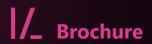# NASSTAR | FORTINET

Navigating the Future of Secure, Flexible Networking with Nasstar

Brochure

Introduction

Digital transformation is accelerating at an unprecedented pace, and the need for secure and flexible networking solutions has never been more critical.

The increasing demand for cloud services, remote work capabilities, and cutting-edge security highlights the need for innovative approaches. Industry predictions show that emerging frameworks like secure access service edge (SASE) and new technologies like generative AI will redefine how organisations manage and secure their networks. By 2026, most SD-WAN purchases are expected to integrate SASE models, while generative AI is set to have a significant impact on the automation of network configuration by 2026*.

Nasstar, a trusted leader in secure networking, has developed a unique set of expertise in SD-WAN, Operational Technology (OT), and Security Operations (SecOps). We've partnered with Fortinet to deliver tailored solutions that align with these emerging trends. This article explores a variety of case studies and innovations to prepare you for the future of networking.

Building adaptable networks

Taking control with SD-WAN

Traditional wide area network (WAN) systems were designed for office-to-data centre traffic, but these legacy setups struggle to meet the demands of modern cloud-based workflows. Software-defined wide area network (SD-WAN) takes connectivity to the next level by using software to dynamically manage traffic, improving performance, reliability, and cost efficiency.

SASE: The next step in secure networking

SASE combines SD-WAN capabilities with advanced security features like secure web gateways and zero-trust network access. It simplifies network management, enhances security, and ensures seamless connectivity for distributed enterprises. Gartner predicts a significant uptick in SASE adoption, driven by the growing complexity of cloud services and remote work.

Traditional network approaches simply no longer provide the levels of security and access control required by cloud-enabled organisations. SASE offers more control and visibility over the users, traffic, and data in a corporate network. This helps IT teams strengthen systems and react quickly to cyber threats. Networks built with SASE are also flexible and scalable. They can connect globally distributed employees and offices across any location, via any device.

What are the benefits?

Combining technologies like SD-WAN and zero-trust network access (ZTNA) into one system provides a lot of benefits. SASE allows users to securely access applications from any location and provides administrators with more control over IT environments.

Through SASE, multiple threat surfaces are automatically monitored and mitigated. Security and resource optimisation tasks can be carried out in real time without impacting the performance of systems and applications. SASE tools allow users to benefit from high-quality, secure IT environments.

Harnessing Gen AI in networking

What is Generative AI?

Generative AI (Gen AI) is a type of artificial intelligence that creates new content like text, images, or configurations based on patterns it has learned. In networking, it helps automate tasks, improve accuracy, and boost efficiency.

Current progress and future potential

GenAI in network configuration is just getting started, but its potential is huge. By 2026, GenAI could handle 20% of initial network configurations, a big jump from almost none in 2023*. This will transform network management by automating manual, time-consuming tasks.

AI-enabled automation allows businesses to streamline operations. It frees up valuable human resources for more complex and creative activities. Automation improves efficiency as well as employee satisfaction by reducing monotonous and error-prone workloads.

As AI evolves, the right tools will analyse network needs and suggest the best setups, reducing errors and enhancing performance. Companies starting their adoption journeys now will gain a competitive edge in crowded marketplaces.

Preparing for an AI-driven future

With three-quarters of businesses investing in AI already, we are already seeing this technology reshaping digital transformation by adding intelligence and new customer experiences to products and services, providing better insights, and automating mundane tasks in all industries.

However, the adoption of AI isn't without its challenges. If they're not addressed, skills gaps, data governance and security, and ethical concerns each prove barriers to effective AI implementation. For businesses to implement AI to its full potential, data quality and security, an AI-ready infrastructure and staff reskilling are all crucial steps.

Businesses should partner with an experienced AI specialist who can help guide them through the complexities of AI integration. We're helping our customers build AI-ready infrastructure. With cutting-edge technology and an expert team, we can help you design, develop, and secure an environment ready for innovation.

Addressing industry challenges

Operational Technology (OT)

Legacy OT systems, designed to operate in isolation, are now exposed to network threats due to increased connectivity. Additionally, the convergence of OT and IT has introduced new risks, and there is a shortage of professionals with OT cybersecurity expertise.

At Nasstar, we're addressing these challenges with tailored networking strategies, threat protection, and ongoing support. By leveraging Fortinet's tools, our experts provide visibility into OT networks and implement multi-layered security measures to protect against threats.

Security Operations (SecOps)

Traditional security and IT operations teams often operate in silos, leading to inefficiencies and slower response times. The rise in cyber-attacks and the need for integrated security practices have made SecOps essential for modern businesses.

Nasstar enhances SecOps capabilities with threat intelligence, automation, AI, and machine learning. Fortinet's global threat database provides up-to-date information on risks, while automation and AI improve threat detection and response times.

Secure SD-WAN

With the accelerations of digital transformation, traditional WANs are buckling under the pressure of modern requirements like remote work, multi-cloud environments, and edge computing. The mismatch has led to slow connections, high costs, and security risks.

Nasstar's SD-WAN solutions combine Fortinet's advanced routing technology with integrated security features. Our approach ensures fast and secure routing and reliable access to applications and data, regardless of location.

»» Case Study:

Jaguar Land Rover's Transformation

Jaguar Land Rover faced challenges with outdated OT systems, siloed technical processes, and poor data visibility. Nasstar introduced a cloud-native analytics platform that collects data about the car manufacturing process. Insights from the solution are being used to improve vehicle functionality and production efficiency.

»» Case Study:

Cyber defences for an emergency responder

Our customer's legacy equipment was struggling to keep up with modern security needs and has left critical gaps in its network. With Fortinet's Next-Generation Firewall (NGFW), we're helping the organisation detect, investigate, and respond to security incidents.

»» Case Study:

A utility provider's SD-WAN transformation

A utility provider faced challenges with outdated, costly networks that couldn't keep up with its business goals. We introduced centralised network management and control over OT assets, reducing deployment time and minimising cyber-attack opportunities. The solution also implemented a zero-trust approach, providing consistent role-based enforcement and contextualised access controls.

Nasstar and Fortinet: A partnership that delivers

Choosing the right partner ensures your network stays secure and efficient. With over 200 Fortinet certifications, Nasstar has the expertise to navigate complex IT environments. We also hold specialisations in SD-WAN, Operational Technology, and Security Operations, showcasing our leadership in secure networking and solving industry challenges.

Our experts provide tailored solutions, follow best practices, and offer proactive support to address emerging threats. Using Fortinet's advanced technologies, we build and manage solutions that enhance security, improve performance, and drive digital transformation.

Partnering with us lets you focus on your business while we handle critical infrastructure.

Enhancing your capabilities

Expertise and experience:

Work with a partner that understands the complexities of modern IT environments.

Tailored solutions:

Customisable services help you address unique challenges and achieve your networking goals.

Proactive support:

Benefit from ongoing support and proactive threat management, ensuring that you stay ahead of emerging threats.

As industries embrace digital transformation, secure and flexible networking is vital for success. By partnering with Nasstar, you gain tailored solutions, proactive support, and cutting-edge technologies to future-proof your networks. Our focus on secure, flexible networking allows you to drive growth and innovation with confidence, knowing your infrastructure is protected.

Ready to enhance your networking? Partner with Nasstar to secure your infrastructure and unlock new possibilities.

Our goal is to provide solutions for business challenges. We know every organisation has its priorities. So, we begin by understanding what matters most to them. Acting as trusted advisors, we become an extension of their team for ongoing success. We ensure continuous optimisation and comprehensive insights into their operations, giving them the advantage, now and in the future.

Get in touch →

NASSTAR