Zingbox IoT Command Center – Cisco Integration

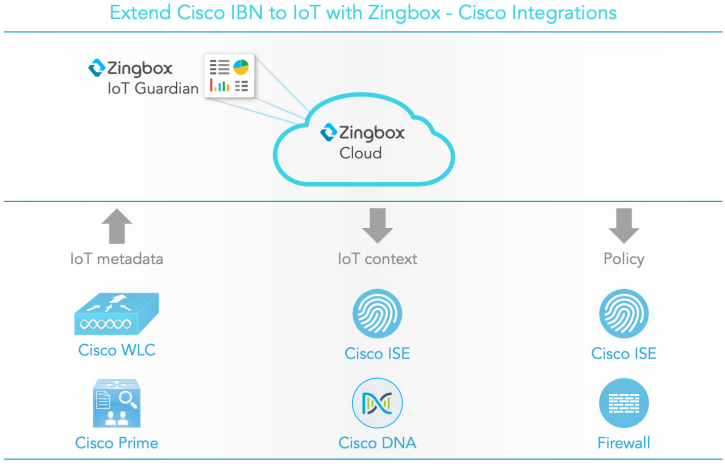
According to the McKinsey Global Institute, 127 new IoT devices connect to the Internet every second.[1] These devices are attractive targets for cyber criminals and there are many solutions available to help solve the security problem for IT and IoT. However, the integration between these solutions is often an overlooked yet critical component for the management and security of IoT devices.

Zingbox IoT Command Center provides advanced IoT solutions that complement organizations' existing management and security solutions such as Cisco DNA Center and ISE. The integration between Zingbox and Cisco technologies represents the first and true integration between IT and IoT and eliminates the need to administer multiple, disparate systems.

Cisco-Zingbox integration

The success of intent-based networking and Cisco DNA Center's ability to capture business intent and automatically configure networks to adapt to ever-changing business needs is dependent on understanding the context of devices. However, largely due to the lack of device agents, most IT departments have no visibility into the make, model, behavior, or vulnerabilities of unmanaged IT and IoT devices accessing their network.

By integrating Zingbox and its unique IoT lifecycle management capabilities with Cisco environments, the vision of intent-based networking can be fully realized.

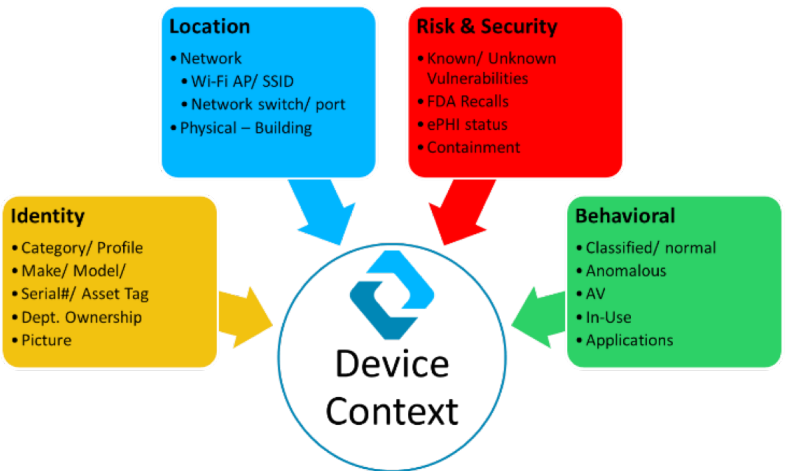


1 Christo Petrov, "Internet of Things Statistics 2019", Stats Attack (blog), Tech Jury, March 22, 2019, https://techjury.net/stats-about/internet-of-things-statistics/

Zingbox IoT Command Center is an IoT lifecycle management solution that automates the orchestration of the IoT lifecycle to provide security, optimization, and management of all your assets. At the heart of IoT Command Center is Zingbox IoT Guardian, which creates a baseline of normal behavior for each IoT device, continuously monitors it for anomalous behavior, and then alerts administrators whenever it finds such anomalies. Zingbox IoT Guardian adopts a unique, IoT personality-based approach to securing, managing, and optimizing IoT devices throughout their entire lifecycle, from discovery through retirement. It allows customers to automate threat detection and response for their IT and IoT infrastructures from a single system.

Asset Discovery and Management

Zingbox IoT Guardian complements Cisco ISE (Identity Services Engine) by allowing organizations to enrich custom endpoint attributes on an ISE instance with Zingbox-learned device profiles and alerts.

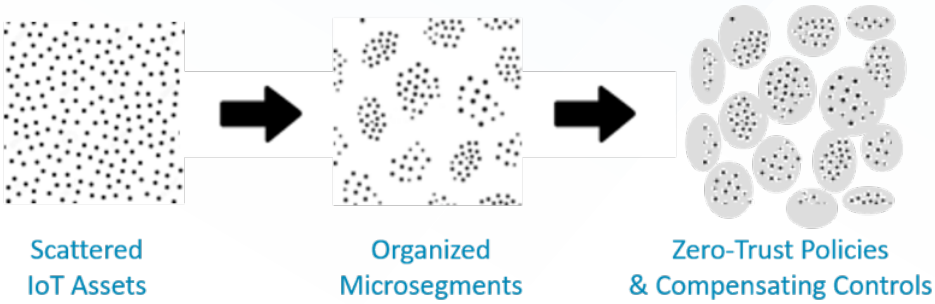


IoT Guardian discovers, identifies, and inventories IoT devices through its always-on machine-learning algorithm. It shares its contextually enriched actionable device data with Cisco ISE through Cisco pxGrid, a platform that enables various network security products to share information so they can discover and respond to threats quickly. ISE can then use these comprehensive profiles in network access control policies and segmentation to more effectively reduce risk exposure.

The integration of Zingbox IoT Guardian and Cisco WLAN controllers provides rich network contexts of access points, wireless clients, and their applications to enable further policy enhancement from Cisco ISE. The visibility of connected Bluetooth devices in the network and their granular location information (example: floor/desk) helps organizations to maintain an optimized IT and IoT network with the lowest cost.

Microsegmentation

Zingbox can transform networks from scattered and manually provisioned IoT devices to a well-organized, microsegmented one. Zingbox IoT Guardian allows its AI-derived device context to be shared across the network to enable dynamic segmentation for reduced risk exposure.



Cisco ISE uses the actionable information about device context to organize scattered IoT assets more effectively into “security groups” and categorize the network into IoT context-aware microsegments (Figure 3). Based on preconfigured rules, devices can be automatically assigned to different VLANs for access control. Devices can also be manually quarantined through ISE to mitigate risk and later removed from quarantine once the threat subsides.

Policy Definition

Zingbox IoT Guardian continuously monitors and learns real-time behaviors of IoT devices and generates profiles, tags, and ACLs within Cisco ISE and TrustSec to implement automatic IoT device onboarding and dynamic access control. It can apply principles of least privilege to IoT assets and generate ACLs to only allow trusted behaviors.

For example, unauthorized Bluetooth devices or rogue devices continue to be a serious security threat. Policies can be created that determine how to contain rogue endpoints and then automatically isolate and disconnect a device to contain the threat.

Security Enforcement

Using AI-learned normal behaviors of IoT devices, Zingbox IoT Guardian can detect any deviations or compromises, and integrate with Cisco ISE, TrustSec, Prime, or DNA Center for real-time threat detection and containment.

Zingbox IoT Guardian provides organizations with a much richer, more comprehensive understanding of managed and unmanaged IT and IoT devices, and their behaviors and risks. With this knowledge, organizations can better detect misconfigurations and anomalies that threaten network security. IoT Guardian also provides a simple, centralized, and automated way to manage the entire IT/IoT network.

For example, a Zingbox-Cisco Prime integration works by importing device (or endpoint) information from the Cisco Prime infrastructure into IoT Guardian and incorporating this information into the data it has already gathered about the devices being monitored. With this enriched information, IoT Guardian can provide more granular endpoint reports that give customers holistic visibility into unmanaged IT and IoT devices, eliminating IoT security and management blind spots.

Conclusion

Zingbox complements Cisco environments such as Cisco DNA Center, ISE, TrustSec, Prime and WLC by making full contextual device data available to customers, a critical requirement to enable intent-based networking.

By combining Cisco information with the data IoT Guardian gathers, organizations can enrich their Cisco environments with real-time, contextual IoT data and gain the ability to secure, optimize, and manage IoT devices throughout their entire lifecycle.

With a Zingbox-Cisco integration, customers no longer need to deploy separate solutions and resources to manage their IT and IoT infrastructures. They can expand the devices they manage while continuing to use tools they are already familiar with. Not only does a Zingbox-Cisco integration maximize the ROI for customers, it also optimizes business outcomes and streamlines day-to-day operations.