appgate McAfee™

SOLUTION BRIEF

SAFEGUARD ENTERPRISE ACCESS

Appgate SDP integrates with McAfee Endpoint Security and MVISION Unified Cloud Edge to deliver a Secure Access Service Edge (SASE) solution

THE PROBLEM

Enterprises need to secure all access for internet, cloud, SaaS and private access—for any user, any device, any resource from anywhere. While this need is not new, three growing trends have created greater importance and urgency:

1. Resources are everywhere: increased rates of cloud-native app development with containers that places more internal apps outside of the corporate datacenter
2. People are everywhere: the accelerated adoption of remote work means users rely more heavily on BYOD smartphones, laptops and other potentially risky or compromised devices to access corporate assets
3. Evolving threat landscape: attackers are well funded and getting more sophisticated with ransomware and other tactics, techniques, procedures

Legacy technologies haven't kept up with these changes, proving expensive to scale while complicating and slowing down cloud access.

At the same time, the trends driving demand for secure access to business-critical applications and data are part of a larger movement to detach the corporate network from the data center. This enables work-from-anywhere for a distributed workforce, providing connectivity and security as a service from the cloud in a framework known as SASE.

THE SOLUTION

McAfee's Endpoint Security and MVISION Unified Cloud Edge (UCE) fuses with Appgate SDP, the industry's leading Zero Trust Network Access provider, to deliver a comprehensive SASE solution. This new technology partnership performs threat and data protection at every control point in a single pass to deliver:

- **Comprehensive internet, SaaS and private access protection**
- **Improved user experience and productivity**

In addition, Appgate SDP securely delivers and enforces McAfee PAC files to all users and can deliver specific PAC files based on policy and risk. This ensures that no user, attacker or malware on a compromised device can disable, alter or remove the PAC file.

With the Appgate SDP integration, enterprises can shift to a high-security SASE framework with industry-leading data and threat protection.

This partnership means that the intelligence from the McAfee ecosystem boosts the power of Appgate SDP, particularly for customers in the defense sector and Fortune 500 clients with the most stringent security requirements.

Get secure access with confidence and zero compromise for all internet traffic, SaaS applications and private resources. No matter your users' ultimate destination, protection and security are assured.

HIGHLIGHTS

Certified interoperability with McAfee MVISION and Endpoint Security solutions

Integration with McAfee enhances Appgate SDP by providing contextual device posture and threat information from McAfee endpoints

Appgate's inclusion within exclusive McAfee Security Innovation Alliance Program gives enterprises the building blocks for a SASE framework when coupled with MVISION Unified Cloud Edge

APPGATE SDP ADVANTAGES

Ability to overlay on top of systems that have already been deployed, allowing customers to leverage existing security investments

Support for hybrid IT environments, including McAfee's install base

Powerful APIs support inbound and outbound integrations building blocks for a SASE framework

> "We describe SASE as an emerging architecture combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS and ZTNA) to support the dynamic secure access needs of digital enterprises."
>
> **-Gartner "SASE Will Improve Your Distributed Security Everywhere," Richard Bartley, 8 December 2020**

DEPLOYMENT OVERVIEW

IN THE COMBINED SOLUTION:

- McAfee Endpoint Security provides Appgate SDP endpoint telemetry and threat intelligence, enabling enhanced device posture checks before allowing secure access to private apps or data.
- When an enterprise user accesses a private app, Appgate SDP evaluates the security posture of the endpoint, including threats detected by McAfee Endpoint Security to make an adaptive decision based on risk to authorize access.
- Compromised endpoints can be quarantined, prompted for MFA or blocked from accessing certain internal apps depending on the level of risk.
- Device posture and threats are continuously evaluated for changes in risk posture, protecting against insiders or bad actors attempting lateral movement through an enterprise network.
- Appgate SDP provides the McAfee EPO management server a secure connection to endpoints for updates on or off network.
- Appgate SDP deploys and enforces the Proxy Auto-Configuration (PAC) file by policy to ensure internet and SaaS bound traffic are routed to MVISION Cloud and properly inspected and filtered based on endpoint risk and user role or group.
- Appgate SDP provides MVISION-rich identity-based log data tied to the device and resource to make more informed decisions and for incident response.

> **"We've invested in an open approach for our platform to deliver top quality integrations with ZTNA providers, sharing posture information from our massive endpoint security base. This provides customers with the best option for their environment, enhancing their deployment with valuable intelligence from the McAfee ecosystem. Together with our SIA partners, we are strengthening security for the critical apps that enterprises rely on every day."**
>
> **- Javad Hasan, Global Head,**
> **Product Strategy and Alliances at McAfee**

USE CASE SCENARIOS:

The integrations between Appgate SDP and McAfee MVISION and Endpoint Security provide different benefits. The following examples demonstrate how Appgate and McAfee security technologies combine to provide a robust SASE framework for government and enterprise alike.

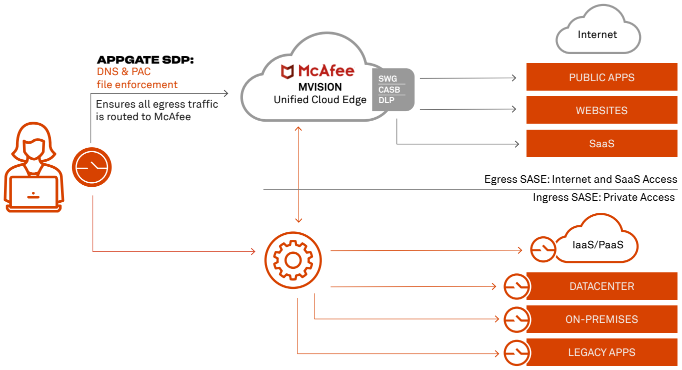
MCAFEE MVISION UNIFIED CLOUD EDGE (UCE) INTEGRATION

In this scenario, McAfee MVISION leverages Appgate SDP to deliver the proxy auto-configuration (PAC) file and direct egress traffic through the McAfee Unified Cloud Edge.

All internet bound traffic is directed through the use of PAC files that Appgate SDP delivers and and enforces via policy.

Appgate SDP can deliver different PAC files based on user risk, role or group and device risk.

With this approach, even if a savvy user removes or alters the PAC in an attempt to bypass the McAfee MVISION Unified Cloud Edge, Appgate SDP replaces it within a few seconds.



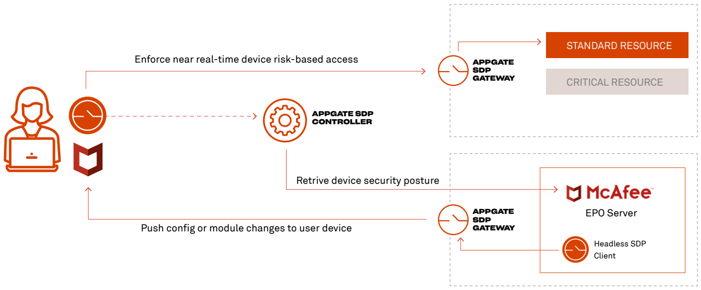
MCAFEE ENDPOINT SECURITY (EPOLICY ORCHESTRATOR (EPO) INTEGRATION)

In this scenario, Appgate SDP consumes endpoint risk posture and telemetry information for use in dynamic near-real time private access policy decisions.

By reaching into the McAfee management console via API, Appgate SDP leverages McAfee's endpoint agent visibility to acquire rich context about the risk of a particular user and device—augmenting what is already used by SDP.

If a process is determined to be malicious, McAfee can notify Appgate SDP and any user accessing private resources on a device this running process can have access revoked, modified or be prompted for MFA.

Additionally, Appgate SDP secures the McAfee EPO server, ensuring it can securely connect to and update the devices under management on or off network.



LEARN MORE ABOUT APPGATE SDP AT APPGATE.COM

appgate