White paper

Secure Access Service Edge (SASE)

Choosing the right partner for a managed SASE solution can deliver benefits from day one

New ways of working demand new solutions for network security

With the accelerated adoption of cloud, and hybrid work becoming the new workforce reality, organizations are actively looking for solutions to secure their digital infrastructure. Secure access service edge (SASE), which integrates the networking functionality of SD-WAN with zero trust and other cloud security features, is becoming the architecture of choice for many organizations looking to modernize their network and security solutions, and reduce the operational complexity of managing fragmented point solutions.

This white paper explores how managed SASE solution can meet a range of business requirements – improved operational efficiency, optimized network performance and increased agility – while consolidating essential security capabilities within a single, unified, easy-to-manage platform architecture.

Contents

Rethinking network security: Why now is the time 03
SASE: The path to secure cloud access and zero trust 03
The SASE appeal: Implementing a robust framework 04
The strategic value of managed SASE for growing businesses 05
Introducing NTT's Managed Networks with Palo Alto Networks Prisma SASE 05
Discover the benefits of NTT's Managed Networks with Palo Alto Networks Prisma SASE 06
An integrated solutions framework, built to last 07
Joining forces to simplify digital transformation for enterprises 08
Conclusion 08

Rethinking network security: Why now is the time

The past few years have brought rapid change to workplaces around the globe, along with the IT infrastructures they depend upon. Organizations had begun implementing digitalization and cloud-migration long before the pandemic's outbreak, while a growing number of businesses allowed their employees to work from home or other remote locations, using an ever-greater variety of corporate-owned and personal devices.

The shift toward a more dispersed workforce widened the attack surface of many organizations' IT infrastructures.

Large numbers of users are now located outside the traditional corporate network perimeter. And attempts to extend it using traditional remote access solutions create multiple challenges, including management complexity, poor user experiences, and restricted visibility for security and network teams.

As many as 63% of high-growth companies currently adhere to a "productivity anywhere" model,[2] while 76% of employees would prefer to work according to a hybrid model on a permanent basis.[3]

Whether employees are in the office or working from home, at a coffee shop or on a plane, providing always-on access to the applications and services they need to get their jobs done is now more important to businesses than ever. And this working-model shift requires a concomitant change in network security.

Rethinking network security doesn't have to be a burden. Most importantly, it should not be an afterthought. Staying ahead of cyberthreats and bad actors to avoid security breaches must be at the front of every IT leader's mind when creating a strategic plan to best protect their end-to-end infrastructure.

This is where a managed secure access service edge (SASE) solution comes into play.

> At least 75% of ransomware attacks and breaches fielded by Unit 42's incident response team in 2022 resulted from attack surface exposures, up from 40% a year prior.[1]

SASE: The path to secure cloud access and zero trust

SASE is the convergence of software-defined wide-area networking (SD-WAN) and network security services like cloud access security broker (CASB), firewall as a service (FWaaS), and zero trust network access (ZTNA) into a single, cloud-delivered service model.

Organizations need effective and efficient security solutions that are able to stop sophisticated ransomware attacks and advanced threats in the nick of time. They also need to modernize outmoded technology infrastructures if they're to operate in a manner that will allow them to reduce costs, optimize for growth, and remain agile in a fast-changing digital environment.

SASE solutions promise to deliver these things while consolidating essential security capabilities within a single, unified, easy-to-manage platform architecture.

> Gartner® predicts that: "Over the next four years, the SASE market will grow at a CAGR of 32%, reaching almost $15 billion by 2025."[6]

3 key factors are driving present-day increases in SASE adoption :

An expanded attack surface caused by the shift from office-based work to flexible and hybrid working, requiring organizations to pivot from perimeter-based to identity-driven security architectures.

Cloud adoption continues to climb. IDC Research predicts that 65% of enterprises will prioritize cloud-delivered as-a-service consumption models for all or most of their technology purchases by 2026.[4] *Additionally, the vast majority of organizations (80%, according to Flexera) have adopted a hybrid cloud strategy.*[5]

Legacy security approaches are ineffective in these cloud-first environments. It's unduly complex, if not entirely unfeasible, to deploy a physical or virtual security appliance to protect every cloud workload.

[1]Unit 42/Palo Alto Networks. 2023. 2023 Ransomware and Extortion Report.
[2]World Economic Forum. November 2022. The future of the office is changing: here's how to improve the occupant experience.
[3]Global Workplace Analytics. 2021. Global Work-from-Home Experience Survey.
[4]IDC Research, December 2022. IDC FutureScape: Worldwide Future of Digital Infrastructure 2023 Predictions.
[5]Flexera. 2022. Trends in Cloud Computing: 2022 State of the Cloud Report.
[6]Gartner, Market Guide for Single Vendor SASE. Published 28 September 2022. By Neil McDonald et al. ID G00768660. *GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.*

As cloud adoption accelerates, changing traffic patterns are straining legacy network infrastructures. To make matters worse, Multiprotocol Label Switching (MPLS) connectivity was not designed to handle the massive amounts of traffic to cloud destinations and SaaS applications that today's corporate office and branch network users generate. In a SASE architecture, cloud-delivered SD-WAN capabilities enable automated routing decisions and smart bandwidth allocation based on user needs.

As a model, SASE consolidates much-needed security and networking capabilities. This means it can simplify both IT and security operations, while delivering complete visibility and centralized control to improve user experience and workforce productivity. SASE's SD-WAN functionality drives greater network agility, and its flexible WAN architecture is well suited to enable cloud applications. These capabilities make SASE deployments a good match for changing business requirements.

Furthermore, SASE is able to deliver advanced security features, such as ZTNA, which make it possible for organizations to adopt the zero trust approach to cybersecurity, shifting from perimeter-based to identity-level security. In addition to ZTNA, SASE incorporates advanced threat-protection capabilities like CASB and secure web gateway (SWG) that enhance access security for SaaS applications and provide content-filtering functionality for accessing the internet. All of these capabilities are delivered through a flexible and scalable cloud-based model.

The SASE appeal: Implementing a robust framework

As organizations move away from legacy approaches for security and networking and begin to adopt a modern SASE architecture, they confront a variety of challenges along the way. A skills shortage makes it difficult to find the expertise they need to implement and manage a SASE solution.[7]

Meanwhile, the cost of capital has grown significantly as governments try to rein in inflation. These factors combine to make a fully managed SASE solution – one that's available on a cost-efficient, consumption-based, monthly-subscription basis – attractive for businesses.

In the remainder of this white paper, we'll delve deeper into how SASE is helping enterprises overcome networking and security challenges and discuss what to look for in an end-to-end managed SASE service provider – and why this matters.

> **76%** of enterprises are already outsourcing their network management or plan to fully outsource it to a managed service provider by 2024.
>
> — NTT's 2022–2023 Global Network Report

[7]CompTIA, Tech Jobs Report. February 2023.

The strategic value of managed SASE for growing businesses

The additional support that comes with a fully managed SASE solution puts SASE's benefits within reach for organizations of all sizes, across industries and geographies, no matter how large or small their internal teams are. As businesses expand into new markets, it becomes increasingly difficult to manage a global network with disparate branch locations. A managed network service provider can assume the burden on your behalf.

Your managed service provider can ensure that your organization has ample access to all the resources needed to deploy, integrate, manage and maintain a comprehensive SASE solution. They can also take on the ongoing responsibility for finding, hiring and retaining talent. This means your internal teams can focus their energy on what matters most: strengthening the business's technology strategy.

When a single managed service provider is responsible for the entire the SASE deployment, they'll serve as a one-stop shop, and you'll enjoy the operational efficiencies that come with not having to handle multiple vendors, siloed technology solutions, and different infrastructures across branch locations.

A fully managed SASE solution that's delivered through a services platform and incorporates AIOps, automation and advanced analytic capabilities can give you top-notch performance, threat-detection capabilities and enhanced network reliability.

Introducing NTT's Managed Networks with Palo Alto Networks Prisma SASE

NTT has partnered with Palo Alto Networks to deliver NTT's Managed Networks with Prisma SASE as an end-to-end managed service.

This new offering not only brings together networking and security capabilities, it also incorporates all the technical and management expertise needed to deploy, integrate and manage them on an ongoing basis. It's powered by the industry's most complete SASE solution, purpose-built to help organizations achieve the best performance – and derive the most value – from their SASE transformation.

Adopting Prisma SASE reduces risk, speeds up cloud and digital transformation, and reduces costs overall. Palo Alto Networks is the only vendor to be recognized as a Leader in the 2023 Magic Quadrant™ for SSE and 2022 Magic Quadrant for SD-WAN by Gartner.[8] A large enterprise can expect a return on investment of up to 270%, according to research from Forrester,[9] and this alone is a strong foundation for justifying the business case for SASE.

Prisma SASE operates within a unified, single-vendor approach, which is ideal for organizations looking to maximize security and efficiency. They can leverage AI and ML across security, networking and user experience management, all unified across the same data lake. In addition, Prisma SASE offers multidomain analytics and advanced data correlation across endpoints, applications, networks and security policies – all within a single dashboard. This makes it quick and easy to discover network anomalies.

This offering also brings together the Prisma SASE technology platform and NTT's extensive network management expertise. NTT has long-established experience as an integrated services provider and leader in managed networking. The capabilities of NTT's managed network service platform, including advanced automation and analytics, are incorporated in this offering. This means that NTT's Managed Prisma SASE clients will enjoy the improved network performance that NTT's comprehensive monitoring capabilities make possible, while also gaining all the benefits of SASE.

[8]See Gartner reports: Magic Quadrant for SD-WAN. 12 September 2022. Magic Quadrant for Security Service Edge. Published 10 April 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, MAGIC QUADRANT is a trademark of Gartner, Inc. and/or its affiliates and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

[9]Palo Alto Networks Prisma SASE Estimator (totaleconomicimpact.com)

Discover the benefits of NTT's Managed Networks with Palo Alto Networks Prisma SASE

NTT's Managed Networks Service with Palo Alto Networks Prisma SASE gives organizations access to the resources, tools and technologies they need to meet even the most demanding networking and security requirements on a global scale, without all the complexity. The result is a winning combination of robust security and business agility.

NTT's Managed SASE customers can take advantage of the flexibility and efficiencies that are built into NTT's Network as a Service offering. NTT's integrated network services are both deep and broad, including LAN, SD-WAN, wireless communications and integrated security capabilities. These offerings are supported by best-in-class monitoring and management services, delivered through NTT's comprehensive managed network service framework. NTT's highly skilled team can support clients by working alongside their internal teams, helping to bring network and security operations together, or can assume full responsibility for managing the SASE solution.

NTT is well prepared to support Prisma SASE at scale, across all the geographies where its clients operate. Plus, NTT's always-on monitoring services detect threats proactively, at any time of day or night, thanks to alerts on anomalous behaviors observed on the network or in the environment. NTT also leverages automation to implement changes to policies dynamically.

The benefits of this approach include:

Best-in-class, end-to-end managed SASE

The Prisma SASE platform is a full-featured SASE offering that includes the advanced ZTNA 2.0 capabilities pioneered by Palo Alto Networks to protect all users, devices, applications and data, everywhere. ZTNA 2.0 combines fine-grained, least-privileged access with continuous trust-verification and deep, ongoing traffic-security inspection to mitigate risks and stop zero-day threats quickly. Prisma SASE's best-of-breed security capabilities are delivered in conjunction with the advanced AI and automation functionalities of NTT's SPEKTRA Platform to enable a top-performing service from end to end.

Reduced complexity and cost

With SASE, uniform security policies can be enforced across the entire organization from a single state-of-the-art platform that also incorporates software-defined networking functionalities. Rather than maintaining fleets of point security solutions in an environment of ever-growing complexity, there's just one vendor to manage, one set of contracts to negotiate and a single toolset to administer.

Simple and scalable model

The consumption-based network-as-a-service (NaaS) delivery model for this SASE solution ensures that implementation can be right-sized for your needs and budget. There's a full lifecycle of services, with entry points tailored to individual clients' journeys and needs. As your business grows and your objectives change, you can evolve and expand your SASE deployment as needed.

An integrated solutions framework, built to last

Managed Networks Platform + Palo Alto Networks SASE Technology

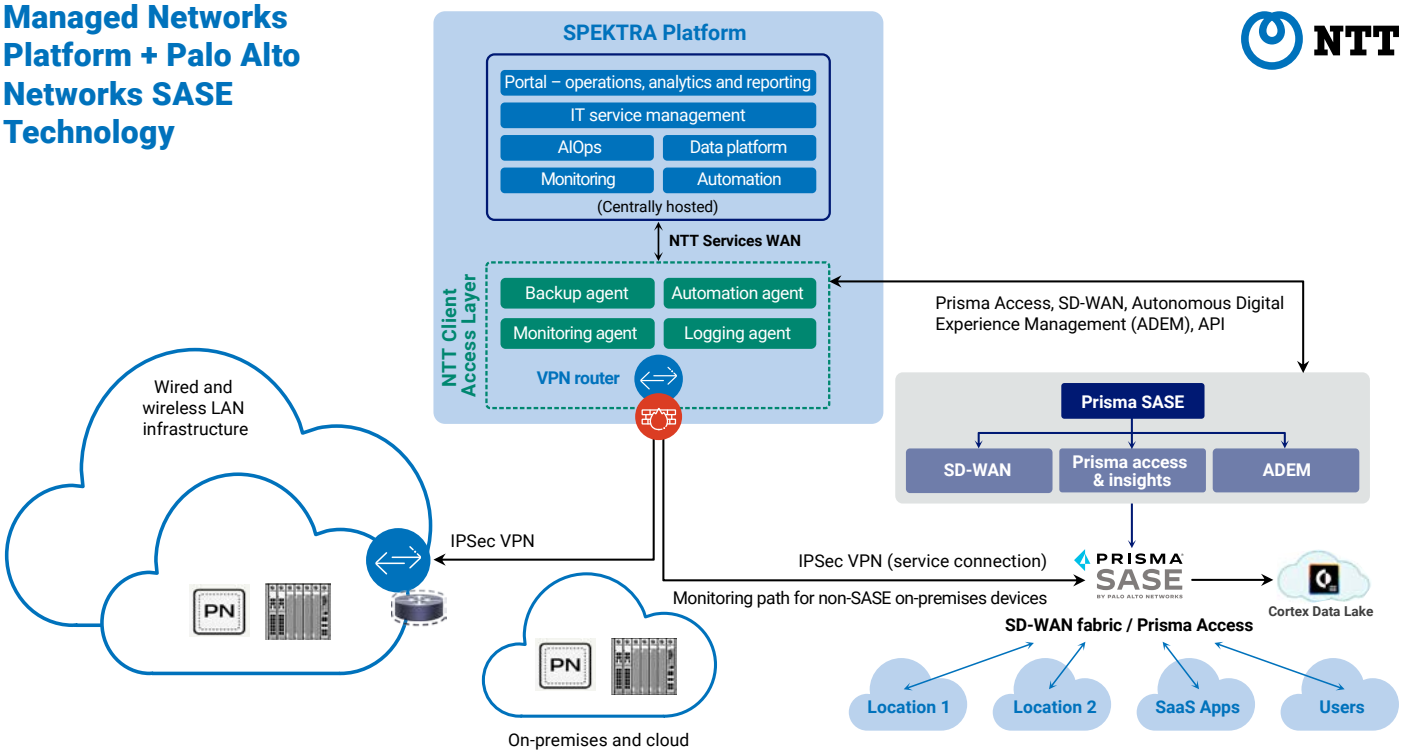

Figure 1: NTT and Palo Alto Networks – an integrated solutions framework

As an integrated solutions framework, NTT's Managed Networks with Prisma SASE combines the comprehensive capabilities of the industry's most complete SASE solution with the proven expertise of a global leader in managed network services in a holistic, end-to-end, cloud-delivered solution.

A SASE implementation doesn't happen overnight. As is the case with any significant technology transformation project, success requires planning, design, implementation and project management expertise.

NTT brings in-house, industry-leading network, security and implementation expertise to every managed SASE implementation project that it undertakes. The result is a speedy, streamlined deployment process and accelerated time-to-value. NTT's lifecycle services approach extends from the consultative phase through to the design and build, deployment, operationalization and optimization phases.

During the initial consultative phase, a thorough network assessment is completed. This is followed by the development of a precisely defined pathway to implementing SASE.

In the design and build phases, the solution is planned and deployed. Careful attention is paid to making migration and implementation smooth. NTT also ensures that the SASE architecture will be seamlessly integrated with the client's specific applications and services. In this phase, the NTT team will draw upon their deep expertise in setting policies and rules to ensure all client requirements are satisfied.

Once the new SASE architecture has been operationalized, ongoing service management will be critical for realizing its full potential. The scope of service management includes comprehensive monitoring, analytics and reporting, as well as technical account management and ticketing. NTT clients get detailed insights into their service experience, allowing them to understand how their campus technologies are performing and how frequently events are taking place. With the additional layer of NTT's AI-driven incident management and anomaly-detection engines, clients can stay one step ahead of threats and incidents. The platform also enables rapid response through process orchestration and the ability to initiate automated runbooks.

Managed Prisma SASE clients benefit from a full suite of integrated networking capabilities, all from a single vendor. These include:

- Wired and wireless LAN
- Secure VPN connectivity
- On-premises networking and SD-WAN
- Prisma SASE access and gateways

These advanced platform technology features are complemented by the 24x7 technical support that's provided through NTT's delivery centers. Experts from NTT continuously monitor network performance, adjusting policies and engineering traffic to ensure the network is optimized for the best user experiences.

Clients can leverage a wide array of adjacent managed service offerings from NTT, including:

- Managed Detection and Response (MDR)
- Managed Network Underlay Services
- Multicloud as a Service
- Edge as a Service
- Private 5G and IoT
- Data Center Services
- Digital Collaboration Services

Joining forces to simplify digital transformation for enterprises

Palo Alto Networks and NTT have joined forces to bring clients a best-in-class SASE solution with best-in-class managed services. This partnership simplifies technology consumption and optimizes deployment within a fully integrated, holistic service offering.

NTT works closely with Palo Alto Networks to prevalidate all integrations. This ensures the smooth deployment of a joint solution that works from day one. one – which means clients can derive full value from the single-pane-of-glass dashboard and all included analytic capabilities immediately. Naturally, accelerating time-to-insight also accelerates time-to-value.

Clients can lean on a pair of strong leaders in technology, security and managed network services, with a long history of successful partnerships.

In additon, streamlined, cloud-delivered security can mitigate a host of security risks, from devastating data breaches to expensive ransomware attacks.

This fully managed service can also improve bandwidth efficiency and optimize application performance so that users can enjoy better experiences and enhanced productivity.

Plus, the simple, scalable consumption model is designed for agility and flexibility, so organizations can be confident that they are ready for the future, no matter what it may bring.

Conclusion

SASE addresses many of the biggest and most pressing challenges that digitally transforming organizations face. It's able to add efficiencies, enhance security, and support hybrid and distributed workforces. And it provides a path to further modernize the business for security, speed, growth and cost savings. **But implementing SASE successfully demands the right skill sets and capabilities.**

A fully managed solution lets you conserve scarce IT resources, reduce the complexity of managing your network and security infrastructure, and achieve improved outcomes. Adopting Prisma SASE reduces risk, speeds up cloud and digital transformation, and reduces costs overall.

NTT and Palo Alto Networks together offer an efficient, agile solution that's purpose-built to support zero trust and other cloud security methodologies in modern cloud environments, safeguarding today's distributed workforces.

Learn more about how NTT's Managed Networks with Palo Alto Networks Prisma SASE can help you modernize and transform your digital infrastructure to protect against threats, reduce infrastructure and operational costs, and strengthen your cyber resilience.


NTT
paloalto
NETWORKS