CASE STUDY

HOW A TOP 5 CLOUD PROVIDER SECURES IOT DEVICES FOR ITS DATA CENTERS WORLDWIDE

This multi-billion dollar cloud provider builds, tests, and manages applications and services for Global 2000 companies. To support this growing business, this cloud provider is building data centers in dozens of locations around the world. The data centers are a source of fast-growing revenue. Protecting and maintaining efficient operations of the data centers themselves was essential for safety, brand reputation, and continued customer satisfaction of this large and growing corporation.

THE PROBLEM

IoT devices required to manage data centers

The explosive growth of the SaaS offerings and subsequent growth of the data centers needed to support those offerings presented a logistical challenge. How to control access to smart buildings around the world? How could the company maintain and monitor the temperature and humidity levels required to keep the hardware housed in the data centers running safely and efficiently? These questions were largely handled by IoT devices such as door card readers, CCTV cameras, temperature sensors and other HVAC controls.

IoT devices increase the attack surface

As this cloud provider connected more and more IoT devices to their networks to optimize operations, the company boards became increasingly concerned about the expanding attack surface and corporate liability they represented. Because these connected devices can't easily be protected by agent-based technologies — and are often unpatched or misconfigured — they can be compromised by adversaries who pivot deeper into corporate networks to threaten safety, cause downtime, steal intellectual property, conduct ransomware attacks, and siphon resources for DDoS botnets and cryptojacking.

HIGHLIGHTS

- Multi-billion dollar organization turns to IoT devices to help manage growing number of data centers
- IoT devices are difficult to inventory, manage, and protect using traditional IT security tools
- CyberX provides agentless security through asset discovery, vulnerability management, continuous threat monitoring, and integration into existing IT security stacks
- With CyberX in place, organization is able to continue to expand data centers and grow cloud services while mitigating risk posed by IoT devices

THE SOLUTION

CyberX Provides IoT Asset Discovery

After meeting CyberX representatives at a security conference the cloud provider wasted no time setting up a proof of concept to see if CyberX could help mitigate the problems posed by the increased attack surface. Initial results were encouraging. Remarked one evaluator: "Within minutes of connecting, the asset map was filling up with the devices we knew we had and other devices which we either weren't aware of or had forgotten about."

CyberX Provides Unified IT/OT Security Monitoring & Governance

In addition, the evaluation required that CyberX send alerts to a SIEM. The evaluators expected CyberX to require days or weeks to integrate with their existing SIEM, but the CyberX alerts were operationalized in the SIEM and providing threat visibility in the SOC in less than an hour. The proof of concept went so quickly and successfully that the choice to use CyberX for global rollout across data centers was an easy one.

Risk and Threat Mitigation Provided by CyberX

With CyberX providing risk and vulnerability management, continuous IoT network security monitoring, and insight into operational inefficiencies, this corporation was able to answer 3 additional questions:

1) What are the risks to our "crown jewel" IoT assets – and how do we prioritize mitigation?
2) Do we have any IoT threats in our network – and how do we quickly respond to them?
3) How do I identify & rapidly eliminate inefficiencies from misconfigured or malfunctioning networks/equipment.

Why CyberX?

The proof of concept populated the asset map within minutes and was integrated with the company's SIEM ahead of schedule. In addition, the organization benefits from CyberX's recognized threat intelligence, faster and more accurate threat detection enabled by patented M2M analytics, and proven IoT security expertise.

THE BENEFITS

Reduced Business Risk

In the SaaS business, cyber risk = business risk. With CyberX in place, this Cloud Provider is able to avoid financial loss, limit corporate liability, avoid compliance violations and adverse impact to their brand, and strengthen their competitive advantage. With CyberX in place this cloud provider is able to leverage IoT technology to continue to grow and manage its data centers without sacrificing security.

ABOUT CYBERX

We know what it takes.

CyberX delivers the only cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure. That difference is the foundation for the most widely-deployed platform for continuously reducing IoT/OT risk and preventing costly production outages, safety failures, environmental incidents, and theft of sensitive intellectual property.

CyberX delivers the only IoT/OT security platform addressing all five requirements of the NIST CSF and all four requirements of Gartner's Adaptive Security Architecture. CyberX is also the only IoT/OT security company to have been awarded a patent for its M2M-aware threat analytics and machine learning technology.

Notable CyberX customers include three of the top ten US energy utilities; three of the top 10 global pharmaceutical companies; Global 2000 companies across other diverse industries including manufacturing, chemicals, oil & gas, mining, transportation, and healthcare; multiple government agencies including the US Department of Energy; and national electric and gas utilities across Europe and Asia-Pacific. Integration partners and MSSPs include industry leaders such as Splunk, IBM Security, Palo Alto Networks, ServiceNow, Fortinet, HPE/Aruba, Cisco, RSA, McAfee, Optiv Security, DXC Technology, Toshiba, Singtel/Trustwave, and Deutsche-Telekom/T-Systems.

Customers choose CyberX because it's the simplest, most mature, and most interoperable solution for auto-discovering their assets, identifying critical vulnerabilities and attack vectors, and continuously monitoring their IoT and OT networks for malware and targeted attacks. What's more, CyberX provides the most seamless integration with existing SOC workflows for unified IT/OT security governance.

CYBERX
BATTLE-TESTED CYBERSECURITY

For more information, visit CyberX.io or follow @CyberX_Labs.