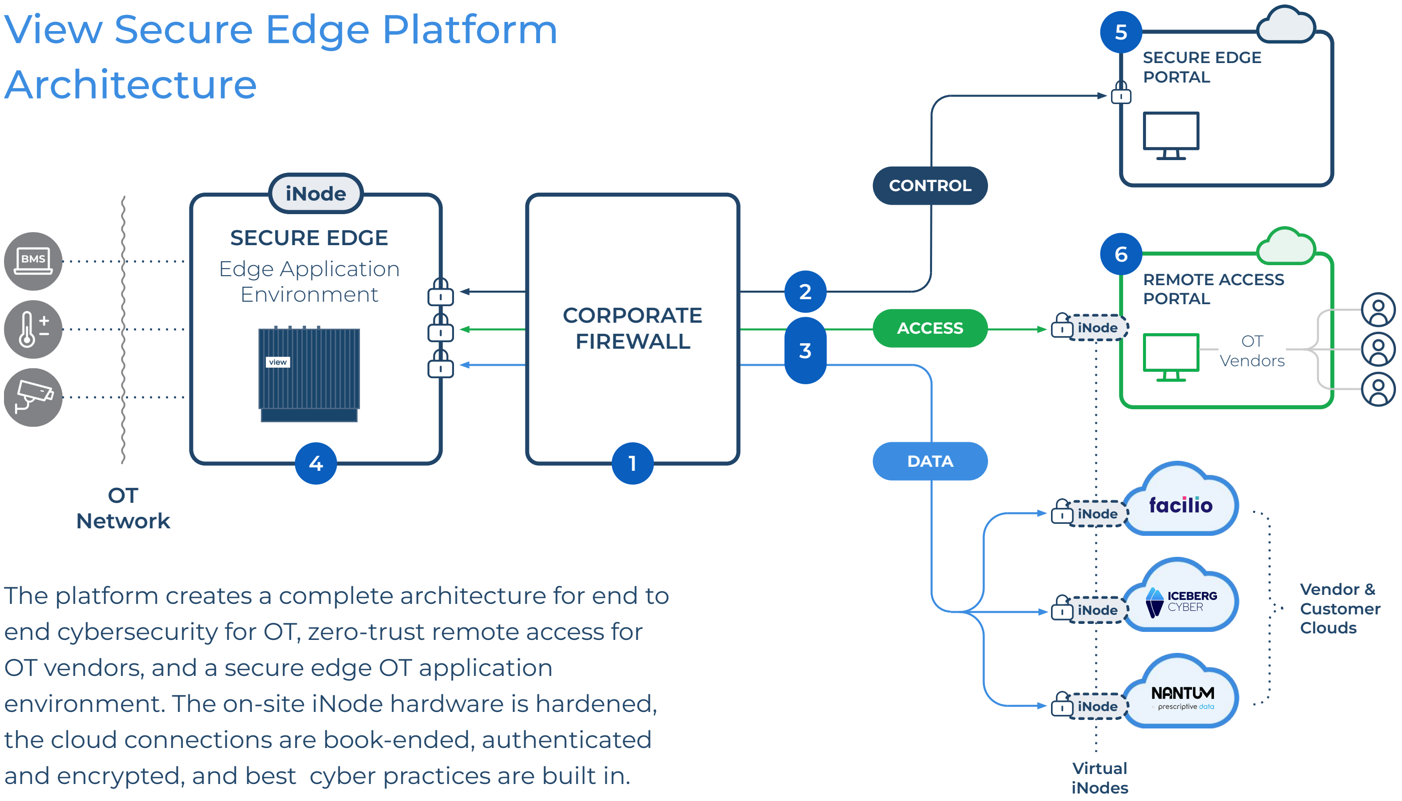
view
SMART BUILDING CLOUD

View Secure Edge – Security

View 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 iNode hardware is hardened, the cloud connections are book-ended, authenticated and encrypted, and best cyber practices are built in.

1 Corporate Firewall

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

2 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

Data VPN Tunnel

3

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

4 Hardened iNode 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

5 Portal Access Control, Authn/Authz and Audit

- **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

Cyber Security Architecture

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

Infrastructure

iNode 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
- No Password Logins!

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/Virtual iNode 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 iNode to Virtual iNode

- Mutual-TLS, 2-way authentication
- TLS 1.2, ECDHE-ECDSA-AES256-GCM-SHA384 cipher

Browser to Cloud Portal

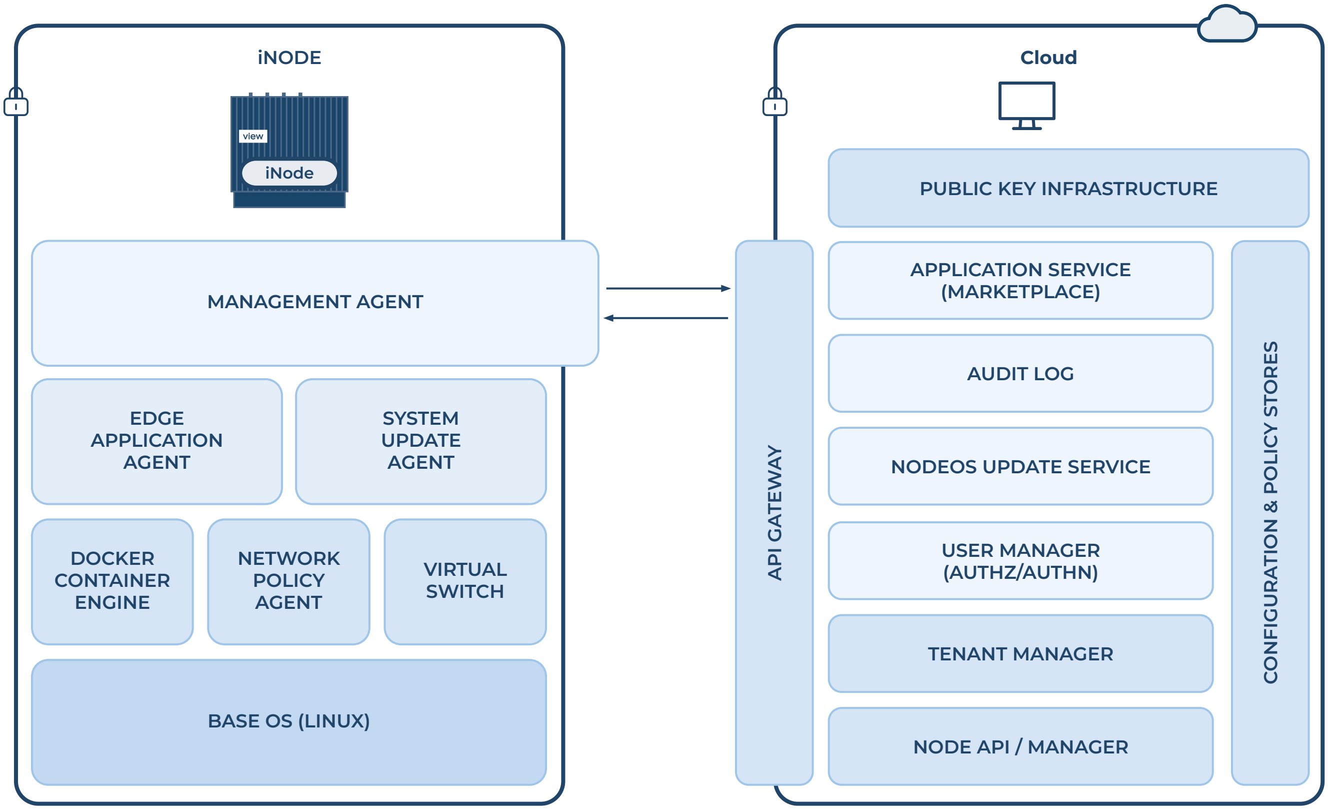
- TLS 1.3/1.2 (favouring TLS 1.3),
- ECDHE-ECDSA-AES256-GCM-SHA384 cipher

iNode 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
   - iNode 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 Stores
   - 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.

Information Security Management ISO 27001 Certified

SOC2 TYPE II

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations

PRESCIENT SECURITY

Node OS

iNode 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

sonarqube

BISHOPFOX

Cloud Platform

- 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
- Continuous Cloud scans via **Orca Security** for vulnerabilities, exposures, policy violations
- AWS Best practices for security

sonarqube

BISHOPFOX

orca security

Realize the promise of smart buildings

About The Smart Building Cloud

View 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 View

View 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, View 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@view.com
1.408.514.6512