Zingbox

Enabling ZingBox to Secure the Internet of Things

Securing a Container-based Security Solution Running on AWS

Company

Enabling the Internet of *Trusted* Things, ZingBox provides hospitals, companies and manufacturing facilities with Internet of Things (IoT) security solution that ensures service delivery.

PROJECT SUMMARY

Provide deep visibility into container traffic running inside of AWS-based Internet of Things security solution.

ENVIRONMENT

Must keep containers safe and secure in runtime environment so that customer data never leaves the cloud.

- ✓ AWS
- ✓ Docker
- ✓ Open Shift
- ✓ NeuVector Container Security

TAGS

Customer, IoT, healthcare, container, multi-vector, cloud security

ZingBox is dedicated to enabling the Internet of *Trusted* Things meaning the company is in the business of providing leading edge security solutions for IoT devices across multiple industries including healthcare, manufacturing and enterprise.

To deliver a SaaS service with rapid and seamless feature enhancements, ZingBox built its solution on a container-based architecture running on AWS. The containers manage volumes of extracted IoT device data flowing from a customer's network into the ZingBox cloud instance where the data is monitored, analyzed and protected from malware, DDoS and other malicious attacks.

ZingBox's architecture demands a container-specific firewall capable of continuous monitoring and deep visibility into the east/west container traffic. Additionally ZingBox demands an automated runtime solution so that customer data never leaves the ZingBox cloud.

"Being a security company ourselves, we knew we needed to find a unique, container-specific security solution for ultimate protection. We rely on NeuVector to provide deep protection of our containers. NeuVector exposes the latest security issues and we were thrilled with its rapid deployment, requiring only two days to deploy."

- Jianlin Zeng, VP of engineering and co-founder, ZingBox

The NeuVector Solution

ZingBox quickly realized the need for a security solution built specifically to address the needs of container-based architecture. They turned to NeuVector with its unique Multi-Vector Container Firewall combining east/west container firewall capability with container protection and host security.

Additional NeuVector strengths important to ZingBox include:

- ✓ Capability to find threats in real-time
- ✓ Ease of deployment and minimal configuration requirements
- ✓ Runtime solution means customer data never leaves the ZingBox cloud.