Zingbox

DATASHEET

IoT Guardian

KEY BENEFITS

- Discover IoT devices in the network
- Classify IoT assets into categories
- Assign a risk rating for each IoT device
- Identify anomalous device behaviors
- Identify zero-day attacks
- Maximize existing security investments via integration

KEY FEATURES

- Agentless IoT discovery capability
- 70+ characteristics to assess device personality
- Patent-pending 3-tier profiling
- Integration with existing security solutions including SIEM and firewalls

Gartner Cool Vendor 2017™

Zingbox IoT Guardian is the industry's first and only IoT security solution to leverage the individual personalities of IoT devices to provide accurate visibility and protection of organizations' IoT assets. As a SaaS-based security solution, IoT Guardian leverages machine learning to identify, classify, and profile individual personalities; assess risk; and enforce trusted behaviors.

IoT Security Challenges

As organizations increasingly adopt and deploy new IoT devices, they quickly come to the realization that the traditional security solutions are simply not designed to cope with the unique characteristics of IoT devices.

DEVICE CONTEXT Traditional security solutions rely on recognition of operating systems, plug-ins, and installed applications to classify and provide device context. Unfortunately, contexts for IoT devices are not well understood. Identifying X-ray machines, industrial automation systems, or point-of-sale devices simply as Windows-based devices offers little insight into how best to manage and secure these devices.

RISK ASSESSMENT The risks of a device, according to traditional security solutions, are often calculated by comparing the device behaviors against the normal/trusted behaviors of a typical user. Such patterns are often used to detect viruses. Unfortunately, this approach cannot be applied to IoT devices. To accurately assess risk to IoT devices, the security solution must have full knowledge of the device including its trusted and intended behaviors. Without such details, many organizations are relying on inaccurate risk assessments of their IoT assets.

MANAGEABILITY Traditional security solutions rely on tools such as Enterprise System Management (EMS) for laptops and Mobile Device Management (MDM) for mobile devices to manage and upgrade end-point devices. These solutions ensure that the latest patch and best-practice configurations are enforced. Unfortunately, this approach is not applicable to IoT devices. IoT devices are purpose-built and not designed to be serviceable by end-users. Any attempt to upgrade their software or even impede their communication can lead to unpredictable behaviors.

Zingbox IoT Guardian

With the limited effectiveness of traditional malware-based security solutions, IoT Guardian takes an innovative approach to IoT security. Designed from the ground up to secure IoT devices, IoT Guardian discovers and categorizes all IoT devices, detects threats and risks associated with each device, and provides the necessary means to defend against those threats.

Discover IoT Devices

IoT Guardian provides unparalleled visibility into your IoT assets. It first identifies every IoT device in the network. Based on the detailed analytics of these personalities, it then classifies each device based on its function and behaviors. This enhanced visibility is available without installing or managing endpoint agents and is 100% transparent to the IoT devices.

Detect Security Risks and Threats

IoT Guardian leverages machine learning to baseline acceptable behaviors of every IoT device including their communication patterns with other devices. Zingbox's patent-pending technology analyzes over 70 device characteristics and leverages 3-tier profiling to accurately determine each device's unique personality. It can detect abnormal and anomalous

Zingbox IoT Guardian

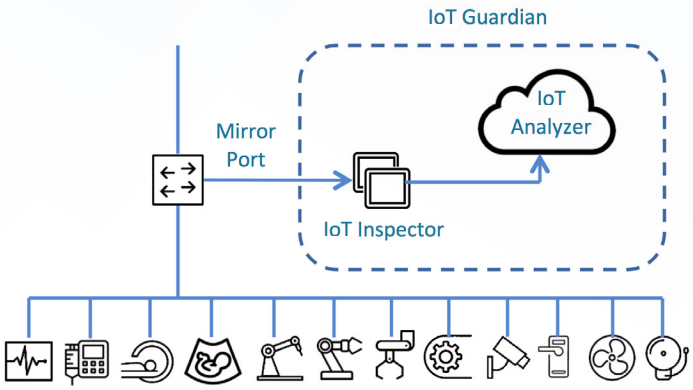
Zingbox IoT Guardian leverages patent-pending machine learning capabilities to discover IoT devices, assess risk, baseline normal behavior, detect anomalous activities, and provide real-time remediation across an organization's entire IoT footprint.

activities for each device based on the deviation from the accepted norm. Every IoT device is automatically assigned a risk rating, enabling organizations to easily identify the devices requiring immediate attention.

Defend Against Threats

IoT Guardian continuously monitors an organization's network for abnormal or anomalous activities and upon detection, isolates or quarantines the device. Through the integration with SIEM and other security solutions, IoT Guardian can trigger real-time action to minimize the risk to the organization and other IoT devices. Unlike pattern/signature-based solutions, IoT Guardian can also detect zero-day attacks.

Deployment



Solutions

	DISCOVERY	DISCOVERY & THREAT DETECTION	DATA RETENTION PACKAGE
Discover all IoT devices	○	○	○
Classify device types	○	○	○
Baseline normal behavior		○	○
Assess device risk rating		○	○
Detect anomalous behavior		○	○
Integration w/ existing infrastructure		○	○
Retain metadata up to 1 yr			○

About Zingbox

Zingbox IoT Guardian is an Internet of Things security solution that provides visibility into and protection for enterprise IoT assets against cyber and insider threats. A **non-intrusive, agent-less, signature-less** solution, IoT Guardian uses machine learning for asset discovery, risk assessment, baselining the normal behavior of devices, and discovery of threats. Zingbox was founded by Silicon Valley IT industry leaders and experts in networking, big data, IoT, and security.