appviewx

IoT Device Security

Protect IoT Devices in Everchanging and Untrusted Environments

Weave security into your IoT fabric with digital identity management from AppViewX

www.appviewx.com

Accelerated IoT Adoption Creates Unique Security Challenges

In today's data driven world, the value of interconnected devices can greatly improve operations and business performance. As a result, IoT adoption is rapidly increasing which is leading to new security challenges and concerns.

Lack of Visibility

IoT devices are largely distributed across the edge, outside the purview of the security perimeter, making it difficult to monitor and manage them.

Data Breaches

Device communications often happen over unsecured channels using weak authentication and encryption standards, risking data exposure.

Firmware or Software Corruption

The firmware or software powering IoT devices can be tampered with during provisioning and upgrades, causing security breaches.

Non-Compliance

Different IoT devices running different and even outdated software versions leads to security non-compliance issues.

Reimagine IoT Security with Digital Identity Management from AppViewX

An effective IoT security strategy starts with device trust enabled by public key infrastructure and digital certificates. When every “thing” has a trusted identity, IoT devices can securely authenticate and transmit encrypted data. With AppViewX, organizations can gain visibility and control of digital certificates for IoT devices across complex hybrid multi-cloud infrastructures by automating certificate discovery, inventory, provisioning, and lifecycle management.

Reliable PKI-base Device Authentication

Provision trusted identities to IoT devices right off the assembly line or in the field to monitor and tamper-proof them throughout their lifecycle.

Secure Device Communication

Implement end-to-end encryption with TLS certificates and renew symmetric and asymmetric keys to minimize the risk of data exposure and theft.

Software and Application Level Security

Follow code signing and firmware signing practices to prevent hackers from tampering with IoT device software and firmware.

Conditional Access and Compliance

Enforce a uniform PKI policy and conditional access to ensure all devices are running the latest, most secure software versions for device trust, data security and industry-standard compliance.

Protect Your IoT Devices Throughout Their Lifecycle with End-to-End Device Identity Management from AppViewX

Automated Enrollment and Provisioning of Digital Identities

- Provision X.509 certificates from any Certificate Authority easily and quickly using any auto-enrollment protocol that the IoT device supports (EST, SCEP, NDES, CEP/CES, CMP, ACME).
- Leverage one-touch provisioning and automated push-to-device workflows to minimize manual effort and human errors.

Network-wide Visibility, Analytics, Monitoring and Reporting

- Auto-scan environments, discover and maintain inventory to gain holistic visibility of certificates and prevent outages and security vulnerabilities.
- Get insights into crypto standards such as cipher strength, hashing algorithms, and key sizes to improve the security posture.
- Set up built-in alerts to monitor and renew certificates before expiry. Generate reports and logs for compliance validation.

Highly Scalable Cloud-based PKI Engine with Next-Gen Automation

- Get instant access to a turn-key cloud-based PKI that enables you to scale from zero to millions of certificates on demand without investing in costly PKI hardware and software.
- Fully automate the entire certificate lifecycle from discovery, installation and renewal to reduce manual effort, improve productivity, and cut costs.

Key Storage and Security

- Store private keys securely in FIPS 140-2 Level 3 HSM or in an AES-256-bit Encrypted Database to prevent key compromises.

Code Signing and Firmware Signing

- Integrate code signing with the manufacturing assembly line or CI/CD pipeline for secure boot.
- Implement code signing to ensure over-the-air upgrades and patching are valid, safe and compliant.

Out-of-the-Box Vendor Integrations

- Certificate Management via MDM Integration - Enforce closed-loop identity management for IoT devices using direct API integration with mobile device managers (MDMs) such as SOTI and MaaS360.
- Certificate Management via AppViewX Agent - In case of an IoT device not supporting standard protocols, provision certificates with your choice of protocol or adapter using the AppViewX agent.

Robust Policy and Compliance Engine

- Define systemic live policies and enforce conditional access to key enterprise resources for enterprise-level OT compliance.

Software Development Kit (SDK) Support

- Enable developers to create and implement custom functionality for IoT devices—from encryption, orchestration, and security to code signing—with immersive SDK support.

Get Started

Simplify IoT device management and security with automated certificate lifecycle management from AppViewX. To learn more and request a demo, visit www.appviewx.com

AppViewX Inc.,

City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+44 (0) 203-514-2226