ZTNA strengthens security and business operations

Schnellecke Logistics secures its digital ecosystem with a zero trust approach

Schnellecke Logistics works with some of the world's largest automakers, serving as a critical link in the global supply chain. To protect access to its on-premises and digital workflows, the company is adopting zero trust access with HPE Aruba Networking Secure Service Edge (SSE), as it optimizes its security strategy.

Industry: Logistics
Country: Germany

Logistics excellence at the heart of global supply chains

It has been over a hundred years since Henry Ford famously said, "Any customer can have a car painted any color that he wants, so long as it is black."

While many aspects of Ford's production line revolution remain, the automotive industry has evolved since. Today, car buyers have an increasingly large range of ways to customize their new cars. Even among mass-market manufacturers, it's not unusual to offer a choice of seven exterior colors, along with options for upholstery, trim, stitching, and alloys. No two cars need to look the same.

For car manufacturers, the challenge is to balance customer choice with production efficiency. With modern cars consisting of up to 30,000 individual components, and different parts coming from all corners of the world, too much choice could disrupt production processes.

Schnellecke Logistics is a specialist logistics service provider, working with some of the world's largest automotive manufacturers. Its solutions range from transport and warehousing to preassemblies and sequential production of individual parts. Schnellecke Logistics sits at the heart of global supply chains, a critical component in just-in-time production.

For its customers, the key to Schnellecke's success is to know the exact location of every part and container at any given moment, anywhere in the world. At its core is the Digital Control Tower (DCT), a digital twin of Schnellecke's global operations. This creates a dashboard that tracks the location and progress of every item, whether on the road or in the warehouse. The data feeding this dashboard is being further refined with the addition of new sensors and the application of AI.

All this relies on a high performance network with built-in zero trust security. As the business becomes increasingly digital, the high availability of the network becomes more critical, as does the ability to securely access its resources.

"There can be no disruption," says Markus Werner, Head of Group Competence Center-IT Infrastructure at Schnellecke Logistics. "Our network cannot drop, even for 30 minutes. There are stiff penalties for any outage."

This task would be challenging on a calm day. It becomes monumental when there are numerous malicious actors looking to exploit the Schnellecke Logistics network through internet-based attacks like DDoS, ransomware, malware, and more.

"The reality is that digital workflows lead to a greater attack surface, and we're regularly attacked by hackers. We must contain any such attempts," says Werner.

Vision

Streamline global logistics through the adoption of digital tracking, Internet of Things (IoT), and automated workflows

Strategy

Unify SD-WAN and cloud-native zero trust security to strengthen global network and establish continuous network access validation

Outcomes

— Restricts network access to specific applications and resources

— Maximizes network uptime to safeguard global supply chains

— Underpins secure roll out of further IoT and digital innovation

— Limits exposure to internet-based attacks like distributed denial of service (DDoS)

Strengthening resilience with zero trust network access

To protect its global operations, Schnellecke Logistics has transformed how it structures and manages its global network. It has created standard network templates that bring a new level of consistency. This allows local operations—Schnellecke Logistics has more than 80 locations across 12 countries—to maintain a degree of local independence while establishing central oversight.

"There are occasions when it is necessary to take a flexible approach to global standards," Werner admits. Other aspects are non-negotiable. Schnellecke Logistics is implementing a zero trust network access (ZTNA) approach.

"By focusing on identity and access management rather than perimeter security, zero trust networks can simplify the overall network architecture. This makes it easier to manage and secure the network," Werner says.

> "There can be no disruption. Our network cannot drop, even for 30 minutes. There are stiff penalties for any outage."
>
> – **Markus Werner**, Head of Group Competence Center-IT Infrastructure, Schnellecke Logistics

Schnellecke Logistics is streamlining network operations, using templates and automation to reduce the burden on the IT team. Continuous automated monitoring of user and device activity provides comprehensive visibility into network traffic. This helps in detecting and responding to suspicious activities more effectively. In addition, ZTNA enables the enforcement of least privilege access to only the apps, services, and resources relevant to each user, and no more.

"The more you automate and digitize, the greater the exposure to potential risks," says Karsten Keil, Vice President Group IT & Digitization at Schnellecke Logistics. "Adopting a zero trust approach is fundamental to ensuring our business resilience."

Zero trust minimizes any disruption to the network and keeps Schnellecke Logistics compliant with the latest industry regulations. Crucially, it meets the requirements of Trusted Information Security Assessment Exchange (TISAX), a global information security standard for the automotive industry. By adhering to TISAX standards, Schnellecke Logistics can demonstrate its commitment to information security and establish trust with new partners.

"Not taking a top-down approach initially has helped local adoption. The local teams feel part of this change," explains Werner. "But there are some elements that must be strictly enforced. Zero trust network access is one."

Validating access to specific applications or resources

Schnellecke Logistics' ZTNA is built on HPE Aruba Networking SSE. This platform enables Schnellecke Logistics to connect users, devices, and servers, to the business resources needed for work. ZTNA is one of the key features within SSE.

ZTNA verifies the identity of users and devices and enforces least privilege access based on predefined policies. This ensures that access is granted only to specific applications or resources, rather than the entire network, limiting any exposure. The network is divided into smaller, isolated segments, minimizing the potential impact of a breach.

The adoption of SSE marks the latest chapter in Schnellecke Logistics' engagement with HPE Aruba Networking. Schnellecke Logistics' SD-WAN environment is based on the HPE Aruba Networking EdgeConnect SD-Branch platform, underpinned by the HPE Aruba Networking CX series of data center and campus switches and HPE Aruba Networking Wi-Fi 6/6E series wireless access points—all managed through HPE Aruba Networking Central. Network access control and authentication are all defined and automated through the HPE Aruba Networking ClearPass Policy Manager platform. By combining the HPE Aruba Networking EdgeConnect SD-Branch and SSE, Schnellecke Logistics is now enjoying the benefits of a unified SASE approach, avoiding vulnerabilities through legacy VPN connections and reliance on perimeter firewalls.

"By focusing on identity and access management rather than perimeter security, zero trust networks can simplify the overall network architecture. This makes it easier to manage and secure the network."

– **Markus Werner**, Head of Group Competence Center-IT Infrastructure, Schnellecke Logistics

"We have an excellent partnership with HPE Aruba Networking," says Werner. "They're the ones who opened our eyes to SSE, and helped develop the ZTNA proof of concept."

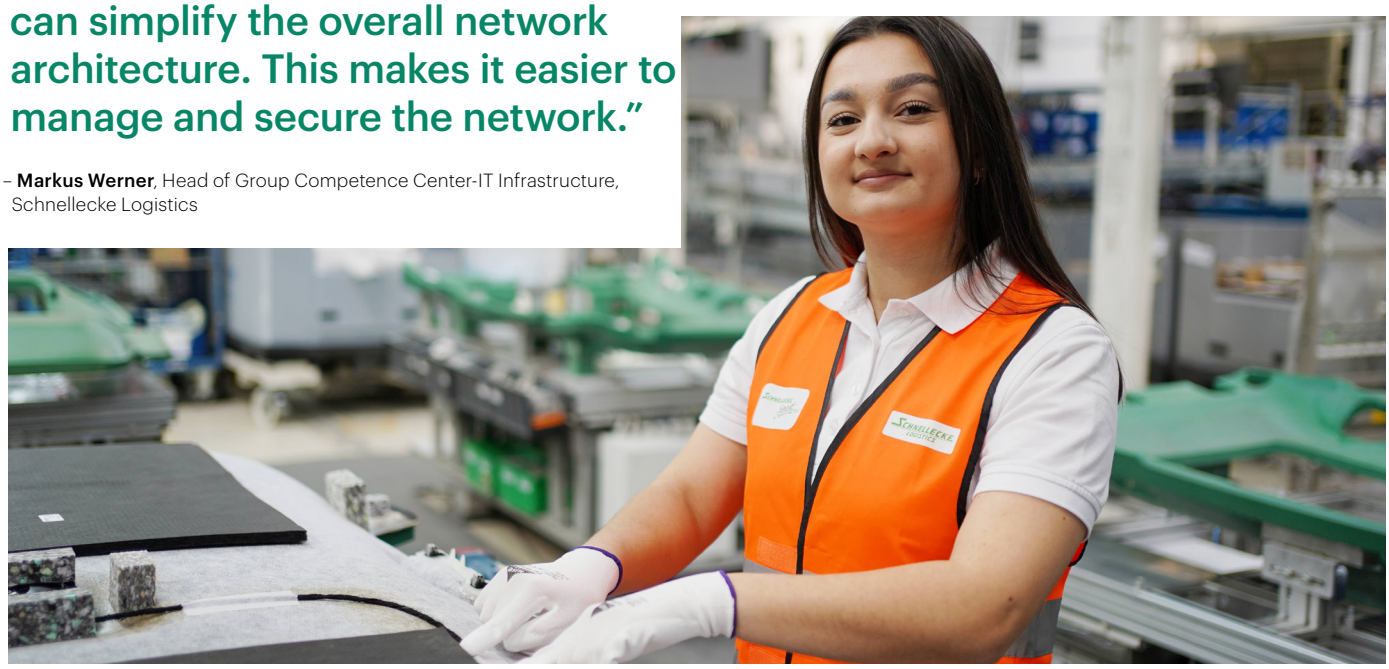
In line with Schnellecke Logistics' move toward cloud services, HPE Aruba Networking SSE enables seamless cloud security management. Schnellecke Logistics can now orchestrate user access to apps and resources from one place, with a clear policy-tagging system for simplicity. This approach has allowed the IT team to offload tasks from the perimeter firewall and mitigate the impact of threats such as DDoS attacks.

The first phase includes 1500 users, such as external consultants, on HPE Aruba Networking SSE. There are 5000 Schnellecke Logistics employees with a corporate email address, and many more employees and IoT devices connected to the network. The plan is for everyone and everything to be managed by HPE Aruba Networking SSE by 2030.

The SSE platform will maintain a dynamic response to the changing threat landscape. ZTNA continuously monitors and verifies user and device behavior. This ongoing validation ensures that access remains secure and that any suspicious activity can be quickly addressed.

For Schnellecke Logistics, this real-time updating allows the business to accelerate its digital transformation in a secure fashion. It can move forward with adding new IoT sensors or bringing new partners onto the network. It has the assurance that new users and devices are contained. For home or remote workers, secure access to corporate resources is available from any location.

"We're not utilizing all of the HPE Aruba Networking SSE capabilities today but are confident that it provides us with a robust and future-proof feature set that empowers our vision for a secure modern network," says Werner.



> **"The more you automate and digitize, the greater the exposure to potential risks. Adopting a zero trust approach is fundamental to ensuring our business resilience."**
>
> – **Karsten Keil**, Vice President Group IT & Digitization, Schnellecke Logistics

Explore more

Learn more about HPE Networking

Learn more about HPE Aruba Networking security service edge (SSE)

Find more HPE case studies

Visit HPE.com

Chat now

a50012934ENW

HEWLETT PACKARD ENTERPRISE

hpe.com

Solution

Hardware

- HPE Aruba Networking EdgeConnect SD-Branch Gateways (SD-WAN)
- HPE Aruba Networking CX series core and access switches
- HPE Aruba Networking Wi-Fi 6/6E series wireless access points

Software

- HPE Aruba Networking SSE
- HPE Aruba Networking Central
- HPE Aruba Networking ClearPass Policy Manager