NASSTAR

Mapping your Journey to Secure, Flexible Networking

Brochure

A network that connects and protects

Secure networking is more essential than ever, with increasing pressure to protect infrastructure while optimising connectivity. For over a decade, we've been helping businesses overcome these challenges, expanding our capabilities and earning recognition in the process.

A shared vision

FORTINET

Our long-standing partnerships have ensured our customers stay ahead as networking evolves rapidly. Over the past 15 years, our collaboration with Fortinet has helped us deliver smarter, stronger security.

Our partnership with Fortinet →

NASSTAR

A leader in Fortinet services

We're proud to have earned Fortinet's SD-WAN, Operational Technology (OT), and Security Operations specialisations, making us one of just two Expert Partners in the UK to achieve this rare combination.

With over 200 Fortinet certifications under our belt, we're experts in tackling the toughest challenges across the most dynamic industries including manufacturing, logistics, energy, and utilities.

Find out more

Our customers get the best of both worlds: industry-leading technology from Fortinet and tailored solutions from a team that truly understands their needs. From improving operations to protecting against cyber threats, we're on hand to help businesses succeed.

In this guide, we'll highlight the key components of our Fortinet expertise:

- Operational Technology (OT)
- Security Operations (SecOps)
- Secure SD-WAN

By combining Fortinet's advanced technology with our expertise, we help businesses shift from reactive to proactive network management. This lets them focus on growth, knowing their systems are optimised and well-protected. Our Fortinet-powered offerings give businesses the confidence to handle whatever comes their way.

Leigh Walgate

Managing Director, Secure Networks at Nasstar

NASSTAR

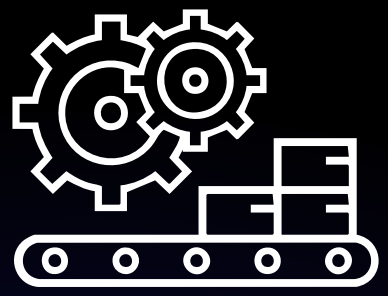
Operational Technology (OT)

Protecting the heart of industry

Picture this...a manufacturing plant is brought to a standstill due to a network breach.

Critical communication between operational technology (OT) systems is disrupted and production must stop for days, costing precious resources and revenue.

This isn't just a cautionary tale. It's a growing reality for manufacturing, logistics, energy, and utilities businesses. As more systems are digitised and connected, vulnerabilities in OT systems have become prime targets for attacks.



What is Operational Technology?

OT is the hardware and software that controls physical processes in certain industries. Examples of OT include systems that control power generation; platforms that monitor fleet vehicle locations and optimise routes; and technology that oversees industrial machinery used in assembly sequences.

Whether used in a production line or a power grid, OT systems are an essential component of modern society.

As the pace of digital transformation accelerates, OT and IT systems are becoming more interconnected. While the convergence has boosted efficiency, it's also helping businesses make smarter, data-driven choices. However, despite the benefits, combining OT and IT has introduced new risks to complex and delicate operations.

Legacy OT systems, designed to work in isolation, are now being exposed to network threats and the consequences of IT misconfigurations.

The challenges of securing OT

Protecting OT systems isn't easy. Some of the biggest hurdles include:

Legacy infrastructure: Many old systems have fallen behind today's networking and security best practices and bringing them into compliance is proving difficult.

Increasing connectivity: Greater integration with IT services is expanding attack surfaces faster than in-house technical teams can handle.

Sophisticated threats: The OT-IT convergence has presented attackers with a unique opportunity. Malware designed to disrupt physical operations is now on the rise.

Skill gaps: Despite the urgent need to secure these vulnerabilities, there's a shortage of professionals with OT cyber security expertise.

NASSTAR

How Nasstar and Fortinet can help

We're working with Fortinet to secure OT environments with a multi-layered approach:

- **Tailored solutions:** As manufacturing, logistics, energy, and utilities experts, we design security strategies that match industrial needs.
- **Threat protection:** Through automation and best practice, Fortinet's market-leading tools provide visibility into networks and strong defences against threats.
- **On-going support:** Our connectivity experts will act as an extension of your team by providing continuous value and proactive support.

Chris Briers

Regional Manager, MSSP UKI at Fortinet

"The convergence of OT and IT is transforming industries, but it also introduces new risks. Forward-thinking organisations are prioritising cyber security as a core component of their digital strategy. With technologies advancing quickly, the future of OT security lies in proactive threat hunting and adaptive protection. With Nasstar and Fortinet on your side, you can secure your operations while embracing the opportunities of Industry 4.0."

Case study:

A global automotive manufacturer

- **The brief:** Jaguar Land Rover struggled with outdated OT systems, siloed technical processes, and poor data visibility.
- **The solution:** We introduced a cloud-native analytics platform that collects data about the car manufacturing process.
- **The benefits:** Insights are now fed back into car design and engineering to improve the functionality and operation of vehicles, as well as increase production efficiency.

We remain engaged with Jaguar Land Rover, providing important consultancy as well as a 24/7 managed service to ensure that OT and IT operate in unison. As JLR and the wider automotive industry begin to focus on electric cars, a partnership with Nasstar is crucial to success.

JAGUAR LAND ROVER

NASSTAR

Security Operations (SecOps)

Staying one step ahead

50% of UK businesses reported experiencing cyber-attacks or security breaches in 2024.

That figure rises to **74%** for large businesses*. With customer data, intellectual property, and organisations' reputations at stake, now is the time to bridge the gap between traditional security and IT operations teams.

*UK Government – Cyber Security Breaches Survey 2024

NASSTAR

What is SecOps?

SecOps emphasises breaking down barriers between security and IT teams ensuring that security practices are integrated into every aspect of IT operations, from development to deployment and maintenance.

Businesses that practice SecOps combine tools, processes, and teams to spot and stop cyber threats before they impact critical infrastructure like OT systems.

In other words, SecOps encourages a proactive approach to security. It's powered by cutting-edge technology such as automation, analytics, and real-time monitoring to keep threats at bay.

A great SecOps strategy helps businesses detect threats early, respond fast, and adapt to new risks quickly.

The building blocks of SecOps

With Fortinet's help, we've taken our SecOps capabilities to the next level. Our partnership makes businesses safer while bringing security and IT teams closer together.

Threat intelligence: Access to up-to-date information on the latest risks. Fortinet's global threat database will provide your team with the latest insights.

Automation: Repetitive tasks are handled automatically, and incidents are resolved in seconds. That means faster containment and mitigation while eliminating human error.

AI and machine learning: Insights powered by AI to detect patterns and anomalies. Advanced analytics tools will find and respond to threats faster and with greater accuracy.

NASSTAR

Case study:

Next-Gen Threat Protection for an Emergency Response Partner

- **The brief:** Our customer's legacy firewall equipment was struggling to keep up with modern security needs and has left critical gaps in its network.
- **The solution:** We're helping the organisation replace outdated equipment with Fortinet's Next-Generation Firewall (NGFW). We'll improve security, performance, and scalability across the emergency responder's network.
- **The benefits:** We are transforming the IT team's ability to detect, investigate, and respond to security incidents across the organisation's infrastructure.

Stevan Judd

Account Director at Nasstar

"By working closely with Fortinet, we've been able to deliver a solution that meets our customer's security and performance needs. Our blend of technical and public sector expertise has once again made us the organisation's first choice. This project is another step in supporting its goal of modernising emergency response."

Secure SD-WAN

Connecting the modern business

NASSTAR

Wide-area networks (WANs)

have come a long way.

Traditional WANs, built to handle traffic between offices and data centres, worked well in the pre-cloud era. However, as businesses shifted to cloud services and remote work, older networks started to show their limits, causing slow connections, high costs, and security risks.

The limitations of legacy networks have led to the adoption of Secure SD-WAN - the next step in software-defined wide-area networking.

Secure SD-WAN provides fast and secure data routing, giving businesses reliable access to their applications and data, wherever they are.

How Secure SD-WAN works

Secure SD-WAN transforms networking with advanced routing technology that finds the best path for data, boosting speed and performance. With integrated security features like encryption, firewalls, and zero-trust access policies, Secure SD-WAN is purpose-built for dynamic businesses with remote teams and complex IT setups.

Solving business challenges

Remote work: Secure connections are non-negotiable in a remote-first era. Secure SD-WAN encrypts data and ensures users access only what they need, keeping businesses protected.

Multi-cloud: Managing multiple cloud platforms can be complex. Secure SD-WAN simplifies the process with centralised visibility and seamless management.

Edge computing: Real-time operations demand low latency and high bandwidth. Secure SD-WAN delivers both, empowering businesses to process data efficiently at the edge.

NASSTAR

Fortinet-powered SD-WAN

Our SD-WAN solutions combine Fortinet's industry-leading technology with Nasstar's tailored approach to implementation and support. The platforms we deliver balance networking and security needs to create intelligent traffic routing and real-time threat detection for complete visibility.

Our experts begin with a deep dive into your current network setup. Based on the information gathered, we'll design and deploy a Secure SD-WAN that meets your specific needs.

Deployment is fast and efficient, and we offer ongoing management to ensure your network stays secure and optimised.

Case study:

A utility provider's SD-WAN transformation

NASSTAR

A provider of low-carbon services was struggling with outdated, costly networks that couldn't keep up with modern demands. The provider's system faced frequent security and connectivity issues, leaving networks exposed to nation-state hackers and advanced persistent threats (APTs).

By introducing centralised network management and control over OT assets in place, we have:

/01 Reduced deployment time and minimise opportunities for cyber-attacks.

/02 Introduced a zero-trust approach, which provides the business with consistent role-based enforcement and contextualised access controls.

/03 Established a blueprint for mass deployment across the organisation's extensive branch network.

Dan O'Connor

Senior Account Manager at Nasstar

"This project has showcased the transformative power of SD-WAN. We've not only delivered enhanced security, but we've laid the foundation for a cost-efficient, scalable solution that can be replicated across the customer's extensive branch network. This is another milestone in our commitment to innovative, pragmatic, and impactful solutions."

Building a safer, smarter future together

Businesses like yours need more than just tools

With a trusted partner like Nasstar, you'll be ready to face the complexities of secure networking.

Our experience in manufacturing, logistics, energy, and utilities ensures that critical systems stay secure, efficient, and flexible. Whether you need to protect OT systems from evolving threats, optimise security operations for faster response, or enable seamless connectivity, we've got you covered.

Leigh Walgate

Managing Director, Secure Networks at Nasstar

"Our goal is to build secure and adaptable networks that empower businesses to focus on what matters most - growth and innovation. With Fortinet as our trusted partner, we're leading the charge to create resilient networks that support our customers' long-term success."

Let’s secure your success

Ready to transform networking in your organisation? Partner with Nasstar to unlock the full potential of OT, SecOps, and SD-WAN.

Safeguard your critical infrastructure today.

Get in touch →

nasstar.com
0345 003 0000
salesenquiries@nasstar.com