Solution Brief

# Enable Secure Manufacturing with Fortanix

### Security for distributed manufacturing that can scale with demand.

## Problem

Today, most devices are being manufactured in remote or offshore sites that do not have the same level of security standards as the corporate headquarters. Introduction of IoT into manufacturing has also created serious cybersecurity challenges. Cybercriminals now have an opportunity to hack into sensitive information that is stored on the devices manufactured within unsecured environments and introduce counterfeit units causing financial loss and irrevocable damage to the brand's reputation. Manufacturing organizations are looking to implement advanced security systems that can ensure smarter, secure factory workflows, protect business critical information, and safeguard IP.

## What is required?

To address this problem, organizations have traditionally been relying on HSMs to inject cryptographic keys into devices during manufacturing. But the traditional HSMs have limited availability in the cloud and offer limited built-in capabilities that make it less reliable for distributed manufacturing.

An advanced security solution for secure manufacturing should have the following attributes:

- **High availability**
  Production systems must always be operational, thus requiring high availability and fault tolerance.
- **Scalable architecture**
  A successful production line needs to ramp up from dozens of items during the prototyping phase to hundreds of millions in the production phase. The security solution should be able to scale as the demand surges.
- **Suited for distributed operations**
  Factories are spread out, often having limited network connectivity, different operating conditions, and security standards. The solution must meet these demands while being simple and easy to use for personnel with varied backgrounds.
- **Enables secure business logic**
  Security in manufacturing almost always requires some level of customization to match existing systems and processes. The solution needs to offer in-field customization and should be extensible across different manufacturing sites.
- **Support for distributed approvals**
  Remote processes in manufacturing requires sensitive approvals without physical presence of the approver.

## Fortanix Solution Overview

Fortanix offers a unified data security platform that delivers a scalable cloud-native solution to securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data. Secured with Intel® SGX, Fortanix runs the entire key management inside a FIPS 140-2 certified HSM. No one other than the authorized user has access to the keys. The scale-out distributed design ensures that it can scale to also meet the rising demand for PKI fueled by Internet of Things (IoT).

## Solution Benefits

Fortanix offers the ideal solution for securing manufacturing process across global sites, including those not connected to the Internet.

### Highly reliable and resistant to failure

A Fortanix cluster supports high availability and is resistant to a high number of node failures. The cluster remains available even when a node fails, and the tolerance to such faults increases with a greater number of nodes in the cluster.

### Scalable architecture that scales with surge in demand

Fortanix provides horizontal scalability and can easily respond to a surge in demand. Scale out architecture can handle millions of keys and devices in manufacturing and in the field.

### Centralized control and visibility into distributed operations

Fortanix provides control of and visibility into your key management operations across multiple sites and distributed operations with centralized management, enterprise level access controls and single sign-on support.

### Securely run sensitive business logic inside the Key Management Service (KMS)

Plugins are a powerful system allowing users and/or applications to securely run sensitive business logic inside the Key Management Service (KMS). Plugins may be used for operations like imposing custom access control policies for keys, get distributed approvals from a quorum, use RSA keys to sign certificate with specific attributes and to create wrapped keys signed by root CA based certificates.

## Solution Highlights

- **FIPS 140-2 level 3 certified HSM**
  Fortanix provides a FIPS 140-2 level 3 HSM root of trust that can also manage legacy HSMs spread across remote manufacturing sites.

- **Single pane of glass for management**
  Corporate manufacturing HQ can standardize on a single source of cryptographic services and security teams can get a single pane of glass for management.

- **Quorum based approval policy**
  A group administrator may enable a quorum approval policy on a group. Doing so mandates that all security-sensitive operations like key deletion, encryption and decryption, key export, key wrapping and unwrapping etc. would require approval by a quorum.

- **Encrypt provisioned keys**
  Fortanix keeps the keys to be provisioned in the devices secure by encrypting them when stored in rest, when in transit and even when its being used/processed.

- **Chain of trust based on the root CA**
  Every cluster is issued a certificate which is chained to the certificate of the Fortanix cluster. The Fortanix cluster certificate in turn is issued by the root CA of the manufacturing company.

## Common Use Cases

- Securely transfer keys and authorization from HQ to the factory.
- Extend trust across disconnected entities.
- Secure the life cycle of an IoT device and provide strong identity.
- Streamline the supply chain processes.
- Control manufacturing processes, licenses, and components.

## Case Study 1: Manufacturing of Home IoT devices

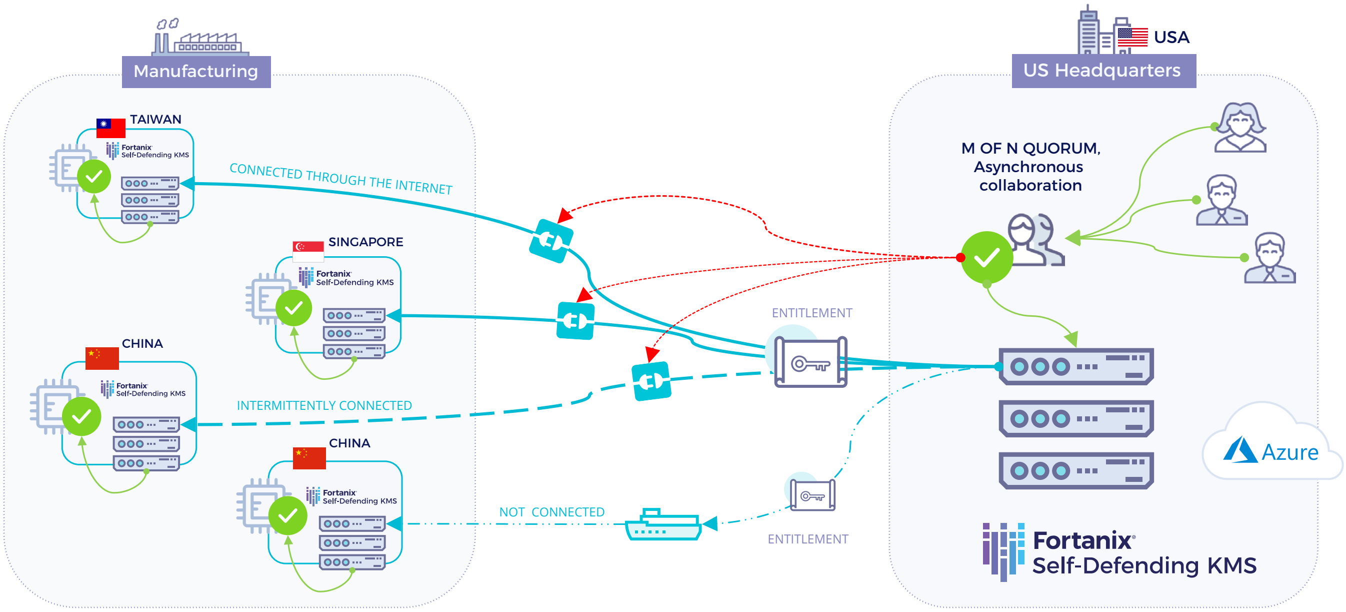
Fortanix is helping a world leader that is producing and marketing smart home products to secure their IoT devices.

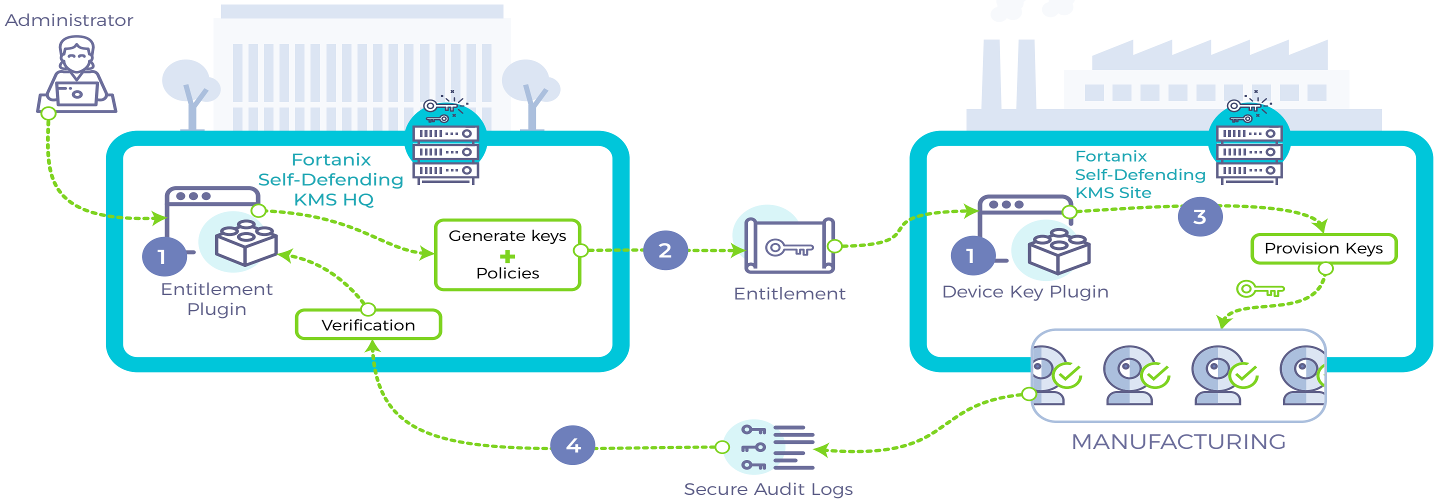
### Challenge

The primary challenge was to secure home IoT devices by embedding a certificate at the point of manufacturing.

### Solution offered

Fortanix offered a unified Hardware Security Module (HSM) and Key Management Service (KMS) to establish trust throughout the entire device life cycle with unmatched scalability. Fortanix custom integrated with manufacturing systems using plugins. The Runtime Encryption Plugin feature in Fortanix Key Management Service (KMS) allows custom code to run in a trusted execution environment. This allowed the device manufacturer to define policies for usage and access control of keys. These can be enforced by the manufacturer across multiple sites.


Manufacturing
TAIWAN
Fortanix Self-Defending KMS
CONNECTED THROUGH THE INTERNET
SINGAPORE
CHINA
INTERMITTENTLY CONNECTED
CHINA
NOT CONNECTED
USA
US Headquarters
M OF N QUORUM, Asynchronous collaboration
ENTITLEMENT
ENTITLEMENT
Azure
Fortanix Self-Defending KMS



## How the solution works?

1. **Distinct KMS clusters for Corporate HQ and manufacturing site with Runtime Encryption Plugins is created:** The manufacturer creates two clusters of Fortanix KMS -One at the corporate HQ and another one at the manufacturing site. Runtime Encryption Plugins inside the KMS are used to process at both ends. “Entitlement Plugin” at the Corporate HQ and the “Device Key Plugin” for the site is created.

2. **‘Entitlement Package’ is created at the Corporate HQ using the ‘Entitlement Plugin’:** A package with the set of keys and associated policy for usage is generated by the Entitlement plugin. Public key of the device key plugin is used to encrypt the package.

3. **Verify the ‘Entitlement Package’ at the site:** Entitlement is transmitted to the KMS cluster at the manufacturing site. ‘Device Key Plugin’ at the site receives the entitlement and verifies whether the entitlement is signed by a trusted plugin using the certificates issued by PKI infrastructure.

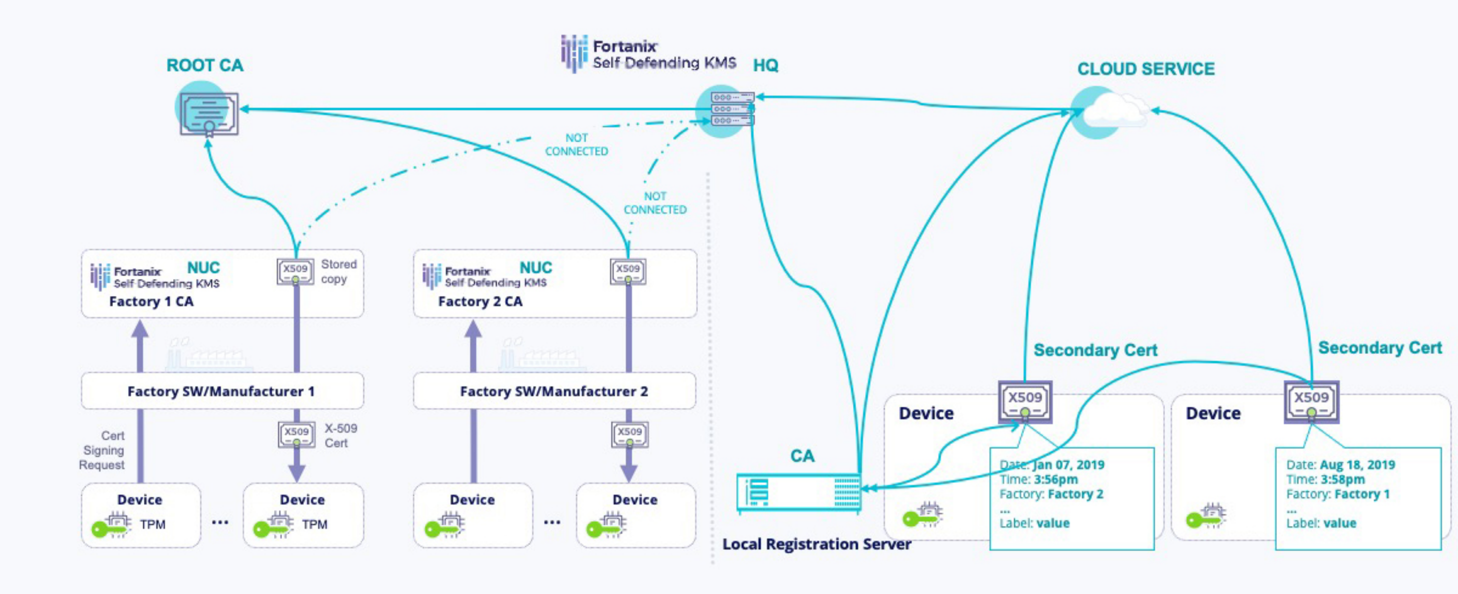
4. **Decrypt and provision the keys:** Private keys are used to decrypt the entitlement and the process of provisioning the keys as per the policy set by the ‘Entitlement Package’ is initiated.

**5. Audit log created and sent back to the HQ:**
The plugin logs its activities. This audit log is then encrypted using the public key of the 'Entitlement Plugin', signed using the private key of the 'Device Key Plugin' and sent back to Fortanix KMS HQ.

**6. Corporate HQ verifies the logs and ensures policy enforcement:**
The Entitlement plugin at the Corporate HQ verifies the logs that it can trust and decrypts the logs. The plugin then analyzes the decrypted logs to verify that the policy of key usage has been enforced at the manufacturing site.

# Case Study 2:
# Manufacturing and secure deployment of Building systems

Fortanix is helping a market leading smart glass manufacturing company to secure its manufacturing process.



## Challenge

The company needed a solution that could help secure its manufacturing process and ensure that the factory certified high-quality devices were installed on the customer site (building). The challenge was two pronged: At the manufacturing site, the need was to generate key pairs, store private keys and certificates. And second, they needed to upload these certificates and transmit them to the customer site to verify and authenticate before deploying the factory certified devices.

## Solution offered

There are two aspects of the complete solution.

- **Manufacturing Site**
Fortanix Key Management Service (KMS) setup in the factory where devices are manufactured to issue certificates including building controller.

- **Customer Site**
Fortanix KMS setup in customer deployment to verify and authenticate the factory certificate.

## How the Solution Works

### Pre-deployment (Manufacturing site)

- Trusted Platform Module (TPM) generates key pair and securely stores private key and factory certificate on device.
- Certificates are signed by the Factory NUC.
- A copy of the certificates are also saved on the NUC and uploaded offline to the Fortanix KMS HQ.

### Post Deployment (Customer site)

- Device in the building connects to the local registration server and gets verified with its factory certificate.
- The local server then issues a secondary certificate to the device used for all future communications.
- The registration server also gets the AES Service Payload Encryption Key from Fortanix KMS and installs it in the device.
- Devices are discoverable and addressable on a MQTT network based on a small set of topics defined by a device's unique identifier. Access is granted to these topics on MQTT using Secondary Certificates.
- MQTT transmission and communication is secured and encrypted using TLS mutual authentication.
- AES key payload encryption is also enabled on the device for communications over MQTT.
- If a factory key is compromised (creates more devices than authorized), Fortanix can revoke certificates for those devices.