Simplify and integrate your cybersecurity

Securely enable your organization to take advantage of new opportunities for growth

Contents

Cybersecurity: A key business enabler

Managing networks and security in isolation no longer aligns with the realities of an AI-powered edge-to-cloud ecosystem. You need simplified and integrated cybersecurity to shield your organization from an AI-enabled threat landscape.

Cybersecurity has evolved from a mere risk management function to a strategic business enabler. It's no longer only about locking doors to keep threats out, but also about keeping doors open to let the right opportunities in. In this way, you can innovate without hesitation, knowing that your data, operations and customer trust are always protected, which in turn enables growth in a digital-first environment.

The new reality

In an edge-to-cloud ecosystem, unmanaged devices — from personal smartphones and tablets to IoT devices — can introduce significant cyber risks.

GenAI is also creating challenges. Networks need to support the high bandwidth and low latency needed for GenAI workloads while warding off AI-driven threats, while modern applications, running containerized, microservice-based environments, demand adaptive, real-time security.

And this must all be achieved despite limited budgets and scarce cybersecurity talent, leaving organizations continually trying to do more for less.

Therefore, we need efficient, cost-effective cybersecurity solutions that are flexible enough to accommodate the agile and scalable networks that are so critical to AI-driven business growth.

This involves embedding robust security measures such as zero trust principles, network segmentation and advanced threat detection across your edge-to-cloud ecosystem.

Once you have simplified and integrated your cybersecurity environment, it reduces cost, blind spots and operational risks. However, this can be easier said than done: According to The State of Cloud-Native Security 2024, a report by Palo Alto Networks, 98% of organizations recognize the need for simplification and consolidation, yet the number of tools dedicated to cloud security increased by 60% from 2023.

Complexity therefore remains a persistent and costly challenge, raising the urgent need for simplification to free up resources and accelerate digital transformation.

Cyber resilience: A driver of growth

For CISOs, an agile, adaptive framework for cyber resilience is foundational for business stability and confidence. Only with comprehensive cyberdefense strategies, proactive threat mitigation and the ability to protect, respond and recover quickly does cybersecurity become a driver of growth.

Organizations that prioritize cyber resilience can explore opportunities for growth with confidence, backed by confident stakeholders. This is how proactive cybersecurity becomes the backbone of resilience, innovation and competitive advantage.

Protection with less complexity

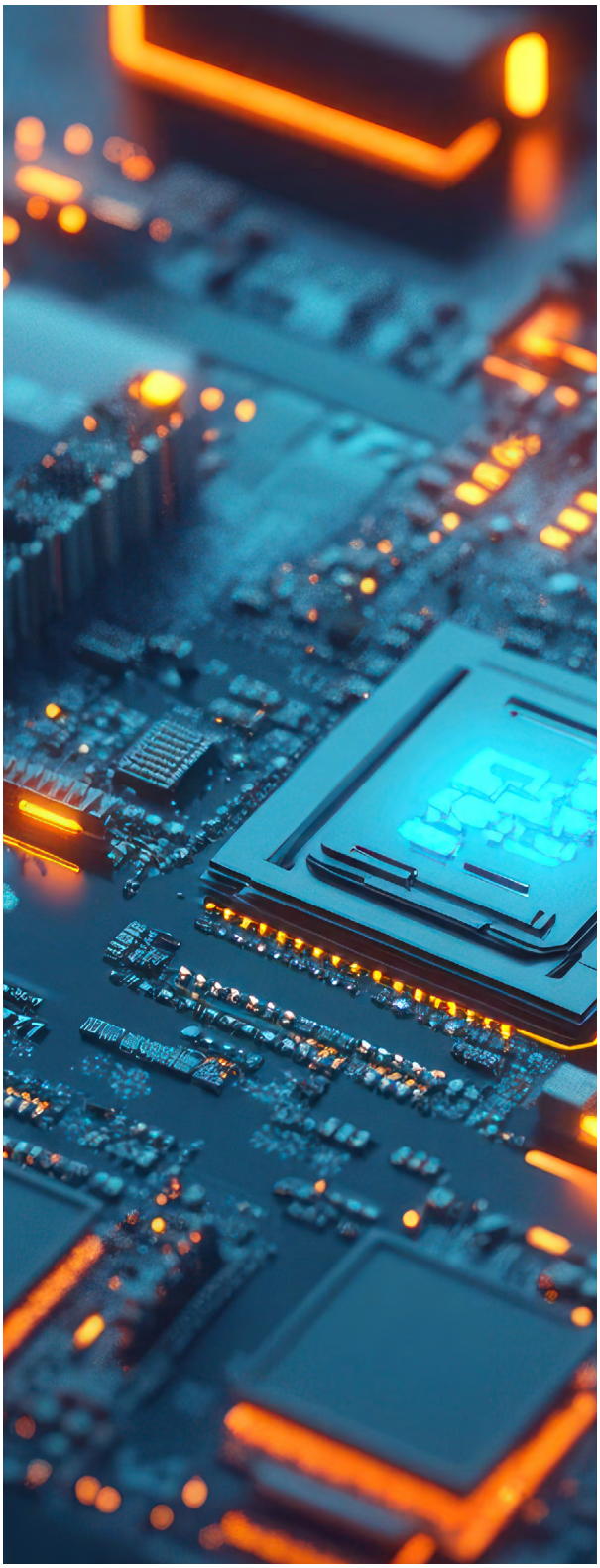
CISOs need to simplify their cybersecurity environments by rationalizing, standardizing and unifying their technology sprawl while focusing on AI-enabled and automated security operations.

Instead of layering on more and more separate tools that can create further confusion, simplified, integrated and outcomes-focused cybersecurity strategy needs to bring together security and networking solutions in one cohesive approach. With a single-pane-of-glass view of your organization's security posture and controls, you gain clarity and decision-making power while reducing the cost and effort of managing fragmented systems.

This streamlined approach protects your critical data and digital assets across AI, multicloud and hybrid infrastructures, improving trust among your customers, suppliers, employees and the board.

When you integrate network and security functions in this way, you minimize vulnerabilities and maintain robust defenses.

Some organizations achieve this goal by outsourcing their cybersecurity to service providers who use AI and automation to deliver efficient and reliable managed security services.



An outcomes-focused approach

The ability to adapt swiftly and respond to cyberthreats as they arise is vital in maintaining business continuity and safeguarding your data.

An outcomes-focused approach to cybersecurity reduces complexity by bringing together automation, AI-driven threat intelligence, agentic AI for alert triage and detailed incident response playbooks into one coordinated framework.

Instead of your security team having to manage disparate tools and manual processes, this level of integration speeds up detection and response times, produces fewer false alerts and contains costs.

The result: Better protection with less complexity.

The solution

NTT DATA and Palo Alto Networks: Elevating your security posture.

Through a strategic partnership, NTT DATA and Palo Alto Networks offer advanced tools, solutions and expertise to bolster your security posture. These include:

- **Best-in-class cybersecurity products from Palo Alto Networks:** A comprehensive suite of natively integrated security services delivered from the cloud provides protection for your entire network, securing all users, applications, devices and data, regardless of their location.
- **NTT DATA's expertise in security and networks**: Our Cybersecurity and Managed Network Services keep your infrastructure resilient, responsive and adaptable. From risk assessment to incident response, we offer end-to-end network and security solutions.
- **Cloud-delivered security solutions:** We offer robust cloud-delivered security as a managed service, using Prisma SASE® from Palo Alto Networks. Prisma SASE facilitates secure access service edge (SASE) by combining advanced security and networking capabilities as part of a unified platform — as well as zero trust network access and software-defined wide area network (SD-WAN) and application security.
- **Simplified, reliable deployment:** As part of our fully integrated implementation services, we validate all integrations before deployment, so your solutions work as they should from day one.
- **AI and automation:** NTT DATA's AI-powered network platform, SPEKTRA, integrates with Palo Alto Networks solutions to leverage AI and automation for autonomous cybersecurity operations. This leads to faster threat responses, better detection and response times and deep insights into vulnerabilities for proactive defense. Automation also reduces the possibility of human error and gives IT teams time to focus on strategic priorities.
- **A platform-driven approach:** Our AI-powered platforms simplify management, monitoring and remediation and apply intelligent insights to improve visibility and observability. These platforms include advanced management tools that centralize control and automate processes to reduce complexity and deliver operational efficiency.

By partnering with NTT DATA and Palo Alto Networks, you create a secure, resilient edge-to-cloud environment that securely enables AI-driven innovation and business growth while protecting against evolving threats.

Managed Prisma SASE in action

Protecting a leading beverage manufacturer's network

One of the world's leading beverage companies, known for their diverse global portfolio of soft drinks, faced significant challenges in their network and security environment. With over 160 manufacturing sites, warehouses and offices worldwide, they needed a robust, scalable security solution to support their digital transformation. They sought partners who could improve visibility, resilience and scalability in their digital ecosystem.

Creating the right strategy

Experts from NTT DATA and Palo Alto Networks collaborated with the client to develop a unified security strategy tailored to their specific needs and maturity level. We prioritize proactive risk management and a collective understanding of the importance of security across the organization.

We implemented NTT DATA's Network as a Service as part of the transition from on-premises security to cloud-based zero trust security. Shifting from traditional, hardware-based security to a more flexible, software-defined approach meant the network infrastructure could adapt to evolving threats and business needs.

Managing growing complexity

To take control of the beverage manufacturer's complex network and security environment, we implemented a managed, integrated solution using Prisma SASE from Palo Alto Networks.

This means many disparate systems can now be managed centrally. Advanced threat intelligence, machine learning and automation provide real-time threat detection and response to protect their entire network.

NTT DATA's Managed Prisma SASE solution, powered by SPEKTRA, enables proactive threat detection, allowing the beverage manufacturer to streamline their cybersecurity functions and focus their IT resources on strategic initiatives.

Building cyber resilience

NTT DATA and Palo Alto Networks took a comprehensive approach to building cyber resilience for the beverage manufacturer. Prisma SASE's advanced security capabilities, including zero trust network access (ZTNA) and cloud access security broker (CASB), provide continuous monitoring and real-time analysis of network activities.

In tandem with our Managed Prisma SASE solution, our SPEKTRA platform uses predictive analytics, AI and machine learning to anticipate and respond quickly to threats to avoid disruptions to business operations. Only authorized users can access critical resources, and the company has granular control over the use of their cloud applications and data.

Our approach also includes thorough risk assessments, security audits and advanced incident response protocols. These measures, along with regularly updating security protocols and incorporating feedback from security assessments, also strengthen the manufacturer's ability to withstand cyberthreats in real time.

> "The new cybersecurity model improved global operations by reducing cyber risks and bolstering cyber resilience that helps to avoid costly disruptions and maintain stakeholder trust."

Simplifying security and network management for a human resources (HR) group

Liantis, a leading HR group in Belgium that offers everything from workplace and absence management to payroll services, faced network obsolescence and the end of network security updates. For an organization that handles highly confidential information, this presented a significant risk of cyberattacks.

Liantis saw an opportunity to upgrade their network security and transition from capital-intensive up-front investments in hardware to a more flexible, opex-based network-as-a-service model. They partnered with NTT DATA and Palo Alto Networks to design and deploy a secure access service edge (SASE) solution.

NTT DATA had been managing data center infrastructure for Liantis, so we understood their business and technology requirements. We collaborated with their teams to design a tailored solution that combines internet connectivity, a software-defined wide area network (SD-WAN) and cloud-based security. This included applying zero trust principles to protect data, users and applications across remote and on-premises environments.

Following in-depth consultations and a proof-of-value exercise, we deployed the solution across four data centers and 50 locations. The results were immediate and impactful.

We simplified network management, with NTT DATA acting as a single point of contact to enable fast issue resolution through a single portal. The fully managed network provides stability and high-performance connectivity, and employees can work from anywhere more securely and efficiently. Local support teams, backed by global NTT DATA expertise, can easily address regional requirements and regulatory nuances.

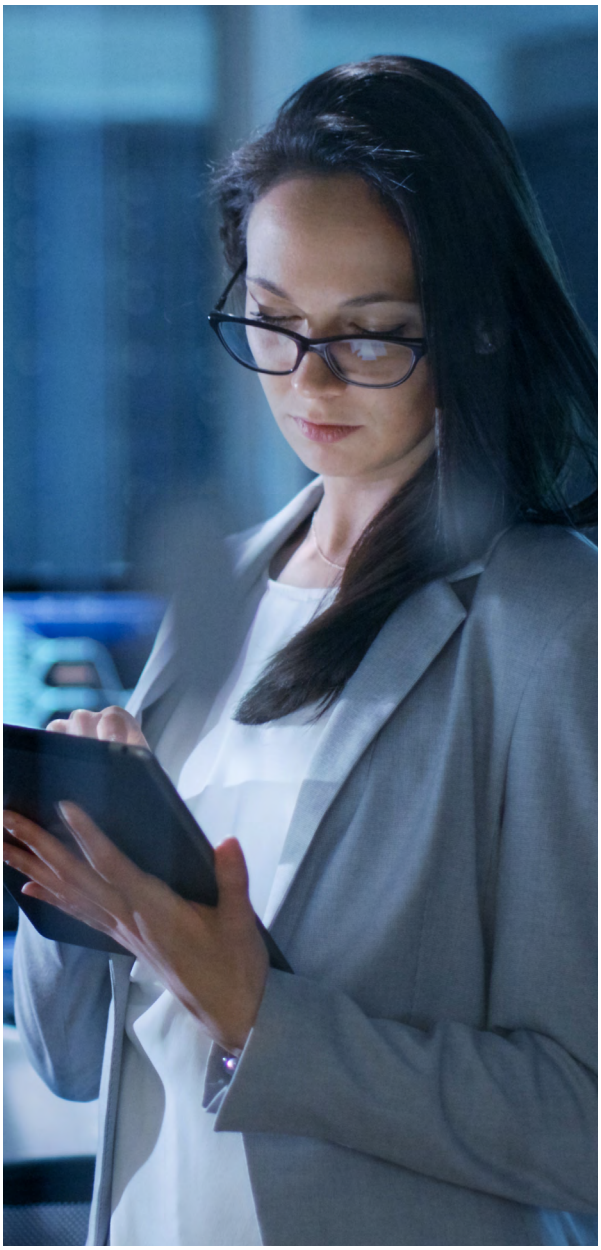
The solution is also scalable — as the organization grows and changes, the solution grows with it.

Why NTT DATA and Palo Alto Networks

The collaboration between NTT DATA and Palo Alto Networks brings together the strengths of two industry leaders to provide powerful security solutions tailored to the evolving needs of your organization.

Here's how we can transform your security posture:

- **Comprehensive combined security expertise:** NTT DATA has a track record in networking and cybersecurity services. Palo Alto Networks is renowned for providing cutting-edge security solutions, with advanced threat intelligence, machine learning and automation capabilities delivering robust protection against evolving cyberthreats.
- **End-to-end security solutions:** Our solutions cover every aspect of your network infrastructure. From risk assessment and threat prevention to incident response and recovery, we keep your environment resilient, responsive and adaptable. NTT DATA's cybersecurity services, combined with leading Palo Alto Networks security technologies, give you a holistic approach to security that aligns with your broader business goals. We help you simplify technology consumption, optimize deployment and ensure a smooth implementation right from the start.
- **Commitment to innovation:** NTT DATA and Palo Alto Networks are committed to developing integrated, AI-powered security solutions. Our efforts have led to innovations such as Managed Prisma SASE that simplify SASE adoption with an integrated, fully managed approach. Our ongoing investment in new technologies means your organization remains well-equipped to handle any security challenge.



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