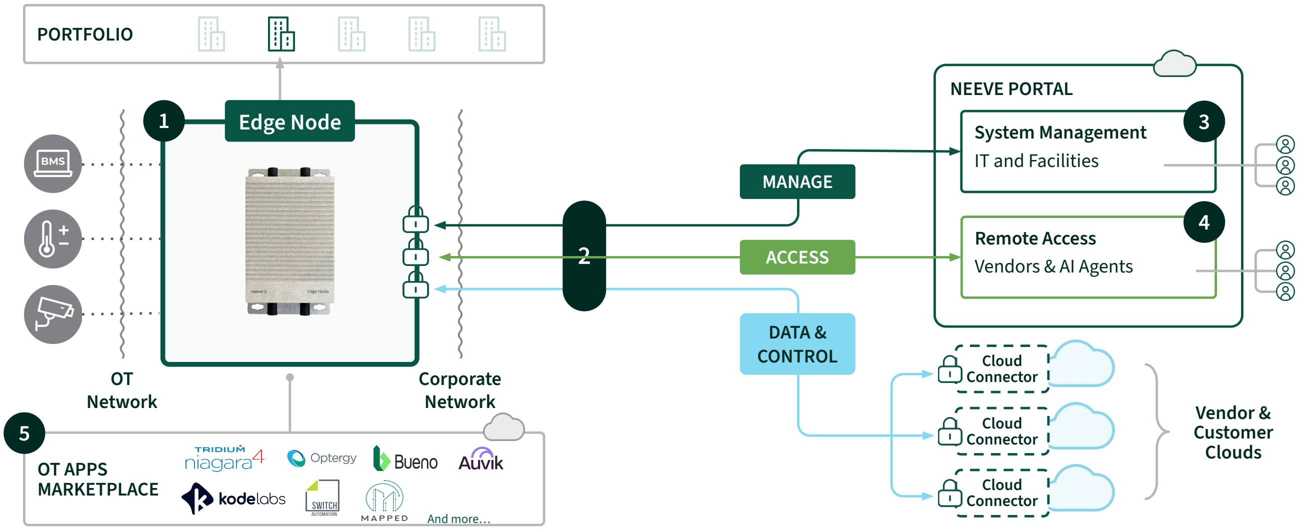
Neeve Secure Edge℠ – Security

Neeve Secure Edge 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 AES-256 encryption

2 SECURE CONNECTIVITY

- Connections using x509v3 certificates with two-way authentication.
- Sessions use AES-256 encryption
- Secures all data traffic from building network to cloud
- Only requires use of port
- 443 outbound

3 SYSTEM MANAGEMENT

- Bi-directional channel to manage configuration and network policy updates
- Simple hierarchy based user access and device management

4 REMOTE ACCESS

- Browser-based access for high-adoption
- Role-based access controls
- Support for SSO and MFA
- Comprehensive audit and access logs

5 EDGE APPLICATION ENVIRONMENT

- Docker run-time environment
- Cloud deployed and fully managed
- Secure connectivity to cloud with support for AWS, GCP, Azure and OpenStack

Cyber Security Architecture

Cybersecurity is built into the hardware and cloud-based software infrastructure as well into all the connections. The Edge Node architecture and cloud architecture work together, each following the highest standards of cybersecurity to provide end to end protection.

Infrastructure

EDGE NODE HARDWARE

- UEFI/Secure Boot/Measured Boot based on Hardware TPM2.0
- Full Disk Encryption: OS Image and data at rest using AES-XTS-PLAIN64, SHA256 with 512-bit key size
- Encryption key stored in TPM, unlocked on boot measurement
- Boot stages measured – BIOS, Boot command line, kernel image
- Signed kernel image for verified boot
- Boot failure on:
  - BIOS changes
  - TPM compromise (reset)
  - UEFI PK/KEK/db changes
  - Boot command line changes
  - Kernel image signature validation failure
- TPM PCR Measurements recorded on hardware factory install – Root Of Trust

CLOUD PORTAL INFRASTRUCTURE

- Hosted on AWS, Kubernetes
- Data at rest encrypted using AWS best practices
- Bastion Hosts
- No shared keys
- Access Firewalls – IP whitelists
- 2FA Authentication, Key rotation

Connectivity

EDGE TO CLOUD PORTAL

- Mutual-TLS, 2-way authentication for both client and server
- TLS1.3, AES-256-GCM-SHA384 cipher
- Certificate renewals via PKI, with revocation support

EDGE TO CLOUD CONNECTORS

- Mutual-TLS, 2-way authentication
- TLS 1.3, ECDHE-ECDSA-AES256-GCM-SHA384 cipher

BROWSER TO CLOUD PORTAL

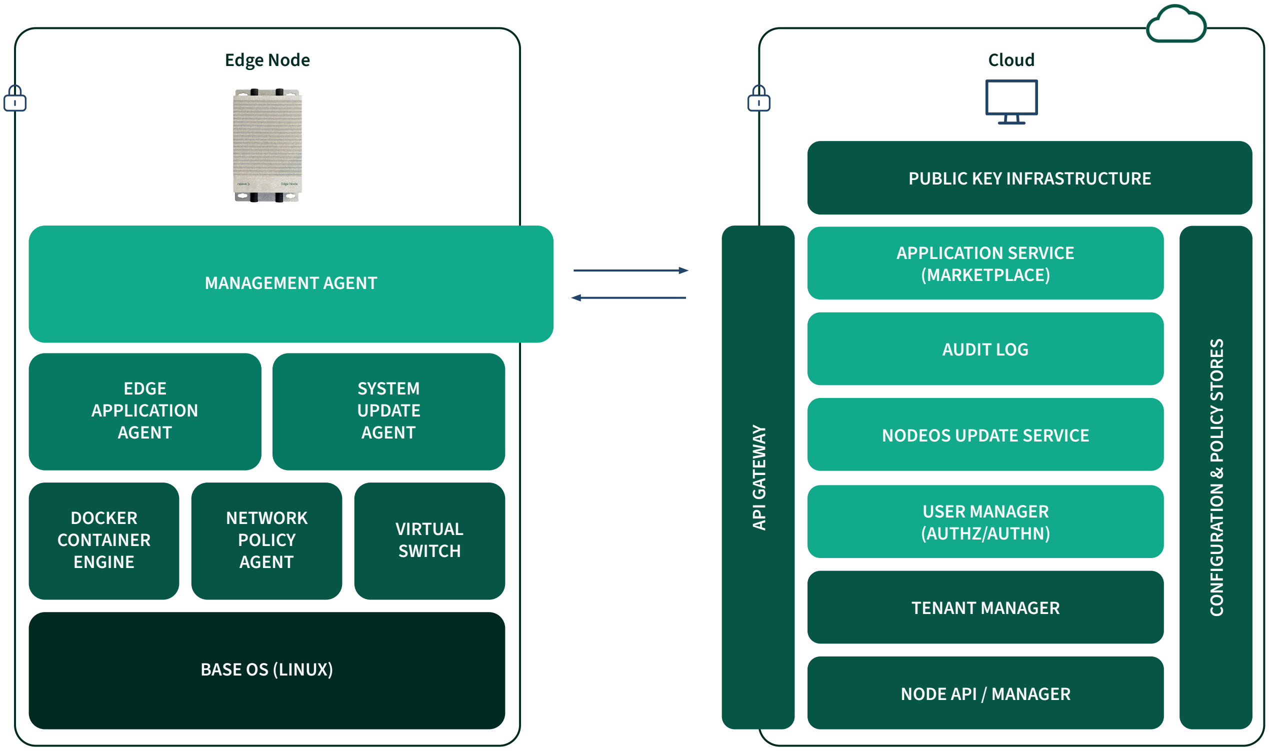
- MTLS 1.3/1.2 (favoring TLS 1.3),
- ECDHE-ECDSA-AES256-GCM-SHA384 cipher

Edge Node Architecture

1. **HARDENED, MINIMALIST LINUX OS**
2. **TWO PARTITION, FAILURE RESILIENT IMAGE BOOT PROCESS**
    - Fallback to last-known good boot image
3. **UEFI + TPM BACKED BOOTUP**
    - Disk decrypted only on successful boot state measurements
4. **SOFTWARE ETHERNET SWITCH FOR FINE-GRAINED NETWORK POLICY ENFORCEMENT**
    - Deny/Allow Flow
    - Complex Routing policies
    - Isolation between WAN and OT Networks
    - Isolation between OT Network – OT Network
5. **SYSTEM UPDATE AGENT**
    - Automated, remote managed OS image update
6. **EDGE APPLICATION AGENT**
    - Local Orchestration of edge applications – resource allocations/ reservation, volume management, network policy, etc

Cloud Portal Architecture

1. **PUBLIC KEY INFRASTRUCTURE**
    - Issue certificates/keys to hardware and virtual nodes
    - API to manage certificate issue, renewals, expiry and revocation
2. **API GATEWAY**
    - User API (UI Frontend) and Tenant API
    - Node API – bi-directional RPC style, binary. Secured via 2-way TLS authentication using x509 v3 certificates
3. **NODE MANAGER**
    - Edge Node policy manager
    - Validate and Apply policy changes/updates to edge and virtual node
4. **TENANT MANAGER**
    - API provider for Tenants, Node, Users, Network Policy, Application Service
    - Core orchestration entity for Node <> Network <> Policy
5. **POLICY STORIES**
    - Database holding configuration for nodes, networks, tunnels, firewall policies, etc.
    - Storage encrypted at rest



Secure Lifecycle Development Practices

Secure software and hardware development practices across the full development lifecycle protect you from zero-day vulnerabilities as well as ensuring all systems are hardened top to bottom. This is how we earned ISO 27001 and SOC 2 Type 2 for the Secure Edge Platform.

Node OS

EDGE NODE HARDWARE

- Static Code Analysis using **Sonarqube**
- Monitor CVE for potential exploits affecting OS libraries/binaries
- Following SOC2 compliant processes and in review for Type 2 report
- Bi-Annual, third-party Pentesting – **BishopFox**
    - Deep testing – employ combination of BIOS, UEFI, kernel exploits
    - Scan for open ports, attack vectors
    - Man-In-the-Middle attacks

Cloud Platform

EDGE TO CLOUD PORTAL

- Static Code Analysis using **Sonarqube**
- Continuously monitor CVE for potential exploits affecting OS libraries/binaries
- Following SOC2 compliant processes and in review for Type 2 report (expected EOY)
- Bi-Annual, third-party Pentesting – **BishopFox**
    - Deep testing – employ combination of BIOS, UEFI, kernel exploits
    - Scan for open ports, attack vectors
    - Man-In-the-Middle attacks
    - API Docs
- Continuously monitor CVE for potential exploits affecting OS libraries/binaries
- Following SOC2 compliant processes and in review for Type 2 report

Realize the promise of smart buildings

About Neeve Secure Edge

Neeve Secure Edge is a component of The Smart Building Cloud, the industry's first complete, modular, vertically integrated, and cloud-native platform to deliver on the promise of smart buildings. The Smart Building Cloud enables you to optimize every aspect of your building to improve occupant health, decrease energy consumption, reduce friction in the workplace, and maximize operational efficiency — all with minimal upfront investment and maximum cybersecurity protection.

LEARN MORE

About Neeve

Neeve transforms buildings into responsive environments that continuously adjust to meet human needs for natural light, connection to nature, fresh air, and comfortable temperatures, while improving energy efficiency and increasing profits for building owners and their tenants.

Today, Neeve is installed and designed into more than 100 million square feet of buildings, including offices, apartments, schools, hospitals, airports, and hotels.

Get in touch

info@neeve.ai
1.408.514.6512