Case Study

Global Packaging Firm Improves Security and Cuts Costs

The client

For going on 60 years, the client has developed innovative fulfillment and packaging solutions for global food suppliers and commercial enterprises. The company currently serves more than 100 countries, operates dozens of labs, research, and manufacturing facilities, and holds nearly 3,000 patents (including pending) worldwide.

The challenge: Balancing security, scale, and cost needs at a critical juncture

The company recently experienced significant turnover within their IT and security teams — not an uncommon event in the modern business world. Their new Chief Information Security Officer (CISO), an internal hire, believed that big changes were needed to improve the company's security posture.

With the CISO's leadership, the company had mapped out a five-year security strategy. Their plans unfortunately called for cuts on their security team due to impacts of COVID-19 on the global supply chain. Their top question was: How do we achieve our objectives with a smaller internal team? They were also concerned about current budget requirements for their existing Security Information and Event Management (SIEM), as well as their inability to scale that environment both in financial terms and skill sets.

In addition to meeting cost objectives, the CISO and team were looking to improve the company's network security through better visibility of their infrastructure and cloud environment. They wanted to alleviate internal resource constraints brought about by complex SIEM and management processes. Lastly, they hoped to reduce security alerts and transition to a managed services model for log monitoring and alert remediation.

Industry:

Fulfillment and packaging

CDCT provided:

- Security environment and existing SIEM assessment
- Design and detailed implementation of Azure Sentinel
- Cutover to Insight's Cloud Solution Provider (CSP) program
- Ongoing managed care of the new security environment

CDCT services:

- Services for Azure Sentinel
- Insight's CSP program
- Managed Security services

The solution: Shifting to a new SIEM and managed services model

To start, Insight Cloud + Data Center Transformation (CDCT) had to ensure that the company's rule customizations within their existing SIEM solution were migrated to the new solution. The client opted to implement Microsoft® Azure Sentinel™ through our Services for Azure Sentinel offering.

We properly assessed the client's current security environment, considering their business and cost requirements, industry standards, and security best practices. This foundational work enabled us to design the client's Azure Sentinel environment, ensuring no extra costs were incurred for ingestion of logs (at a rate of roughly 500GB per day) and storage of unnecessary log data.

To make the solution manageable and high performance over time, we brought the client into Insight's Cloud Solution Provider (CSP) program and Managed Security services. The CSP program gives the client the ultimate in flexibility, visibility, security, and control over their Azure® cloud, with ongoing cost benefits. Our Managed Security services help the company ensure all systems are safe and secure, leveraging a combination of Azure Sentinel tools and our experienced security professionals.

The benefits: A more secure and lower maintenance environment

The client has been able to reduce their log data ingested, reduce security alerts, and reduce remediation needed by their internal team by working with Insight throughout this project and into the future. Both near- and long-term cost targets are being met, while the client benefits from a more scalable and intelligent security environment. This was all accomplished despite the generous size and scope of the client's environment and the high degree of customization required for queries, workbooks, and playbooks for automation.

Benefits:

- Better scalability and cost-efficiency
- Successful move off existing SIEM to Azure Sentinel
- Seamless transition despite extensive customization and scope
- Fewer security alerts and less log data ingested
- Less remediation required thanks to Managed Security services team
- Improved visibility and control
- Greater cloud cost savings through Insight's CSP program