



Get
comfortable
with SASE



LEGACY.



FIREWALL.



SASE.

Take your seat in the SASE market with Exclusive Networks

Ready?

Sit back and let's get you comfortable with SASE

What exactly is SASE?

A simple, agile alternative to multi-vendor, hardware-based solutions, SASE provides remote access for employees, with control over what they can and can't do. And it's all managed through a single pane of glass – giving every user a great experience that's underpinned by best-in-class security.

**Secure Access
Service Edge**

=

SD-WAN

+

Network security

+

Cloud delivery



Did you know?

45%

of enterprises will adopt managed SASE services by 2026¹

And why does it matter?

Hybrid working offers great flexibility, but ensuring secure, seamless access for everyone? That can feel uncomfortable for your customers. Unauthorised apps, unsecured devices and evolving threats pose real challenges for hybrid security.

With SASE, you can address these obstacles for your customers, bringing security to where their users actually work – anywhere, anytime, on any device.

We get that you may not be familiar with SASE – and we know your customers will be feeling the same. That's why in this guide you'll find everything you need to get comfortable with the opportunity, so you can develop the right portfolio of solutions that will give you the upper hand in this rising (and lucrative) market.

SASE under the hood

Get to know key SASE components

Treat this as your quick reference guide to SASE's USPs.

SD-WAN: SWG:

Software-defined Wide-Area Network

Think of SD-WAN as your customers' smart network traffic controller. Instead of expensive hardware boxes at every location, SD-WAN uses software to intelligently route data across the internet, choosing the best path for performance and cost.

CASB:

Secure Web Gateway

SWG acts as an internet bodyguard for your customers. Whether employees are in the office or working remotely, SWG sits between users and the web to block malicious websites, filter inappropriate content and maintain company policies.

ZTNA:

Cloud Access Security Brokers

Poised like a cloud watchdog, CASB keeps track of which cloud apps employees are using, where sensitive data is stored and who has access to what. It provides greater visibility across cloud services, and can reveal dangerous shadow IT.

FWaaS:

Firewall-as-a-Service

Imagine FWaaS like a cloud-based security checkpoint that's active 24/7. Instead of buying expensive firewall hardware for each premises, FWaaS delivers protection through the cloud that's automatically scalable and always up to date.

Sit easy with Prisma® SASE from Palo Alto Networks

When you deliver a Palo Alto Networks solution with Exclusive Networks, you know you're giving your customers the best from the best. Here are the components that make Prisma® SASE so special – you can deliver them as a full SASE solution, individually or as a mix.

Prisma® Access

Prisma® Access offers industry-leading security powered by Precision AI® through a single, cloud-delivered solution. It's like a security umbrella that provides complete coverage for users, apps, devices and data regardless of where they are.



Threat prevention

Stops 30.9 billion daily threats with real-time security powered by Precision AI® and the industry's largest threat intelligence database.



Universal deployment

Delivers industry-leading 99.999% uptime SLA with a hyperscale backbone that avoids outages and enhances user experience.



Unified management

Boosts efficiency in managing SASE and making policy changes by 75% thanks to seamless management capabilities.

Prisma SD-WAN

As a cloud-delivered service, Prisma SD-WAN transforms traditional WANs into a simplified, secure and cost-effective alternative. Think of it like a hardware box that operates from the cloud, enabling your customers to avoid investing in new physical hardware for firewall solutions.



Cost-effective

Minimises costs and complexity compared to traditional WAN solutions.



Enterprise-secure

Securely connects customers' branch offices and data centres.



Future-ready

Eliminates the need for new hardware investments while supporting business developments.

Sit easy with Prisma® SASE from Palo Alto Networks

Prisma® Access Browser

As the industry's only SASE-native integrated secure browser, Prisma® Access Browser is built to secure web access at the browser level. It's ideal for unmanaged or personal devices, with the ability to deploy rapidly to users in remote locations, cutting the need to ship laptops directly.



Zero Trust

Applies Zero-Trust policies and granular data controls across BYOD and independent workers' devices.



Data protection

Increases visibility and strengthens control with last-mile data protection capabilities.



Precision AI®

Keeps every user safe with 347K new and unique malicious URLs prevented every day.



Did you know?

25%

of enterprises will use managed browsers or extensions by 2026 – up from 10% in 2023²

Autonomous Digital Experience Management (ADEM)

ADEM assesses enterprise-wide digital experience, application SLAs, incidents and IT infrastructure from a unified dashboard. It's designed to proactively detect and resolve issues and degraded user experiences through its built-in AIOps and root-cause analysis capabilities – making it one of the most attached 'add-on' products to Prisma® SASE.



Accelerates resolution

Supports IT to rapidly resolve app performance issues while ensuring an exceptional user experience.



Performance monitoring

ADEM monitors device performance, Wi-Fi and ISP quality – and offers users real-time guidance.



Streamlines operations

Reduces internal friction and waste of internal resources when diagnosing problems.

Case study 1

SASE inspiration in the wild

Real-world examples
of deployment success



Wealden District Council

Local government organisation in East Sussex now seamlessly delivering public services faster and with tighter security.



The challenges:

- Hybrid workforce needed secure service delivery
- Existing network security solution was overly complex
- Concerns around resilience of legacy firewall



The technology:

- Prisma® Access
- Prisma® SASE
- Advanced Threat Prevention
- Advanced URL filtering
- Panorama
- WildFire



The results:

- **Granular visibility** of application traffic and continuous security inspection through the Prisma® SASE platform's ZTNA 2.0
- **Enhanced and consistent agility** across SaaS, cloud and on-premises applications
- **Reduced friction** for staff who can now work more productively from their own homes, in the office or on the go



The end-to-end implementation and support have been brilliant. The Palo Alto Networks team are incredibly responsive, taking control of problems and resolving them very quickly. I don't think it could have gone much better.

Robert Manktelow, Digital Services Network Architect, Wealden Council



SASE inspiration in the wild

Real-world examples
of deployment success

NetApp

Global unified data storage company uses Prisma® Access Browser to keep its users and data under control.



The challenges:

- SaaS solutions were moving security requirements into the application layer
- Controlled and secure access required for users and devices



The technology:

- Prisma® Access Browser



The results:

- **Reliable productivity** for all users, regardless of location or resource use
- **Comprehensive protection** from a singular source, eliminating the need for additional agents
- **Consistent security** across both managed and unmanaged devices



I can control who has access to what and what they do. That aligns with Zero Trust. And I can overlay other capabilities on user and device activity and get ahead of threats. It's like a one-size-fits-all solution for our environment.

Sarah Mignona Coté, CISO, NetApp



SASE inspiration in the wild

Real-world examples
of deployment success



Westfield Group

Westfield unified network and security through Prisma® SASE to enhance user experiences, simplify operations, and cut costs across 34 global retail destinations.



The challenges:

- Rapid digital transformation and a shifting retail landscape
- Securing public websites and mobile applications used by millions of shoppers
- Maintaining visibility and cost control across a distributed IT environment



The technology:

- Prisma® SASE integrating Prisma® Access and Prisma® SD-WAN
- Unified, cloud-delivered networking and security management
- Clear line-of-sight and policy control across sites and cloud resources
- Streamlined application delivery through a single SASE platform



The results:

- **Centralised visibility and control** of network services across all mall locations and in the cloud
- **Streamlined application development** and business processes while strengthening security
- **Increased customer satisfaction** and employee productivity through secure, reliable access
- **Reduced costs** while preventing unauthorised access and ensuring compliance confidence



When people are making connections to your SaaS platforms or your other applications, you know they're going where they're supposed to go – and if they try to go somewhere they shouldn't, they're blocked. So from a control aspect, Prisma SASE is a great positive for CISOs and Compliance Officers.

Ken Ogami, CIO/CISO, Westfield Group Worldwide



SASE inspiration in the wild

Real-world examples
of deployment success

Ministry of Justice

The Ministry of Justice modernised its network security infrastructure with a unified SASE platform, delivering secure, responsive digital services across prisons, courts, and probation offices.



The challenges:

- Integrating fragmented network security into a single solution to meet growing demand and enable fast deployment of new services
- Consolidating limited security visibility to enable proactive incident resolution and reduce operational risk
- Reducing the burden of manual incident management to free resources for strategic threat-hunting work



The technology:

- Prisma® SASE, consolidating Prisma® Access and Prisma® SD-WAN
- Cortex® XSIAM
- Next-generation firewalls



The results:

- **Centralised security monitoring**, with 15TB of data ingested daily, 6-12x daily increase in incidents resolved and detection times cut to minutes
- **Enhanced performance and optimised costs** through five-fold average bandwidth uplift, consolidation of three monitoring tools, and cost-effective internet access circuits
- **Proactive Zero Trust security** across every user, routing traffic directly to destinations while strengthening overall security



We're creating an evergreen network security environment with Palo Alto Networks. Security consolidation will continue to make our justice services simpler, faster, and better for everyone.

Nava Ramanan, Deputy Director, Digital Infrastructure and Security Operations,
Ministry of Justice



Simple routes to SASE adoption

Now you've been inspired by real-world deployments, it's time to get practical. In the next few pages, we're outlining four easy routes for bringing Prisma® SASE to your customers in style.

Route one: Consolidating network and security

Traditionally, SWG, CASB and DLP were siloed, but Prisma® Access SASE integrates them all – providing completely secure web access, whether users are in the office or working remotely.

SWG ensures safe internet browsing and access to SaaS applications, while CASB provides visibility and control over data in the cloud. DLP keeps sensitive data secure from loss or theft, maintaining compliance with industry regulations.

Did you know?

\$21 billion

SWG market value is expected to reach \$21 billion by 2033, a 10.08% CAGR



Customer pain points this route addresses

- Managing multiple, independent security products can be complex and inefficient
- Ensuring consistent data protection across on-premises and cloud environments
- Maintaining compliance with various industry regulations and standards



Conversation starters for this route

- How do you currently manage security for your web traffic and cloud applications?
- Are you facing challenges in protecting sensitive data across different environments?
- What are your main concerns regarding compliance with industry regulations?



Route one products:

- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)

Palo Alto Networks insights

ChatGPT hit 18 billion weekly messages from 700 million users in less than three years. This sheer scale and speed of data means that it's increasingly impractical to separate connectivity from security. The source, destination, and pathway of data are all potential vectors for attack – and security architectures have to account for them all.

The more fragmented your infrastructure, the greater the risk. Consolidating SWG, CASB, and DLP into a unified SASE architecture removes blind spots, strengthens your security posture, and simplifies compliance. Prisma® Access delivers this integration seamlessly – with one stack, one policy, and complete protection.

Simple routes to SASE adoption

Route two: VPN replacement with a cloud-delivered remote access solution



Route two products:

Zero Trust Network Access (ZTNA)

The ever-expanding attack surface makes connecting to enterprise networks over a VPN no longer secure.

ZTNA goes beyond VPN encryption to reduce the attack surface through least-privileged access while inspecting traffic for threats and protecting applications. Prisma® Access SASE consolidates multiple security and networking features, including ZTNA, delivering them inside a future-ready package that's built for cloud architectures.



Customer pain points this route addresses

- Traditional VPNs can introduce latency and degrade user experience
- Scaling VPN infrastructure to accommodate a growing remote workforce can be challenging
- Managing and maintaining on-premises VPN concentrators can be resource-intensive



Conversation starters for this route

- How do you currently provide remote access to your employees?
- Are you experiencing performance issues with your existing VPN?
- How do you manage the scalability and maintenance of your remote access infrastructure?

Palo Alto Networks insights

Would you choose a real private network over a virtual one? That's what Zero Trust Network Access (ZTNA) delivers, with continuous monitoring and verification of every user, device, and application, both at and after login.

Where traditional VPNs are 'connect and forget', Prisma® Access delivers ZTNA inside a cloud-delivered SASE platform, to minimise the attack surface while inspecting all traffic for threats. That means always-on visibility, zero-trust control, and a better user experience.

Did you know?

\$262 billion

ZTNA market value is expected to reach \$262 billion by 2033, a 23.54% CAGR



Simple routes to SASE adoption

Route three: Extending SASE protection seamlessly to every device



Route three products:

Prisma® Access Browser

Prisma® Access Browser provides secure access to applications from unmanaged devices – making it ideal for organisations with a remote or hybrid workforce where employees access corporate resources through personal devices.

Prisma® Access Browser leverages a secure, Chromium-based browser to inspect and secure all traffic, reducing the need for expensive Virtual Desktop Infrastructure (VDI) environments. This strengthens security while improving the user experience by allowing employees to use familiar devices.



Customer pain points this route addresses

- Ensuring secure access from personal or unmanaged devices
- Managing and maintaining virtual desktop infrastructure can be expensive
- Providing a seamless and secure user experience for remote workers



Conversation starters for this route

- Do your employees use personal devices to access corporate applications?
- Are you looking for ways to reduce the cost and complexity of your VDI environment?
- How do you ensure secure access from unmanaged devices?

Palo Alto Networks insights

The explosion of web, SaaS, and GenAI applications has expanded the attack surface far beyond the corporate perimeter. Data is currency, and every connection – whether through an employee or a third-party contractor – can be a potential entry point for risk and malicious actors. That's why it's critical for your customers to understand which apps are being used, who's using them, and what data is being shared. And if they don't have that visibility or control – especially across third party apps – it's time for Prisma® Access Browser.

Built on a secure Chromium foundation, Prisma® Access Browser extends SASE protection to unmanaged devices with no VDI required, helping keep users productive, sensitive data protected, and businesses secure.

Did you know?



62%

of the workforce uses unmanaged devices to access company data

Simple routes to SASE adoption

Route four: Secure, optimised connectivity for branch offices and remote sites

Integrating SD-WAN with FWaaS provides a flexible and scalable solution for connecting distributed locations, while also simplifying network management and enhancing security.

Prisma SD-WAN enables efficient routing of traffic over multiple connections, reducing reliance on expensive MPLS circuits. While FWaaS through Prisma® Access inspects and secures all traffic, no matter the connection type.

Did you know?

65%

of new SD-WAN purchases will be part of a single-vendor SASE offering by 2027



Customer pain points this route addresses

- Network performance: Ensuring reliable and high-performance connectivity for branch offices
- Reducing the cost of MPLS circuits and other traditional networking solutions
- Providing consistent security across all connections and locations



Conversation starters for this route

- Do you need to connect distributed locations?
- Are you trying to make cost savings across your networking solutions?
- Are your branch offices able to work as productively as your main premises?



Route four products:

Software-defined Wide-Area Network (SD-WAN)

Firewall-as-a-Service (FWaaS)

Palo Alto Networks insights

Secure branch connectivity is critical across every location, from offices and retail stores to manufacturing sites, schools, clinics, and pop-up locations. While users are often seen as the weak link, distributed devices and sites pose an equal or greater risk. Security cameras, machinery, and medical equipment are examples of connected IoT devices that can expand the attack surface – and many organisations have limited visibility into the number of online devices, as well as the risks they pose.

Prisma® SD-WAN and FWaaS, working together within the Prisma Access SASE platform, deliver secure, high-performance connectivity with integrated security across every branch, connection, and cloud. This unified approach simplifies management, scales protection, and ensures consistent policy enforcement, helping secure all users, devices, and data.

Start a new conversation, comfortably

When you're looking to spark a conversation on SASE solutions, we recommend you consider these three focus areas as a starting point:

1. The needs of the customer

Consider suggesting SASE as a better option to their existing setup, like replacing outdated VPNs or assisting with cloud migration.

2. The size of the customer

SASE is ideal for customers with hybrid or fully remote workforces, especially those with high digital maturity and over 1,000 highly dispersed users.

3. The focus of the customer

When customers want simplicity, scalability, visibility and control, SASE is the perfect choice for their needs.

It's also worth considering your customers' primary motivators for moving to SASE solutions, and building these into your conversations where you can:



Security and threat concerns:

- Ransomware attacks and insider threats
- Unsecured devices
- Alert fatigue



Workforce and infrastructure changes:

- Remote workforce
- Multi-vendor infrastructure
- Resource constraints



Technology evolution:

- Cloud services adoption
- The increasing cost of traditional network architecture
- The desire to move away from outdated VPNs
- The need to tackle performance issues with business-critical SaaS apps



Did you know?

\$26 billion

will be the SASE market value by 2027³

The opportunity is yours for the taking



Average deal size:
\$325k⁴



Total addressable market:
\$21 billion



Market growth:
26%
predicted for FY24-27
in EMEA and LATAM⁵



ROI: Up to
270%
over a 3-year period



Renewal opportunities:
5-7 years
of seamless renewal
opportunities



Upgrades and add-ons:
an increase
in licences is all that is needed
to account for additional usage

Relax with partners that do the heavy lifting for you

Exclusive Networks: Your go-to SASE specialist

- The highest-level Palo Alto Networks Authorised Support Centre (ASC) partner
- First distributor to bring Palo Alto Networks to the channel over 16 years ago
- A Palo Alto Networks Authorised Training Centre
- 24/7 support with 9.2/10 satisfaction score
- EMEA Certified Professional Services Partner – delivering over 400 consulting days a year
- Pre and post-sales and installation support
- Flexible payment solutions
- SASE resources
- Accreditation Acceleration Workshops
- Tailored workshops to support your SASE skills
- SASE Demo Labs
- SASE Titans Training

Palo Alto Networks: True SASE specialists

- Named a Leader five times, and the only one to be named in all three Gartner reports:
 - 2024 Gartner® Magic Quadrant™ for Single-Vendor SASE
 - 2024 Gartner® Magic Quadrant™ for Security Service Edge (SSE)
 - 2024 Gartner® Magic Quadrant™ for SD-WAN

Rest. Assured. Take the easy journey to SASE.

From start to finish we can guide you through the opportunity

We have everything you need to bring your new specialism to your customers – all wrapped around market-leading SASE from Palo Alto Networks.



Technical support

From installation to pre and post-sales, we can help you scale your SASE offering quickly.



Authorised training

As an authorised Palo Alto Networks training centre, we can support your journey to becoming a specialist.



Specialisation support

Our team are ready to design a specialisation roadmap to accelerate your pathway to accreditation.

Take a seat in our Prisma® SASE Demo Lab

- Upskill your teams with free training
- Showcase Prisma® SASE solutions in a controlled environment
- Demonstrate your SASE expertise to your customers
- Accelerate deal closure
- Identify influential customers and decision makers
- Recognise opportunities for add-on sales

Prisma® Access demo

Discover the interface and management console, with a walkthrough on how to configure and set up policies.

Ultimate test drive

In just three hours, you'll experience a simulated desktop scenario that compares legacy and less-secure technology against Prisma® SASE.

Prisma® Access Browser

In this real use case demo, see what happens when a user tries to take a blocked action, like using generative AI.

Ready to get comfortable?

[VISIT OUR HUB](#)

Your new comfortable is a specialist away

Become a trusted expert in the growing SASE market

As the first distributor to bring Palo Alto Networks to the UK, we offer unmatched expertise, guiding you from presales to installation and ongoing support. Our services include rapid quote delivery in just four hours and expert consulting as an EMEA Certified Partner. With our training, advice and wraparound services, we'll help you and your customers sit comfortably with SASE.

To learn more about Palo Alto Networks products and offerings, please check out our hub or contact us today.

Secure your seat in the SASE opportunity

CONTACT US NOW



- 1 Gartner, Magic Quadrant
- 2 Gartner, Emerging Tech
- 3 Gartner, Forecast Analysis
- 4 Palo Alto Networks and Exclusive Networks: Based on existing-pipeline and historical-deal data
- 5 Palo Alto Networks Market Intelligence: Based on data from Gartner, IDC, Omdia Dell'Oro and Other Research Firms