CASE STUDY

How One Manufacturer is Managing Risk in a Connected World

When one manufacturing company's IT leadership team realized the firm's security posture needed to evolve to modern industry standards to protect itself against the readily available malware used by modern malicious actors, it sought to expand its security portfolio by partnering with Trustwave.

Trustwave®

Client Spotlight

As a large supplier of fixed and configurable components for the manufacturing industry, security is a top priority for both the organization and their partners. In a move to transform its security posture, the organization partnered with Trustwave in 2018. One of its senior executives proved to be pivotal in the evolution of the company's security posture with Trustwave.

The Challenge

When the executive first joined the company five years ago, he came prepared with a list of due diligence questions on the status and capability of the organization's security programs. The executive quickly became concerned when he could not obtain answers for basic questions, such as when was the last time the firm conducted an audit. Considering the company operates in a world where the number of threats being faced daily is extensive, and even non-tech savvy threat actors have easy access to off-the-shelf malware, the executive knew changes had to be made quickly.

Industry Threat

Historically, the manufacturing sector has been less susceptible to cyberattacks as its operational technology generally did not face the Internet. However, this has changed over the last few years, with OT systems now being directly connected to the web. By being so exposed, threat actors can endanger companies by using readily available threat tools, such as ransomware-as-a-service.

"You couldn't partner with a better company to develop both a foundational understanding of security and what needs to be done in an organization, helping educate the end-user and providing critical resources in times of need."

The Solution

One of the executives first orders of business was to gain a stronger sense of its overall security posture. Since the organization had no standardized security audit process in place, he sought out a trusted partner in Trustwave. In 2018 the security firm conducted an in-depth review of the company's security system against third-party best practices and began testing the organization's defenses with red team engagements.

The first red team probe indicated the organization had more than 100 weaknesses. Some of the issues uncovered were the use of vulnerable legacy software and a problematical operating system that threat actors often attacked.

Once this stage was completed, Trustwave brought the company's leadership to its Chicago headquarters to discuss the audit's findings. During this meeting, a specially designed 13-point plan to bolster the firm's cyber defenses was also discussed. Over the next year, implementation of the plan took place.

Eighteen months later, Trustwave conducted a second audit and found the company's security posture had dramatically improved. The two companies now hold quarterly pen tests to maintain progress.

With the Trustwave team on board, the client had the breathing room to raise its overall cybersecurity standards. The company began taking an asymmetrical approach to its security, implementing several new tactics. One such tactic was to suddenly make their IT environment different to throw off attackers. The internal IT team replaced its Windows machines with Macs that run Windows in only a VM environment. Additionally, the organization is looking at cloud-based solutions to replace their inherently weak Active Directory with a third-party product.

"When our day-to-day business isn't IT security, we can't rest on our laurels and say, 'we're secure' after an audit is complete," the executive said. "The work needs to be ongoing; having a partner as sophisticated as Trustwave ensures we're actively testing hypotheses and applying best practices to keep our security at the industry forefront — where it needs to be."

Trustwave®

CSMan_0122