Compliance in IoT, an Ongoing Mission

Ensuring compliance is a constant challenge for organizations deploying IoT solutions as it requires the ongoing monitoring of two main categories:

Cyber Security Compliance

IoT devices are often deployed with default passwords and vulnerable firmware versions, allowing easy access to hackers.

The manual handling of these vulnerabilities contributes to the extension of organizations' cyber-attack surface.

Potential threats

· Physical security breach
· Data breach and theft
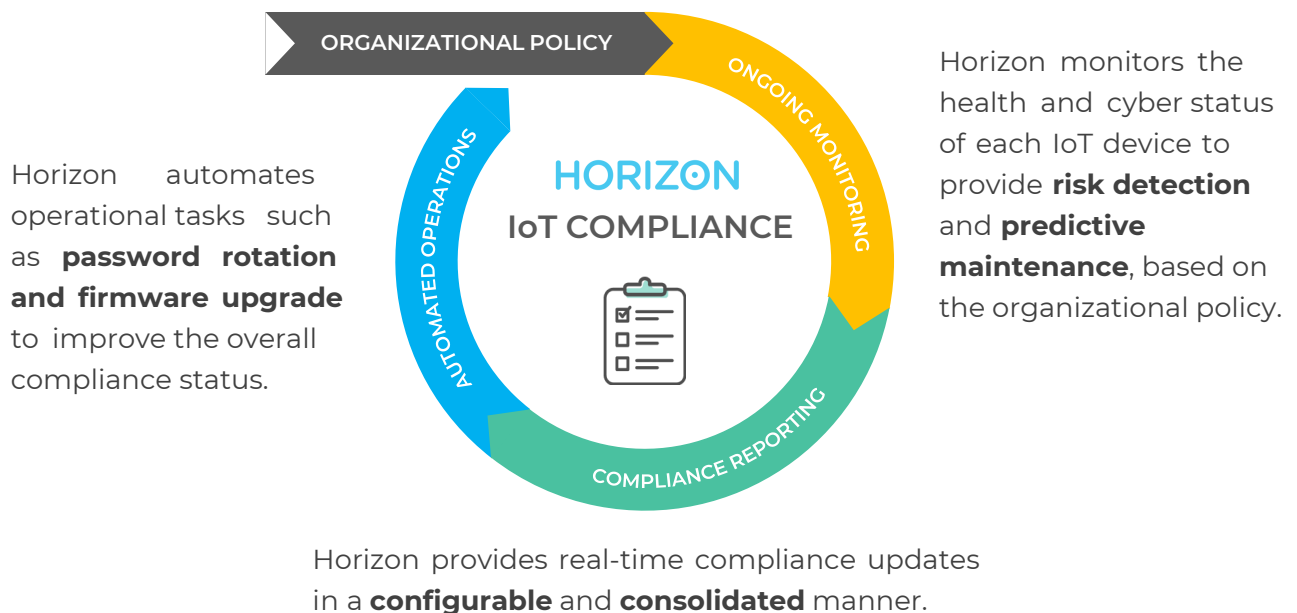· Shutdown of / Tampering with critical assets

Operational Compliance

IoT devices deployed in the field are prone to failures, which can affect or completely disrupt organizations' activity.

The manual maintenance of IoT devices can jeopardize organizations' operational posture and create compliance issues.

Potential threats

· Unavailable device & frequent disconnections
· Data loss & data retention
· Fines, penalties and other legal actions

Horizon automates operational tasks such as **password rotation and firmware upgrade** to improve the overall compliance status.

ORGANIZATIONAL POLICY

ONGOING MONITORING

AUTOMATED OPERATIONS

HORIZON
IoT COMPLIANCE

COMPLIANCE REPORTING

Horizon monitors the health and cyber status of each IoT device to provide **risk detection** and **predictive maintenance**, based on the organizational policy.

Horizon provides real-time compliance updates in a **configurable** and **consolidated** manner.

ENSURE COMPLIANCE for your IoT devices
with SecuriThings Horizon, the first IoTOps solution.

SECURITHINGS
MANAGING IoT OPERATIONS AT SCALE