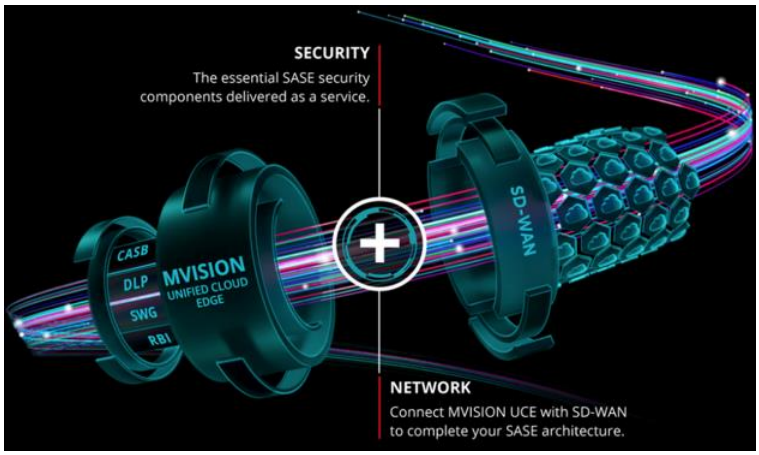
SASE & Zero Trust Integrated Security Framework

Solution Introduction

The McAfee Enterprise and Appgate partnership was purpose-built to provide an initial, minimum viable product delivering a SASE cloud-based, Zero Trust network solution. Our solution addresses the most prominent threats facing the DoD and its rapid migration to the cloud: misconfigurations, identity and access management, malware, and insider threats.

Our approach starts with the threat, especially as cloud breaches have now exceeded those experienced on-premise. We deliver a cloud common operational picture with command-and-control capabilities across an array of multi-cloud and multi-app environments, including critical mission apps. Our solution allows zero-trust data protection at every access point. This creates a secure environment for the adoption of cloud services, enabling cloud access from any device anywhere to improve the user's experience and productivity.



Digital transformation represents the next great technological revolution. The government's ability to move to the cloud and empower its distributed workforces with fast, secure, simple, and reliable access will set the tempo for innovation and advancement into the new age. It is clear that there is a better approach to applying security to this challenge. It's a mindset change from the old perimeter-oriented view to an approach based on adaptive trust and access control. Data is considered a strategic asset within the DoD; demonstrating a sound data protection strategy will become a priority as cloud adoption becomes more commonplace.

McAfee Enterprise and AppGate's collective goal is to ensure that the government can support its mission objectives in a secure way, deliver new functionality, improved processes, and provide better return on investments through interoperable and integrated solutions.

Secure Access Service Edge Capability Delivery

Secure Access Service Edge (SASE) – defined by Gartner – is a security framework prescribing the convergence of security and network connectivity technologies into a single cloud-delivered platform to enable secure and fast cloud transformation. SASE's convergence of networking and network security meets the challenges of digital business transformation, edge computing, and workforce mobility. SASE merges network traffic and security priorities, ubiquitous threat and data protection, and ultra-fast, direct

network-to-cloud connectivity. While SASE used to be a matter of sacrificing speed vs. control, our approach has been to integrate Appgate's ZTNA solution, which is part of the USAF's Platform/Cloud One architecture, and McAfee Enterprise's cloud security solution, which is widely deployed across the Federal government and top-right on Gartner Magic Quadrant. This integrated solution provides both speed to mission *and* complete control to protect against the full range of cloud threats, in a zero-trust manner, including: unauthorized access, data spillage/leaks, vulnerable configurations, malware, negligent or malicious insiders and shadow IT. Our recommended framework is designed to allow government enterprise security resources to apply identity and context in order to specify the exact level of performance, reliability, security, and cost desired for every network session.

The development of our SASE approach was done in large part to improve the efficiency and security efficacy of a growing mobile workforce. The use of the Internet through public Wi-Fi can become a great security risk. Therefore, accessing DoD applications and data in a timely, secure manner is a challenge. A SASE framework provides the construct to maintaining higher access speed and performance, while also enabling stringent control of users, data, cloud services, and devices traversing networks – regardless of when, where, and how they're doing it. SASE represents the best way to achieve a direct-to-cloud architecture that doesn't compromise on security visibility, control, performance, complexity, or cost. Successful SASE transformation is dependent on the security foundation you start building from.

The primary SASE component of our solution is provided by McAfee Enterprise's MVISION Unified Cloud Edge (UCE). It represents a first-of-its-kind cloud-native and cloud-delivered solution that provides unified data and threat protection from device to cloud, fully integrating data loss prevention (DLP), device/user control and other security technologies into web filtering (SWG), endpoint management and cloud control (CASB). UCE provides unified policy management which enables shared data protection policies and incident management between endpoints, web, and cloud with no increase in operational overhead.

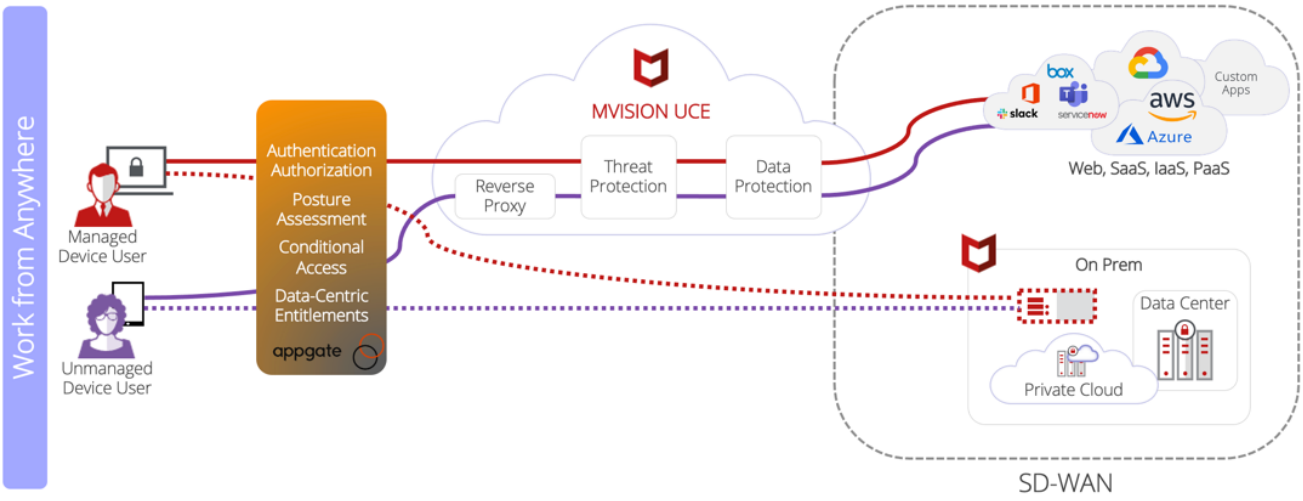


Figure 1: McAfee Enterprise and Appgate's Converged Reference Architecture

UCE uses common cloud-based management capabilities and systems that share information (e.g., ePolicy Orchestrator – ePO, Data Exchange Layer – DxL) so its decisions are based on multiple parameters. By enforcing consistent data context and policies across endpoints, web, and cloud, UCE protects data as it leaves the device, travels to and from the cloud, and within cloud services to create a new secure cloud edge for the enterprise. This unified solution blocks cloud-native breach attempts previously invisible to the NIPR or SIPR. UCE minimizes inefficient traffic with efficient, intelligent, and secure direct-to-cloud access (network peering) to secure Flow 3 access. Our solution protects remote sites via SD-WAN integrations utilizing Dynamic IPSec and GRE protocols leveraging SD-WAN technologies that connect physical sites to cloud resources faster and more directly. In developing the UCE platform it was vital to deliver a low latency/high scalability platform to secure a global cloud footprint and an expanding DoD cloud-native architecture, including Peering Point of Presence to reduce delays. Reliability is also a strategic benefit of the UCE platform as it delivers 99.999% uptime (maintained service availability) and internet speeds faster than a direct connection will improve the productivity of the government's mobile resources.

Integrating Customer Edge Security Stacks at the DISN Point of Presence

The McAfee Enterprise platform provides native security for the customer edge and application security layers. Specifically, our platform incorporates native security controls for collaboration tools and cloud applications like M365, Teams, OneDrive/SharePoint, and ServiceNOW. The DISN is an MPLS network which defines "who is where" and provides that level of basic traffic control. The challenge is the DoD is contemplating extension of the DISN Points of Presence into the cloud while adopting Zero Trust Network Access (ZTNA) to enhance security, while not impacting network performance. What is not currently possible is for the government to provide conditional access, tagging, and traffic prioritization/segmentation. In a nutshell, the limitation is the current inability to segment networks based on conditional access or application rules – SD-WAN provides that capability. Our solution integrates with the Gartner Magic Quadrant SD-WAN leaders. The Appgate Software Defined Perimeter (AG SDP) is a ZTNA platform that integrates with the UCE platform to enable to DoD to rapidly adapt to how users access protected resources and applications. Appgate applies zero-trust conditional-based access policies that are continually monitored and re-evaluated throughout the user's session. AG SDP creates a highly-elastic and distributed edge constructed of multiple policy enforcement and decision points. This puts security controls as close to the data as possible and allows users to connect to multiple sites/locations in parallel, with each user having one-to-many secure connections. This capability creates a unified security boundary across any infrastructure; on-premise and cloud, providing the DoD a next generation common operating picture.

Traditional network security approaches are failing to adequately protect DoD. Trust is presumed allowing users to "connect first, authenticate second" and is typically binary in nature (access is granted to everything or nothing); meaning, the DoD Information Network (DoDIN) must defend against open listening ports exposed to reconnaissance, denial of service, unauthorized users consuming unauthorized services, inherent over-entitlement, and a broad lateral attack surface.

Integrating Scalable Application Security Stacks in Front of Application Workloads

UCE was designed to provide protections for SaaS applications such as: Office 365, Teams, OneDrive, ServiceNow, Skype, Workday, DropBox, Adobe, and others. McAfee Enterprise's has the largest, most comprehensive SaaS catalog available in the industry. The platform provides a mechanism for expansion for COTS and GOTS applications.

We also incorporate ZTNA principals to GOTS applications. We understand that the DoD will require access to internal-facing, GOTS apps that often contain sensitive information. VPNs (Flow 2) have traditionally been used for this use case, but they suffer from performance/scalability constraints and also make it difficult to enforce tight security controls. ZTNA provides fast, direct access to private data center or cloud applications while utilizing granular dynamic access policies that prevent oversharing or lateral movement.

AG SDP employs principles of Zero Trust by taking an Identity and Data Centric approach to security. Users and devices are authenticated before they are allowed to connect. Authorized users must meet access criteria and meet the appropriate conditions before and after access is granted. In essence, our integrated platform provides the ICAM capability, extended visibility to endpoints, as well as a comply-to-connect capability.

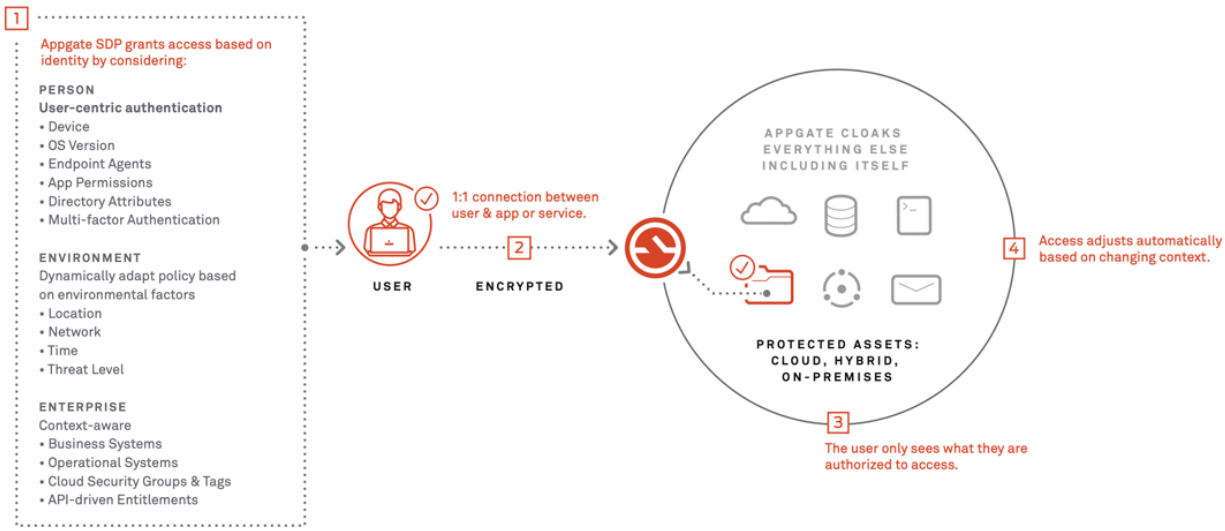


Figure 2: Appgate SDP's Connection and Authentication Workflow

To make the DoD's enterprise edge undiscoverable, AG SDP uses Single Packet Authorization (SPA) technology, a sophisticated version of port knocking to enforce the "authenticate first, connect second" approach. SPA cloaks infrastructure so that it is invisible to port scans. It ensures that only authorized users can connect to network resources. AG SDP's use of SPA and FIPS-certified mutual TLS have been proven to mitigate man-in-the-middle, denial of service, stolen credentials/access tokens.

The UCE platform protects applications (COTS and GOTS) through reverse proxy and/or via the integration of the application APIs. The government can apply full platform features to these applications. The "integration point" is created from what we call "CASB Connect". CASB Connect is an innovative, self-serve program which enables any cloud service provider, customer, or partner to rapidly build lightweight API connectors to the

UCE platform. CASB Connect API allows users direct access to the SaaS app without any intermediate proxies and offers DLP (on upload activity), UEBA + Activity Monitoring, and Collaboration Control to protect data and address cloud based threats.

The CASB component of the UCE platform – MVISION Cloud – considers all applications as untrusted and must be authenticated and explicitly authorized to the least privilege required in this context it supports the discovery of "Shadow IT", unapproved applications (security noncompliant applications and infrastructure) being utilized on the network putting data at risks (e.g., Fire Sharing Services, Cloud-based document processing apps, etc.). This further propagates the application of security at the application layer and ensures that proper security is in place to protect the user, the device accessing the SaaS or IaaS app, and the data residing in the app. MVISION Cloud ingests SWG logs and performs analysis against the logs to identify users accessing cloud-based PaaS/IaaS/SaaS services. MVISION Cloud then "communicates" back to the SWG to take action on what MVISION Cloud determines to be risky. Our solution's approach enforces access controls on out-of-the-box and custom apps based on contextual parameters such as user, data, location, activity, and group.

Micro-Segmentation and Traffic Flow Prioritization

Our approach leverages a zero trust architecture that is focused on device and cloud policy enforcement points and produces unified security operations through management, threat intelligence sharing, analytics, and orchestration. Integrated with SD-WAN technologies, government application performance will accommodate evolving requirements, utilizing unique and adequate network segmentation.

The McAfee Enterprise-Appgate solution is purpose-architected to take an agnostic approach to SD-WAN integration. We will integrate the SD-WAN with the SWG faction of the UCE platform to address challenges that the government has in moving its applications and data to the cloud environment. Integration with SD-WAN enables better support for both hybrid (Flow 2) and direct-access cloud (Flow 3) customers, specifically simplifying a sprawling set of remote sites and greater mobility among resources. Our approach provides a simple, performant, reliable way to achieve security for internet breakout and private WAN elimination.

With SD-WAN providing segmentation for both the network and application layers for comprehensive inbound and outbound protection. When integrating UCE, AG SDP, and SD-WAN, the government will benefit from a power toolset which prevents intellectual property and sensitive data exfiltration, regulatory compliance, and forensic data availability in the event of an incident.

McAfee Enterprise, in particular, has certified interoperability with six (6) of the industry's leading SD-WAN providers (Silver Peak (HPE), Versa Networks, Viptela (Cisco), VeloCloud (VMWare), and Citrix). By bringing together UCE, AG SDP, and SD-WAN in a seamlessly integrated solution, the government can deliver SASE and build a network security architecture fit for its digital transformation and rapid cloud adoption. Security is addressed by AG SDP's access control and through UCE's threat, data, and cloud

application protection capabilities, as well as the distributed firewall capabilities delivered by SD-WAN. Through a single, fast internet connection, SD-WAN intelligently and efficiently routes traffic directly to cloud resources or back to the on-premise environment. With UCE and SDP providing security directly in the cloud, SD-WAN will forward web- and cloud-bound traffic directly, without any excessive latency. Cost savings are realized from removing expensive MPLS lines, and since the majority of traffic no longer needs to backhaul through the data center/on-premise environment, additional savings can be achieved by reducing central network bandwidth and infrastructure capacity.

Integrating with Capabilities at IL4/5 and Preparing for IL6

McAfee Enterprise's platform currently integrates, out-of-the-box, with existing government capabilities at NIPR (IL4-5), including: M365, Teams, GovCloud, MilCloud, ServiceNOW, Adobe, and others. No matter which SaaS applications the government wishes to consume on the DISN, the McAfee Enterprise platform can address it. Our platform provides the "last mile" to connect an untrusted network (through Appgate), to the endpoint, and to IL4/5 capabilities. The McAfee Enterprise tenant currently resides in GovCloud. As our cloud boundary (CASB) achieves IL5 this summer we will continue to work with DISA RME to achieve IL6 certification for our cloud boundary that will operate in the AWS Secret Region. Appgate is currently deployed as a Customer Edge Security Stack for the USAF's IL5 environment. This capability is also being leveraged to replace legacy VPN across Air Force bases and is being referred to as the Zero Trust Network Access Point (ZTAP). ZTAP has been targeted by USAF to be implemented in their IL6 environment and is currently in prototype.

We provide integrations with IaaS, PaaS, SaaS capabilities. Currently, the government's focal point for IL6 is on the IaaS/PaaS environments. As SaaS capabilities achieve operations at IL6 we are preparing to provide data and threat protection in a zero trust matter for those applications.

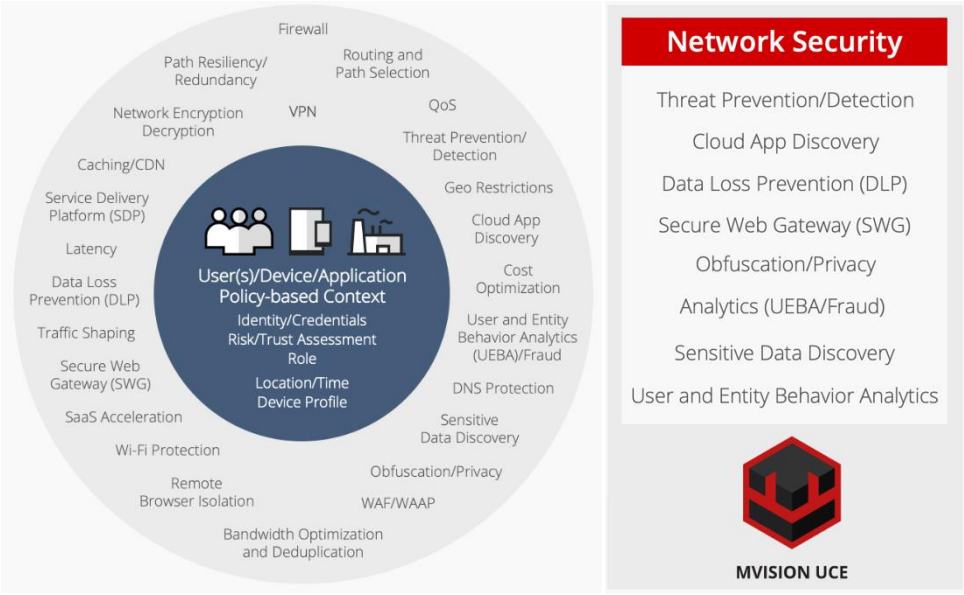


Figure 3: Gartner's definition of SASE and the Network Security component mapping to McAfee Enterprise's UCE Platform

McAfee

Considerations for SASE/ZT Architecture

No.	Recommendations/Considerations
1	Solution enables a data centric approach to resource authorization; consuming meta-data tags/labels for policy alignment
2	Solution must provide a unified policy enforcement & decision point that leverages ICAM attributes, device posture telemetry for Comply-to-Connect, meta-data tags/labels, and additional context derived from other security or mission tools
3	Provide a government-authorized alternative to the Cloud Access Point. Solution must provide the ability to connect users to cloud and on-premise resources with a distributed and elastic perimeter
4	Solution must provide multi-vector data protection, including: Blocking upload of sensitive docs; block or limit access to risky sites and enforce tenant restrictions; provide in-tenant scans to prevent malware and data loss; prevent file uploads and emails to unauthorized sites or parties; prevent copy to cloud personal apps USB, print, screen capture; enable email of sensitive files to internal recipient and not to unapproved 3rd parties; enable transfer of sensitive files to internal recipient and prevent sharing to unapproved 3rd parties.
5	Operate at 99.999% uptime
6	Solution must provide threat protection controls that adapt to changes in risk and context.
7	The solution must deliver complete visibility and control over data at every policy decision point regardless of whether it's at the endpoint, through the web, or in the cloud.
8	Provides a security approach for both cloud-native application threats (e.g., Teams, M365) as well as providing protection from cloud misconfigurations.
9	We recommend that the government's solution leverage one or many identity sources (e.g., distributed or federated) to authenticate users and natively support multiple authentication, including PKI, to continuously challenge the "least privileged" ZT caveat.
10	We recommend that the government further consider, clarify, and define ingress, egress, and network services categories of ZTNA. Ingress SASE should be considered as private access where IP, PII, and mission-critical data are housed and prioritized. Egress SASE secures access to the internet and internet-based SaaS applications. Egress SASE is where SWG and CASB components of the SASE architecture are incorporated to secure access to internet and SaaS apps. Lastly, the network layer is solved for by SD-WAN.
11	We recommend that the government consider incorporating behavioral analytics and data loss prevention factors when considering its ZT/SASE architecture.
12	The solution should deliver a micro-segmented software defined perimeter that is able to control North/South and East/West flows between the user and its applications.
13	Due to the expanse of the current DoD DevOps pipeline, the solution should be built to integrate into CI/CD pipelines to deliver security as code.
14	We also recommend that the government consider re-aligning its definition of SASE according to the Gartner definition. *Please see Figure 2 below for additional information.*
15	The solution should provide support for micro-segmentation within cloud native applications in support of containers.