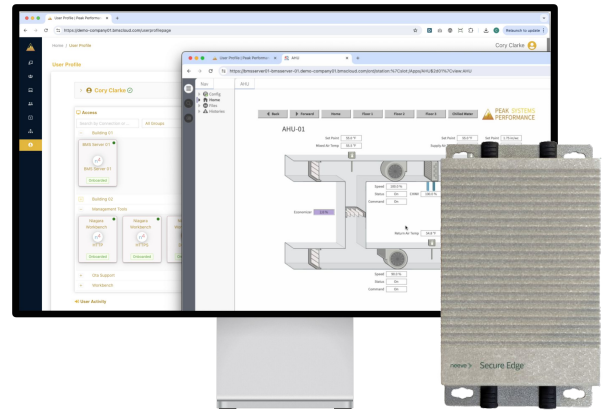# neeve

Neeve Security Products

Neeve's security products - Secure Edge and Secure Link - empower OT teams to safeguard building networks and devices, grant secure remote access, enable cloud connectivity, and deploy edge applications for real-time building optimization. This unified offering reduces costs, strengthens security, and accelerates innovation.

Zero-trust Security for OT

Implementing zero-trust network architecture, with certificate management and encryption, greatly reduces risks to your OT cybersecurity. Gain complete network and device visibility with automated discovery tools and centralized management.

- Hardened OS, trusted platform module hardware, and BIOS trusted boot verification
- Multi-factor authentication with SSO support
- X509v3 certificate-based authentication Automated device discovery service
- Advanced tunnel firewall with granular, 7-tuple rules
- Open APIs for integration into SIEM platforms

Secure Remote Access

Neeve Secure Edge delivers secure, agentless, auditable, time-bound remote access that centralizes all user management across staff and vendors to ensure enforcement of policies and improve operational hygiene. Simplify remote access from any OT device with no software download or installation required.

- Web-based cloud portal for all devices and networks
- No end-user application download or end device agent required
- Role and schedule-based access control
- Centralized user management, policy control, and event logs and reports

Innovative Edge Compute

Optimize building performance, reduce hardware footprint, and decrease management of applications with our edge cloud. Neeve Secure Edge supports cloud-based container management and orchestration, including clustering, for high-performance edge computing.

- Secure run-time environment on Edge Node
- Cloud-based container orchestration
- Turn-key marketplace with leading application providers like Niagara, Switch Automation, Iceberg, Auvik, Mapped, Nantum and open-source tools.

Fully Managed Service

Neeve's software-defined platform is a fully managed service, ensuring your infrastructure is always up to date and delivers a superior user experience while boosting operational efficiency.

- All-in-one product subscription including managed and support services. Fully automated releases and patch updates
- 24/7 monitoring and assistance from highly responsive technical support
- Fully and centrally managed to reduce support staff

Neeve Security Platform Architecture
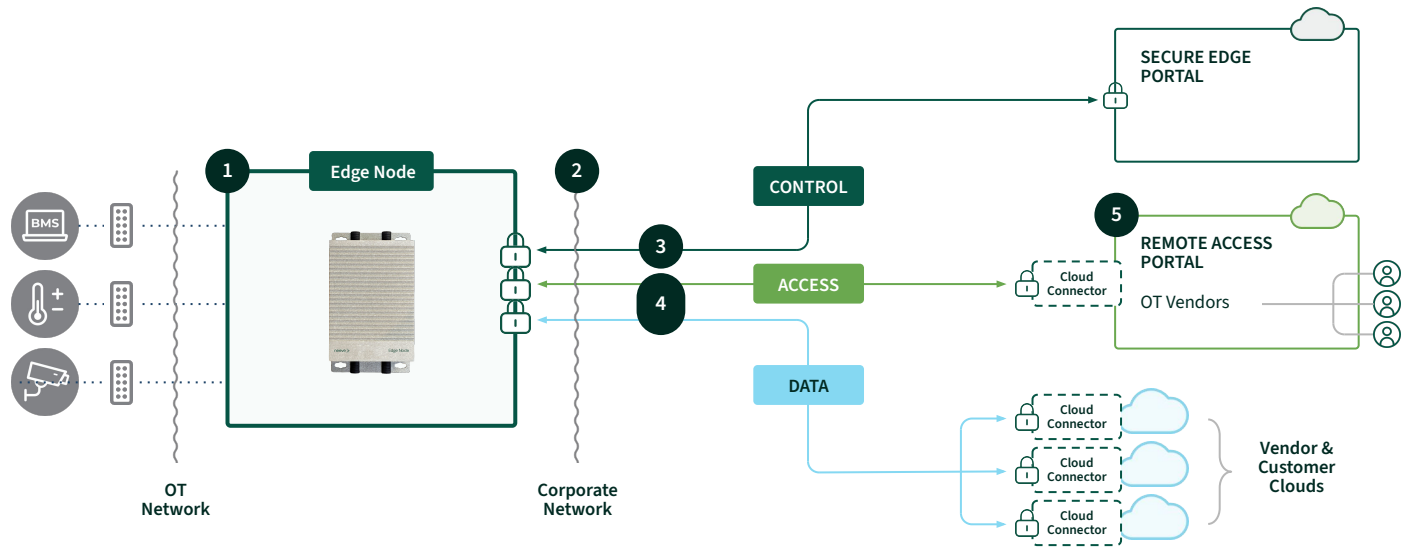
The platform creates a complete architecture for end to end cybersecurity for OT, zero-trust remote access for OT vendors, and a secure edge OT application environment. The on-site appliance and OS are hardened, the cloud connections are book-ended, authenticated and encrypted, and best cyber practices are built into every element.

1 HARDENED OS

- Secure network operating system, custom-hardened Linux OS
- Hardware Trusted Platform Module (TPM) UEFI/Secure Boot.
- Full disk encryption (AES-256) for secure data storage (both system binaries and customer data)
- Built-in firewall with default DENY rule on both directions – Zero-Trust
- Policy-based destinations and ports whitelisted for OT network connectivity

2 SIMPLE AND SECURE INTERFACE TO NETWORK

- Requires use of **port 443 outbound**
- No inbound open port

3 CONNECTION POLICY AND CONTROL

- Connection is established based on **x509v3 certificates with two-way authentication**. Session uses AES-256 encryption
- Configuration, network policy updates, bi-directional channel to manage node element

4 DATA TUNNEL

- Connection based on **x509v3 certificates with two-way authentication**
- All Data Traffic from sensor network to cloud (Data lake, SaaS applications, etc)

5 REMOTE ACCESS PORTAL

- Role-based security access controls
- 2FA can be enabled for enhanced user access security
- Audit log of policy changes and any other actions taken by a user

neeve

Neeve Security Suite of Products

Our family of security products is developed to cover a wide range of needs, from securing a single device in the field to providing highly resilient digital infrastructure at critical sites.

SECURE LINK

A simple industrial grade solution for security and remote access. Core use cases are:

- Cybersecurity for OT systems and devices
- Secure remote access to building systems for commissioning and maintenance

SECURE EDGE

A robust solution for security, remote access, edge applications and high-availability. Core uses cases are:

All the use cases of Secure Link plus

- Secure extraction of building system to cloud for AI and insights
- Offloading building systems to the cloud
- Converging OT networks in the cloud

	SECURE LINK		SECURE EDGE		
	LINK 5	**LINK 15**	**BASIC**	**PROFESSIONAL**	**ENTERPRISE**
Cybersecurity & Network					
Security Policies & ZTNA	✓	✓	✓	✓	✓
LANs Supported	1	2	2	Unlimited	Unlimited
Secure Tunnels (SDWAN)	1	1	5	Unlimited	Unlimited
Threat Intelligence	✗	✗	✓	✓	✓
Remote Access					
Cloud Management	✓	✓	✓	✓	✓
Supported Endpoints*	5	15	Unlimited	Unlimited	Unlimited
Simultaneous Users	1	3	Unlimited	Unlimited	Unlimited
Edge Compute					
App Marketplace	✗	✗	✓	✓	✓
Edge Applications	✗	✗	Up to 2	Unlimited	Unlimited
Hardware Configuration					
LAN Ports	2 x RJ45	2 x RJ45	2 x RJ45	4 x RJ45	4 x RJ45
Serial Ports	✗	✗	✗	4 x RS 232/485	4 x RS 232/485
High Availability	✗	✗	✗	✗	2 or 3 device config

* An Endpoint is a unique combination of device (IP address) and port for remote access (e.g. remote access to the BMS web UI on port 80 is 1 endpoint)