ZingBox IoT Guardian leverages patent-pending machine learning capabilities to discover IoT devices, assess risk, baseline normal behaviors or IoT personalities, detect anomalous activities, and provide real-time remediation across an organization's entire IoT footprint. ZingBox IoT Guardian is available in four subscription models.

Discovery & Visibility

Discover all IoT Devices – ZingBox Inspector, available as an appliance or a virtual appliance, is a network sensor that monitors all traffic traversing the network. Machine learning technologies optimized for IoT devices are used to discover connected devices such as industrial sensors, devices on factory floors, medical equipment, HVAC systems, fire alarm panels, and surveillance cameras. Analysis of real-world IoT device traffic paired with ZingBox's cloud infrastructure provides unparalleled discovery, recognition, and identification of devices.

Classify Device Types – Patent-pending machine learning algorithms designed specifically for automatic IoT classification are used to categorize different devices. These algorithms can detect unique feature sets that belong to a common group of devices and also identify rich context specific to each IoT deployment and environment.

Risk Analysis & Threat Detection

Baseline IoT Personalities – IoT Guardian uses hundreds of unique indicators to create profiles that characterize each IoT device's "normal personalities." Device personalities are derived from network analysis including inspection of packet headers, analysis of network sessions, automatic recognition of applications and services, calculation of multiple level derivatives, review of time series data, and discovery of network topologies and user interaction behaviors. Baseline of normal IoT personalities is further refined by multi-tier profiling consisting of device category, device vendor, and device instance. The multi-tier profiling provides unique baselines derived by the type of device, model number, and specific context of the device.

Detect Anomalous Behavior – IoT Guardian employs a real-time detection engine to identify abnormal/anomalous behaviors based on deviations across multi-dimensional metrics. The types of detections include deviations from historical behavioral data, typical behaviors in the vicinity group, environment specific context, and user-defined IoT behaviors. Through machine learning, IoT Guardian can also detect various cyber attack phases; Reconnaissance, Infiltration, Command and Control, Assault, and Obfuscation.

Create Custom Policies – IoT Guardian's built-in policy editor enables context based custom policies to generate alerts upon detection of specific behaviors. The policies can also be configured to raise alert on behaviors outside of what has been defined as trusted. The ability to blacklist suspicious behaviors and whitelist normal behaviors provides the highest flexibility and accuracy for policy enforcement.

Policy Enforcement

Enforcement via Existing Infrastructure – IoT Guardian's integration with existing security infrastructure enables seamless enforcement of policies upon detection of anomalous and custom-defined activities. The interoperability with SIEM solutions, firewalls, NACs, and UTMs enable remedial actions such as quarantine or session termination without the need to invest in additional inline security gear.

Extended Data Retention

Retain Metadata – Records of past network activities are often required for compliance, forensic analysis, audits, and other business requirements. IoT Guardian can retain metadata for up to 1 year.

About ZingBox

Enabling the Internet of *Trusted* Things, ZingBox is the industry's first and only IoT security solution provider to leverage the individual personalities of IoT devices to provide accurate visibility and protection of an organization's IoT assets. IoT Guardian, ZingBox's SaaS-based security solution, leverages machine learning to discover, assess risk, baseline normal behavior, detect anomalous activities, and provide real-time remediation across an organization's entire IoT footprint.