CASE STUDY
Manufacturing

Global Lock Manufacturer

Secures IoT Devices Using RiskSense Platform

CUSTOMER PROFILE

A global leader in manufacturing door opening solutions. Today, they manufacture a variety of locking mechanisms, including, but not limited to, mechanical, electromechanical, and electronic locks; access control smart cards; RFID readers; and more.

"I would recommend RiskSense to my colleagues without hesitation. RiskSense's technical expertise is beyond expectation. Their team is very knowledgeable about security best practices, understands IoT-specific risk factors, and provides differentiated value with the RiskSense Platform."

– CISO of Global Lock Manufacturer

THE CHALLENGE

Internet of Things (IoT) devices are gaining more and more popularity, and one major concern for manufacturers involves device security. The global company is dedicated to the security of their devices, and protection for their customers, which is exactly why they were in the market for a vendor to assess their IoT digital lock mechanisms and their associated applications and validate their security.

Although traditional penetration testing is offered by numerous vendors, IoT testing strongly differs from the traditional testing model. While many penetration testing groups could conduct these tests for the company's web applications, there were very few organizations that could test the actual locking mechanism. They needed to find a vendor that could understand how the IoT device works and communicates to find any weaknesses that could be exploited by malicious adversaries.

The company's engineers had looked at several vendors and were introduced to RiskSense through Level 3 Communications (now CenturyLink). After meeting the RiskSense team, the company's engineers were impressed with their approach, including their testing methodology.

THE SOLUTION

RiskSense conducted penetration testing services for several of the company's locking mechanisms and their associated web applications. The company sent RiskSense a laptop with software to register key cards and two locking units (Wi-Fi and Ethernet) for testing. When conducting IoT assessments, RiskSense builds a customized testing process based on device functionality.

In order to address the unique needs and requirements for IoT device testing, RiskSense delivered a specialized penetration test assessment report via the RiskSense Platform containing the methodology used to conduct the tests, the vulnerabilities discovered with supporting evidence, and steps to remediate the discovered vulnerabilities. RiskSense provided the company with an executive summary report for a high-level overview of the assessment results and a developer report with detailed findings and remediation strategies.

The RiskSense Platform provided near-real time results for faster remediation efforts.

"The RiskSense Platform provided us with near real-time results, allowing us to make changes along the way, rather than having to wait for a final report. There is no other company out there doing this-amazing."

– CISO of Global Lock Manufacturer

The RiskSense Platform provided the company with a comprehensive view of their IoT device and application security posture. The Platform provided the company with near-real time results, allowing them to start remediation efforts within hours of the initial penetration testing and long before the final penetration testing report was delivered. This capability, and the near real time view into the penetration results, allowed the company to start the remediation process of securing their applications and devices, validate that remediation efforts were completed, and see how addressing vulnerabilities improved their security posture.

THE RESULTS

The company was impressed with the extent RiskSense tested their devices and presented the findings. Instead of being provided with a spreadsheet of vulnerabilities like many other companies, RiskSense provided the company a detailed report with the discovered vulnerability, proof of compromise, and a concrete remediation strategy. In addition to the report, RiskSense had meetings with the team to discuss the findings and provide additional context as needed.

The company found value in the way that RiskSense managed the project. The way RiskSense approached the project resonated with the team, pushing their engineers to think outside of their traditional penetration testing approach. They were impressed with the knowledge and expertise provided by RiskSense.

In addition to the services provided, the company was pleased with RiskSense's competitive pricing and overall value. The RiskSense Platform's near real-time delivery of results allowed the company to take remediation steps along the way instead of having to wait for the delivery of the final report.

NEXT STEPS

As a global company, each division of the company currently operates as separate business units. They are currently working on taking a unified approach to the products they deliver and the vendors they use. The company's CISO is part of a global security council. He is working on aligning key vendors globally. He and his boss aim to conduct penetration tests an annual basis across their business units.

In the future, he plans on strengthening the partnership by participating in an IoT conference with RiskSense and bringing in the RiskSense team to speak to the company's security council.

WHY RISKSENSE

In-depth penetration testing for applications and IoT devices
Near-real time result delivery, allowing for fast remediation efforts
Efficient project management
Highly skilled security analysts
Competitive pricing with ongoing value through the Platform
Security conscious leadership

RISKSENSE®

Contact Us Today to Learn More About RiskSense

RiskSense, Inc. | +1 844.234.RISK | +1 505.217.9422 | info@RiskSense.com

CONTACT US | SCHEDULE A DEMO | READ OUR BLOG