Zingbox

SMART CITY
SOLUTION BRIEF

IoT Command Center: Secure, Manage, Optimize

CHALLENGES AND THREATS

- Citizens' physical safety and uninterrupted access to public services must be maintained
- Critical smart-city infrastructure, such as traffic lights and emergency alerts, are vulnerable to hackers due to lack of visibility into devices, their behaviors, and device context
- Smart-city IoT devices are open to botnet attacks that can result in a distributed denial of service

ZINGBOX BENEFITS

- Provides real-time 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 real-time 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

KEY COMPANY STATS

- 1,100 deployments
- 1.6+ petabytes of IoT traffic analyzed per day
- 11.2+ million devices secured

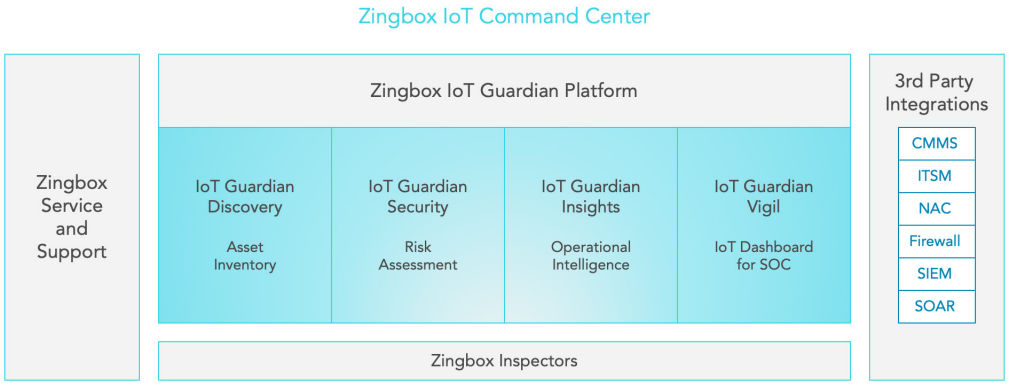
An IoT-enabled smart city creates new experiences for people, taming the pressures of urbanization, enabling more social interaction, improving city efficiency, and reducing waste. IoT-empowered smart traffic, smart buildings, smart hospitals, and smart lifestyles have already been adopted by many cities worldwide. As a result, IoT devices like cameras, sensors, traffic lights, alarms, robots, and controllers are now integrated into 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 increasing IoT devices forming the backbone of smart cities, the impact of a security breach has become more serious.

Zingbox IoT Command Center

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

At the core of the IoT Command Center is Zingbox IoT Guardian, which uses machine learning and artificial intelligence 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 and integrated third-party solutions to take swift action.



USE CASES

Visibility

Zingbox provides complete situational awareness for IoT-enabled smart cities with a dynamic, real-time, and context-aware inventory. Based on deep insight into your unmanaged devices, Zingbox constructs and maintains records for each device: its 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 and 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 city-wide operational continuity.

Operational Efficiency

To help city officials reduce 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 more informed purchasing and maintenance decisions.

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

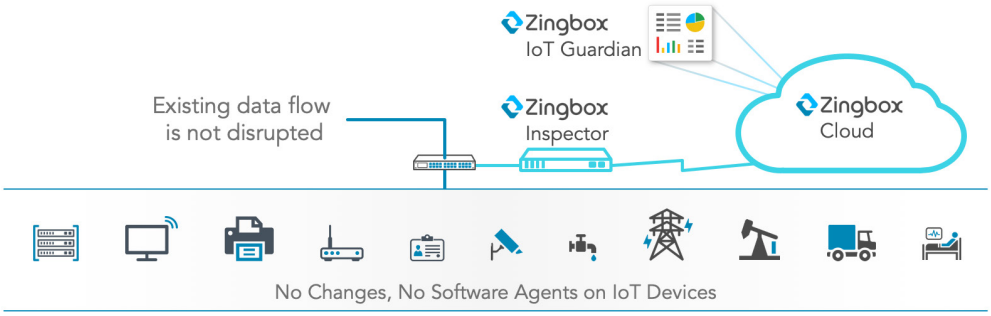
- Minimize downtime through predictive maintenance
- Simplify the monitoring, reporting, and upgrading of IoT devices
- Provide central management of IoT devices across cities, states, and countries

Optimize

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

Deployment

Zingbox IoT Command Center is a cloud-based, easy-to-deploy solution that seamlessly integrates with existing security infrastructures.



Integrations

With the broadest portfolio of integrations available, Zingbox makes it easy to integrate with existing, previously standalone systems (SIEM, NAC, and firewalls) and orchestrate all integrated activities from a single pane of glass. Zingbox can also harness IoT data from integrated systems to enhance its business insights.

Support Services

Zingbox ensures you get excellent customer service, offering an array of flexible service and support options, from technical support and training to professional services and ongoing management.