QUANT ICT
Smart Network

Say goodbye to VPN. Why Zero Trust is the new standard

How Zero Trust Network Access (ZTNA) and Secure Service Edge (SSE) are replacing classic VPNs: more secure, simpler and ready for NIS2

HPE

Why the VPN has had its day

There was a time when the Virtual Private Network (VPN) was the gold standard for secure remote access. If you were outside the office, the VPN was your bridge back in.
VPN worked by creating a secure "tunnel" that routes a user's traffic through an encrypted connection into the corporate network.

Think of it as the castle wall of the digital workplace. For years, the moat and drawbridge (VPN + firewall) kept intruders out, while employees inside could move freely. And in many cases, that wall still stands. The problem is: today's threats no longer come just from outside. Attackers find ways over, under, and even through the walls.

The limitations of VPN aren't just technical. They stem from how work itself has evolved. Employees are no longer just logging in from a home office. They are connecting from client sites, co-working spaces, airport lounges, and hotel rooms. Many of the applications they use aren't even inside your corporate network anymore. They're in the cloud, hosted somewhere halfway across the world.

At the same time, your ecosystem of users has grown more complex. It's not just employees who need access: external vendors, contractors, consultants, and partners often require connectivity to your systems.

This creates a problem. Classic VPNs were never designed for this reality.

- They funnel all traffic through a single gateway, creating bottlenecks.
- They give broad network access after one login, which creates security blind spots.
- And they make life harder for both users and IT teams.

In an era of increasing ransomware threats, phishing, and supply chain attacks, the VPN has become a dangerous shortcut. With a VPN, once you're in, you're in. There's no granular control, no ongoing verification. That's a big risk today.

The solution is to stop assuming that anyone, or anything, should be trusted by default. That is the foundation of Zero Trust.

What is Zero Trust (and what is it not)?

Zero Trust is not a product you buy, plug in, and forget. It's a security philosophy that flips the old model on its head.
In the old castle model, the focus was on keeping intruders outside the walls. Zero Trust takes a different approach: it assumes threats are already inside.

Therefore, Zero Trust means:

- No implicit trust.
- Every user, device, and application must prove its identity every time.
- Access is limited to the specific resources needed, nothing more.

It's like replacing the castle's single gate with multiple guarded checkpoints inside the walls. Every room has a badge reader. Every corridor has a guard. If a hacker compromises a user's credentials, they don't get the keys to the kingdom. They get access to one small, monitored room.

Zero Trust is about shifting your mindset. Security is no longer about building a single fixed barrier and hoping it holds. It's about making sure every interaction, no matter how small, is verified and appropriate. That's why Zero Trust is continuous by design. It checks again and again whether a connection should still be allowed.

Zero Trust for NIS2

The European NIS2 directive explicitly calls for the kinds of capabilities that Zero Trust delivers. Aimed at strengthening cybersecurity in essential and important sectors such as energy, healthcare, manufacturing, and government, NIS2 sets clear expectations for how organizations control and monitor access. In practice, this means:

- Visibility into who is accessing what: the ability to track and log all user activity across applications, systems, and data
- The "least privilege" principle: ensuring users only get the access they truly need to perform their role, nothing more
- Continuous monitoring and auditing: ongoing oversight to detect suspicious behavior and prove compliance during audits

ZTNA, SSE and SASE simply explained

Zero Trust is the principle. To make it operational, you need technologies that enforce it. This is where three key acronyms come in.

ZTNA – Zero Trust Network Access

ZTNA is the front-line enforcer of Zero Trust. Instead of connecting you to the whole network, it connects you only to the specific service or application you need. If you're a supplier who needs to work on a single machine's control software, ZTNA gives you that, and nothing else. It works by authenticating the user and device, verifying their security posture, and then creating a direct, encrypted connection to the authorized resource without exposing the broader network.

SSE – Secure Service Edge

SSE is the broader cloud-based security stack. It includes:

- ZTNA for application-level access control.
- Secure Web Gateway (SWG), which filters and inspects all web traffic to block malicious sites, phishing attempts, and unsafe downloads before they can harm users or systems.
- Cloud Access Security Broker (CASB): this sits between users and cloud applications like Microsoft 365 or Salesforce to monitor usage, enforce policies, and prevent unauthorized data sharing.
- Data Loss Prevention (DLP): scans data in motion and at rest to detect and stop sensitive information (like personal data or trade secrets) from leaving the organization without permission.

SSE is about securing user access wherever they are, while giving administrators full visibility and control.

SASE – Secure Access Service Edge

SASE combines SSE with SD-WAN (Software-Defined Wide Area Networking). In addition to security, it optimizes network performance across sites, data centers, and cloud services. With SASE, security follows the user. It's not tied to the office, the firewall, or the VPN gateway.

Why switch?
The 6 biggest advantages

1. Much more secure than VPN

VPNs work on the assumption that the network boundary is the gatekeeper. But once a connection is established, a user has broad access, even to systems they don't need. That means if a hacker steals credentials or exploits a VPN vulnerability, they can quickly move laterally across the network, searching for weaknesses and causing more damage. ZTNA/SSE removes this blind trust:

- **Access is application-specific.**
- **Permissions are continuously checked.**
- **Every session is authenticated, authorized and logged.**

Security also shifts from the network to the user. It no longer matters where the user is connecting from. Security is built into every request. Think of VPN as a master key to the building. ZTNA on the other hand is a badge that only opens the rooms you are authorized for, and only while you need them.

2. Access, anytime, anywhere

For users, VPN often means:

- **Remembering to connect.**
- **Waiting for the secure connection to start.**
- **Coping with slow performance as traffic is sent through the company network first.**

ZTNA/SSE remove these hassles entirely. Connections are seamless, and protection is always on, no matter where the user is. Performance is often better because traffic can go directly to the (cloud) application rather than detouring through a central VPN gateway.
And as long as the internet connection and the data center are operational, the service stays available without any action from the user. When security works quietly in the background like this, people don't complain about it. They simply get their work done. That's exactly what ZTNA gets right.

3. Less complex for IT

In many organizations, the VPN estate is a patchwork of clients, versions, and configurations. Supporting it consumes time and creates risk.
ZTNA/SSE simplify things:

- **One cloud-based platform for all access policies.**
- **Consistent enforcement for all users and devices.**
- **Instant policy changes without reconfiguring endpoints.**

With one central policy, you can apply changes across the entire organization instantly, without touching every individual ZTNA client. That shift removes a major operational burden from IT teams and reduces the chance of misconfigurations that could open security gaps.

4. Give external parties access without risk

One of the most common sources of over-permissioning is external access. A contractor needs to work on one system, but to get to it via VPN, they end up with far wider access than necessary.
With ZTNA:

- **They log into a secure, browser-based portal.**
- **They see only what's relevant to them.**
- **There's no VPN software to install, and no permanent network connection.**

This is especially valuable for short-term projects, where you can grant and deactivate access instantly.

5. Full visibility, as required by NIS2

VPN tells you who connected and for how long. ZTNA/SSE tell you:

- **Which apps they accessed.**
- **Which actions they took.**
- **Where they connected from.**

And all of this is logged for auditing, compliance, and incident response.
That level of insight turns visibility into control. Without it, you're relying on luck to catch problems before they escalate. With ZTNA/SSE, you can detect suspicious activity in real time and take action before it becomes a breach.

6. Future-proof and ready for compliance

The threat landscape will keep evolving. So will regulations like NIS2 and GDPR. ZTNA/SSE prepare you for both:

- **The principle of minimizing data exposure: users can't see or download data they don't need.**
- **Built-in data loss prevention and content inspection.**
- **Easier compliance reporting thanks to detailed logs.**

Sectors where Zero Trust makes a difference

Zero Trust, SSE, and SASE aren't niche solutions. They address challenges that many organizations face. In sectors covered by NIS2, the stakes are even higher: a breach isn't just bad news, it can also mean heavy fines, lost trust, and costly downtime. Here are three situations where moving to a Zero Trust approach makes a real difference.

Healthcare

A GP can remotely and securely access hospital records from their practice, without exposing other parts of the network. The hospital meets NIS2's visibility and access control requirements, and patient data remains protected.

Industry

A technician in another country can securely log into the control system for a production line, without touching anything else in the factory network.

Government & education

Staff and contractors can connect securely from any location. Administrators can see and control exactly what's being accessed, which is critical for public-sector compliance.

How to get started with Zero Trust

Making the switch to Zero Trust doesn't have to be overwhelming. In fact, the most successful implementations are often the ones that start small, prove their value quickly, and then scale across the organization. Here are six steps you can take to get started:

1. **Focus on the biggest risks:** Identify systems or data that would cause the most damage if breached, and start there.
2. **Map access needs:** Determine exactly who needs access to what. This often reveals unused accounts or overly broad permissions you can close immediately.
3. **Run a pilot:** Roll out ZTNA/SSE to a small group or department. Use their feedback to fine-tune policies and processes.
4. **Keep it seamless:** Integrate single sign-on (SSO) and multi-factor authentication (MFA) so security doesn't slow people down.
5. **Monitor and adapt**: Use the platform's visibility to track usage, detect anomalies, and refine rules. Digital experience monitoring can help IT spot performance issues before users do.
6. **Expand in stages**: Once the pilot is stable, extend it to more teams, locations, and partners.

Remember, Zero Trust is a journey, not a single project. Each step reduces your attack surface, improves resilience, and strengthens compliance, all while keeping the business running smoothly.

Why choose Quant as your partner?

Zero Trust is as much about expertise as technology. Quant brings:

- **Vendor independence:** We integrate ZTNA/SSE into mixed environments.
- **Smooth adoption:** We connect it to your existing identity systems like Azure AD or Microsoft MFA.
- **Proven tech:** HPE Aruba Networking provides the secure, cloud-based infrastructure that underpins our solution. This platform delivers the scalability, resilience, and policy control needed for Zero Trust, while ensuring a seamless user experience.
- **Ongoing service:** With Quant-as-a-Service, you get continuous monitoring, updates, and support.

> *“We don’t just implement and leave. We stay, we monitor, we adapt, because threats and needs change.”*

Is your VPN in need of replacement?

VPN was built for a different time. Today, it can slow you down, create security blind spots, and fail to meet compliance needs.
Zero Trust, enforced through ZTNA/SSE, is the new standard. It gives you:

- **Stronger security by limiting trust.**
- **Simpler IT management.**
- **A smoother user experience.**
- **Full visibility for compliance.**

With Quant, you can move to Zero Trust at your own pace, starting small, growing smart, and staying ahead of threats.

QUANT ICT

Smart Network

QUANT ICT
Industrieweg 4 bus 5
3001 – Heverlee

www.quant.be
+ 32 16 380 840
info@quant.be