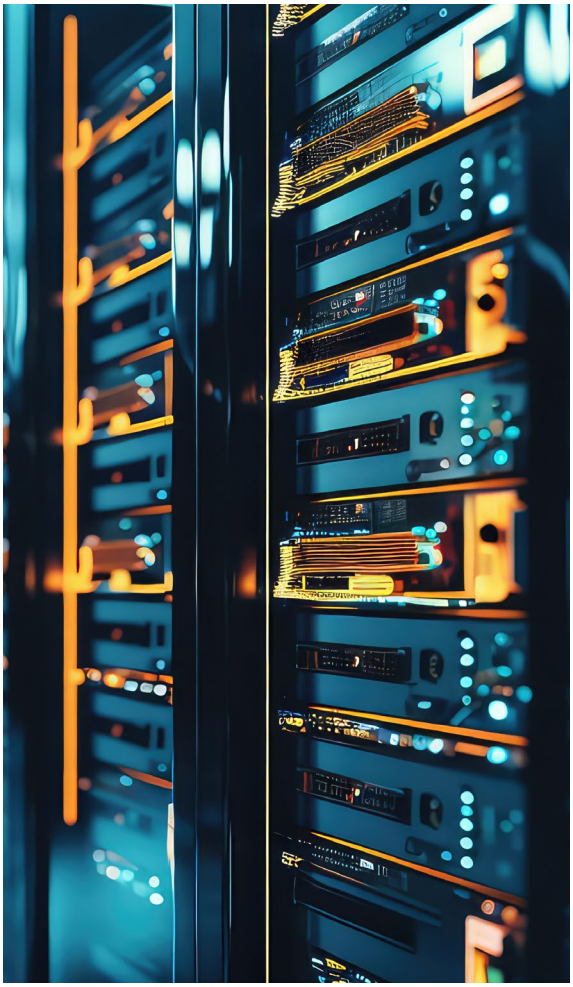
Network security for new ways of working

NTT DATA and Palo Alto Networks Managed SASE

Rethinking network security

With Managed SASE from NTT DATA and Palo Alto Networks, you can replace outmoded network architectures and security approaches. Partner with us to secure your entire network, reduce costs and complexities and improve business agility.



The past few years have brought significant 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. Then, when work from home became the norm, there were suddenly many corporate-owned and personal devices being used outside the traditional corporate network.

More work locations and more devices means a much wider attack surface for IT infrastructures. But attempts to extend the network perimeter using traditional remote access solutions only create more problems — think management complexity, poor user experiences and restricted visibility for security and network teams.

Add to this, the growing complexity of a multifaceted IT environment from AI technologies to multicloud and hybrid environments and a fast-approaching quantum future that continues to stretch networks.

This new working model requires a new approach to network security.

A new strategy for staying ahead of cyberthreats

Employees need reliable, 24x7 access to their work applications and services, whether they're in the office, at home, at the airport or on the move. Organizations need security solutions that can stop sophisticated ransomware attacks and advanced threats in the nick of time. SASE delivers both.

SASE brings together the networking functionality 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.

> "SASE consolidates essential security capabilities into a single, easy-to-manage platform architecture."

The benefits of our fully managed solution

Legacy network architectures and security solutions don't work in a cloud-first and hybrid workforce environment.

Our cloud-delivered solution provides complete visibility of your entire enterprise network environment. It incorporates the latest zero trust network access technologies from Palo Alto Networks, including Zero Trust Network Access (ZTNA) 2.0, which combines fine-grained, least-privilege access with continuous trust verification and deep, ongoing security inspection to protect all users, devices, apps and data everywhere. High-performance threat prevention and security is integrated into our solution.

Optimize app performance and security

Prisma® Access from Palo Alto Networks also provides cloud access security broker (CASB) and secure web gateway (SWG) features that enhance the security of cloud applications. Integration capabilities are available for key applications and multiple cloud environments.

Centralized control over network policies helps to improve workforce productivity.

AI Access Security from Palo Alto Networks enables you to safely adopt GenAI applications by mitigating the risks posed by inadvertent data leakage in prompts and malicious content in responses.

Leveraging AI-aware protection powered by Precision AI®, Prisma® Access Browser secures work on any device, managed or unmanaged, against AI-generated phishing attempts and advanced malware that target the organization and offers an alternative to solutions like virtual desktop infrastructure (VDI).

Manage a global network with dispersed branch locations

Our cloud-native architecture and leading SLAs ensure we deliver uncompromising performance.

Unified, simplified operations and management eliminate the need for point security solutions and large, highly skilled internal teams, while advanced AI and automation techniques enable proactive and predictive monitoring and incident management.

> “SASE is becoming the architecture of choice for organizations looking to secure their digital infrastructure without the complexity of fragmented point solutions.”

Prisma SASE add-ons

Autonomous Digital Experience Management (ADEM) gives your end-to-end visibility of and insights into mobile and branch users to support optimal user experiences.

Prisma Access Browser (PAB) addresses the increasing security challenge of unmanaged and third-party devices accessing corporate services and private applications. PAB can be used as an alternative to VDI – virtual desktop infrastructure.

AI Secure Access provides real-time threat detection for both sanctioned and shadow AI apps. This allows you to prevent AI-related data loss and improve your overall risk posture while empowering users to securely leverage GenAI.

Reduce costs and leverage the benefits of an opex model

Our flexible, consumption-based services and models help you budget for and manage costs more efficiently.

By replacing on-premises security hardware with cloud-delivered security, you can reduce operations and maintenance costs. And improved bandwidth efficiency and optimized application performance mean you get more from your investment, including better productivity.

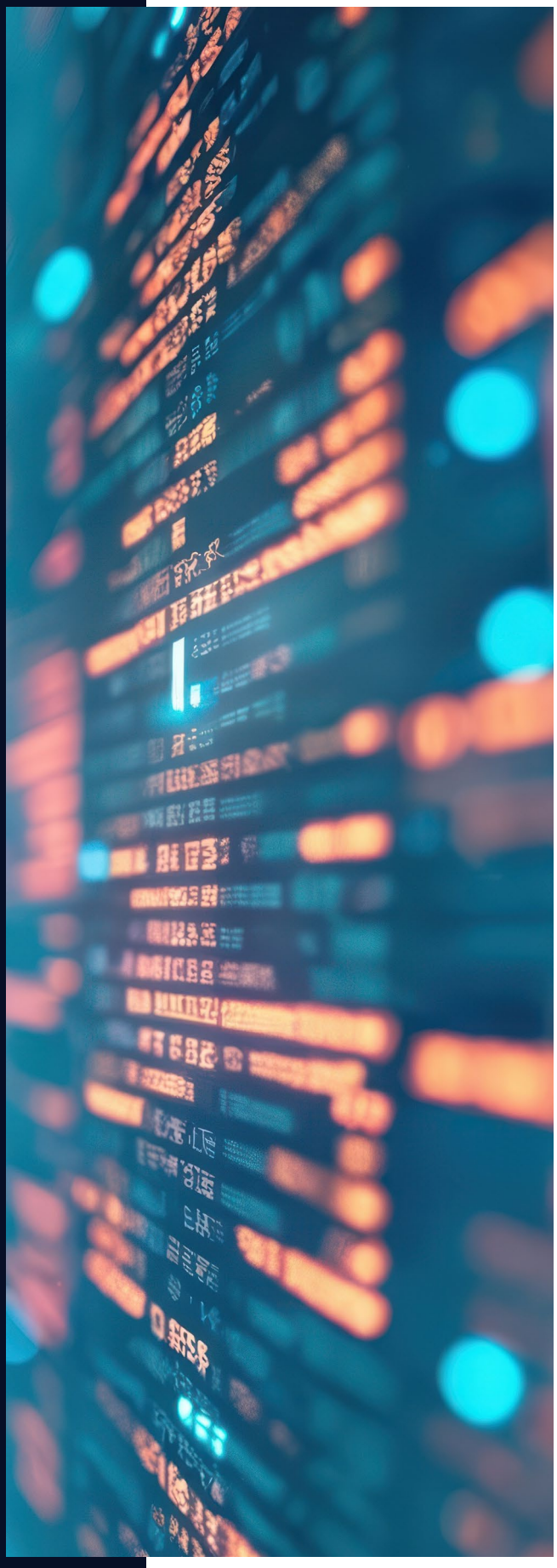
Our simple and scalable model delivers full lifecycle services with entry points that match your unique requirements.

Access to SASE skills

Our fully managed service gives you access to our extensive network and security expertise — including a team of network and security operation engineers in our global delivery centers offering 24x7 support.

The platform is tailored and tuned to monitor and manage SASE environments and has advanced AI and automation capabilities.

Managed SASE brings together best-of-breed security from a cloud-delivered SASE incorporating AI Security, Enterprise Browser protection with managed LAN & SD-WAN, all from an NTT DATA Managed Service.



> “Network security doesn’t have to be a burden. Most importantly, it should not be an afterthought.”

Managed SASE use cases

Virtual private network (VPN) replacement

VPN technologies are not designed for the rapid scale, high performance and consistent delivery of advanced security services required to connect a hybrid workforce to a wide range of applications. Replacing legacy VPN technologies with a modern ZTNA 2.0 solution can help overcome performance bottlenecks and simplify management.

Securing internet access

As organizations and their mobile and hybrid workforces grow, it becomes increasingly difficult to protect remote users from threats as they access various applications. The cloud SWG capabilities of Prisma SASE remove latency issues and improve security capabilities.

Advanced SaaS security

Enterprises using legacy CASB solutions can't keep up with the rapid growth of SaaS applications, shadow IT, data volumes and a growing number of hybrid and remote workers. The CASB capabilities of Prisma SASE give you complete coverage, securing all applications, whether on-premises or in the cloud. In this way, you get full visibility of shadow IT along with easy-to-use workflows, so you can safely enable the use of SaaS applications.

Use GenAI safely

AI Access Security facilitates the safe use of GenAI apps, categorizing thousands of apps and generating risk scores that empower InfoSec teams to make informed decisions. This not only gives you a clearer view of GenAI adoption, it also helps prevent data loss. With real-time threat detection for both sanctioned and shadow AI apps, IT teams can improve your organization's risk posture while empowering users to securely leverage GenAI.

Place security in the browser while allowing managed and unmanaged devices to safely access your systems. Prisma Access Browser, designed specifically for enterprise use and is fortified with security features to protect users and organizations against cyberthreats like phishing, malware, eavesdropping and data exfiltration.

Branch transformation

Organizations are fundamentally changing the role of branches. Rather than serving as primary places of work, branches are becoming collaboration hubs. Retailers are also transforming how they engage with in-store customers. These shifts are driving demand for WAN transformation, from legacy MPLS to SD-WAN and SASE.

Why NTT DATA and Palo Alto Networks

- Industry-leading expertise in managed network and security solutions
- Cutting-edge AIOps technologies and automation techniques for enhanced network performance, reporting, monitoring and management
- Scalable, modularized solution set for best fit to meet individual client requirements and business objectives
- Cloud-delivered to reduce the need for hardware investment
- Flexible as a service consumption model for improved cost management
- ZTNA 2.0 enables zero trust security at the user level, protecting enterprise resources for a distributed workforce

We transform organizations for success. NTT DATA and Palo Alto Networks are helping organizations around the world innovate with confidence so they can build a secure and resilient digital future.

Think fewer vendors, less fragmentation and greater resilience — with end-to-end visibility and control where it matters most. NTT DATA brings global expertise in networking and cybersecurity. Not just deploying Palo Alto Networks, but scaling it with the services, support and strategy to drive real business advantage. We unlock agility with managed SASE and advanced zero trust enforcement for users, devices and workloads. We keep your cybersecurity future-ready, guiding you through the entire security lifecycle.

Visit nttdata.com to learn more.

NTT DATA is a global innovator of digital business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.


NTT DATA