view

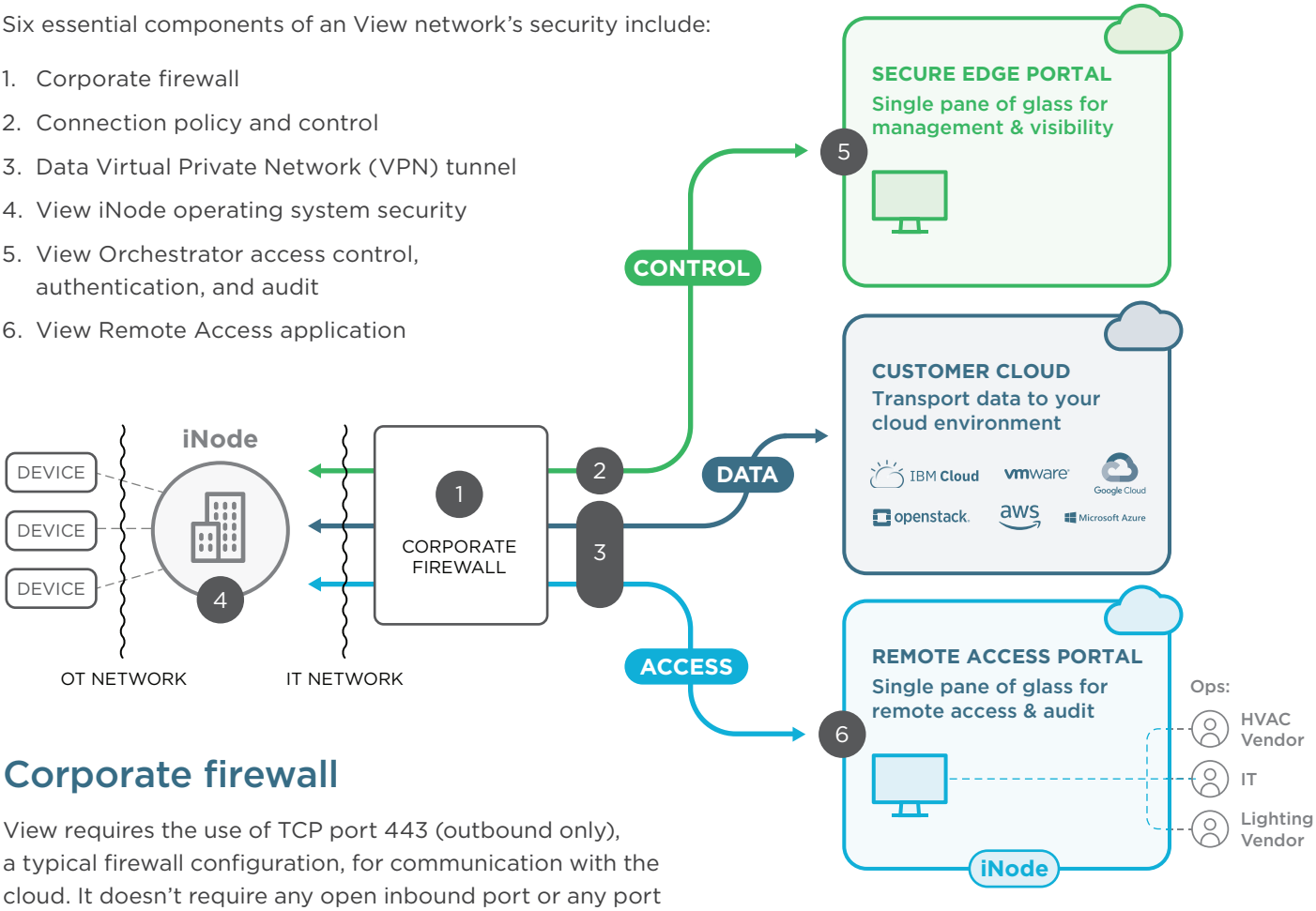
Security overview

Secure Edge & Remote Access

View provides a highly secure IoT network as a service using industry-standard cryptographic technologies. This summary describes how View provides secure deployment and management of assets.

Six essential components of an View network's security include:

1. Corporate firewall
2. Connection policy and control
3. Data Virtual Private Network (VPN) tunnel
4. View iNode operating system security
5. View Orchestrator access control, authentication, and audit
6. View Remote Access application



Corporate firewall

View requires the use of TCP port 443 (outbound only), a typical firewall configuration, for communication with the cloud. It doesn't require any open inbound port or any port mapping. Discovery of network proxy is automatic.

Connection policy and control and data VPN

Policy and control of connections (item 2 in Figure 1) and data security (item 3 in Figure 1) are managed by the iNode operating system establishing a secure connection to View Orchestrator over outbound TCP port 443. This connection is established based on x509v3 certifications with two-way authentication. The session uses AES-256 encryption. (For more detail on AES-256 encryption, see "Encryption Details."

View iNode security

View iNode security is established through a secure network operating system called iNodeOS, which is based on a custom-hardened Linux kernel, and the underlying security provided by hardware, including Trusted Platform Module (TPM), UEFI/Secure Boot, and Full disk encryption. The iNodeOS's built-in firewall uses the default deny rule in both directions, which requires explicit allowance of ports and protocols.

The operational technology (OT) network is a virtual network that overlays the physical IT network. The OT network has no connectivity with the physical IT network. Only policy-based destinations and ports are whitelisted for OT network connectivity. Traffic from any device behind an iNode can go only to a destination behind another iNode.

The iNode firewall created by the View virtual overlay network enforces network policies through different ingress and egress points, including:

- Access to the protected local network from the data VPN tunnel is a through a built-in firewall that enforces policies at the packet level in both directions
- Access to the cloud network is controlled by the built-in firewall in the Virtual iNode
- Traffic from the protected local network is by default allowed to access only the cloud network and vice versa
- If the user chooses, devices on the local side can access other networks (such as the internet) through a Virtual iNode. Choosing to do this also provides an opportunity to enforce another layer of policies on this traffic because it is a single ingress/egress point.
- Each application service running on an Edge iNode is independently protected by its own instance of a virtual firewall. The user can enforce policies to control access to and from the service.

View Orchestrator security

View Orchestrator uses industrial-strength role-based security access controls and best practices. Two- factor authentication can be enabled for enhanced user access security. View Orchestrator collects a complete audit log of policy changes and any other actions a user takes, with non-repudiation.

View Remote Access security

View Remote Access uses industrial-strength role-based security access controls and best practices. Remote Access supports OIDC 2.0 SSO to integrate with your corporate identity policies. Two-factor authentication can also be enabled to secure local accounts. Remote Access collects audit logs of user access and any other actions taken with non-repudiation.

Encryption details

The sections that follow describe the ciphers in use with the AES-256 encryption algorithm for browser access to View Orchestrator, Edge iNode access to View Orchestrator, and Edge iNode to Virtual iNode. We support Transport Layer Security (TLS) 1.2 and 1.3.

BROWSER ACCESS TO VIEW ORCHESTRATOR AND REMOTE ACCESS

TLS 1.3/1.2 are used. View Orchestrator negotiates one of the two, favoring TLS 1.3, with the browser. For either, this is the preferred cipher: ECDHE-ECDSA-AES256-GCM-SHA384.

- Protocol is TLS 1.3 or 1.2
- Key Exchange Mechanism is ECDHE
- Key Exchange Algorithm is ECDSA
- Symmetric Encryption Algorithm is AES
- Size of the Symmetric Encryption Algorithm is 256
- Mode of the Symmetric Encryption Algorithm is GCM
- MAC used by the algorithm isSHA384

EDGE INODE ACCESS TO VIEW ORCHESTRATOR

TLS 1.3 is used. This is the cipher: TLS_AES_256_GCM_SHA384. Following are the cipher details:

- Protocol is TLS 1.3
- Symmetric Encryption Algorithm is AES
- Size of the Symmetric Encryption Algorithm is 256
- Mode of the Symmetric Encryption Algorithm is GCM
- MAC used by the algorithm is SHA384

EDGE INODE CONNECTION TO VIRTUAL INODE

For Edge iNode access to Virtual iNode, TLS1.2 is used. This is the cipher: ECDHE-ECDSA-AES256-GCM-SHA384. Following are the cipher details:

- Protocol is TLS 1.2
- Key Exchange Mechanism is ECDHE
- Key Exchange Algorithm is ECDSA
- Symmetric Encryption Algorithm is AES
- Size of the Symmetric Encryption Algorithm is 256
- Mode of the Symmetric Encryption Algorithm is GCM
- MAC used by the algorithm is SHA384

View cloud environment security

We host View cloud services on Amazon Web Services (AWS). We secure the cloud environment with industry- leading security practices, including (and not limited to) access controls such as:

- Bastion hosts
- No shared keys
- Access firewalls
- Two-factor authentication
- Data access controls like need to know, identified roles and access
- Periodic automated and manual penetration testing

Our penetration partner is Bishop Fox. Documents on penetration testing are available upon request.

View development process

View follows SDLC CI/CD, SCM and deployment workflow for software development, testing and release, software change management and deployment. The process includes sign-offs from leads of respective processes.

X509 certificates

Modulus and other technical details of your x509 certificates can be found on our production cert in any browser.

The certificate for the View Orchestrator is the following:

- Signature Algorithm is SHA-256 with RSA Encryption
- Public Key Info:
- Algorithm is RSA Encryption
- Key Size is 2048 bits

The certificate for the iNode is the following:

- Signature Algorithm is ECDSA-with-SHA512
- Public Key Info: secp384r1
- Algorithm is Elliptic Curve
- Key Size: 384 bits

Application deployment access

View customers control who is permitted to deploy applications in their View network and what access they permit to those apps.