CASE STUDY
Manufacturing

Global Secure Payment Company

Now More Secure with RiskSense

CUSTOMER PROFILE

This company provides a full range of payment processing solutions, including Internet of Things (IoT)-based solutions and Software as a Service (SaaS) connectivity solutions for payments. The goal of this division of the company is to connect hardware to networks to communicate data and secure the information transmitted.

"The specific, detailed examples that RiskSense provided really illustrated what our risks were, provided guidance on mitigating IoT device findings, and drove changes in our application security program. This was amazing"

– Director of Operations

THE CHALLENGE

At the corporate level, the company has had an information technology (IT) security program in place for years. It operated a traditional cyber security program focused on protecting internal systems and data. While this protects their internal assets, they were growing more concerned with the different solutions that they sell to their customers and wanted to ensure that these devices were secure and well protected too.

In the fall of 2017, the company's Director of Operations, was tasked to put together a cross-functional team to secure all of their products, including IoT devices and physical devices that communicate with their SaaS products. They wanted to start with an initial assessment so that the team could identify their greatest vulnerabilities and security risks. Around that time, he was put in touch with CenturyLink through the company's CIO. He shared with CenturyLink their goal to run these assessments through penetration testing as that would provide a good baseline to assess the security of these devices.

A big challenge was that although traditional cyber security penetration testing is offered by many vendors as commercial scanning tools, IoT testing is different from the conventional model. Because of this, the company needed to find an organization who could examine the device, understand its application, and analyze the device's physical risks with expertise in IoT and the unique challenges IoT devices present. Another challenge was the company's thousands of devices that are spread across both North America and Europe. They would need a solution that would minimize service visits and support over-the-air patching.

With prominent breaches featured across news headlines, the team wanted to make sure that they acted quickly to get their older devices secured. The company needed to find a vendor who could conduct their comprehensive assessments on both their web applications and their physical IoT devices. After hearing all of their challenges, CenturyLink suggested that he talk with the RiskSense team about how they could assist with the company's security penetration testing needs.

THE SOLUTION

After meeting with RiskSense and hearing how their penetration testing services could assist the company with their goals, he was impressed with how knowledgeable the team was with IoT penetration testing compared to other companies. Because of this, they decided to bring in the RiskSense penetration testing team.

RiskSense discovered unique IoT vulnerabilities and provided comprehensive remediation tactics.

"Getting this project completed quickly was critical for the success of our business, and RiskSense maintained the sense of urgency needed to get the job done."

– Director of Operations

The company supplied RiskSense with several devices for testing, and RiskSense's security analysts employed a methodical testing approach--understand how these devices operate, analyze their communication methods, and search for common vulnerabilities and, more importantly unique, device-specific methods of compromise. In one instance, RiskSense was able to compromise the method the company used for updating their devices, providing the analysts the ability to push out updates to these IoT devices over-the-air. The analysts found other unconventional methods to compromise these devices that surprised the company, and showed how thoroughly RiskSense tested the devices and applications.

Finally, at the end of the assessment process, RiskSense's security analysts provided his team with a comprehensive exit briefing. This would be an educational meeting where RiskSense security analysts would train the team and present them with finding demonstrations so the company could improve their internal processes.

THE RESULTS

RiskSense provided the company with access to the RiskSense platform and daily updates when any compromises were found. This was unique and allowed the company to start remediation efforts as soon as the testing began. In addition, RiskSense provided a two-part report at the conclusion of their penetration testing that the company could utilize to review their remediation efforts to date and ensure that going forward they had these compromises documented. The first report was an executive summary of the complete assessment. He was able to bring this to the company's CEO and have a candid conversation about the results. The second report provided more details for the engineers, including graphics highlighting the vulnerabilities found.

These reports were delivered through the RiskSense Platform. The company received huge value from these reports as they documented vulnerabilities that they had never accounted for. RiskSense provided them with specific examples and detailed information that illustrated where their biggest risks were. In addition to delivering the reports, the RiskSense Platform provides context to threat and vulnerability data, prioritizes remediation efforts, and provides visibility through rich, interactive visualizations. The Platform provided synchronous delivery of results, so the company could track vulnerabilities as they are discovered and begin the remediation process before the final report's delivery.

Additionally, RiskSense provided guidance on how to mitigate these findings, both immediately and in the future. The team at the company then took this information and was able to instantly start strengthening the security of their IoT devices.

He thought the project was well planned and executed and the team was amazed with the achieved results. Due to their critical need to complete this project, the company appreciated the sense of urgency shown by the RiskSense team.

NEXT STEPS

In addition to their current application and IoT testing, the company is also looking to conduct a network assessment with RiskSense in the future. They have also started to discuss how the RiskSense Platform could benefit their risk management efforts. One thing that the team is very interested in is the RiskSense Security Score (RS3) and would like to see how that could work with their IoT devices. The company and RiskSense look forward to maintaining a strong relationship as their partnership expands.

WHY RISKSENSE

Synchronous delivery of penetration testing results allows for faster remediation
Comprehensive IoT and web application assessment reports with detailed findings and remediation steps
Highly skilled security analysts with experience in IoT testing
Excellent project management and collaboration
Efficient and comprehensive testing with swift result delivery

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