Nasstar

The new rules for securing energy & industry

A practical guide to SASE for
manufacturing, logistics, energy, and utilities

2025

Nasstar

Navigate complexity, with confidence

Hello, we're Nasstar - your specialist technology partner. We help you embrace change, work smarter, and cut costs.

For over 25 years, we've supported manufacturing, logistics, energy, and utilities organisations achieve digital transformation for improved security and scalability.

With a phased, consultative approach to SASE, we'll help you regain control of complex infrastructure, reduce risk, and unlock operational value.

Speak to Nasstar about SASE

Nasstar in numbers

780+

strong team of experts

176+

engineers

10+

years as a Microsoft partner

24/7/365

support team

25+

years of experience

Nasstar

Contents

Executive summary

Cyber threats to the industrial and energy sectors are at an all-time high, accounting for a growing share of global attacks. 80% of breaches exploit users through techniques like phishing and credential theft. Meanwhile, with IT/OT convergence, regulatory pressure, and rising costs to contend with, security is now a boardroom priority.

Build a more secure operation with SASE.

Nasstar

80%

of breaches target users through phishing, social engineering, or stolen credentials.

Talos IR data

The energy and industrial sectors are evolving fast. Systems once isolated are now always-on and interconnected. While digitisation has driven efficiency, it has also exposed critical infrastructure to rising cyber threats. Manufacturing, logistics, energy, and utilities (MLEU) organisations must modernise securely, or risk falling behind.

Secure Access Service Edge (SASE, pronounced “sassy” for the uninitiated) is emerging as the clearest path forward. SASE offers a strategic approach that unifies your network and security environment.

In summary

In today’s threat landscape, operating with traditional security is like managing critical infrastructure without modern monitoring systems. SASE provides the comprehensive dashboard you need. It shows you exactly what’s happening across every plant and site in real time.

Why your security stack could be working against you

Your infrastructure has grown around the needs of different teams, priorities, and eras. Over time, it's become a patchwork.

There are legacy VPNs (Virtual Private Networks) that can't verify users or devices. You likely rely on multiple vendors for firewalls, cloud gateways, access control, and endpoint tools. Meanwhile, OT (Operational Technology) protections, if present at all, are inconsistent across sites and asset types.

It might seem odd, but piling on more security layers can make things less secure.

All that extra complexity creates confusion, leaves gaps, and makes the whole setup harder to manage. In most cases, keeping things simpler and using fewer, well-integrated tools works better for closing gaps and staying protected.

68%

of organisations operate between 10 and 49 security tools or platforms.

CDW Cybersecurity Report 2024

This scenario is especially dangerous for operationally intricate MLEU organisations that depend on things like:

- Remote engineers connecting to SCADA (Supervisory Control and Data Acquisition) systems
- Third-party vendors accessing platforms such as warehouse logistics or remote asset management systems
- Field teams relying on real-time data from IIoT (Industrial Internet of Things) devices
- Engineers connecting to remote substations to run diagnostics
- Maintenance teams working on sewage plants using mobile apps
- Drivers uploading location data from logistics vehicles in the field

If these issues feel familiar, you're not alone. Many organisations are juggling dozens of tools and endpoints, and hundreds of access rules. Not only is this extremely inefficient and inconvenient for all involved but, worst of all, it still leaves you at risk.

In summary

Think of your legacy security setup like this... You have a few smart meters but still do manual readings in other areas. That means you're only seeing part of the picture. SASE gives you full monitoring across your whole operation, so there are no blind spots or hidden risks.

You've made a start (but you're still at risk!)

Most MLEU organisations have already put pieces of a stronger security system in place.

For example, you might already be using an endpoint detection tool, have cloud security policies set up, rely on VPNs for remote access, and apply some limited Zero Trust principles.

5%

of organisations reported 100% visibility of OT activities in 2024.

2024 State of Operational Technology and Cybersecurity Report

The way these tools are stitched together creates a new set of issues:

- **Overlapping capabilities**
  which mean you're paying for the same thing twice
- **Gaps between tools**
  and IT/OT integration points
- **Interoperability problems**
  limiting the flow of data and alerts

Even if you've avoided security breaches, chances are that your systems are strained. As threats inevitably evolve, gaps widen and vulnerabilities multiply.

What you need is a way to bring these capabilities together and manage them as one.

In summary

Your existing security investments are like having some smart meters but still relying on manual readings elsewhere - giving you incomplete visibility. SASE provides comprehensive monitoring across your entire operation, eliminating blind spots and vulnerabilities.

SASE: A simple solution to a complex problem

Traditional, perimeter-based security models are like having a lone security guard at the front gate of your facility. Once trust is granted, access is unrestricted. This approach has failed to keep pace with IT/OT convergence, hybrid workforces, and cloud-driven operations.

Secure Access Service Edge (SASE) is a cloud-native architecture that consolidates your networking and security functions into one unified model. It replaces the ‘lone security guard’ with intelligent checkpoints at every doorway, constantly verifying who goes where, and when.

SASE brings together concepts that may be familiar, like SSE (Security Service Edge), ZTNA (Zero Trust Network Access), CASB (Cloud Access Security Broker), and SWG (Secure Web Gateway).

25%

SASE has been shown to deliver a 25% reduction in security incidents and a 20% improvement in network performance.

Forrester

Nasstar

Let’s explore what the core elements of SASE mean in practice.

- **Zero Trust Access**
  No one gets blanket access. Identity, devices, and context (things like location and time of access) are considered and verified every time.
- **Cloud-first delivery**
  Security services like firewall, traffic inspection, and threat detection are closer to the user, not locked in a central data centre.
- **Single-pane visibility**
  From OT devices to remote user sessions, everything is monitored in one place.

Security and convenience, without compromise.

For MLEU, SASE removes the age-old friction between security and productivity. Site engineers can securely log in from mobile devices without clunky VPN gateways. Third-party vendors only get access to what they need, and only when they need it. Operational staff spend less time battling authentication workflows and more time focusing on running safe, efficient operations.

With fewer moving parts, fewer vendors, and fewer unknowns, the beauty of SASE lies in its simplicity.

In summary

Traditional security resembles a single checkpoint at your facility entrance. SASE implements smart access control at every critical point - doors, hallways, and workstations. It ensures only authorised personnel can access sensitive areas.

From factory floor to vendor access: What Unified SASE delivers

SASE isn't just IT simplification. It delivers specific, measurable outcomes for MLEU operators:

- **Strengthen OT protection**
  Get visibility into SCADA networks and industrial controls without jeopardising uptime.
- **Simplify and fortify access control**
  Grant role-specific access to vendors, engineers, and support teams with zero-trust boundaries.
- **Enhance compliance**
  Generate audit-ready reports with unified logging, no matter where access is happening.
- **Reduce your human error risk factor**
  Flag risky configurations and isolate breaches to prevent threats from spreading laterally across your network.
- **Improve your user experience**
  Save time and frustration with less friction, fewer multi-factor authentication (MFA) prompts, and fast access to the right apps from any location.
- **Lower cost of ownership**
  Consolidate overlapping tools, reduce management overhead, and simplify your vendor contracts.

Nasstar

270%

Large enterprises can expect a return on investment of up to 270% from SASE adoption

Forrester

Make SASE your strategic advantage

The benefits of SASE are clear. But the reality is that most MLEU organisations will have to appeal to numerous stakeholders, each of whom will have differing priorities.

- **CEOs care about continuity, trust, and maintaining a competitive advantage.**
- **CFOs are motivated by cost predictability, ROI, and reduced insurance premiums.**
- **CISOs want to ensure uptime, compliance, and visibility.**

✦ In summary

SASE enables seamless, secure connections between operational sites, remote engineers, and third-party vendors while maintaining complete visibility.

Evolution not revolution: How to simplify SASE transformation

With Nasstar, transformation never means disruption. Our approach to SASE is phased, consultative, and always focussed on delivering long-term value.

Aligned to the NIST (National Institute of Standards and Technology) Zero Trust Architecture, our framework follows three key principles:

- **Assume breach**
  Always be prepared for security threats.
- **Verify explicitly**
  Authenticate every access request.
- **Least privilege access**
  Limit access to only what's necessary.

70%

of all transformation projects fail to deliver as promised, falling to 20% or below when proper management processes are followed.

TeamStage

We start where you are, and build from there:

1. **Identify & prioritise**
   Pinpoint critical gaps and align efforts with your business goals.
2. **Audit & inventory**
   Catalogue your systems, tools, policies, and OT/IT integrations.
3. **Assess**
   Pilot new approaches in low-risk zones, such as remote diagnostics or supplier access.
4. **Implement**
   Roll out protections, step by step, with minimal disruption.
5. **Run & optimise**
   Continuously refine posture, monitor threats, and evolve alongside your operations.

In summary

Implementing SASE is like transitioning from manual logistics to modern tracking systems. It's a strategic evolution that enhances capabilities without disrupting operations. Your data becomes as secure as a shipping container: sealed, tracked, and tamper-proof throughout its journey.

Where to start: Cyber Security Assessment

Before building a more secure setup for the future, you need clarity on your current posture.

> “SASE adoption shouldn’t be considered another complex technology project. Instead, view it as a transformation that’s designed to recover lost operational value and redirect resources toward achieving core commercial objectives.”

Leigh Walgate, Managing Director, Nasstar

Nasstar

That is exactly what Nasstar’s Cyber Security Assessment delivers:

- **External testing:**
  Penetration tests simulate attacks on external-facing systems - from supplier portals to field service apps.
- **Internal scans:**
  Scan for unpatched control systems, outdated engineering work stations, or unauthorised asset connections.
- **OT analysis:**
  Review SCADA protocols, remote PLC (Programmable Logic Controller) access points, and other vulnerable OT endpoints.

We provide a concise report showing your vulnerabilities ranked by severity, your exposure across IT/OT integrations, and a clear roadmap to risk mitigation.

This is the first step on your journey to SASE transformation, giving you confidence to move forward with purpose.

✦ In summary

Before modernising your security infrastructure, you need to understand your current environment - just as SCADA provides visibility into substation operations. A Cyber Security Assessment gives you this critical baseline, identifying vulnerabilities before they become critical failures.

Nasstar

Case Study

Driving security, compliance, performance, and profits with SASE

Challenge:

A UK-based utility provider was struggling with inconsistent security across multiple remote substations, legacy SCADA systems, and an expanding remote workforce. Its existing tools lacked integration, and compliance audits were growing more complex.

Solution:

Nasstar conducted a full assessment and implemented a phased SASE adoption strategy.

Impact

- **Stronger security**
  with real-time OT and IT threat visibility
- **Better performance**
  for field teams accessing critical apps
- **Simplified compliance**
  with unified audit logs and policy enforcement
- **Lower operational costs**
  through vendor consolidation and reduced manual processes

SASE became a strategic enabler, giving the organisation real-time control over OT and IT environments, stronger resilience against regulatory scrutiny, and a foundation for future innovation. With risk reduced and complexity cut, the business was able to redirect resources toward performance and profitability.

✦ In summary

This utility provider transformed its security operations by implementing SASE. Now, it benefits from comprehensive visibility, streamlined compliance, and significant cost savings.

Build a smarter, more secure operation with SASE

In MLEU, SASE isn't just another framework or the latest technological fad. It represents a necessary evolution that allows organisations to stay ahead of the curve.

SASE will help you regain control over your sprawling vendor ecosystem. It reduces risk without slowing operations. It can secure your legacy OT and enable digital transformation. SASE provides a scalable, adaptive security posture attuned to the modern threat landscape.

Nasstar

> "SASE is helping organisations tackle various cyber threats at once, giving them better protection and visibility, all managed from one central place. It's the smart way to stay ahead and keep your business secure."

Andrew Hasnip, Senior Sales Director, Nasstar

Make SASE your strategic advantage

With Nasstar, security becomes a strategic advantage. As your long-term partner, we can help you embrace SASE and achieve ongoing value.

We'll help you cut through complexity, simplify your stack, and protect your business.

Speak to Nasstar about SASE

Contact Us

Your specialist technology partner for
secure, scalable industrial transformation.

Nasstar