Prisma SASE for US Public Sector

At-a-Glance

Prisma SASE Highlights

Palo Alto Networks Prisma SASE is the industry's most complete DoD SRG, FedRAMP and StateRAMP authorized secure access service edge (SASE) solution, delivering:

- **Protection for all applications and data:** Secure access to all privileged data across web- and non-web-based traffic reduces the risk of data breaches.
- **Complete security for multiple use cases:** Multiple capabilities converged in a single cloud-delivered service provide centralized visibility, networking, and security. With Prisma SASE, agencies can connect users and branch locations to sanctioned cloud apps, data centers, and the internet and offload internet traffic from private networks.
- **Optimized user experience:** A massively scalable network with global coverage for FedRAMP Moderate environments provides ultra-low latency backed by industry-leading SLAs, ensuring the best digital experience possible for end users.
- **Maximized existing security investments:** Agencies using Palo Alto Networks Next-Generation Firewalls (NGFWs) can leverage their existing security policies in Prisma Access and manage the service using the same familiar, centralized management.

Key Challenges in US Public Sector Agencies

Executive Order 14028, issued in May of 2021, mandates modernizing government networking and security infrastructures to address legacy shortcomings and help US public sector agencies realize the benefits of a cloud-based approach while moving to a zero-trust architecture to mitigate risks. Working alongside other programs and initiatives such as the Trusted Internet Connections (TIC) 3.0, federal as well as state and local agencies are now under pressure to rapidly enable secure connectivity for remote locations and employees while securing data, networks, and boundaries as well as providing visibility into all agency traffic, including in the cloud.

The Industry's Only DoD SRG, FedRAMP and StateRAMP SASE Solution

Palo Alto Networks Prisma SASE brings together best-of-breed security and next-generation SD-WAN into a cloud-delivered platform. It consolidates multiple point products, including Zero Trust Network Access (ZTNA) 2.0, Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaas) and software-defined wide area network (SD-WAN) into a single integrated service, reducing network and security complexity while increasing organizational agility.

The superior security of ZTNA 2.0 protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach.

Prisma SASE is built in the cloud to secure at cloud scale while delivering exceptional user experience. A truly cloud-native architecture provides uncompromising performance backed by leading SLAs. The industry's only SASE-native Autonomous Digital Experience Management (ADEM) helps ensure an exceptional experience for end users.

Prisma SASE holds the following certifications:

- Prisma SD-WAN - FedRAMP Moderate (ATO) & StateRAMP Moderate
- Prisma Access - FedRAMP Moderate (ATO) and High (In Process), StateRAMP (Moderate & High), and DOD/IL5 (P-ATO)

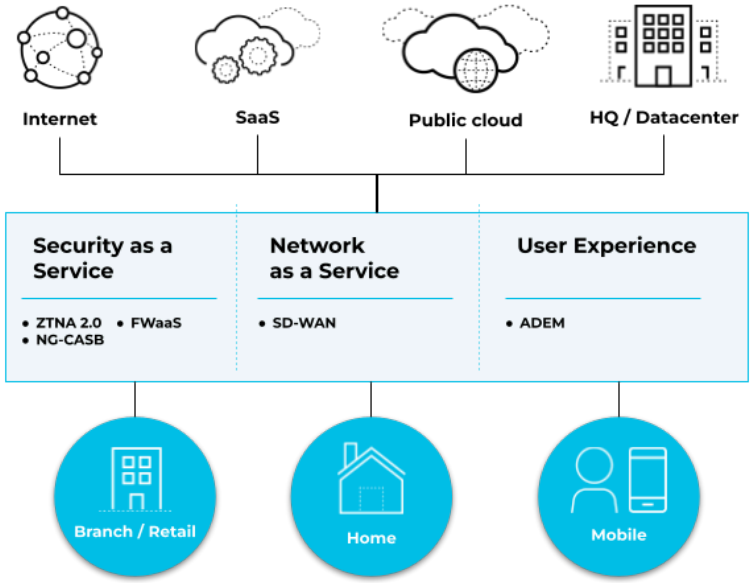

Figure 1: Prisma SASE architecture

Prisma SASE Use Cases

Three fundamental shifts are driving the need for network and security transformation in the US public sector: tele- and hybrid work, cloud and digital transformation and branch transformation.

- **Tele- and hybrid work** has been a tremendous advantage throughout the recent pandemic according to a federal employee survey. As a result, federal as well as state and local agencies are exploring many options for accommodating flexible, or hybrid, work environments. Some workers may return to the office, but remote-first, hybrid, or telework days are all possible.

Prisma SASE for US Public Sector

At-a-Glance

Whether they are in the office, at home or across the country, US public sector workers should have the same seamless access to the tools they need to complete their missions—without putting department operations or data at risk.

- **Cloud and digital initiatives** are driving US public sector agencies to invest more in SaaS and other cloud services. The Cloud Smart strategy released in 2019 paved the way for massive adoption of cloud and as-a-service solutions in federal as well as state and local agencies, and as a result more than half of state and local governments now store mission-critical data in the cloud.. FedRAMP and StatRAMP-authorized SASE solutions help ensure robust security measures are in place to safeguard sensitive data in government cloud environments.
- **Branch transformation** is well underway as federal agencies expand their use of commercial cloud, SaaS applications, and the Internet to fulfill their missions. As a result, they are modifying their network architectures and migrating away from legacy WAN and MPLS to SD-WAN and SASE, leveraging the flexibility inherent in modern SD-WAN solutions to support carrier-independent WAN connections and intelligent traffic steering across WAN links such as 5G/LTE, broadband and satellite.

Complete Digital Experience Management for SASE

The Autonomous Digital Experience Management (ADEM) add-on for Prisma SASE helps public sector IT teams see, understand, and improve digital experiences for all their users and branch locations. ADEM delivers SASE-native visibility into digital experiences, with segment-wise insights across the entire service delivery path, including intelligence gathered from endpoint devices, synthetic tests, and real user traffic. It also monitors application and endpoint performance at branch locations and natively integrates with Prisma SD-WAN for comprehensive overlay and underlay remote network performance visibility on all configured WAN paths. With ADEM, IT can solve application performance problems quickly and keep their agency flowing.

Prisma SASE for US Public Sector Features

Autonomous Digital Experience Management (ADEM): Provides segment-wise insights across the entire service delivery path with real and synthetic traffic analysis to driver proactive remediation of digital experience problems.

Cloud Access Security Broker (CASB): Applies governance, data classification and stops threats with both inline and API-based security for SaaS applications.

Data Loss Prevention (DLP): Comprehensive data protection that keeps sensitive data safe by categorizing it and protecting it while in motion across remote users and branch or remote locations.

DNS Security: Uses advanced analytics and machine learning for protection against threats in DNS traffic.

Firewall as a Service (FWaaS): Protects remote locations with Palo Alto Networks Next-Generation Firewall security, delivered as a service from the cloud.

ML-Powered Security: Leverage machine learning for proactive real-time and inline zero-day protection with automated policy recommendations

App-ID Cloud Engine: Download App-IDs from the cloud for applications that do not have specific predefined App-IDs

SD-WAN: Deep, seamless integration with Prisma SD-WAN, the industry's first FedRAMP, and StateRAMP authorized next-generation SD-WAN that is application-defined, autonomous and cloud-delivered.

Threat Prevention: Block exploits, malware, and command-and-control traffic using the combined threat intelligence of the entire Palo Alto Networks ecosystem.

VPN: IPsec, SSL, and clientless VPN provide options for connecting users and networks into the secure access service edge environment.

Zero Trust Network Access (ZTNA) 2.0: Combines fine-grained, least privilege access with behavior-based continuous trust verification and deep, ongoing security inspection as well as enterprise DLP to consistently protect all users, devices, apps and data everywhere.

App-ID Cloud Engine: Download App-IDs from the cloud for applications that do not have specific predefined App-IDs

Cloud Identity Engine: Accurately enforce security decisions for all your users at all times, with assured synchronization of all identity-related data in the cloud

Cloud Management or Panorama Management

Learn More

Visit paloaltonetworks.com/sase/federal