paloalto® NETWORKS

Driving the future of work through enterprise-wide SASE

A CIO'S GUIDE TO PLANNING AND IMPLEMENTATION

Introducing a **transformative** idea

We all know the trends that are driving the digital transformation of our businesses. The shift to remote and hybrid work is now a reality. The benefits of cloud, which allow us to dive deeper into data, innovate faster with AI, and compete better. The evolution of the marketplace, requiring us to reach our customers where and when they need us.

If you're like most CIOs today, you're finding that limitations in your infrastructure and gaps in network security impede your ability to deal with these changes. Legacy systems and the old ways of thinking about security just aren't capable of meeting the demands of our new normal.

Addressing this challenge presents an opportunity like never before to prepare your business for the future.

That's made possible by SASE, or secure access service edge. Gartner coined the term in 2019 to describe the convergence of security and the network at the architectural level, and it's creating a paradigm shift in the way we think about the foundations of digital transformation.

We hope you find this guide helpful—and that it gives you the confidence to take the next step toward your SASE transformation.

paloalto ®
NETWORKS

SASE improves network performance, reduces complexity, and closes gaps in security

The 10,000-foot view

SASE converges software-defined networking and security services into a single, cloud-delivered solution. By integrating security into the network architecture, we're solving the problem of delivering consistent, secure access wherever users, applications, or devices are located.
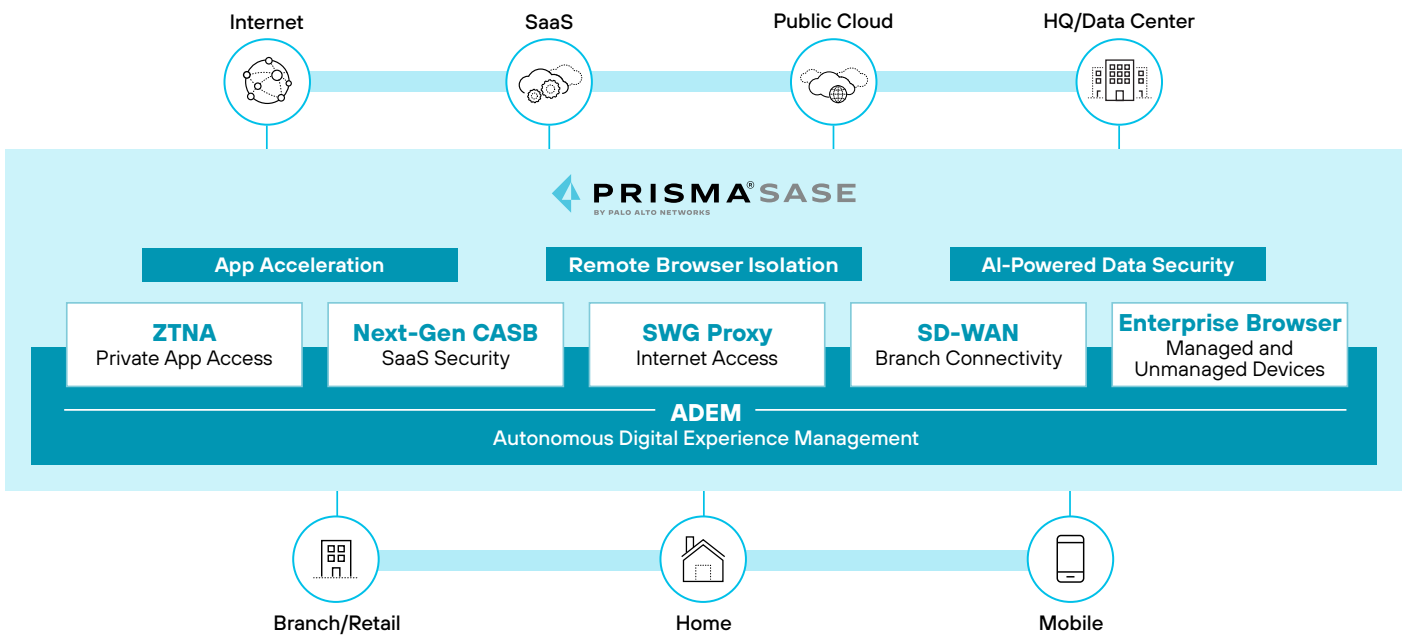
This unified approach radically simplifies the management and protection of the network.

Technologies, IT departments, and the marketplace have traditionally considered networking and security to be separate disciplines, so SASE represents a fundamental shift in thinking. In many cases, bringing networking and security teams together to create a unified team culture is one of the biggest challenges to a successful SASE implementation.

Overcoming that challenge requires leadership from the C-suite. For many CIOs, that's an exciting opportunity to lead the adoption of a transformative technology—and to start knocking down the walls between siloed disciplines. Just as cloud allows us to create more interoperability between data silos, SASE will drive the convergence of traditionally separate specialties, creating a more dynamic and innovation-oriented approach to IT.

This is IT's time to shine

Where we work has now shifted. Businesses around the world have adapted and applied technology to meet the needs of the organization and its users. Whether that means enabling remote work, migrating to the cloud, pushing customer-facing services online, or increasing the use of IoT, it's likely your IT organization has innovated to ensure minimal downtime for the rest of the business.

Now we're finding a new normal. Nearly three-quarters (74%) of businesses have a permanent hybrid work model.[1] A whopping 95% of organizations experienced a security incident originating from the browser across all devices.[2] At 92%, the vast majority of businesses have a multicloud strategy in place.[3] The upshot: Offices have transformed; branches are open; and remote workers and contractors are all around.

Businesses have moved rapidly from a networking and security architecture focused on the enterprise data center to a diversified technology estate that includes cloud, SaaS, and remote access from a wide variety of devices. Most IT organizations have adapted on the fly, doing what needed to be done to keep their workforces productive and their companies operating.

That's why so many businesses are now embracing SASE—building a secure, flexible, cloud-native network that provides a future-proof foundation for your digital transformation.

The way we work has changed.

Embrace a more **stable**, **secure**, and **permanent** solution. You're likely already leading that effort in your organization:

- Meeting digital customer experience requirements
- Improving resilience in cybersecurity and privacy
- Investing in new, technology-enabled business models
- Enhancing visibility by simplifying the IT landscape

1. 30 ESSENTIAL HYBRID WORK STATISTICS [2023]: HYBRID WORK MODEL, DATA, AND PRODUCTIVITY, Zippia, June 15, 2023.
2. The State of Security in the Modern Organization," Palo Alto Networks, April 3, 2024.
3. Bob Laliberte and Leah Matuson, "Flexible SD-WAN Has Arrived," ESG Research, April 2022.

paloalto NETWORKS®

SASE accelerates
digital transformation

As companies continue to adapt to hybrid work, two significant challenges have emerged as barriers to digital transformation. SASE is a way to address both of these challenges simultaneously.

1   **Limitations of legacy networks**

Legacy multiprotocol label switching (MPLS) networks are ill prepared to handle the demand placed on them by the widespread use of cloud services. Tunneling all traffic back to the data center degrades the user experience and limits employee productivity.

Traditional architectures implement their data centers as VPN concentrators to which remote users connect to access cloud services. Along with placing significant constraints on data center resources, this "tromboning" effect adds latency resulting in poor user experience.

2   **Gaps in Security**

The skyrocketing use of cloud services and SaaS applications; the challenge of providing access to users anywhere, regardless of location or device; the proliferation of IoT devices; securing contractors and BYOD devices; and other factors create security gaps that are difficult and costly to fill.

Using different security solutions for different use cases, with fundamentally different security capabilities, makes it a challenge to enforce consistent security policies.

If your company is like most, you've also likely seen a dramatic increase in complexity across your network, driven by the adoption of new infrastructure and services as you've adapted to meet changing needs. Although it's a natural by-product of fast-paced change, complexity limits visibility, increases security risks, and makes the network hard to manage.

paloalto
NETWORKS

Rather than focusing network security architecture on maintaining a data center perimeter protected through a collection of security appliances, converging networking and network security in the cloud allows us to transform the perimeter into a set of cloud-based capabilities that can be deployed where and when they're needed.

Using this approach enables companies to improve network performance and close security gaps.

A strong SASE solution provides:

+ Cloud-delivered SD-WAN for direct-to-app access and improved performance

+ Consistent policy enforcement

+ Simplified policy management

+ Sensitive data visibility and threat awareness

+ Consistent coverage for all types of access

By removing the barriers to digital transformation, SASE increases the rate at which organizations can empower their remote and hybrid workforces. SASE allows you to move on cloud initiatives and transform branch offices, preparing you to respond to rapid change.

This results in significant gains:

+ Reducing risk and improving security posture

+ Automating the security stack, applied everywhere and all the time

+ Optimizing application performance

+ Supporting the anywhere workforce

+ Simplifying the network, leading to improved efficiency and higher value work

paloalto® NETWORKS
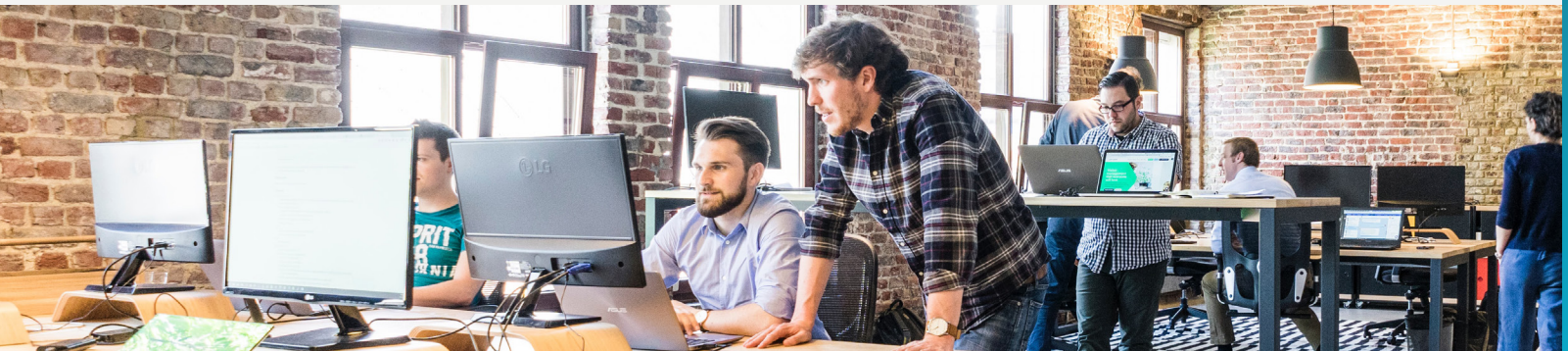
Achieving **true** Zero Trust

As we've moved toward hybrid access and added cloud services, networks have become far more complex. A Zero Trust approach to security for your people, data, and infrastructure helps to reduce the risk of a malicious actor gaining access to your most sensitive data.

It's comparatively easy to implement a Zero Trust approach in greenfield, but achieving that posture in most networks remains a challenge. Legacy architecture, the historical deployment of peer-to-peer and distributed systems, and the varying ages and capabilities of network components make it a challenge to apply consistent policies across every click of every user.

SASE simplifies achieving Zero Trust by focusing security on the behavior of users and applications, rather than managing a perimeter around the data center. This ensures that users are verified at every step, and that consistent policies are applied to every interaction on the network, regardless of where it originates.

True Zero Trust eliminates all implicit trust and continuously validates every stage of a digital interaction.

Users

Applies strong user authentication of least privilege policies on managed and unmanaged devices.

Applications

Removes implicit trust when applications talk to each other and applies consistent monitoring at runtime.

Infrastructure

Addresses everything infrastructure related—routers, switches, cloud, IoT, and supply chain—with a Zero Trust approach.

paloalto NETWORKS

Future-proofing networking and security with SASE

Because it's a cloud-based model, SASE enables a more dynamic network, adapting to changing business requirements, an evolving threat landscape, and the innovations that will change our networks in the future.

A cloud-delivered networking and security solution isn't limited by hardware that you have to purchase, deploy, and maintain yourself. This ensures that the solution is always up to date.

SASE brings the power of AI to help you manage your network more simply and consistently. At the same time, ML-driven threat detection helps you pinpoint issues and make smarter security decisions when compared to disconnected point solutions.

Sourcing all the pillars of network security—ZTNA, SWG, CASB, and FWaaS—from the same vendor simplifies your ability to maintain your security posture and enables unlimited scaling as your company grows.

It's critical that your SASE solution provides maximum extensibility.

As the SASE approach has gained traction and the market has rushed to create solutions, some vendors limit your ability to make third-party enhancements to the platform. Maintaining extensibility allows you the flexibility to incorporate new solutions that may become vital in the future.

paloalto® NETWORKS

The SASE transformation doesn't need to begin with a major IT project. It can be accomplished incrementally, in line with your existing IT priorities.

paloalto®
NETWORKS

Goal #1

Empowering the hybrid workforce

The hybrid workforce is here to stay. Employees and contractors work from corporate and branch offices to home offices and on the road.

Does your IT organization struggle to provide a consistent user experience while also maintaining a robust security posture?

SASE overcomes the leading obstacles to seamless hybrid work.

Network performance

+ The SASE network with a global backbone delivers massive scalability and low latency.

+ Because it's cloud-delivered and autonomous—and application-defined rather than packet-based—SASE-enabled SD-WAN dramatically improves network and application performance.

+ SASE-native digital experience monitoring (DEM) ensures an exceptional end-user experience by providing end-to-end visibility and insights across both mobile and branch users.

+ SASE uses AI to reduce latency and increase app performance.

Security gaps

+ By converging networking and security, SASE improves threat monitoring and prevention, DLP, and security across the internet of things.

+ Achieving true Zero Trust enhances your ability to deliver hybrid access and invest in public cloud services.

+ Sourced from a single vendor, SASE also eliminates gaps that may exist between different vendors' solutions.

Complexity

+ A cloud-delivered, single-solution approach allows you to maintain consistent governance and controls across every aspect of the network.

+ Managing the network and every security appliance from a single hub simplifies management and heightens visibility.

You can incorporate SASE seamlessly as you stabilize and improve the hybrid work environment your IT organization needs to deliver, whether you're planning a major network overhaul or simply making incremental improvements.

paloalto NETWORKS®

Westfield

Industry
Retail

Country
United States of America

Website
www.westfield.com

Palo Alto Networks Prisma SASE helped Westfield adapt quickly to the unprecedented challenges of the COVID-19 pandemic and is enabling the retail giant to keep up with a changing world.

+ Streamlined application development and business processes.

+ Improved the online experience for employees, retail partners, and customers.

+ Realized a 60% reduction in network costs.

paloalto NETWORKS

Goal #2

Supporting cloud and digital initiatives

Almost all of us are now embracing SaaS and other public cloud services to be more agile, efficient, and flexible. And as data center infrastructure amortizes, you may be looking for ways to expand your cloud footprint.

As cloud usage increases, can your network and security keep up?

SASE overcomes the leading obstacles to expanding your cloud footprint.

Performance challenges

+ Next-gen SD-WAN increases bandwidth and improves performance.

+ Cloud-delivered security results in faster performance vs. security within the data center.

+ SASE-native DEM ensures an optimized digital experience.

Cost management

SASE reduces your networking and security spend:

+ Enhanced operational efficiency improves performance and cuts overall costs.

+ Vendor consolidation reduces costs and enhances transparency.

+ Increased visibility simplifies cost management of SaaS and public cloud services.

Data security and privacy

Consistently secure all apps used by your hybrid workforce, providing:

+ Consistent policy enforcement

+ Simplified policy management

+ Zero Trust security posture

+ Security across public cloud services and SaaS applications

paloalto NETWORKS®

Atlantic Health System

Industry
Healthcare

Country
United States of America

Website
www.atlantichealth.org

Large healthcare system turns to Palo Alto Networks to improve outcomes and efficiency with high-speed, secure connectivity while keeping healthcare affordable.

+ Reduce outages due to network hardware issues by up to 33%.

+ High availability, high performance, and strong security.

+ Simplified setup and management.

paloalto NETWORKS®

Goal #3

Enabling branch office transformation

As SaaS and other services allow branch offices to become more independent of the data center, you're probably looking at ways to enhance access, improve the user experience, simplify branch service integration, or dovetail with hybrid work strategies— all without sacrificing security.

Is it time to modernize your branch offices?

SASE overcomes the primary obstacles to branch office transformation.

Hardware limitations

+ SASE integrates branch services without needing to update branch appliances or controllers.

+ Integrated 5G/LTE provides WAN redundancy while reducing infrastructure sprawl at the branches.

+ SD-WAN simplifies deployments compared to hardware-defined networks.

Network access

+ Next-gen SD-WAN significantly increases bandwidth with carrier-independent WAN transport including MPLS, broadband, and 4G LTE/5G.

+ Simplify operations with complete visibility and centralized management from the branch to the data center to the cloud.

+ Improve application performance with a direct-to-app approach and performance SLAs-based forwarding that delivers exceptional user experiences.

Security

+ Simplifying security operations using AI and ML improves threat detection and prevention, and reduces manual admin tasks.

+ FWaaS makes firewalls dynamic and flexible, providing outbound content inspection and sandboxing as well as inbound port blocking.

+ SASE extends security features to IoT devices, allowing the secure ingestion of IoT data without sensors.

paloalto NETWORKS®

SA Recycling

Industry
Recycling

Country
United States of America

Website
www.sarecycling.org

An industry leader in metal recycling trusts Palo Alto Networks to provide fast, secure, and reliable connections while reducing costs and streamlining network administration.

+ Improved bandwidth and resiliency.

+ Lowered cost and administrative overhead.

+ Reduced support tickets by 97%.

paloalto ®
NETWORKS

Goal #4

Securing Contractors and BYOD

As organizations increasingly rely on contractors and embrace BYOD policies, ensuring secure, controlled access becomes crucial.

Are all of your workers secure, regardless of their location or device?

SASE extends security to any device, anywhere.

Browser Threat Prevention

+ With SASE that includes an enterprise browser, it's easy to implement ZTNA across the IT environment to minimize the attack surface.

+ The robust threat protection of SASE solutions can be extended to unmanaged devices used by contractors and in a BYOD scheme through an enterprise browser.

+ An enterprise browser makes ensuring compliance with regulatory and corporate requirements simple, even with a large number of unmanaged devices.

Secure Access

+ With an integrated enterprise browser, SASE enables centralized policy management that applies uniformly to all users.

+ Dynamic, real-time access controls based on user, device health, location, and content ensure that contractors and BYOD users access only what they need to, safely and securely.

+ End-to-end encryption protects data movement across any device, preventing interception and ensuring integrity.

Visibility and Control

+ SASE with an integrated enterprise browser provides comprehensive insights into all browser activities with full logging and reporting capabilities.

+ Unmanaged devices' security posture is automatically assessed at regular intervals, enforcing compliance with corporate security standards regardless of device origin.

+ Built-in data loss prevention controls on the browser keep sensitive SaaS apps and corporate information from being shared with unauthorized parties.

paloalto®
NETWORKS

Lemonade

Industry
Insurance

Country
United States of America

Website
www.lemonade.com

Lemonade, a top-rated consumer insurance company, purchased Prisma Access Browser to extend their cybersecurity policies to a growing number of external partners. Leveraging the browser's native security and visibility features, Lemonade now ensures its company data remains secure, even when accessed by unmanaged devices.

+ Standardized security policies across the IT environment.

+ Increased business agility when onboarding new partners and contractors.

+ Achieved granular, user-based control over access to SaaS applications and corporate resources.

paloalto NETWORKS®

3

Although full implementation of SASE throughout your enterprise architecture can be a multiyear project, it's easy to get started within your current plans.

paloalto®
NETWORKS

Aligning your team

Your leadership will play a critical role in successfully implementing SASE in your enterprise.

Converging networking and security at an architectural level requires close collaboration and tight strategic alignment between the networking and security teams.

In your company today, as in most enterprises, networking and security are likely two separate teams, each with its own responsibilities, priorities, budget, and culture. In many organizations, those two teams don't always see eye to eye because they exist in inherent conflict: the networking team wants to deliver users optimum speed, and the security team necessarily prioritizes protecting against threats.

paloalto®
NETWORKS
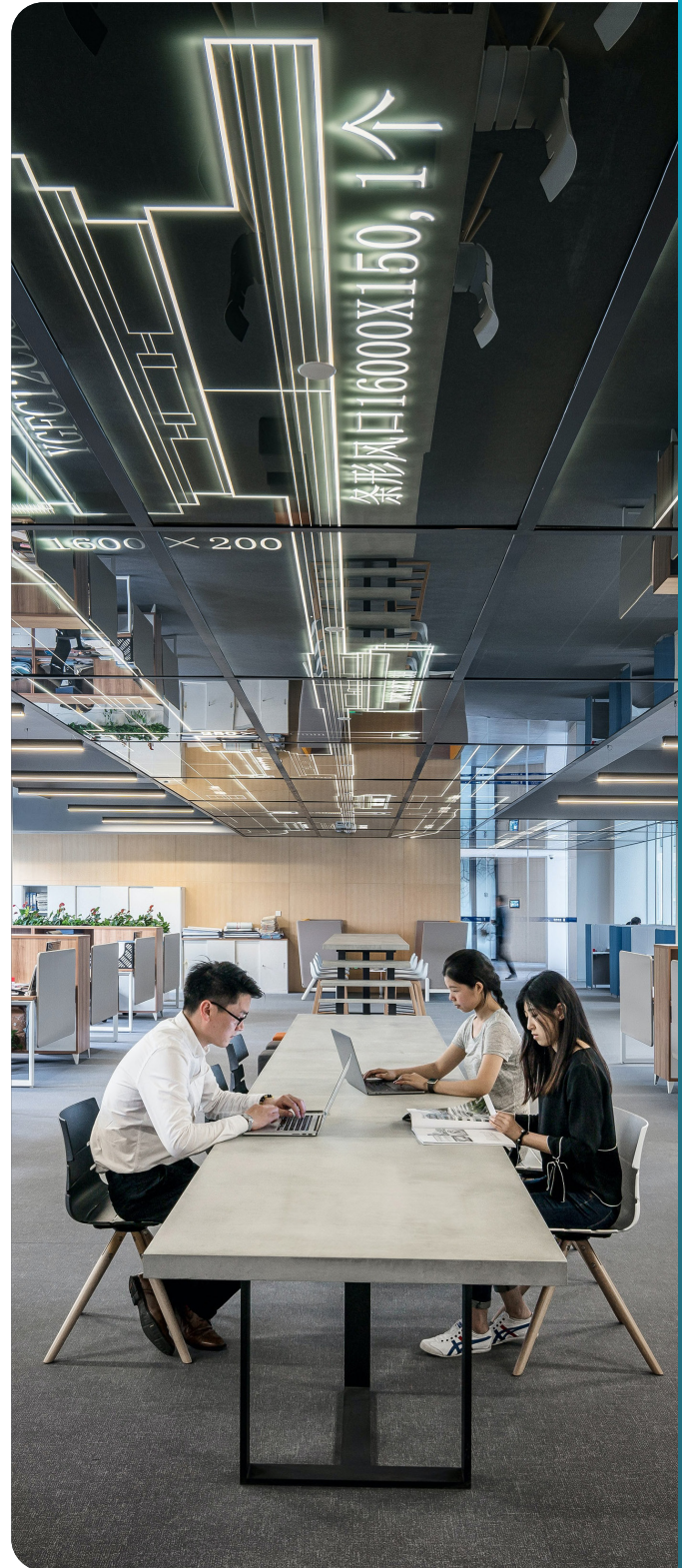
Bringing these teams together to build a culture aimed at achieving the vision of a fast, secure network with SASE is essential.

Create cross-functional teams

Collaboration across departmental silos is critical to align sometimes conflicting priorities toward SASE implementation. These teams include networking, security, workforce transformation, and branch office transformation.

Partner with the CISO (or equivalent)

SASE reduces risk while improving network performance—achieving the CISO's primary mission while reducing pressure to prioritize performance over security. SASE should get the CISO excited.

Draw a parallel to what's happened for the applications side of IT

Using the evolution of DevOps as a model for eliminating silos is an effective way to lessen change anxiety and focus on opportunity. Just as app development has become more dynamic in the cloud, SASE creates new opportunities for collaboration and innovation in networking and security.

Lean on your SASE vendor

As you evaluate vendors, consider how well they will partner with your organization to provide the education, training, and collaboration your teams need to converge their disciplines.

Expert leadership

This is a rare opportunity to lead the implementation of a paradigm-shifting solution that enhances and accelerates the transformation of your entire enterprise. Successful implementation requires strong leadership from the CIO and CISO.

paloalto®
NETWORKS

Preparing a SASE roadmap

The beauty of SASE is that, although it's a comprehensive solution to combine networking and security, that doesn't mean it needs to be adopted all at once. Incorporating SASE into your networking and security plan can—and should—align with your existing IT initiatives and business priorities.

1

SD-WAN modernization

If a WAN upgrade is one of your priorities, using SASE-enabled SD-WAN allows you to improve security while reaching your connectivity goals.

2

Security modernization

If you're planning investments to improve security in on-prem, cloud, or hybrid environments, a SASE security solution prepares you to converge the network with enhanced security over time.

3

Security point product modernization

If you're planning to modernize security point products, like aging SWG devices, working with a SASE vendor allows you to launch implementation with a small project.

4

Securing contractors and BYOD

If you have contractors and employees using BYOD, a SASE solution with an enterprise browser provides visibility and control of these unmanaged devices while maintaining security for your organization.

Because SASE will ultimately touch every part of your network and cloud footprint, a comprehensive roadmap is key.

+ Developing this roadmap in partnership with your selected vendor, managed service provider (MSP), or other partner helps to leverage vendor capabilities to achieve your priorities.

+ Assigning the roadmap to cross-functional teams or working groups encourages collaboration across silos within your organization.

+ The roadmap should be flexible enough to respond to your evolving needs so the SASE initiative facilitates other aspects of your digital transformation.

paloalto NETWORKS®

Selling SASE to the board

Regardless of whether you need board buy-in or just have to explain the value of SASE to the CEO, generating high-level excitement about SASE is important to maintain the support and clarity of the rest of the C-suite.

+ Lean on the demonstrated benefits of cloud-delivered applications. Your SaaS applications are already delivering value, and even non-technical members of the executive team are familiar with those applications—because they use them.

+ Emphasize return on investment. SASE delivers meaningful cost reduction, and it enables increased use of cloud services as an alternative to investing in owned infrastructure.

+ Align the adoption strategy with existing priorities. Because you can implement SASE without changing your current initiatives, there's good reason to achieve the long-term performance and security benefits as you complete other IT projects.

+ Show the value of reducing the number of vendors required to provide networking and security. Consolidating vendors with SASE results in better service, better product knowledge within your organization, fewer security gaps, and better cost management.

+ Stress the need for comprehensive security in the context of increasing threats. Businesses fall victim to malicious actors all the time, and there are constant threats to your network. Closing security gaps should be every leader's goal.

+ Measure the success of each project. As you move forward, ensure that your teams measure success across multiple priorities: threat reduction, network performance, efficiency, ROI, and more.

You can use Palo Alto Networks ROI calculator to estimate the economic benefits you'll achieve by implementing a SASE solution.

FORRESTER®

The Total Economic Impact™ Of Palo Alto Networks Prisma SASE

Cost Savings And Business Benefits Enabled By Palo Alto Networks

DECEMBER 2023

Find the calculator here.

Adopting SASE reduces risk, speeds up cloud and digital transformation, and reduces costs overall. A large enterprise can expect a return on investment of up to 107%, according to Forrester Consulting.

paloalto®
NETWORKS

Key elements
of an effective SASE solution

Soon after SASE was defined by Gartner, it became a buzzword in the networking and security spaces. Several vendors provide robust SASE products, but the term "SASE" is being applied to numerous solutions that don't actually fit the definition. As you consider how best to integrate SASE into your company, these are the most important elements to look for in a solution.

Next-gen SD-WAN

SD-WAN for SASE should be cloud-delivered and autonomous. Legacy SD-WAN based on packet routing requires security functions to be bolted on, not integrated. If either networking or security seems added on, you're not looking at a true SASE solution.

Zero Trust network access

ZTNA protocols should be applied consistently to every user, application, and action on the network. Products based on SDP architecture aren't consistent across all applications and aren't SASE solutions.

SWG

SWG should apply to every user all the time, regardless of location or device. As a standalone service, SWG is often applied unevenly for onsite vs. remote users. That's not a SASE solution.

CASB

An effective SASE solution should include multi-mode CASB, incorporating inline and API-based security as well as contextual controls.

FWaaS

Firewalls integrated into the SASE solution should provide the same features as a next-gen firewall, with the enhanced features of cloud-based security. Watch out for firewall services that use the term SASE without being fully integrated into the network architecture.

Enterprise Browser

An integrated enterprise browser is essential in a modern SASE solution, providing robust security and visibility into web activity on any device. The browser ensures seamless security across web applications, maintaining consistent security policies regardless of user location or device.

paloalto ®
NETWORKS

Key elements of an effective SASE solution

SASE is always fully cloud delivered—not just "in" the cloud, but "of" the cloud.

Digital experience monitoring

The solution should incorporate DEM for comprehensive visibility, automated remediation, and detailed performance insights.

Threat prevention

Robust threat prevention capabilities, including inline machine learning and automated policy recommendations, are essential in a SASE solution to expedite reaction to, and remediation of, threats.

IoT security

Security services for IoT devices aren't always integrated, but these devices are connected to the network. A SASE solution should replace standalone appliances and sensors.

Data security

Data security, with data loss prevention, should be an embedded, cloud-delivered service centered around the data itself, regardless of where it's deployed or its point of egress.

App Acceleration

The SASE solution should also dramatically boost app performance while delivering best-in-class security, tackling the challenges of latency and poor network conditions—and anticipating the processing needs of complex, real-time content—to ensure consistent, personalized user experiences everywhere.

paloalto®
NETWORKS

The industry's most complete SASE solution.

Prisma SASE: Convergence without compromise

We've built the industry's most complete SASE solution, streamlining secure access by connecting all users and locations with all apps from a single product.

Palo Alto Networks Prisma® SASE brings you a massively distributed security service delivering networking and security in one cloud service with a unified architecture. With integrated SD-WAN, Prisma SASE can secure your networks while delivering exceptional user experiences.

+ Consistently secure all apps used by your hybrid workforce.

+ Ensure an exceptional experience for your end users with the industry's only SASE-native autonomous digital experience monitoring (ADEM).

+ Improve networking performance with a 10X increase in bandwidth.

+ Avoid security gaps with the industry's best consolidated security solution integrated into the network from end to end.

+ Achieve true Zero Trust with heightened visibility and reduced complexity.

+ Cut costs with ROI of up to 107%.

Prisma SASE: Solves the biggest challenges enterprises face

Whether you're focused on a digital transformation, empowering your hybrid and remote workforce, or transforming your branch offices from workplaces to collaboration centers, Prisma SASE eliminates barriers and prepares you to stay ahead of the trends driving business today.

For digital transformation

+ Prisma SASE is the most complete cloud-delivered security platform on the market, ensuring you maintain security priorities while expanding in the cloud.

+ You'll see optimized application performance and enjoy infinite scalability.

+ Accelerate digital initiatives that create new ways to drive revenue and engage with your customers.

For the hybrid workforce

+ Prisma SASE delivers the highest possible security effectiveness to reduce the risk of data breaches resulting from remote access.

+ You'll achieve performance SLAs 10x better than the closest competitor.

+ Through the combined infrastructure of AWS and Google Cloud, your employees will experience consistent, best-in-class services anywhere in the world.

For branch office transformation

+ Prisma SASE provides an exceptional user experience for branch office employees through next-gen SD-WAN.

+ Layer 7 visibility simplifies network policy creation and traffic engineering.

+ Network and security functions are easy to manage and constantly improving thanks to AI and ML.

For contractors and BYOD

+ Prisma SASE extends to all users and devices with Prisma Access Browser.

+ You'll secure even more of the devices connecting to your apps and resources.

+ Enhanced visibility and granular controls streamline your security policy enforcement.

paloalto® NETWORKS

![paloalto NETWORKS]

Learn more about Prisma SASE

Begin or accelerate your SASE journey today. Contact us to set up a strategy discussion with a Palo Alto Networks executive.

Click here ⟶