Fortanix®

Case Study

Fortanix helps leading IoT solution provider to deliver secure IoT monitoring capabilities

Customer Profile

Located in Eastern Europe, the company specializes in delivering IoT solutions. Specifically, the company offers a range of advanced environmental and positional monitoring sensors that are managed through its secure IoT platform with end-to-end encryption.

Data security challenges with IoT

The company recognized that there is a deep lack of awareness about security issues in IoT applications. Given the rapidly growing number of IoT devices connected to critical infrastructure and cloud services, a holistic approach to security was needed to prevent cybercriminals from finding and exploiting security loopholes in the system and causing irreparable damage to critical infrastructure. The consequences of a hacker gaining access to critical infrastructure could of course be catastrophic: hostile intrusion could potentially result in tracking of sensitive resources, material loss or physical harm, as well as theft of sensitive data.

This prompted the customer to look for a solution that could protect the critical security parameters within their IoT ecosystem and to ensure the secure flow of data from end-to-end. In a nutshell, the challenges they were facing were as follows:

- Preventing unauthorized access to the IoT systems
- Ensuring that the data security framework was scalable with business growth and holistic in nature to enable end to end security across the system

What were they looking for?

Primary capabilities that the Company was looking for in the solution included:

A unified Hardware Security Module (HSM) and Key Management Service (KMS) to establish trust throughout the entire IoT device lifecycle and ecosystem.

A secure and scalable solution that could support the increasing number of IoT devices across multiple customer applications without the need to change the existing infrastructure.

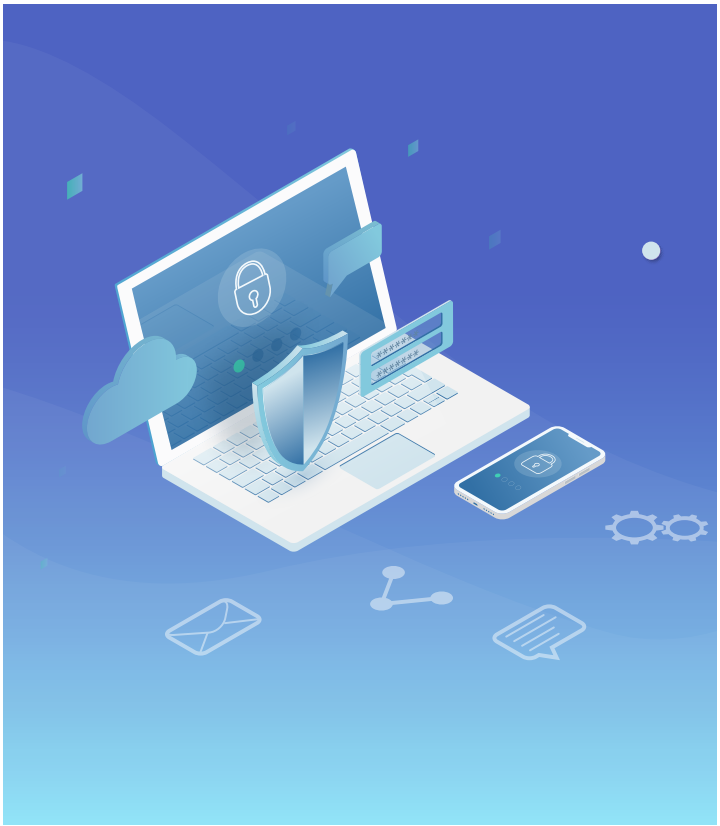
Flexible cryptographic interfaces and technologies enabling easy integration with the Company's Secure Digital IoT Platform.

Why did they choose Fortanix?

The company needed "proven security" and evaluated vendors with FIPS 140-2 approved key management systems. But they also wanted the flexibility to integrate with third party systems which required that the chosen system should support a large variety of security protocols.

Top reasons for choosing Fortanix Data Security Manager were:

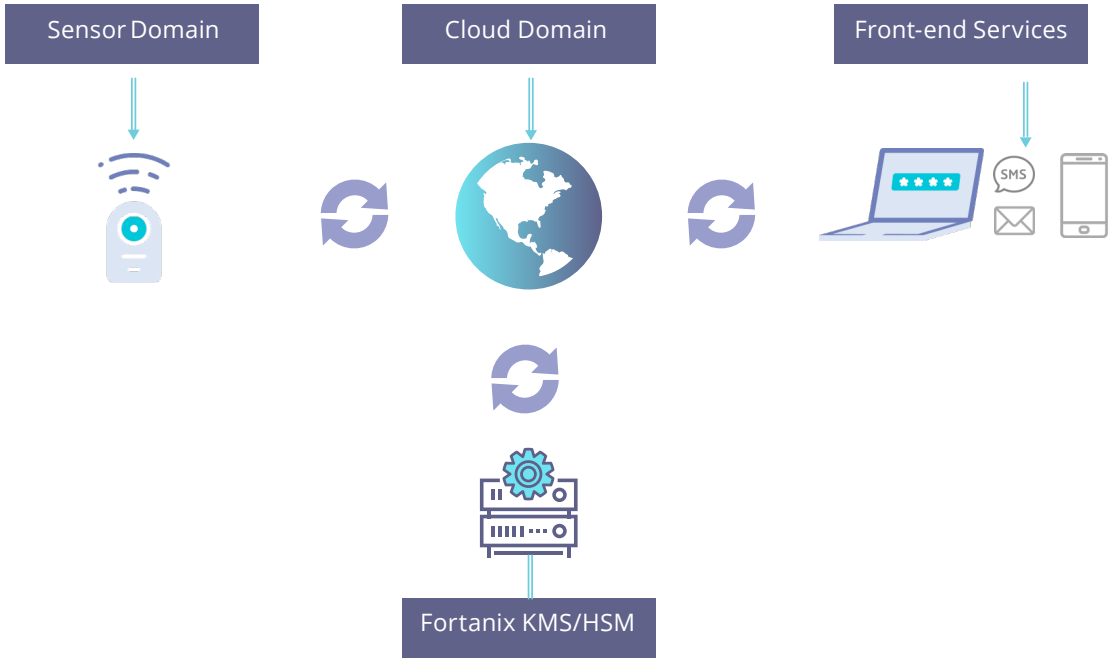
- Proven security with compliance up to FIPS 140-2 level 3
- Future ready with features and roadmap supporting IoT security needs
- Efficient and knowledgeable sales and support teams
- Fortanix solution was based on similar technologies that the rest of the company's IoT Secure Digital Platform was built with, which made it easy to scale as needed
- And finally, ease of deployment, and roadmap that perfectly suited the platform.



What was offered? - Fortanix Solution

The company's secure IoT platform consists of three main components: firstly, proprietary hardened sensor devices, which protect against the possible risk of embedded malware or spyware in sensors that may be sourced from third parties (the generic sensor circuit board can be implemented in a broad range of use cases); secondly, a cloud-based IoT platform for device management, data collection and distribution, which protects against the risk of data intrusion; and thirdly, front-end services that are used for the presentation of data from the users' devices.

Encryption is employed end-to-end to ensure the security of the entire ecosystem.



The company's' secure IoT platform has the flexibility to be used in a broad spectrum of industries and applications and provides a secure end-to-end solution. They have successfully implemented both the on-premises and cloud versions of the Fortanix Data Security Manager (DSM). Each IoT device is pre-loaded with a key generated in Fortanix Data Security Manager (DSM) for authentication and encryption. This secure IoT system is delivered along with an optional dedicated on-prem instance of Fortanix DSM to several high-profile customers across Europe. With Fortanix DSM, the customer is able to deliver:

- **Secure key management throughout the IoT Secure Digital platform, from sensors to end users.**
  Fortanix DSM provides a Key Management System 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,

- **HSM grade security to offer unmatched privacy for the protection of private keys**

  Secured with Intel® SGX, Fortanix runs the entire solution inside a FIPS 140-2 level 3 certified HSM. No one other than the authorized user has access to the keys. The distributed architecture ensures that it can also provide extremely high availability and disaster recovery in mission-critical applications.

- **Centralized control and visibility into distributed operations:** Fortanix provides control of and visibility into key management operations across multiple sites and distributed operations with centralized management, enterprise level access controls and single sign-on support.
- **Process authentication and authorization:** Establish trust during device lifecycle for mutual authentication of devices, processes, and users.
- **Scalable solution that scales with a 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.
- **Advanced key security**
  Fortanix DSM provides 360-degree protection for the keys it manages, encrypting them at rest, in motion, and in use.

SOLUTION HIGHLIGHTS

FULL KEY LIFECYCLE MANAGEMENT

Fortanix delivers full key lifecycle management as a service to ensure secure and consistent key management across on-premises and multicloud environments.

BROAD CRYPTOGRAPHIC OPERATIONS

Support for full NSA Suite B algorithms: RSA, AES, Elliptical Curve2. Perform broad cryptographic operations and key management operations, including key generation, key import, key rotation, key derivation, encryption, decryption, signing, verification, tokenization, and masking

FIPS 140-2 LEVEL 3 CERTIFIED HSM

Fortanix provides a FIPS 140-2 level 3 HSM root of trust.

HIGHLY RELIABLE AND RESISTANT TO FAILURE

A Fortanix DSM cluster supports high availability and DR and is increasingly resilient to node failures as the cluster is scaled.

REST API-DRIVEN

Fortanix Data Security Manager supports RESTful APIs to help easily integrate with cloud and DevOps environments.

SUPPORT FOR A BROAD RANGE OF CRYPTOGRAPHIC INTERFACES

Supports PKCS#11, KMIP, JCE, Microsoft CAPI, and Microsoft CNG.

AUTOMATED KEY OPERATIONS

State of art automation features like automatic key rotation, one click rotation across regions and clouds, automatic key expiration based key rotations, automatic alerting based on key state changes. These automation features simplify and secure key management and operations.

CENTRALIZED CONTROL

Centralized intuitive web-based user interface for management. Role-based access control (RBAC) for users, applications, and groups with segregation of duties. Comprehensive tamper-proof audit logs to track all activity, including administration, authentication, access, and key operations.

The Impact

With increasing incidents of cyberattacks on IoT devices and ecosystem, the company was in dire need to integrate security in a seamless manner into their solutions. Fortanix provided the ability to integrate to any third party systems and interfaces thereby ensuring that the IoT solution offered by the company was able to seamlessly incorporate security into customers' ecosystem.

Helped integrate security into IoT manufacturing and delivery.

Helped in enhancing end-user trust and confidence in the solution offered by the company.

Fortanix®

About Fortanix

Fortanix® is a data-first multicloud security company solving the challenges of cloud security and privacy. Data is the most precious digital asset of businesses, but this data is spread across clouds, SaaS, applications, storage systems, and data centers. Security teams struggle to track, much less secure it. Fortanix empowers customers to secure all this data with a centralized solution. Its pioneering Confidential Computing technology means data remains protected at-rest, in-motion, and in-use, keeping it secure from even the most sophisticated attacks. For more information, see **www.fortanix.com**

REQUEST A DEMO