

The first **IoTops** solution.

Protecting IoT Devices. Maximizing Operational Efficiency.

Managing IoT at Scale Has Become a Liability

In any organization deploying IoT solutions, operational teams are ensuring the devices are **available, secure and in compliance 24/7**.

Ongoing IoT operations represent a significant liability when dealing with scale, generating multiple challenges which are **mostly handled manually – if at all**:

CYBER SECURITY



The inherent vulnerability of IoT devices and their physical accessibility make them prime targets for cyber-attacks. Attackers can reach or affect enterprise networks, critical assets and private data by utilizing IoT devices as weak entry points or shutting them down.

OPERATIONAL MANAGEMENT



Device availability verification, required maintenance activities (such as password rotation, firmware upgrade, etc.) and troubleshooting are mostly performed manually, with limited data. This results in excessive time spent for solving issues.

COMPLIANCE



The lack of edge visibility (outdated firmware versions, expired passwords, known vulnerabilities, and more) can cause regulatory and/or compliance issues, resulting in potential fines, penalties, and other legal actions.

IoTops – A new era for Operational IoT Teams

IoTops encompasses all operational teams that are accountable for the deployment of IoT devices, their availability and their cyber security. These teams are responsible for monitoring the device status, directing technicians, defining and implementing organizational policies, resolving operational issues, overseeing upgrades, and more.

We can categorize the capabilities required for IoTops in 3 buckets:

- **Cyber security**
- **Predictive maintenance**
- **Automated operations**

These capabilities are critical for IoT-based organizations and for the IoT teams within these organizations, and adhere to the following guidelines:



Data is Key

IoTops start with the collection of tremendous amounts of data from each and every managed device. This metadata is analyzed and translated into alerts which should be then prioritized, leveraging AI and Machine Learning capabilities.



Automation is Essential

The scale of IoT deployments prevents the ongoing operations from being performed manually and require IoTops solutions to run multiple tasks such as password rotation and firmware upgrade, across these devices, in an automated manner.



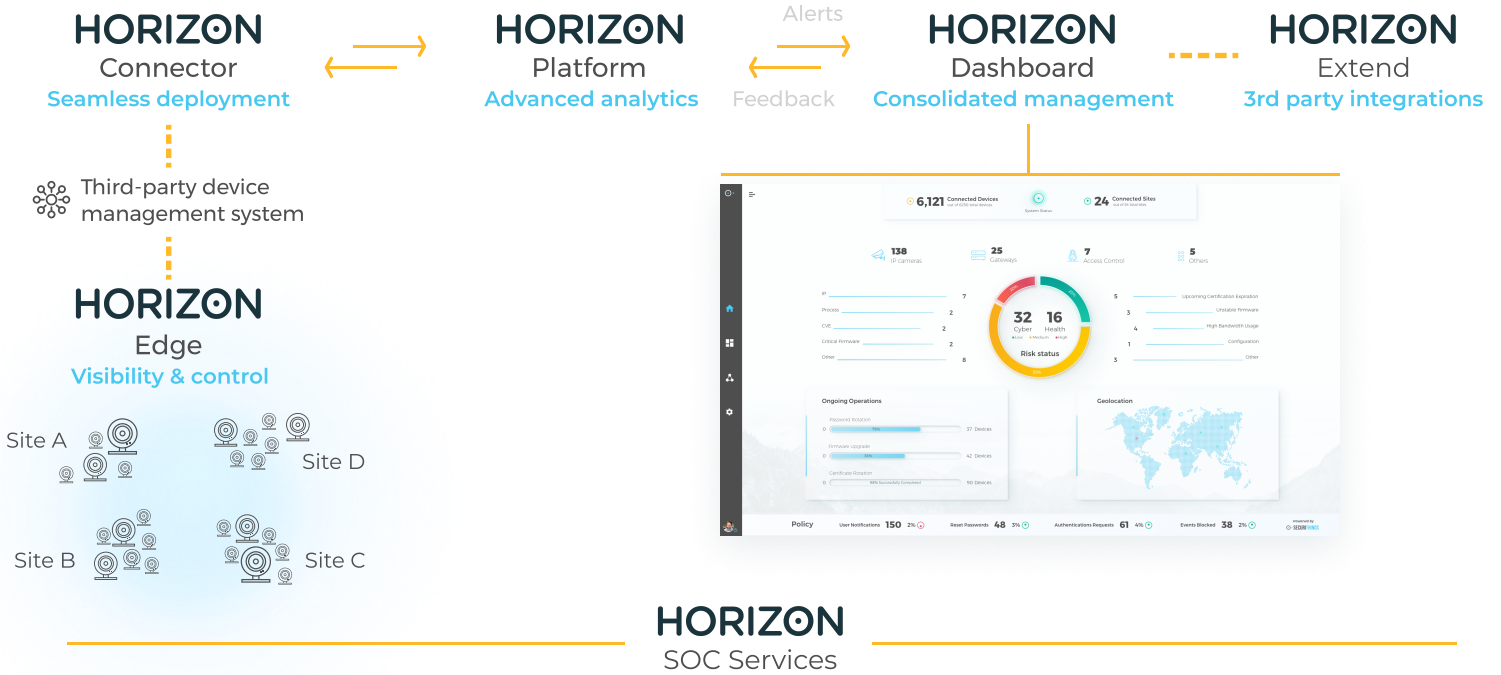
A Consolidated Management

Now that IT is also becoming a key player in IoTops, a unified view is required to get full visibility across all connected devices, and control both their cyber security and ongoing maintenance in one single pane of glass.

IoTops = Cyber Security + Predictive Maintenance + Automated Operations

The First IoTops Solution

SecuriThings' **HORIZON** is a software-only solution automating the management of IoT devices, in one consolidated view. It provides risk detection, predictive maintenance and automated operations for IoT devices. Horizon is comprised of 3 modules:



Horizon Edge - Lightweight software agents or agentless modules which retrieve device level security metadata and device health metrics.

Horizon Connector - Responsible for seamlessly deploying capabilities to the edge, installed on a local appliance or virtual machine.

Horizon Platform - Secure platform utilizing advanced machine learning capabilities to analyze activities and provide a risk score for each device.

Horizon Dashboard - All alerts are presented in one unified view from which operators can manage the operations of all IoT devices.

Horizon Extend - A set of capabilities for integration with 3rd party systems (API, CEF, data export, email alerts, and more).

Horizon SOC Services - In-depth investigation and support on critical alerts, provided by SecuriThings Security Operations Center analysts.

Main capabilities

- + Sites & devices connectivity monitoring
- + Automated password rotation & firmware upgrade
- + Real-time device operational status & metrics
- + Alert prioritization & classification
- + Configurable & detailed compliance reports

Benefits

- (Major operational cost savings)
- (Edge protection and predictive maintenance)
- (Centralized view across IoT devices)
- (Seamless deployment on new and existing devices)

About SecuriThings

SecuriThings is a leading IoT technology provider, helping organizations maximize their operational efficiency when managing IoT at scale. SecuriThings' software-only solution, Horizon, provides risk detection, predictive maintenance and automated operations for managed IoT devices, in one unified view.

SecuriThings Horizon has been deployed in major airports, universities, cities, and large enterprises, and is already monitoring millions of devices globally.

SecuriThings has established partnerships with world-leading global system integrators, device management systems and edge device vendors.

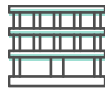
Among our partners



Across verticals



Physical Security



Building Automation



Smart & Safe Cities



Consumer Devices



Industry 4.0

Deployed Across Industries



Airports & ports



Corporate campuses & buildings



Financial Institutions



Municipalities & educational campuses



Casinos

**PROTECT your IoT devices while MAXIMIZING
YOUR OPERATIONAL EFFICIENCY**



info@securithings.com | www.securithings.com

SECURITHINGS
MANAGING IOT OPERATIONS AT SCALE