Case Study: IoT Security for the Connected Kitchen

Situation

A fast casual restaurant chain with over 3000 locations has invested heavily in advanced IoT and OT capabilities and plans to aggressively add more internet-connected systems. The biggest roadblock? These same IoT applications and devices that provide them competitive service and margin advantages had also become their largest cyber attack surface.

Corporate Compliance and Risk identified the IoT attack surface as the top threat to the company because of potential disruption to operations and food safety, impacting customers, employees, and profitability. In addition they were alarmed about reputation damage in the event of a breach and data theft, and potential for higher employee turnover. Competitors had suffered cyber attacks that crippled operations, disrupted customers and supply chains, and resulted in losses totaling hundreds of millions of dollars so the industry was already on notice to improve IoT security.

VIAKOO

Outcome

Initial evaluation of the Viakoo solution was performed in a Corporate test kitchen facility, where it was determined that goals were met in terms of accuracy of asset discovery, speed of remediation, and ability for Viakoo to be deployed quickly at all locations without significant training.

Rollout happened on a regional basis, with all regions deployed within 4 months. Once deployed, long standing vulnerabilities were addressed, such as ensuring all food preparation devices were on a different network than customers could access and having all devices kept at the latest version of firmware.

As their CISO was able to proudly say at the next board meeting “we’ve done more to reduce corporate risk and improve worker and customer safety by deploying Viakoo than any otht".. Going forward all new systems being added had to be interoperabile with Viakoo, and all supply chain partners were encouraged to use Viakoo.

Solution

The unique nature of a food service operation put some additional constraints on the solution needed. It needed to meet all of the Corporate compliance requirements, be easily auditable, work at all times, and generate key reports. Because the IoT systems deployed were not using standard operating systems (and new types of devices would need to be deployed in the future), the decision was made to only focus on agentless security solutions that did not require software being placed on devices. To quickly scale across multiple locations, only cloud-based SaaS offerings would be considered.

With these constraints in mindш Corporate Security defined the solution as needing the following capabilities:

- Highly accurate device and asset discovery
- Vulnerability reporting based on CVEs
- Remediation of vulnerabilities by updating firmwareш changing passwordsш and using certificates to authenticate devices
- Ability to operate across all locations or just a single location

Challenges

Because of the nature of a fast casual restaurant, some key challenges had to be addressed before deploying a solution at the store level:

- No onsite hardware or need to send IT staff onsite
- Uses existing network without modifications
- Limited or no need to train employees on the solution
- No impact on service delivery or customer experience

At the corporate level, some additional challenges were identified:

- Ability to federate data across stores and geographies
- Historical data being maintained for forensic investigations
- Easy to deploy as new locations are added
- Showing ROI within a year