IOT GUARDIAN: SECURE, MANAGE, OPTIMIZE

Benefits

Zingbox IoT Guardian:

- Provides realtime risk and vulnerability assessment with the largest IoT behavioral repository in the IoT security industry.
- Allows a view of the entire smart city IoT network via a security operations center (SOC).
- Provides realtime operational insights into device behaviors and usage to optimize city-wide operations, lower TCO, and reduce the downtime of city services through predictive maintenance.
- Solves the complex integration of IT and OT intelligence, ensuring a true smart city lifestyle.

A smart city empowered by the internet of things (IoT) creates new experiences for its people, taming the pressures of urbanization, enabling more social interaction, improving city efficiency, and reducing waste. Many cities worldwide have already adopted IoT-enabled smart traffic, buildings, hospitals, and lifestyles. As a result, IoT devices—such as cameras, sensors, traffic lights, alarms, robots, and controllers—are integrated with city infrastructures and connected to city networks. Unfortunately, many smart city IoT systems are riddled with critical security vulnerabilities and risks. The threat surface is large, and the consequences of a security breach are significant.

Many smart buildings have network-connected IoT devices, such as security cameras, lighting controls, HVAC systems, locking mechanisms, and fire sensors. IoT-specific attacks target such IoT devices. An attacker might hack an alarm system to remotely open building doors or block a fire sensor from generating an alarm. With IoT devices increasingly forming the backbones of smart cities, the potential impact of a security breach has grown immensely.

Challenges and Threats

Alongside the benefits of an IoT-enabled smart city, there are some important considerations:

- Citizens' physical safety and uninterrupted access to public services must be maintained.
- Lack of visibility into devices, their behaviors, and device context make critical smart city infrastructure, such as traffic lights and emergency alerts, vulnerable to hackers.
- Smart city IoT devices are open to botnet attacks that can cause distributed denial of service (DDoS).

Zingbox IoT Guardian

Zingbox IoT Guardian is an IoT security offering that automates the orchestration of the IoT lifecycle to provide security, management, and optimization of all assets.

Zingbox IoT Guardian uses machine learning and AI to learn the behaviors of connected IoT devices. By closely monitoring IoT device behavior, IoT Guardian can quickly detect the signs of attacks and alert administrators as well as integrated third-party products to take swift action.

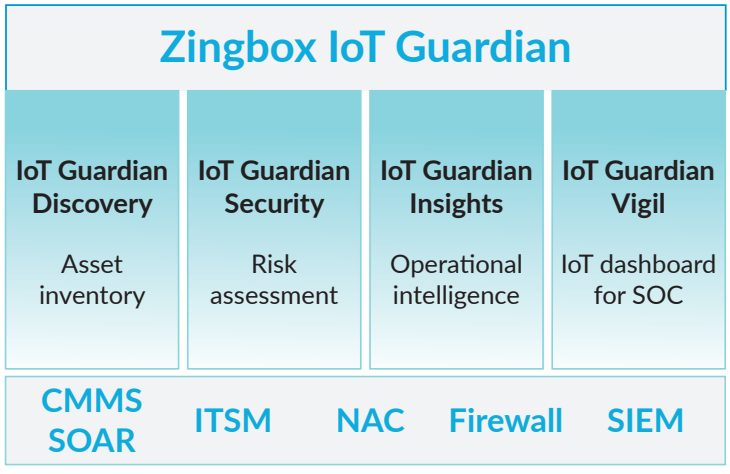

Figure 1: Zingbox IoT Guardian

Use Cases

Visibility

Zingbox provides complete situational awareness for IoT-enabled smart cities with a dynamic, realtime, and context-aware inventory. Based on deep insight into your unmanaged devices, Zingbox constructs and maintains records for each device—vendor, model, serial number, operating system, behavior, and more. You can easily create Zero Trust policies for groups of devices and add compensating controls to ensure a secure, compliant smart city network.

Risk Assessment

Every new device, from traffic signals to transit systems, becomes a potential weakest link for unauthorized access and a possible threat to operations. To detect vulnerabilities and gather the security posture of a device, Zingbox uses passive network analysis instead of intrusive device probing methods. You can assess risks and vulnerabilities across the entire network to ensure citywide operational continuity.

Operational Efficiency

To help city officials reduce total cost of ownership (TCO), Zingbox can generate efficiency scores for your devices, departments, and facilities. It provides valuable operational insights for the study of traffic patterns and utility usage patterns. Through these insights, you can optimize existing equipment and make better-informed purchasing and maintenance decisions.

Deployment

Zingbox IoT Guardian is a cloud-based, easy-to-deploy offering. Its nondisruptive zero-touch deployment ensures business and operational continuity in a citywide environment.

Secure

- Automatically discover, recognize, and assess risks to IoT devices from traffic sensors to smart grids
- View asset records enriched with contextual data
- Alert IoT management when anomalies are detected

Manage

- Minimize downtime through predictive maintenance
- Simplify the monitoring, reporting, and upgrading of IoT devices
- Provide central management of IoT devices across cities, states, and countries

Optimize

- Provide realtime situational awareness and operational monitoring of your IT and OT environment
- Proactively optimize devices to minimize maintenance, reduce TCO, and ensure uninterrupted smart city operations
- Link to enterprise applications, such as IT, OT, and business intelligence

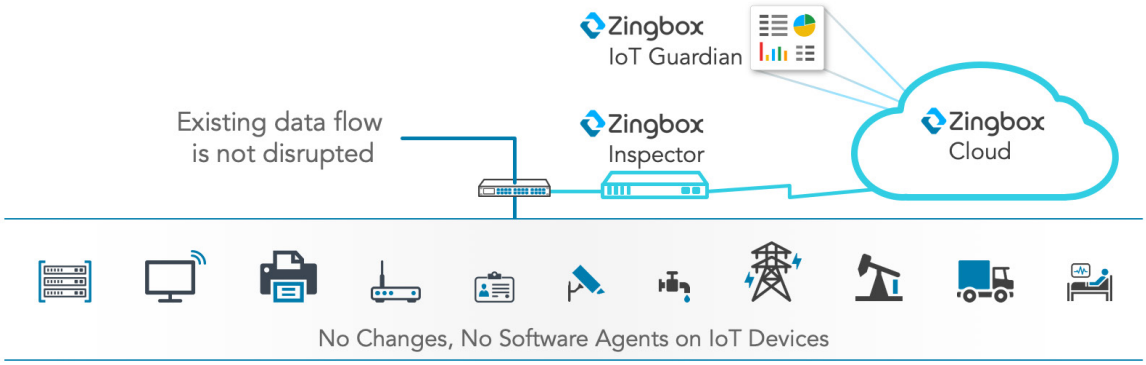

Figure 2: Zero-touch deployment

Integrations

With the broadest portfolio of integrations available, Zingbox IoT Guardian can integrate with existing, previously standalone systems (e.g., SIEM, NAC, and firewalls) and orchestrate all integrated activities from a single pane of glass. It harnesses IoT data from integrated systems to enhance its business insights.

Contact

For inquiries about Zingbox, email Brian de Lemos, VP of Global Strategic Accounts and Programs, Cortex, at **bdelemos@paloaltonetworks.com**.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

iot-guardian-b-100819