# Assure IoT Operations

## with VMware Edge Intelligence

Part of the broader VMware Secure Access Service Edge (SASE) offering, VMware Edge Intelligence helps organizations:

- Simplify the operational complexity of managing IoT devices by providing operational assurance on a per-device basis
- Navigate through the complex cybersecurity challenges associated with using IoT devices

Migration to edge computing and the proliferation of Internet-of-things (IoT) devices continue to be major themes underlying the digital transformation of the economy. Given IoT's potential to reduce costs, improve efficiency, and provide more visibility into day-to-day operations, it is finding increasing use cases across all verticals. The number of IoT connections worldwide is forecasted to rise from 14.6 billion in 2022 to over 30 billion connections by 2027[1]. There are two key concerns for business and IT leaders as they consider adopting IoT devices: Operational complexity and cybersecurity threats.

### IoT devices multiply complexity

Introducing IoT devices increases operational complexity for IT and networking teams. Manual onboarding of new IoT devices and tracking their performance is time consuming, labor intensive, and difficult to scale. Because these devices tend to be extremely critical (for example, bedside monitors in hospitals, security cameras in retail stores), it is imperative to ensure that they are always operational and secure. In some enterprises, functional teams and IT operational teams do not have a clear structure around which team owns the device and is responsible for maintaining its operational status.

### Securing IoT devices is challenging

Adding IoT devices into the enterprise environment introduces significant cybersecurity challenges, including:

- **Exposure to critical vulnerabilities:** Given the multitude of device types and manufacturers along with a constantly evolving threat landscape, IoT devices can introduce risk. Furthermore, if device manufacturers do not add sufficient built-in device security

[1] Ericsson Mobility Report – June 2022

capabilities or if the device is not appropriately hardened and patched, the enterprise is exposed to critical vulnerabilities and susceptible to potential cyber-attacks.

- **Inadequate visibility:** As the number of IoT devices in a network increases, it becomes difficult to manually track and monitor them. Lack of visibility into the operational status and behavior of the device (for example, how many and which external hosts it is interacting with) can directly affect productivity and introduce new risks.
- **Insufficient risk containment:** Considering the wide variety of IoT device types in an environment, it is imperative to categorize devices, evaluate their risk and place them in appropriate network segments. For example, end-user traffic accessing corporate applications should be logically separated from IoT device traffic that is central to an enterprise's operations. Insufficient network segmentation could potentially compromise the whole network by allowing easy lateral movement for attackers.

## Introducing VMware Edge Intelligence

VMware SASE™ helps IT teams address the challenges of operating in the distributed world and managing IoT device operations. VMware Edge Intelligence™ (formerly VMware Edge Network Intelligence) is a vendor-agnostic AIOps solution of VMware SASE that enables IoT device operations by ensuring device performance, security, and self-healing.


Figure 1: VMware Edge Intelligence provides insights across the IoT lifecycle

VMware Edge Intelligence brings the following benefits to organizations:

### IoT device inventory management

Removes the responsibility of IoT device discovery, classification and tracking from end users so that they can focus on business operations. VMware Edge Intelligence is an agentless solution that leverages a machine learning (ML) based hierarchical device classification system

## Learn more

- VMware Edge Intelligence, sase.vmware.com/products/edge-intelligence
- VMware SASE, sase.vmware.com

and uses the detailed behavioral signature of each detected device to automatically inventory and classify them into device groups.

### Critical device operational assurance

Provides seamless critical device operations for business users without them needing to diagnose and troubleshoot issues. VMware Edge Intelligence allows users to indicate which IoT device groups are critical and offers deep visibility into these devices' operations. It does this by establishing performance baselines and alerting IT operational teams in real time whenever performance deviates from the baseline. The solution also benchmarks device performance and behavior with similar devices in the enterprise and across peers in the same industry.

### IoT security

Helps IT operational and security teams manage the security needs of IoT devices in the environment. VMware Edge Intelligence monitors device behavior at a group and individual level and captures information such as device location in the network, number of internal and external hosts communicated with, and types of protocols used to communicate. Based on interactions with suspicious URLs, unauthorized IP addresses and high-risk connections, an overall threat profile is generated. The profile can be compared against devices within a group as well as similar devices in a different client's environment.

VMware Edge Intelligence scans your IoT environment against an up-to-date threat intelligence database consisting over 300 billion global data points to detect and minimize threats in real-time. The solution also monitors over 30 million IoT devices deployed in production across industry verticals.

## Why adopt VMware Edge Intelligence?

If you are considering onboarding IoT devices in your IT environment or already have an IoT portfolio, VMware Edge Intelligence provides a one-stop shop to manage all your operational and cybersecurity needs. With the ability to automatically detect, classify and monitor devices for performance and behavioral deviations, VMware Edge Intelligence helps you gain control and visibility over your IoT ecosystem.