CASE STUDY

enVista®

Global Company Overcomes Ransomware Attack with enVista's Rapid Response & Cloud-First Rebuild

A fast, structured recovery helped restore operations after a ransomware event put the business at risk.

ABOUT

The client is a U.S.-based global company supporting distribution and fulfillment operations. Their business relies heavily on warehouse systems, infrastructure and network connectivity to keep daily operations running.

SCENARIO

The client experienced a ransomware attack that quickly disrupted operations and took critical systems offline. The incident stemmed from gaps in security at the network edge, which allowed unauthorized access into the environment.

Once inside, the threat actor was able to move across systems and ultimately encrypt production environments, making key applications unavailable. At the same time, the company's backup approach did not provide the protection needed in a situation like this. Backups were stored within the same environment and had not been consistently validated or isolated.

As a result, much of the data was rendered inaccessible, and the organization faced the loss of more than a year of operational history. The impact was immediate – systems were down, operations came to a halt, and without rapid recovery, the business risked being unable to continue operating.

SOLUTION

The client turned to enVista to lead the response and recovery effort. The immediate priority was to contain the situation and stabilize the environment.

Given the level of compromise, enVista recommended rebuilding rather than attempting to restore the existing environment. The team took a cloud-first approach, standing up a new environment in Microsoft Azure and restoring critical workloads needed to bring operations back online bypassing outdated hardware, reducing time to procure and deploy their environment. This ultimately provided the client with a new Operational Expenditure (OpEx) model versus having to go through budgeting and planning for a larger Capital Expenditure (CapEx) model.

At the same time, enVista addressed the underlying issues that contributed to the attack. This included implementing multi-factor authentication, resetting credentials and putting stronger access controls and monitoring in place. The rebuilt environment was designed to be more secure, more resilient and better suited to scale with the business.

Beyond the immediate response, the engagement reinforced the value of augmenting internal IT capabilities with a specialized cybersecurity partner. By leveraging enVista's dedicated team, the organization gained continuous expertise, improved risk posture and reduced reliance on internal resources for ongoing security operations.

RESULTS

enVista helped the client regain control of its environment and restore operations after a situation that could have resulted in long-term business disruption.

The company was able to restore shipping operations, re-establish core processes, and move forward with a more secure and modern foundation. Beyond recovery, the engagement positioned the client for future improvements, including expanded managed services and continued security enhancements.

Additionally, the organization is now better protected against future risk through a more resilient operating model that incorporates third-party expertise and reduces dependency on any single internal team member.

A recurring theme that has emerged is that companies should not take a "do-it-yourself" approach to cybersecurity. Instead, organizations benefit from engaging a trusted third party like enVista to complement internal teams with an objective, outside perspective, or to fully manage cybersecurity through enVista's dedicated experts. This approach also mitigates risk associated with employee turnover, ensuring continuity and reducing dependency on any single internal resource.

Supply chains OPTIMIZED.
Results MAXIMIZED.

Let's have a conversation.®
info@envistacorp.com | envistacorp.com