






Empowering operational teams with a tailored solution for managing IoT at scale




In any organization deploying IoT solutions, operational teams – from physical security to building automation – are ensuring connected devices are available and secure 24/7. These teams are responsible for monitoring the status of devices, directing technicians, defining and implementing organizational policies, resolving operational issues, overseeing upgrades, and more.

When dealing with scale, these ongoing operations are generating multiple challenges which are mostly handled manually – if at all:

-  **Cyber incidents**
Malicious actors are exploiting the inherent vulnerability and physical accessibility of IoT devices to reach enterprise networks, assets and data or to shut them down.
-  **Device status verification**
In many cases, devices are found to be offline after a long period of time due to limited capabilities to verify their availability, uptime stats, and performance metrics.
-  **Incident handling**
When performed manually with limited data and tools, issues and incidents are not alerted, resulting in an extended handling period and a longer downtime of devices.
-  **Required maintenance activities**
Organizations are challenged with performing multiple maintenance tasks on large magnitude of devices (password rotation, firmware upgrade, and more).
-  **Compliance**
The lack of real-time visibility on vulnerable firmware versions, weak and outdated passwords, and more, can put organizations in non-compliant state.

Current solutions mostly focus on discovery and network security, and do not solve the very specific challenges faced by IoT teams.

It is essential for IoT-based organizations to ensure the following aspects when considering a solution to solve the very specific needs of IoT operational teams:

-  **Device-level data for edge visibility**
The collection of tremendous amounts of data from each and every managed device drive device health monitoring as well as risk detection which reduces the impact of potentially catastrophic attacks. This metadata is analyzed and translated into alerts which should be then prioritized, leveraging AI and Machine Learning capabilities.
-  **Automated capabilities to handle IoT scalability**
The scale of IoT deployments prevents the ongoing operations from being performed manually. The automation of multiple tasks such as password rotation and firmware upgrade enables risk mitigation and predictive maintenance, resulting in operational cost reduction and shortened SLA.
-  **A centralized view for all IoT operations**
Now that IT is also becoming a key player in IoTops, a unified view is required to get full visibility across all connected devices, control both their cyber security and ongoing maintenance, and adhere to internal compliance and regulation.

Contact us to learn how SecurIThings can help you manage IoT operations at scale, in a secure and cost-efficient manner.