paloalto NETWORKS | PRISMA SD-WAN BY PALO ALTO NETWORKS

The Power of the Zero Trust Branch

Branch Evolution Demands SD-WAN Innovation

Branch transformation brings a swell of digitization.

Digitization addresses changing requirements but comes with challenges.

SaaS adoption continues to grow as businesses seek to enhance productivity and collaboration across branches. The accelerating pace of digitization delivers numerous benefits. It also has seen the rise of several trends that highlight the need to update how services are delivered.

The increased consumption of dynamic and distributed SaaS applications has impacted user experience by increasing latency. This is caused by performance limitations at the SaaS server level.

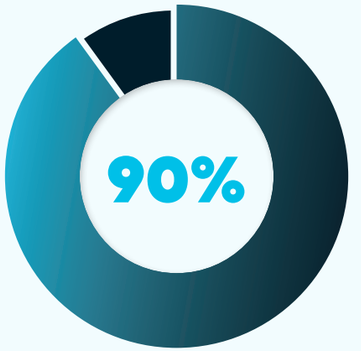
Branches have also seen an explosion of AI applications, BYOD, and IoT devices. This increase in connected devices exposes branches to new, more sophisticated threats.

Network complexity is also growing as traditional SD-WAN deployments are propped up to support greater demand, and point solutions are added to accommodate changing environments.

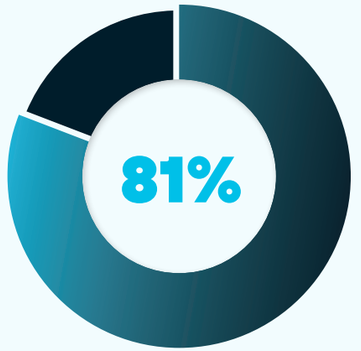
Branches need active-active connectivity for SaaS, internet, and cloud applications, as well as enhanced security for these apps and connected devices. Legacy solutions do not provide availability models that are fully resilient to single-device failure and are not able to deliver the Zero Trust security necessary to protect branch operations.

Get the best of digital transformation with a cloud-delivered branch.

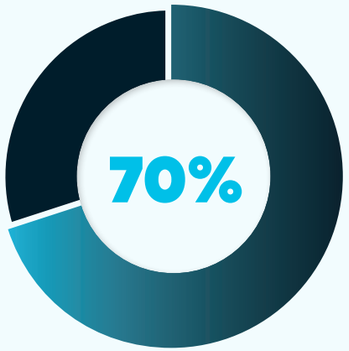
Deliver flexible connectivity, direct-to-app access, and the Zero Trust protection required by today's branches by eliminating the complexity of managing archaic, point solutions that add overhead to IT teams. The right solution delivers application assurance for all apps, including SaaS. It also secures users, apps, and devices like AI and IoT devices while significantly simplifying operations for IT teams and increasing application performance from end to end. Enter secure access service edge (SASE).



of end-to-end latency occurs at the first mile, negatively impacting the performance of distributed and dynamic SaaS applications.*



of businesses have experienced an IoT-focused attack due to built-in vulnerabilities.**



of the M&A as a growth strategy has experienced business impact due to integration issues.***

* Palo Alto Networks ** Starfleet and Palo Alto Networks research *** Source – https://hbr.org/2020/03/dont-make-this-common-ma-mistake

It’s time to rethink branch application delivery.

Shift focus from network to applications.

Because SaaS applications are global, distributed, and always on, it is not possible to run from the branch to the app. With legacy systems, traffic forwarding decisions cannot be controlled, resulting in poor performance and user experience.

SaaS application’s dynamic content requires direct-to-app access to:

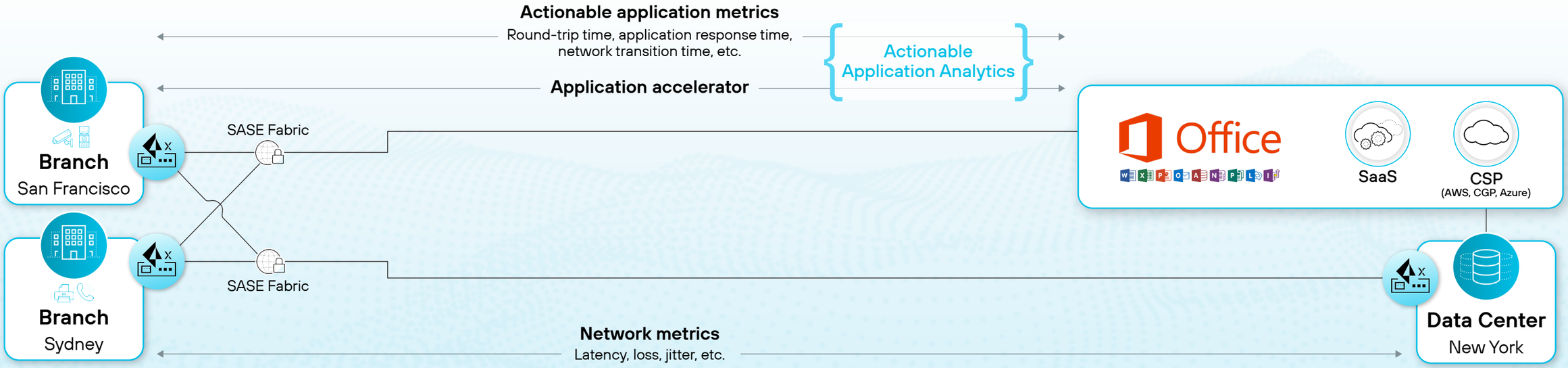
- Accelerate the delivery of application performance for all applications without the hindrance of only network SLAs.
- Move beyond basic caching techniques that fail to optimize performance for dynamic content of SaaS applications.
- Eliminate the need for multiple tools for SD-WAN, segmentation, WAN ops, and visibility.
- Support scalability and eliminate manual interventions, especially for “day two” operations that have substantial administrative overhead for networking and ops teams.

Take an application-session-based approach to traffic.

Switching to an application-session-based approach to traffic engineering eliminates the limitations of most SD-WAN solutions that are packet-based and forced into being bookended.

Natively integrated application acceleration is critical for branch applications. Unlike traditional caching techniques that work on application protocols, this new model requires an understanding of each user’s journey inside the app and the ability to proactively compute the dynamic content for that user to deliver the necessary application performance.

All of this traffic must also be secured. A Zero Trust approach should be employed to protect all users, apps, and devices, including AI apps and IoT devices. Employing Zero Trust policies ensures continuous security inspection and enforcement of least privilege access.



Power the Zero Trust branch with Prisma SASE.

The Right Way to Transform and Protect Branches

Organizations have adopted cloud-delivered security solutions to protect their branches, integrating existing SD-WAN solutions with a security service edge (SSE) solution from a separate vendor. The result is a mix-and-match solution that forces manual IPSec tunneling and manual key management. This leads to a number of issues, including complexity, security gaps, prolonged troubleshooting, and fragmented visibility.

Palo Alto Networks Prisma SASE powers the Zero Trust Branch that is dynamic, digitized, and secure with best-in-class SD-WAN.

Unlike most SD-WAN solutions, Prisma SASE provides:

- Application assurance for all apps based on application SLAs and app acceleration to deliver exceptional user experience.
- A unified solution eliminates the latency, administrative overhead, and other limitations of fragmented approaches.
- Integrated Zero Trust security for users, apps, and devices, including AI apps and IoT devices.

Exceptional user experience

Operational simplicity & resilience

Integrated security

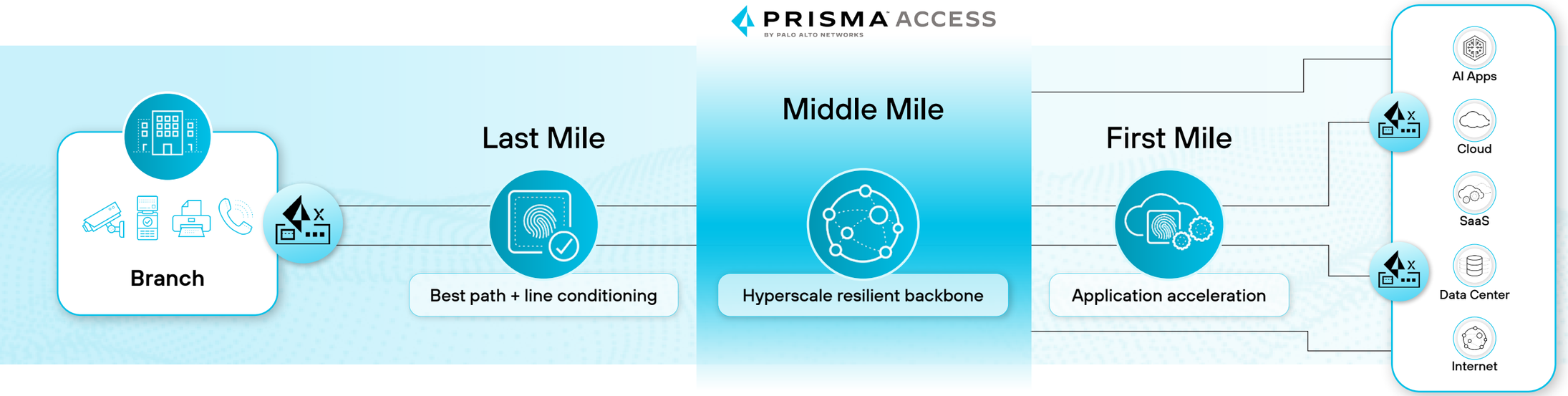
Deliver applications 5x faster with application acceleration and assurance.

Gain end-to-end control from first-mile WAN connectivity to the middle-mile global cloud to the last mile where the application server resides.

Prisma SASE delivers foundational capabilities, like application failover and load balancing, for all applications by providing direct-to-app access. It also ensures exceptional user experience by providing application assurance with application SLAs, optimization techniques like FEC and packet duplication, and application acceleration. Application brownout remediation is also automated.

Additionally, Prisma SASE provides traffic engineering and optimization capabilities to a cloud-delivered security solution (security service edge, SSE) with native integration to Prisma Access. This delivers middle-mile optimization by establishing low latency, redundant connections to Prisma Access nodes that enable customers to leverage its global hyper scaler backbone to provide middle-mile optimization.

Finally, Prisma SASE tackles the last mile, where connections are susceptible to disruptions and slowdowns. Unlike legacy solutions, Prisma SASE can optimize all applications, including SaaS applications. It extends the SD-WAN fabric capabilities even into Prisma Access for enhanced network availability, and it delivers last-mile performance with best-path selection, such as closest geo.



Unlike traditional caching techniques, Plato Alto Networks Application acceleration is context-aware at a per-user, per-application level. This allows it to improve application performance by up to 5X, delivering performance at the first mile, where most application server issues impact user experience.

Protect people, apps, and things at scale.

Bring Zero Trust to the branch.

Seamlessly integrate cloud-delivered security that is distributed at cloud scale to enforce true least-privilege access and ensure only the right people get access to the right information and assets. Prisma SASE provides visibility to all assets, including the rapidly growing IoT devices, to ensure that the right controls and policies are applied to the entire network.

ZTNA 2.0

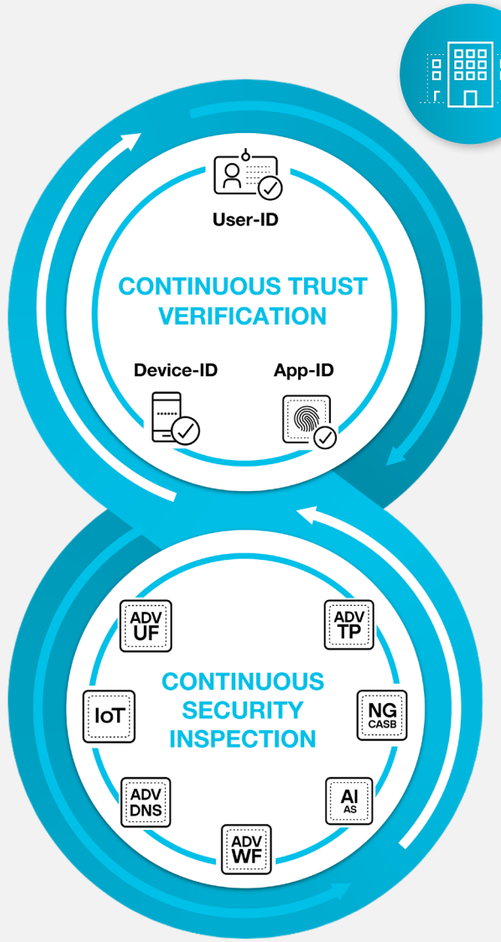
Ensure the comprehensive protection of all users, applications, and devices with ZTNA 2.0, delivered from the cloud with advanced security capabilities and Precision AI. For instance, when SaaS applications are accessed, CASB-like capabilities are enforced, and when a user accesses the Internet, secure web gateway functionality is applied to the traffic.

IoT

Unlike other solutions, Prisma SASE provides IoT security for devices with real-time threat detection based on behavioral analysis. Prisma SASE identifies and secures IoT devices at the device and firmware level without any incremental agents or products needing to be deployed. Enforcement policies are applied based on device and threat signatures. Depending on what is detected, the whole network can be blocked, or specific policies can be applied to deny access to a particular device.

AI and ML

From a security standpoint, access controls are not enough. Deep security inspections are needed for all applications. Prisma SASE performs these inspections using Precision AI capabilities.



Instead of fragmented solutions across the board, all of this can be combined to deliver ZTNA 2.0 fluidly.

Policies can be specified using user ID, app ID, and device ID to grant access

Continuous trust verification and traffic inspection are conducted, regardless of which SSE node is used to access application traffic.

Enforce the Zero Trust network access model everywhere.

Gain operational simplicity and efficiency.

Optimize branch digitization by simplifying network operations with automation and observability.

Simplify Onboarding

Prima SASE automates all connectivity from the branch to the SSE, which is customer access, making it possible to bring up a branch in minutes. A branch can be onboarded with all applications and appropriate security from a single screen. This includes setting up encryption, connectivity to the SSE, and connections to apps.

Increase Availability

98% time saved in SD-WAN policy management with Prisma SD-WAN. This enables flexible connectivity with high bandwidth broadband and 5G to improve capacity, availability, and resilience.

Provide Deep Observability

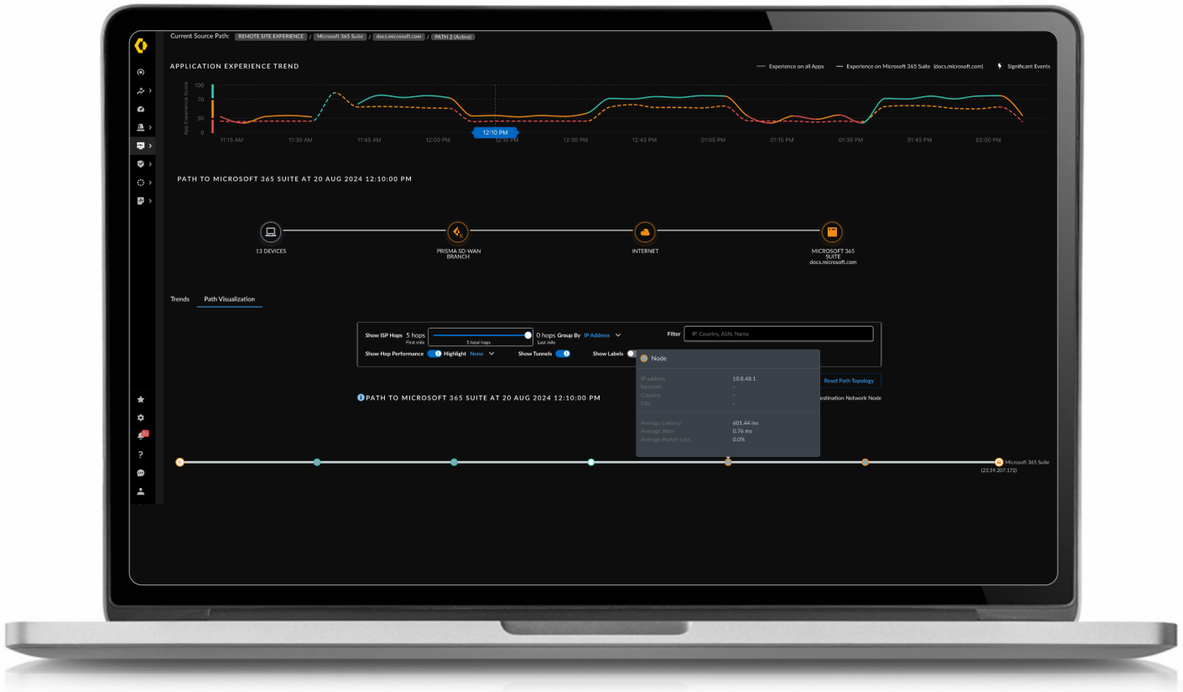
Allow IT teams to drill down into issues while effectively correlating and prioritizing critical network events to resolve issues quickly. For instance, observability from a laptop connection to the Wi-Fi network to connectivity in the branch to ISP connectivity to the application and, finally, to the SSE.

Use Artificial Intelligence to Streamline Issue Resolution

AI-based problem detection and predictive analytics enable proactive and automated issue remediation, which reduces network trouble tickets by 97%. Also, natural language processing (NLP) allows admins to perform natural language queries using free-form and curated questions to assess network health and remediate issues using guided and automated network-centric actions.

Leverage Common Policy Framework

Network and security are combined with unified management, policy, and data to simplify operations significantly. As network and security policies have the same constructs, they can result in operational efficiency improvements of up to 75%*, making them easier to configure, implement, and change.



Prisma SASE delivers a unified policy across networking and security using common policy constructs with consistent identities like App-id, User-id, and Device-id to secure applications, users, and things.

*Prisma SD-WAN Forrester TEI Spotlight

Take a proactive security stance against sophisticated threats arising from AI adoption.

Protect branches from all sophisticated threats with AI Access Security that provides real-time visibility into AI usage, access control for unsanctioned AI apps, and comprehensive data protection by scanning shared data, secrets, and IP.

AI applications enabled by generative AI and AI models are increasing in the branch. AI Access Security, powered by Precision AI, not only provides visibility into all AI apps and models but also gathers their signatures and creates baseline patterns. Using this information, security policies are automated to prevent unsanctioned actions, including preventing sensitive data from being fed into models or blocking it from leaving the network.

Precision AI also provides protection against the latest threats in near real-time. Protections are built into Prisma SASE and delivered automatically. Security services are run in line to detect and prevent known and unknown threats by leveraging rich and holistic threat data from 70K+ customers to identify new and emerging threats better. This enables real-time security, delivered consistently through a robust global cloud infrastructure.

AI Access Security also increases teams' productivity by allowing GenAI apps to be used while controlling usage to ensure safety and security. Using AI Access Security, robust application access controls can be set up to provide real-time visibility into what GenAI apps are being used for and by whom. Additionally, AI Access Security provides comprehensive data protection, AI posture management, and security controls for both sanctioned and shadow AI apps.

Safe and secure usage of GenAI apps is made possible with AI Access Security's innovative features, including:

- **GenAI Posture Management—**Provides visibility and control over GenAI Apps installed via marketplaces to help identify, monitor, and remediate unauthorized AI bots used in SaaS apps.
- **Real-Time User Oversight and Training—**Enhances user experience through real-time user training and allows administrators to detect and respond to sensitive data leakage incidents in real time and coach users on acceptable practices.
- **GenAI Usage and Compliance Reporting—**Generate comprehensive reports on GenAI app usage, risks, security, and compliance.

Prisma SD-WAN Delivers Results

Deliver exceptional user experiences.

Global Leader in Design Software Modernizes Network and Security Architecture with SASE

Catalyst for Change

Autodesk needed to enhance performance to support employees now working in a hybrid fashion, connecting to company resources and tools from multiple locations globally, with more than 80% of the applications accessed over its network being SaaS-based.

Benefits Realized

The results of adding Prisma Access and Prisma SASE to its Prisma SD-WAN included:

- Migrated 60+ branch offices in less than seven months
- Improved remote network availability by 85%
- Optimized app performance by dynamically steering traffic based on real-time patterns
- Gained end-to-end visibility with AI-driven analytics to drive network improvements

> *Prisma SASE has delivered robust network security across all our offices, remote workstations, and application workloads. And it's all managed seamlessly from a single pane of glass.*
>
> **Anish John**
> Senior Manager, Network Engineering, Autodesk

Gain operational simplicity and efficiency.

Healthcare Technology Company Slashed Troubleshooting Time, Increased Uptime, and Reduced Risk with Unified Solution

Catalyst for Change

After more than a dozen acquisitions nationwide, Relias IT team was struggling to ensure reliability and security with systems from multiple vendors.

Benefits Realized

- Eliminated network pain points with an integrated solution that provides seamless connectivity and security
- Reduced troubleshooting time by 95%
- Achieved 99.999% uptime for real-time applications
- Cut time spent maintaining threat-hunting tools from hours a week to only minutes a week
- Minimized the need for senior-level expertise by switching to a single, intuitive console
- Decreased risk by replacing bug-prone firewalls

> *The big win for us is the ability for Palo Alto Networks products to be a force multiplier. Both Prisma SD-WAN and firewalls deliver exceptional ease of use and stability.*
>
> **Todd Webster**
> IT Infrastructure Manager, Relias

Protect people, apps, and things at scale.

World's Third Largest Distiller Takes Integrated SASE Approach to Secure Network and Address Connectivity Challenges

Catalyst for Change

After a major security incident, Beam Suntory's team realized that it not only needed to overhaul security but also update the network architecture to reduce latency and manage data center traffic load for its more than 4,500 users.

Benefits Realized

- Expanded automation, including the ability to create and implement network-wide policies on the fly
- Enabled remote monitoring
- Improved the security posture, network reliability, and performance
- Increased control over all egress traffic with the ability to define whitelists and blacklists from a single location
- Integrated cloud-delivered security solutions (CDSS) that could move security beyond the traditional perimeter

> *The product saved our lives and increased both the performance and the security level.*
>
> **Qun Wei**
> Senior Network Architect, Beam Suntory

See What You Can Get with Zero Trust Branch Powered by Prisma SASE

Deliver Exceptional User Experiences. Gain Operational Simplicity and Efficiency. Protect People, Apps, and Things at Scale.

Palo Alto Networks Prisma SASE powers the Zero Trust Branch with best-in-class SD-WAN. Unlike other SD-WAN solutions, it provides application assurance for all apps, including SaaS apps, which are dynamic in content while enforcing zero trust with integrated security to protect users, apps, and devices, including IoT. It eliminates the challenges of other fragmented solutions with a unified SASE that provides complete SD-WAN visibility, segment-wise insights, and querying using natural language processing to simplify troubleshooting and improve mean time to resolution.

Improve time to:

	**VALUE** **107% return on investment***	Build a network to deliver applications, services, and business capabilities to remote offices with application assurance at the first, middle, and last to realize an improved uptime in business, resulting in an ROI of up to 107%.
	**INNOCENCE** **75% improved operational efficiency***	Bring network and security together with a unified SASE that provides unified policy, data, and management and see operational efficiency improve by up to 75%.
	**REMEDIATION** **97% reduction in trouble tickets****	Automate and simplify operations significantly with native ADEM (autonomous digital experience management), actionable insights, and an NPL-powered copilot to deliver better business outcomes and availability and reduce trouble tickets by up to 97%.

* FORRESTER®

** SA Recycling

paloalto® NETWORKS

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

prisma_eb_the-power-of-the-zero-trust-branch_030725