CASE STUDY

MELILLO BRINGS MANUFACTURING COMPANY BACK FROM A CRIPPLING RANSOMWARE ATTACK

MELILLO
CONSULTING

Overview

When a leading manufacturer of HVAC equipment was hit by a ransomware attack that had the potential to destroy the business, they turned to Melillo to remediate the attack, build a new environment in the Azure Cloud, and fortify it from future attacks.

Challenge

The manufacturing company fell victim to a ransomware attack, bringing the business to a complete standstill. They needed help remediating the attack to stop further damage, backing up the data to the Azure cloud, and securing the environment to prevent reinfection. Melillo was selected as the partner of choice based on their advanced security expertise and reputation for delivering innovative solutions to complex problems.

> "They first identified how the customer was attacked, what was attacked, and what data the cyber hackers had gotten a hold of—then locked it down to prevent further damage. Working with the customer's internal IT team, as well as local law enforcement, the FBI, and its insurance company, the Melillo team took a systematic approach to remediating the attack."

Solution

Melillo immediately stepped in to stem the bleeding. They first identified how the customer was attacked, what was attacked, and what data the cyber hackers had gotten a hold of—then locked it down to prevent further damage. Working with the customer's internal IT team, as well as local law enforcement, the FBI, and its insurance company, the Melillo team took a systematic approach to remediating the attack. They identified the vulnerabilities that left the organization open to the large-scale attack, restored the customer's data, rebuilt the environment in the Azure cloud, validated applications, and remediated issues that arose during the verification process—ultimately fortifying its environment against future attacks.

Results

By the time Melillo intervened, the customer's business had already come to a total halt. Within days of Melillo's involvement, they were back up in a limited capacity, and operating at 100% within a week and a half. Today, the customer enjoys a secure infrastructure that's protected against reinfection. In the words of the company's CIO, "If we hadn't had Melillo, we would have gone out of business."