# Simplify your security for proactive defense

## A secure environment, end-to-end, staves off cyberthreats and helps you take advantage of business opportunities

**NTT DATA and Palo Alto Networks help you create a robust, agile and predictive security posture to manage the growing complexity of your security environment and build network and cyber resilience.**

 

# Content

# Security: a key business enabler

**The traditional approach of managing networks and security in isolation no longer aligns with the realities of doing business in an edge-to-cloud ecosystem. You need proactive, stable and agile security measures to shield your organization from evolving threats.**

Security is about more than just detecting malicious threats. As organizations' traditional IT environments evolve into edge-to-cloud ecosystems, security has become a strategic business enabler – but there is a need for less complexity, a higher level of resilience and proactive measures.

**A simplified security environment minimizes operational risks, contains costs and limits your organization's vulnerability to sophisticated attacks.**

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, including reducing the number of security tools they use.

But complexity is a persistent challenge: at the same time, the number of tools dedicated to cloud security has increased by 60% from 2023.

**For CISOs, a resilient security framework is crucial for business stability and continuity.**

The framework should include comprehensive defense strategies, proactive threat mitigation and a focus on cyber resilience to help systems recover quickly after an incident. If your organization doesn't prioritize resilience, you risk long-term vulnerabilities and operational disruptions.

Leaders in resilient organizations know that robust security fosters confidence while supporting innovation and the exploration of new opportunities.

**Proactive security measures shield your organization from advanced threats and create a stable operational environment.**

Making security a strategic priority requires the active involvement of CISOs, CIOs and other stakeholders. It needs to be integrated into your organizational culture through company-wide discussions and regular training.

 

# Protection with less complexity

Properly securing your assets and data – including through AI-enabled threat prevention – lowers your total cost of ownership and contributes to a better customer experience (CX), as there is a lower risk of downtime or other business disruptions.

## Create the right strategy

**Aligning your security measures with your broader business goals makes security a catalyst for innovation, great CX and high levels of productivity.**

A comprehensive security strategy should encompass security, networking and cloud solutions to protect all aspects of your organization's infrastructure. Integrating security strategically not only protects your data and assets but also contributes to business continuity, fostering greater trust among customers.

Balancing security costs with your digital transformation goals can be challenging, but transformation is essential for business growth – and therefore security is a necessary investment.

## Manage growing complexity

**When you follow a unified approach to managing security complexity, your network and security functions are integrated to minimize vulnerabilities and maintain robust defenses.**

Simplifying these operations makes processes more efficient, reduces risk and saves you money; some organizations achieve this by outsourcing their security services to expert service providers.

## Build cyber resilience

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

A resilient security posture allows you to respond to and recover from these threats as efficiently as possible with minimal data loss or service disruption. Cyber resilience also helps your organization comply with regulations, mitigates financial losses from breaches and fosters trust among your customers.

 

# 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 and solutions to bolster your security posture. These include:

- **Leading Palo Alto Networks security solutions:** These solutions use advanced threat intelligence, machine learning and automation to prevent and mitigate cyberthreats.
- **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 that uses Prisma SASE and Cortex XSOAR from Palo Alto Networks, zero trust network access, and software-defined wide area network (SD-WAN) and application security.
- **Simplified, reliable deployment:** As part of our fully integrated service offering, we first validate all integrations to ensure the smooth deployment of solutions that work 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 security 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 supports business growth and innovation while protecting against evolving threats.

 

## How we applied this approach to protect 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 deliver visibility, resilience and scalability to 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 prioritized proactive risk management and a collective understanding of the importance of security across the organization.

The strategy 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 manage the beverage manufacturer's complex network and security environment, we implemented an integrated solution using Prisma SASE from Palo Alto Networks, which facilitates secure access service edge (SASE) by combining advanced security and networking capabilities as part of a unified platform.

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 Network Services, powered by SPEKTRA, complement the ability of Prisma SASE to deliver proactive threat detection. This collaborative approach has allowed the beverage manufacturer to streamline their security functions and focus their IT resources on strategic initiatives.

The new security model has also improved their global operations by minimizing the risk of cyberattacks leading to operational disruptions.

### 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 Prisma SASE, 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.

# 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 why choosing our partnership will transform your security posture:

1. **Comprehensive combined security expertise:** NTT DATA has a proven 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.
2. **End-to-end security solutions:** Our partnership offers end-to-end security solutions that 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 and Managed Network Services, combined with leading Palo Alto Networks security technologies, follow a holistic approach to security that aligns with your broader business goals. This integration simplifies technology consumption, optimizes deployment and ensures smooth implementation right from the start.
3. **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 Campus Networks with Prisma SASE, simplifying 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.

## Take the next step

Book an NTT DATA Network Assessment

Sign up for a live demo of NTT DATA's SPEKTRA network platform

**About NTT DATA**

Visit nttdata.com to learn more.

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


NTT DATA