Zingbox

Zingbox IoT Guardian™ — Cyber Catalyst Designation

Zingbox IoT Guardian™ has been designated a 2019 Cyber Catalyst solution. It is an Artificial Intelligence-powered, cloud-based platform that discovers, secures, and optimizes Internet of Things (IoT) devices. Its management console enables monitoring of IoT devices across multiple sites via a "single pane-of-glass" dashboard providing both security and operational views.

Unmanaged IoT devices now represent 50% of the endpoints on an organization's network, but traditional endpoint and network security solutions designed to protect computers and smartphones cannot secure internet-connected IoT devices — leaving networks vulnerable to a wide range of cyber threats.

Zingbox IoT Guardian™ uses machine learning, artificial intelligence, and threat intelligence to discover, secure and optimize IoT devices on the network, via three functional modules:

- **Discover** — Zingbox IoT Guardian Discovery

  – Automated, real-time, agentless device detection using machine learning.

  – Identifies and classifies all IoT devices on the network.

  – Monitors and baselines normal device behavior, including communication to the internet and with other devices.

- **Secure** — Zingbox IoT Guardian Security

  – Real-time risk assessment, threat detection, and automated remediation of compromised devices.

– Recommends context-aware network segmentation to reduce threat exposure.

– Performs vulnerability assessments across full IoT device inventory.

– Monitors communications to send alerts and quarantine compromised devices.

– Maintains audit trail to facilitate compliance reporting.

– Integrates with key enterprise security, network and asset management, and trouble ticketing systems.

- **Optimize** — Zingbox IoT Guardian Insights

  – Captures device utilization and maintenance information for IoT devices across the organization

  – Provides deep operational insights on devices to help minimize downtime, reduce total cost of ownership, and improve capital planning.

Zingbox positions IoT Guardian as optimal for any enterprise with a broad set of IoT and unmanaged devices on their networks; security-conscious organizations concerned about IoT network endpoints; regulated industries handling private customer or patient data; and organizations with a shortage of security personnel.

Product information provided by Zingbox

MARSH & McLENNAN COMPANIES

Why Zingbox IoT Guardian™ is a Cyber Catalyst-Designated Solution

Participating insurers rated Zingbox IoT Guardian™ highest on the criteria of viability and flexibility.

In their evaluation, insurers characterized the Zingbox IoT Guardian™ as:

- "Incredibly unique product and approach. With device connectivity becoming the norm, this product addresses the single largest unknown over the new few years and will help companies get ahead of the curve, especially in device-intensive industries like healthcare and finance."

- "Nice data extrusion monitoring system for IoT."

- "Targets a niche in network traffic monitoring – strong use case for healthcare, industrial and manufacturing sectors."

Insurance Policies and Implementation Principle

Organizations that adopt Cyber Catalyst-designated solutions may be considered for enhanced terms and conditions on individually negotiated cyber insurance policies with participating insurers.

Those insurers, when considering potential policy enhancements, will expect organizations to deploy Cyber Catalyst-designated products or services in accordance with certain "implementation principles" that have been developed by the insurers with vendors of Cyber Catalyst-designated solutions.

The implementation principle for the Zingbox IoT Guardian™ is:

- Zingbox IoT Guardian™ has been configured to see all traffic in an internal network.

Evaluation Process

Applications for evaluation of cybersecurity solutions were accepted from March 26 through May 5, 2019. More than 150 cybersecurity offerings, spanning a broad range of categories from hardware to messaging security to IoT security, were submitted for evaluation. Cyber Catalyst participating insurers evaluated eligible solutions along six criteria:

1. *Reduction of cyber risk.*

2. *Key performance metrics.*

3. *Viability.*

4. *Efficiency.*

5. *Flexibility.*

6. *Differentiating features.*

Cyber Catalyst designation was awarded to solutions receiving positive votes from at least six of the eight participating insurers, which voted independently. Neither Microsoft — which served as technical advisor — nor Marsh participated in Cyber Catalyst℠ designation decisions.

The next Cyber Catalyst program is expected to open in 2020.

For more information on the Cyber Catalyst 2019 designated solutions or the program, visit the Cyber Catalyst pages at www. marsh.com/cybercatalyst.

For more information about Marsh's cyber risk management solutions, email cyber.risk@marsh.com, visit marsh.com, or contact your Marsh representative.

For more information about the Zingbox IoT GuardianTM, visit https://www.zingbox.com/iot-guardian/.

2019 CYBER CATALYST DESIGNATED SOLUTIONS

In the inaugural Cyber Catalyst program, 17 cybersecurity products and services have been designated as Cyber Catalyst solutions. More information about all the 2019 Cyber Catalyst-designated cybersecurity solutions is at www.marsh.com/cybercatalyst.