SECURITHINGS

MANAGING IoT OPERATIONS AT SCALE

HORIZON

Automated Operational Management for IoT devices

IoT in a **NUTSHELL**

20.4B
devices deployed by 2020

127
new connected devices every second

$15T
potential revenue by 2025

Managing IoT At Scale Is **BECOMING A LIABILITY**

From multinational corporations with large campuses to critical infrastructures, organizations massively deploy IoT devices to maximize their business, operations, security, safety, and more.

However, the scalability and physical accessibility of IoT deployments create a complex and distinct set of challenges yet to be encountered in the IT space and impact the **organization's operational efficiency** from two perspectives: the **cyber security** and **maintenance** of IoT devices.

Cyber security

The inherent **vulnerability of IoT devices** and their public accessibility (either physically or remotely) make them **prime targets for cyber-attacks.** Attackers' motivation to reach or affect enterprise networks, critical assets and private data can lead them to either utilize IoT devices as weak entry points or shut them down.

Over the last two years, **46% of IoT security buyers experienced cyber-attacks** such as brute force attacks, IoT-specific malware and IoT botnets (Altman Vilandrie & Co, 2018). These attacks are becoming more sophisticated, impacting organizations' security and operations.

- Default Credentials & Brute Force Attacks
- Supply chain threats & Weak Configurations
- Device Malware & Botnets
- Inside Threats & Tampering

Operational management

With the large-scale deployment of IoT devices, enterprises benefit from additional data which drives business, operations and security optimization. To maintain this level, IT teams need to ensure these devices are **always on, remaining fully and constantly operative.**

Companies typically manage ongoing operations, performance issues and failures of their connected devices manually, resulting in overhead costs as well as excessive network and storage usage.

- Performance Issues & Failures
- Manual Maintenance & Upgrades
- Ongoing Troubleshooting
- Excessive Network & Storage Usage

Automated Operational Management **FOR IoT DEVICES**

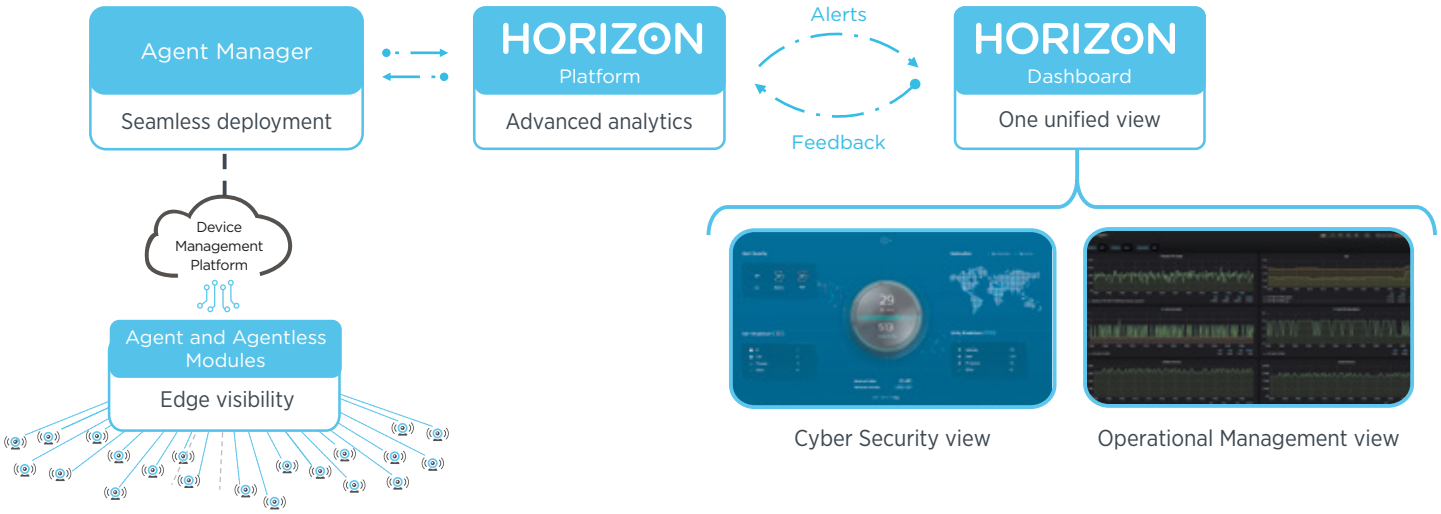
SecuriThings' **HORIZON** is a software-only solution automating the management of IoT devices in one unified view. It provides both the **cyber security posture** and **operational management of IoT devices.**

Horizon's approach is based on three principles:

1 | **Edge visibility and control**
provided in-depth for each IoT device

2 | **Management platform support**
allowing a seamless deployment

3 | **AI-based detection**
enabling automation for scale



Across Verticals

Physical Security | Smart and Safe Cities | Building Automation | Consumer Devices | Industry 4.0

Horizon is comprised of 4 main components:

Agents and Agentless Modules
Lightweight software agents or agentless modules which retrieve device level security metadata and device health metrics.

Agent Manager
Installed on a local appliance or virtual machine, responsible for seamlessly deploying capabilities to the edge.

Horizon Platform
A secure platform which utilizes advanced machine learning capabilities to analysis activities and provide a risk score for each device.

Horizon Dashboard
Suspicious devices are then alerted and presented in a dedicated dashboard that is used by SecuriThings Operations Center or the customers' security team for further investigation.

Benefits

+ Seamless, scalable & centralized deployment
+ Complete edge visibility
+ Automated operations & mitigation

= **Overall improved operational efficiency**

Across Industries

Large-scale deployments | Multi-site and cross networks | Mission critical environments

Airports | Campuses & Buildings | Municipalities | Sport & Entertainment Venues | Retail | Hospitality | Financial Institutions | more