CyphreEdge

Endpoint Protection for Industrial IoT

ENSURE THE INTEGRITY OF IIoT DEVICES

CyphreEdge is an automated key and certificate lifecycle management platform that protects endpoints in Industrial IoT networks for secure, authenticated communication.

Enterprises are adopting digital transformation and deploying new technology and business models in order to remain ahead of the competition. Combining operational technology (OT) and information technology (IT) at the edge provides great value for businesses, but these interconnected endpoint devices are also targets for cyberattacks. Strong endpoint protection is a critical component to securing Industrial IoT networks.

Digital certificates authenticate and establish trusted, secure connections that encrypt information passing between authorized devices, applications, and users in connected industrial systems. But, the longer a certificate or key resides on an endpoint, the more vulnerable that device becomes to attacks and hijacking. With billions of industrial and Internet of Things (IoT) devices to be managed, manual certificate and key management processes are quickly overwhelmed.

Automated Key and Certificate Lifecycle Management

CyphreEdge eliminates costly truck rolls and labor-intensive manual cycling of keys and certificates through automation with policies and policy hierarchies. With CyphreEdge, enterprises are able to secure Industrial IoT (IIoT) at scale with continuous deployment of keys and certificates, while reducing the in-house spend required to integrate and implement a fully-automated, KMIP-compliant certificate lifecycle management system.
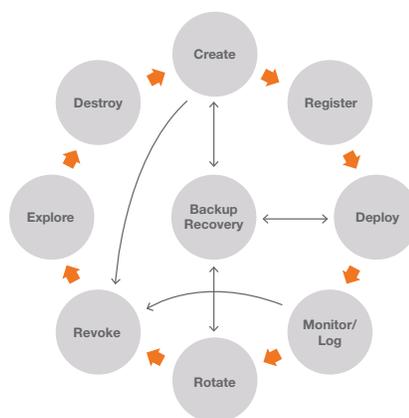

Figure 1. Digital Certificate Management

CyphreEdge's automated lifecycle management solution extends the lifetime of non-upgradable legacy assets by increasing the frequency of key and certificate rotation, and eliminates the risk of stolen keys by avoiding manual update of keys in the field.

From one easy-to-use interface, organizations can centrally manage millions of keys and certificates across any environment using standard supported protocols, such as KMIP or PKCS#11. By grouping devices in a hierarchical method, CyphreEdge applies policy-driven certificate generation and distribution. Since IIoT devices can require multiple certificates (each related to a different function), policies are defined at each hierarchy level
to include the number, length, and details of each certificate generated. Organizations can visualize the key and certificate lifecycle for each endpoint device, enabling streamlined reporting and compliance.

CyphreEdge prevents unauthorized equipment access and potential breaches by automatically expiring old certificates; ensuring a high degree of randomness of the generated encryption material; and providing the key lifecycle visibility and reporting to more quickly identify potential vulnerabilities.

Features

- Automated policy orchestration and visibility for the full lifecycle of keys and certificates
- Centralized management of hundreds of millions of certificates and keys via easy-to-use interface
- True random number generator creates strong cryptographic protection
- KMIP-compliant system that is interoperable with existing authentication systems
- Flexible deployment (on-premise, cloud-based, virtualized,or hybrid)
- Simplified compliance with with government and industrial regulations (NERC/CIP, IEC 62443)

Benefits

- Reduce downtime due to unplanned events by implementing deterministic change management of keys and certificates
- Reduce the cost of truck rolls and manual key and certificate maintenance through secure automation
- Eliminate the risk stolen keys by avoiding the manual update of keys in the field
- Increase the number of IIoT and OT devices that can be managed securely through improved visualization and control
- Reduce the cost of compliance with IEC 62443, NIST SP800-57, 800-53 and 800-63
- Reduce the cost of developing and integrating a compliant key lifecycle management system

CyphreEdge

Automated lifecycle management for the certificates and keys that authenticate and protect devices in IIoT networks

Single Pane of Glass

Centrally manage hundreds of millions of certificates and encryption keys across any environment (cloud-based, on-premise, virtualized) via easy-to-use interface

Policies and Policy Hierarchies

Create policies and policy hierarchies to automate the certificate and key lifecycle for every device to comply with regulatory requirements

Full Lifecycle Management

Automated creation, revocation, cycling, and renewal of certificates and keys for every device, including audit trail

Interoperability

Manage certificates and keys at scale across remote locations – independent of the device type, manufacturer, firmware, operating system, or platform.
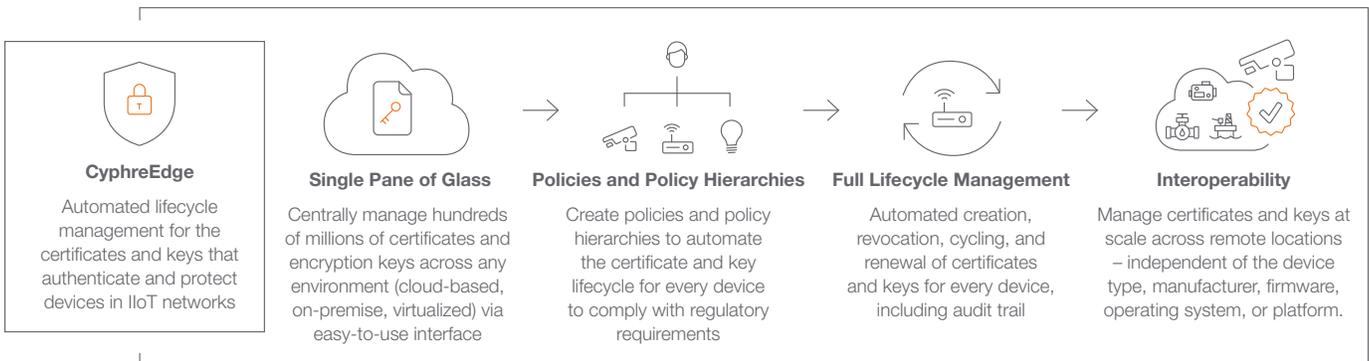
Figure 2. CyphreEdge Endpoint Protection for Industrial IoT

Cyphre, a RigNet company (NASDAQ:RNET), is a cybersecurity company deploying disruptive data protection innovations by enhancing industry standard encryption protocols with our patented BlackTIE® technology.

For more information
visit our website www.**cyphre.com**
or contact us at info@**cyphre.com**

Cyphre

a RigNet company

Enabling Intelligence. Delivering Results.