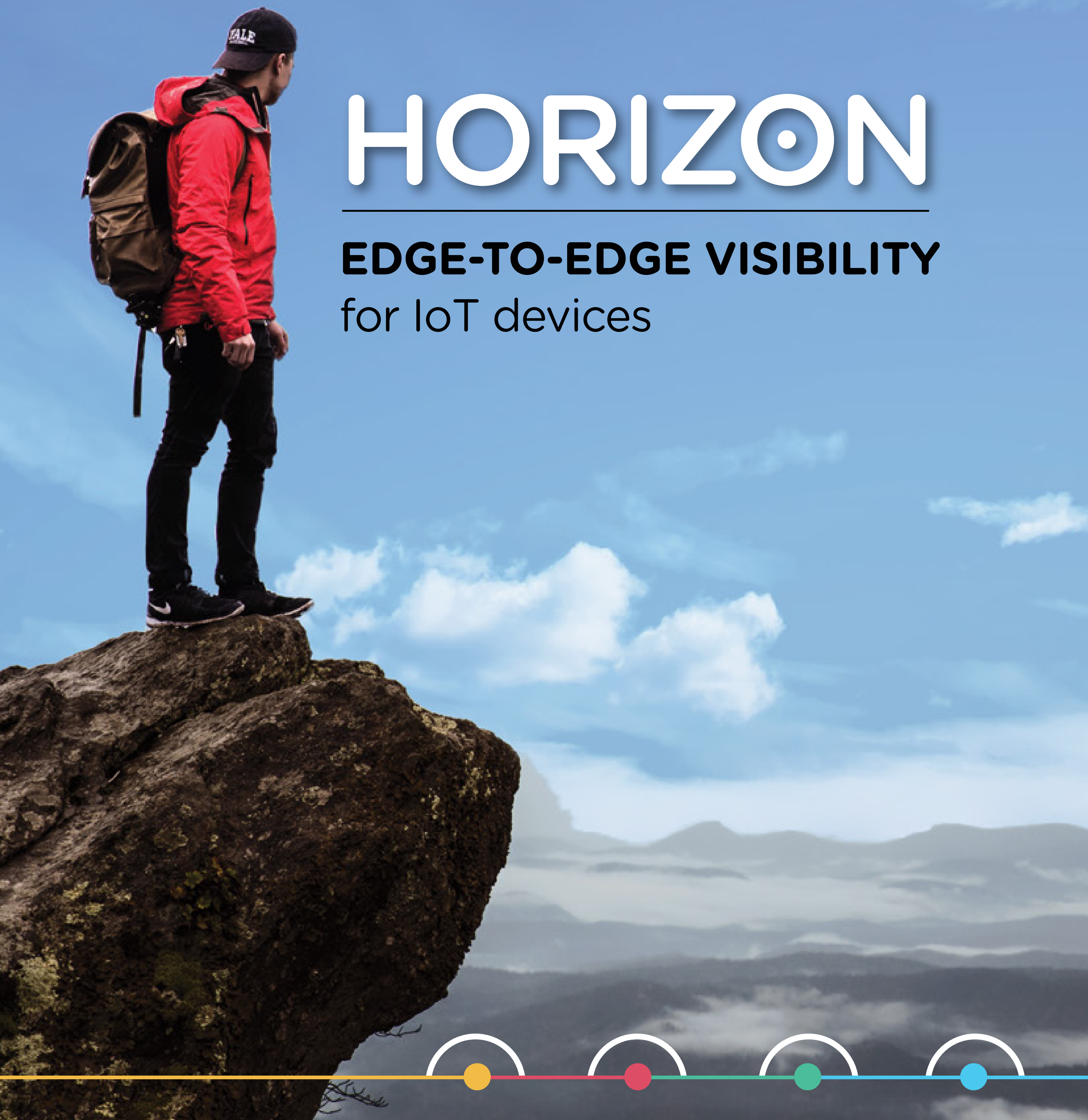
SECURITHINGS

SETTING THE ROUTE FOR IoT VISIBILITY



HORIZON

EDGE-TO-EDGE VISIBILITY

for IoT devices

IoT in a **NUTSHELL**

20.4B	127	$15T
devices deployed by 2020	new connected devices every second	potential revenue by 2025

IoT starts **AT THE EDGE**

IoT devices are presenting a complex and distinct set of challenges yet to be encountered in the IT space. These devices are massively deployed by enterprises and IoT service providers to maximize their business, operations, security, safety, and more.

However, organizations face a **complete lack of visibility and control** over these newly and known connected devices, mainly **from a cyber security and health posture perspectives**. In fact, the existing IT security and health solutions were not designed to support devices with such limited computational capabilities, partially deployed outdoors and on remote sites, raising the need for a dedicated solution.

Cyber-attacks targeting IoT devices

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, creating an additional blind spot.

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

Lack of visibility over device health

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

SOLVING the IoT Blind Spot

SecuriThings' **HORIZON** is a software-only solution offering full visibility and control over IoT devices providing the **ongoing cyber security posture** and **health status of each and every device.**

Horizon's approach is based on three principles:

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

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

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

CYBER SECURITY

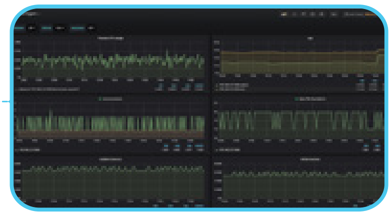
HORIZON

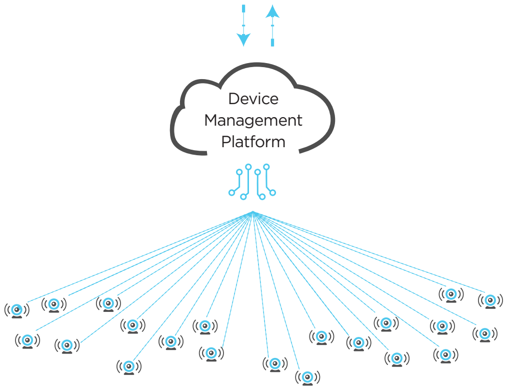
AI-Based Detection

Real-time Mitigation

Device Health Monitoring

HEALTH MONITORING





Across Verticals

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

Benefits

- ✓ Overhead cost reduction
- ✓ Edge protection against cyber attacks
- ✓ Security & operations optimization
- ✓ Predictive maintenance
- ✓ Coverage for already deployed devices

Horizon is comprised of 4 main components:

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

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

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.

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

About SecuriThings

SecuriThings is a leading IoT technology provider, solving the lack of visibility and control faced by enterprises and IoT service providers over their edge devices. The company's software-only solution provides the ongoing cyber security posture and health status of each and every connected device.

Working with SecuriThings , organizations maximize their business, security and operational efficiency by ensuring their large-scale deployments of connected devices are always available and secure.

SecuriThings has established partnerships with leading system integrators, management systems and device vendors, and is already monitoring millions of devices globally.

100M+
Monitored Devices

5 MIN
Set-up and Deployment

10+
Technology Partners

Among Our Partners

Microsoft
Johnson Controls
UNIVERSAL ELECTRONICS.
AXIS COMMUNICATIONS
milestone
Genetec
dahua TECHNOLOGY
HIKVISION
avigilon
illustra From Tyco Security Products
exacqVision

**Maximize the efficiency of your operations
with FULL VISIBILITY AND CONTROL over your IoT devices**

info@securithings.com I www.securithings.com

SECURITHINGS
SETTING THE ROUTE FOR IoT VISIBILITY