Prisma SASE Secure Branch with Shasta Cloud

Palo Alto Networks and Shasta Cloud deliver a fully integrated, secure branch solution that simplifies deployment, operations, and Zero Trust enforcement—delivering seamless connectivity, enhanced security, and operational efficiency for modern enterprises.

Benefits of the Integration

A well-integrated extended SASE solution must include:

- Zero touch provisioning to automate the onboarding of LAN, Wi-Fi, and SD-WAN devices, reducing operational complexity and overhead.
- Unified management for centralized visibility and control across wired, wireless, SD-WAN, and SSE infrastructure.
- Universal security enforcement covering all external and lateral communications between users/devices and applications.

The Challenge

Enterprises are vulnerable to increasingly sophisticated security threats as attackers exploit the inconsistencies and blind spots in their networks. Managing a diverse mesh of disparate wired, wireless, SD-WAN, and on-premises security solutions results in fragmented visibility as well as operations and security challenges across the enterprise.

Insecure branch offices invariably become launching points for lateral exploits. Managing through various consoles complicates troubleshooting and slows down incident response times, impacting overall network performance, reliability, and security. These issues are particularly prevalent in branch offices, which tend to have fewer security enforcement mechanisms and lack qualified on-site IT staff, often leading to misconfigurations that result in security gaps.

These inefficiencies translate to poor business outcomes, including increased operational costs, reduced agility, and a higher risk of costly security breaches.

The Solution

A truly effective solution demands a unified, cloud-managed platform that seamlessly integrates Wi-Fi, LAN, SD-WAN, and SSE functionalities offering unified visibility of the entire network, consistent security policy enforcement, and streamlined operations. It should enable enterprises to enforce a uniform security posture across all network environments, encompassing branch sites, campus offices, and both on-premises and cloud-based data centers.

The platform must be scalable, capable of accommodating varying network sizes and user densities, and support both indoor and outdoor environments. It must offer zero touch provisioning (ZTP) to simplify deployment and reduce operational overhead. To counter external and lateral security threats, the solution should employ a defense-in-depth architecture with granular microsegmentation of the Wi-Fi and LAN infrastructure, robust security inspection on local SD-WAN appliances, and scalable cloud-delivered security. It should also provide an API-driven architecture to enable seamless integration with network and security systems to simplify day 1 and day 2 operations and facilitate the use of future applications such as agentic AI–driven automations.

Shasta Cloud Wi-Fi Access Points and LAN Switches

Shasta Cloud provides a comprehensive portfolio of Wi-Fi access points and LAN switches, designed to support various network sizes from small branches to large campuses. The portfolio includes diverse indoor and outdoor multiband access points as well as access layer switches that support Power over Ethernet (PoE), facilitating efficient powering of Wi-Fi access points. All Shasta Cloud equipment is managed by a centralized cloud UI, simplifying deployment and administration and reducing operational complexity. For a detailed list of supported access points and switches, please refer to the Shasta Cloud Administrator's Guide.

Palo Alto Networks Prisma SASE

Palo Alto Networks Prisma® SASE is the industry's most comprehensive AI-powered platform, delivering SD-WAN, SSE, and digital experience management (DEM) functionalities as a single unified service. Prisma SD-WAN optimizes application performance through intelligent traffic steering and secures branch offices by leveraging the same trusted inline antimalware threat prevention, DNS security, and URL security capabilities that Palo Alto Networks Next-Generation Firewalls are known for.

Prisma Access provides a full suite of cloud-delivered security services, including secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), zero trust network access (ZTNA), and firewall as a service (FWaaS), protecting traffic flows between users/devices and public and private applications. Prisma ADEM offers complete end-to-end visibility and performance monitoring for all user-application interactions.

Palo Alto Networks Strata® Cloud Manager, Prisma SASE's unified cloud portal, manages these services, ensuring consistent visibility and security for all users, devices, and applications, regardless of location. This integrated network security solution simplifies operations, enhances user experience, and strengthens overall security across environments.

Palo Alto Networks and Shasta Cloud

Palo Alto Networks and Shasta Cloud have partnered to offer a secure branch solution, addressing the connectivity, security, and operational efficiency needs of modern enterprises. This collaboration delivers a unified universal zero trust network access (UZTNA) solution that enables programmatic provisioning, unified visibility, and centralized security control across all branch locations and sizes.

Managed by Strata Cloud Manager, the solution extends the benefits of Prisma SASE deep into the branch. It leverages the Palo Alto Networks CloudBlades platform to seamlessly incorporate Shasta Cloud's access points and switches into Prisma SASE, without requiring costly and disruptive deployments or upgrades. The integration enables unified Wi-Fi and LAN management, zero touch provisioning, configuration, and monitoring all accessible through a cloud management platform.

The solution extends Prisma SASE's defense-in-depth security model to the access layer. Prisma SD-WAN devices work in conjunction with Shasta Cloud's access points and LAN switches to inspect both external and lateral traffic flows. This integrated approach allows for granular security policies to be applied at the branch edge as well as the Wi-Fi and switching layers. It can isolate individual hosts at the port level, preventing the lateral movement of threats, limiting the impact of potential breaches, and enhancing overall security posture.

Use Case 1: Zero Touch Provisioning (ZTP) Onboarding

Challenge

Organizations face the challenge of rapidly deploying new branch sites and updating existing Wi-Fi, LAN, and SD-WAN systems. The challenges include:

- **Complex configurations:** Manual setups are time-consuming and error prone.
- **Remote site deployments:** Skilled IT staff may be unavailable.
- **Long onboarding times:** Deploying numerous devices is often time-consuming.
- **Consistency:** Manual configurations lead to variations.

As a result, organizations demand zero touch provisioning, which addresses the above challenges by automating configuration, enabling remote deployments, minimizing onboarding times, and ensuring consistent configurations.

Solution

Effortless deployment and operations are made possible with ZTP for Shasta Cloud switches and access points, and Prisma SD-WAN devices. The intuitive Prisma SASE CloudBlade integration allows for easy onboarding and seamless future device additions with minimal intervention. Strata Cloud Manager's CloudBlade monitoring page provides real-time visibility into every part of the network, now including Wi-Fi and LAN. The centralized dashboard allows administrators to quickly identify and address potential problems during

onboarding by providing instant insights into connectivity status, device performance metrics, and event logs, enabling proactive management and swift incident resolution.

Use Case 2: Unified Visibility and Granular Security Control

Challenge

Many enterprises still struggle with siloed network and security management, treating Wi-Fi, LAN, SD-WAN, and SSE infrastructures as distinct entities. This fragmented approach results in a critical lack of unified visibility, hindering comprehensive monitoring and correlation. Consequently, security policies are often inconsistent and stale, if implemented at all. This disjointed security posture exposes organizations to undetected and uninspected external and lateral threats. The issue is particularly acute at branch locations, where the potential for unmanaged devices and security gaps increases, leaving critical assets exposed to potential breaches and data exfiltration.

Solution

Prisma SASE provides comprehensive visibility and security enforcement across wired, wireless, SD-WAN, and SSE infrastructures. Its centralized cloud portal delivers actionable insights into site health in addition to user and device connectivity, now extending to Wi-Fi and LAN environments. This integrated solution secures all branch devices (including IoT/OT) and traffic (external/lateral) through granular microsegmentation and port-level isolation on Shasta Cloud switches and access points. Additional security inspection on Prisma SD-WAN enforces context-aware security policies and inline threat prevention (anomaly detection, antimalware, DNS security, URL filtering) on all traffic flows. If needed, Prisma Access can further inspect traffic with its comprehensive security services in the cloud.

About Shasta Cloud

Shasta Cloud is a network solution provider, offering enterprise-grade cloud-based networking solutions. For more information, visit: https://www.shasta.cloud.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, empowers businesses to embrace digital transformation with industry-leading, AI-powered solutions for network and cloud security, and security operations. Powered by Precision AI®, our technologies deliver precise threat detection and swift response, minimize false positives, reduce complexity and improve security outcomes. Our platformization approach integrates today's security solutions into a unified, scalable platform, streamlining management and providing operational efficiencies with comprehensive protection. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_pb_shasta-cloud_033125