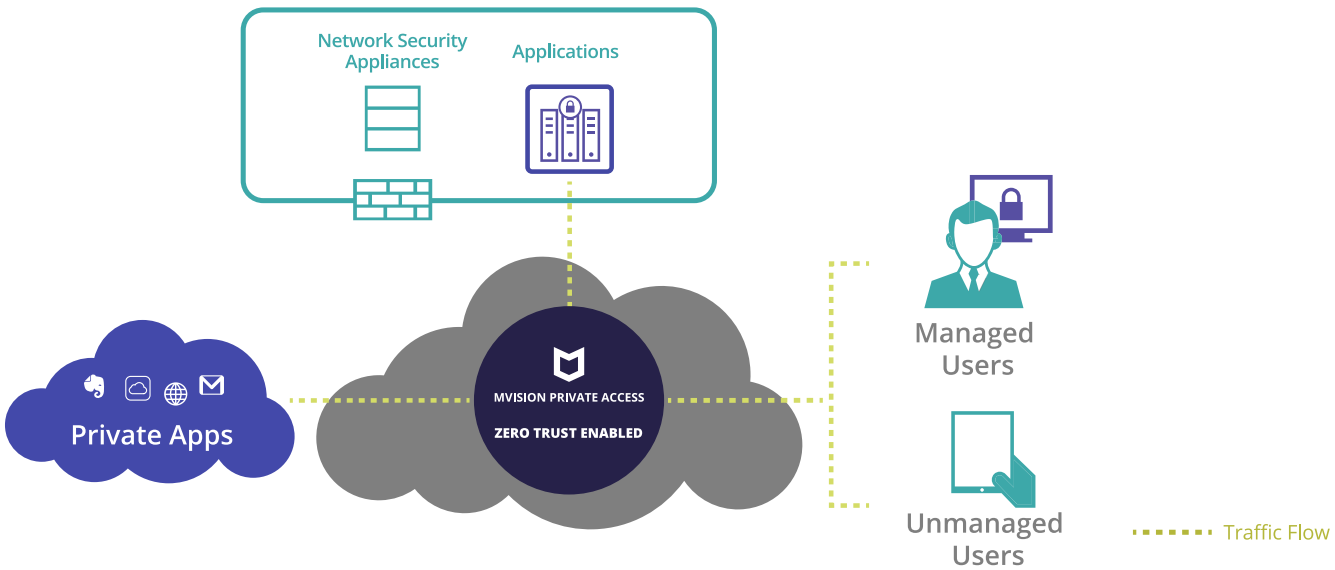

Figure 3. Direct-to-app access with McAfee MVISION Private Access

Integrated Data Protection to Secure Remote Collaboration

While traditional ZTNA vendors focus on securing remote access for private applications, they don't possess the capability to secure the sensitive data within those applications. In a distributed workforce, data can be accessed and collaborated between managed and unmanaged devices, third parties, or connected cloud services. It is highly important to enforce guardrails and prevent data loss from any of the connected entities.

McAfee Solution

MVISION Private Access comes integrated with Data Loss Prevention (DLP) to enable complete control over data collaborated through the private access sessions with inline DLP policies.

Benefits

- Deep data inspection and classification using inline DLP prevents inappropriate handling of sensitive data by remote users, collaborating from any location and device.
- By unifying DLP and threat protection across Private Access, Endpoints, Cloud, and Web, security teams benefit from integrated visibility and control of sensitive data.

Allowing Adaptive Access Control Based on Device Health and Security Posture Assessment

With the increase in remote users connecting from any location and device, policies need to more flexible, and organizations should consider multiple contextual parameters—such as user risk profile or device posture—before allowing access to the applications. Access context may include device type, user type, device OS, antivirus details, access time, location, or services accessed, to name a few.

McAfee Solution

MVISION Private Access leverages industry-leading McAfee Endpoint Security powered by proactive threat intelligence from 1 billion sensors to evaluate device and user posture, which informs a risk-based zero trust decision in real-time. The security posture is determined through a lightweight endpoint client installed on the remote devices that fetches the device attributes and allows users to enforce adaptive access control policies. Users will need to re-authenticate their sessions on detection of a change in the device posture.

Benefits

- McAfee Endpoint Security client goes well beyond the basic posture checking performed by competitive solutions to fetch a rich set of telemetry data, including device type, connected user details, last scanned status, and last software update to highlight the full context of user session through posture assessment.
- Security posture assessment of end-user devices helps in mitigating the risk of bad actors or unknowingly compromised users connecting to private applications, building a more resilient ZTNA environment, and improving the overall security footprint of organizations.
- Continuous monitoring of risk posture allows organizations to terminate risky connections in real-time based on additional contextual insights.

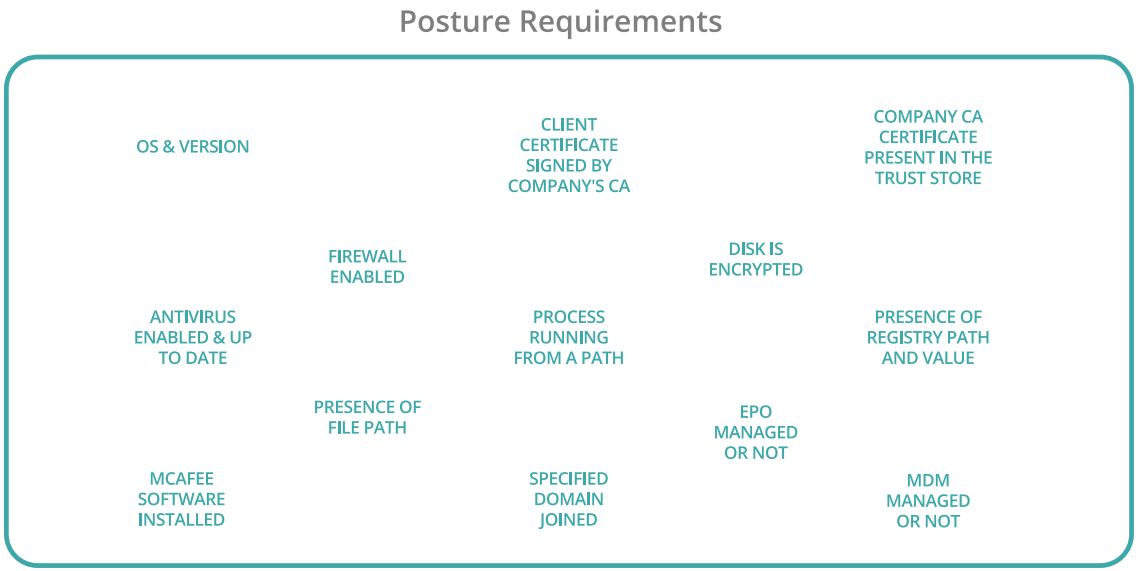

Figure 4. Device posture attributes

Frictionless Support for Unmanaged Devices

The recent shift to remote work environments has significantly increased the percentage of users logging in for work from unmanaged, BYO devices. Oftentimes these devices connect over unsecure remote networks, bypassing the controls of traditional security systems. While organizations encourage cloud-based collaboration to enhance productivity, but unsupervised data access, data sharing through unmanaged devices, and the challenges involved in enforcing endpoint, cloud and web security policies for these devices introduce the risk of sensitive data exposure and cyberattacks.

McAfee Solution

MVISION Private Access secures unmanaged devices through an agentless, browser-based deployment, and also through Remote Browser Isolation (RBI) sessions. The browser-initiated connection enables collaboration between employees, external partners, or third-party contractors in a most frictionless manner.

Benefits

- Facilitate seamless and secure access to private applications from unmanaged devices without requiring any resource-intensive agent installation.
- Isolate access through Remote Browser Isolation (RBI) sessions to protect private applications from risky and untrusted unmanaged devices.
- Define contextual access control policies to limit access to private resources based upon the device classification and security posture.

Accelerating the Roadmap for SASE

Prescribing the convergence of networking and network security into a unified cloud-delivered service model, Secure Access Service Edge (SASE) aims to solve the dynamic and secure access requirements of digital enterprises. By virtue of establishing secure, identity-driven access to applications, ZTNA is considered a core component of SASE architecture.

MVISION Private Access is architected using McAfee's security framework guidelines and it seamlessly integrates with other McAfee Unified Cloud Edge (UCE) components, which include Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Endpoint Protection. The solution integrates with Identity Providers, such as Microsoft Active Directory and Okta, for SAML SSO-based authentication to continuously authenticate and validate the identity of users accessing private applications.

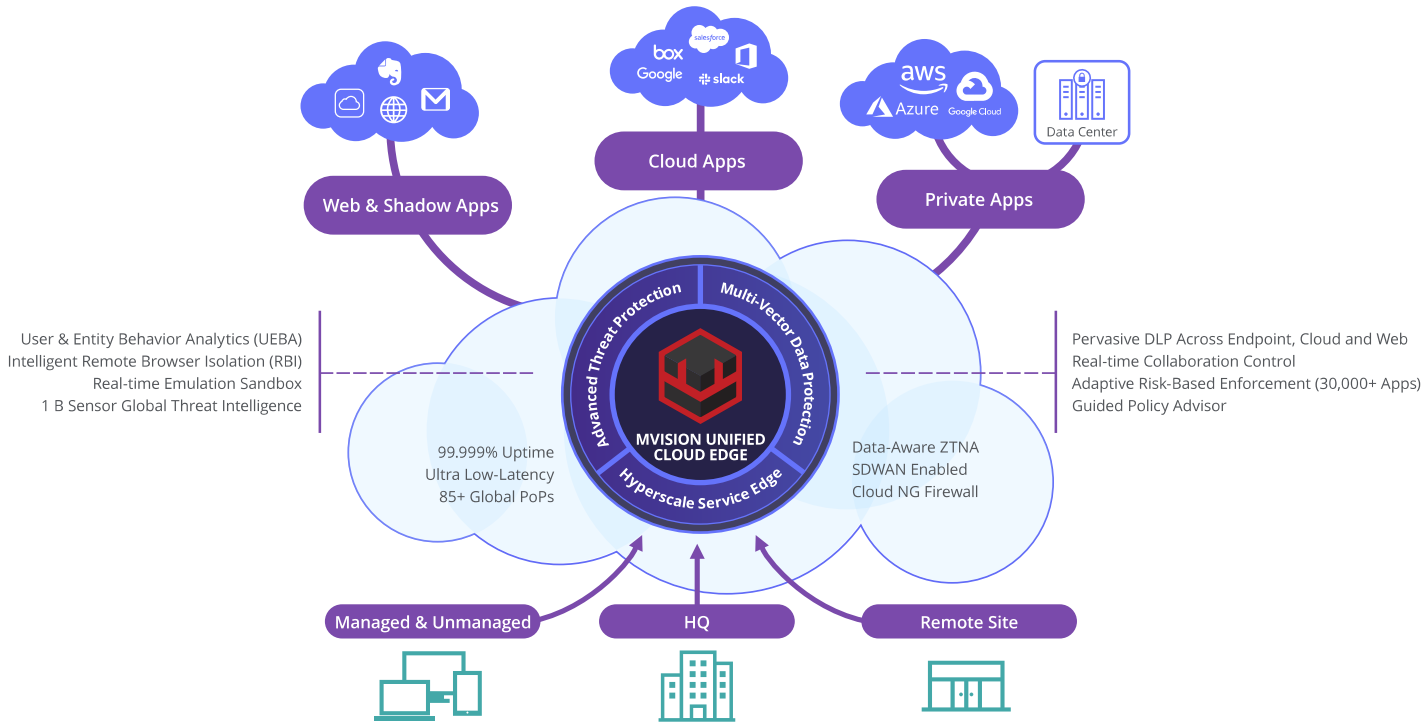

Figure 5. McAfee MVISION Unified Cloud Edge

This uniquely positions McAfee to solve the network security puzzle of SASE with a unified solution that addressing the complexity of remote workforce deployments with centralized visibility and incident management, adaptive and granular access control, end-to-end data protection, and advanced threat protection from device-to-cloud.

By partnering with leading SD-WAN vendors, McAfee couples ubiquitous cloud security with simplified, reliable, and low latency service delivery to establish the roadmap for accelerated SASE deployments.

Learn More

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

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