Solution Overview

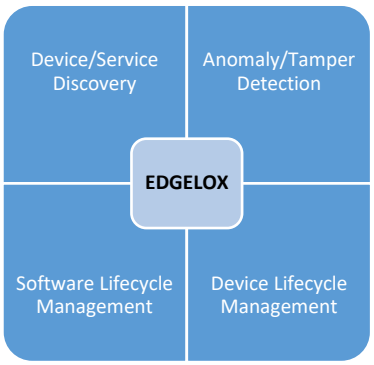
EdgeLox Security for the Enterprise of Things

Key Value:

- **S**ecuring the IoT Edge
- **M**onitoring the IoT infrastructure
- **M**anaging the IoT infrastructure
- **D**iscovering devices & services
- **P**rofiling device behavior
- **D**etecting behavioral anomalies
- **E**nforcing security policies

Key Benefits:

- **S**ecure Device Edge Layer
- **A**gentless for Things
- **E**asy Installation
- **E**asy Thing Interfacing



Explosive growth of the Enterprise of Things

Enterprises are experiencing a massive growth in IoT with organizations using IoT devices to drive their businesses. With IoT opening the door to unprecedented connectivity and innovative services, it has gained strategic importance in organizations, to optimize operations, enable new business models and drive next-generation product designs. Recent estimates put enterprise IoT devices at roughly 30% of all network-connected endpoints, paving the way to shape the next phase of tech innovation with the intelligent cloud and the intelligent edge to meet the needs of advanced business services around AI and real time decision making.

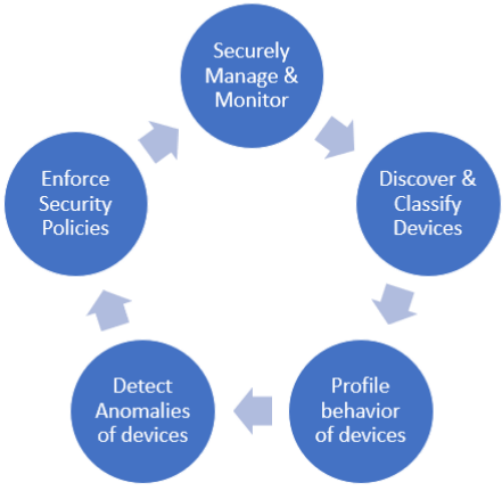
Need for a Secure Management Platform

In order to deliver on this promise of powerful and ubiquitous computing from the edge to the cloud, enterprises need to ensure that the **underlying IoT infrastructure is robust, scalable, secure, monitored and managed** and meets the required standards put forth by IT departments for deployment, asset management, security and compliance. EdgeLox enables enterprise-grade end-to-end IoT infrastructure security, monitoring and management by supporting specific usage models and workflows required by top enterprises as part of their business demands.

Overview

IoT infrastructure in today's enterprise lacks a platform that enables scalable and robust monitoring, management and security. While IoT opens the door for innovative approaches and services in all industries, it presents new cybersecurity risks as well. As mentioned in the security report "2020 Unit 42 IoT Threat Report", the general security posture of IoT devices is declining, leaving organizations vulnerable to new IoT-targeted malware as well as older attack techniques that IT teams have long forgotten. High-profile IoT-focused cyberattacks are forcing industries to recognize and manage security risks to protect their core business operations. Here are the key gaps in the management and security of the IoT infrastructure that need immediate attention.

EdgeLox begins with a secure substrate that supports TPM based onboarding devices either manually using client frameworks or by discovering devices on the network with non-intrusive network traffic capture and analysis. Once under management, the software on devices is kept compliant and its lifecycle is fully managed. The devices are constantly monitored for any tampering or behavioral changes using sophisticated anomaly detection techniques and any remedial actions are enforced with integrations into Intrusion Prevention and Network Management Systems.



Device Lifecycle management involves onboarding gateways and devices for management, configuring them, monitoring them and raising alerts based on configured rules, diagnosing and troubleshooting with remote access, re-provisioning and re-establishing identities during replacement and decommissioning them as required. Ingestion and analysis of metrics from devices will be handled at the Edge and only results of the analysis will be propagated to the cloud.

Software Lifecycle management maintains the software on gateways and devices compliant with configured policies. It involves packaging software or configuration files, pushing them down to gateways and devices, deploying them, activating them, monitoring all systems for software compliance, re-deploying in case of failures and finally de-commissioning them once done. This is an ongoing process for all devices once they have been onboarded.

Security Lifecycle detects devices on the network using non-intrusive network traffic ingestion. Classification models help identify devices that are then onboarded on to the secure management platform. The Device Edge is then subjected to TPM based boot and runtime attestations to detect any kind of tampering. In addition, behavior of all devices is profiled along a set of process and network features that help detect any anomalies from normal behavior. Based on the type of anomaly, EdgeLox bridges the right remedial policies into 3rd party Network Management Systems (NMS) or Intrusion Prevention Systems (IPS).