CYBER AND DATA SECURITY
CASE STUDY

Multinational Healthcare Company Successfully Integrates Global IT Infrastructure After Acquisition

OVERVIEW

Our client is a leading multinational healthcare company with operations in over 100 countries. They had recently completed an acquisition of a technology company that also has a global footprint. Given the increasing number of high-profile breaches following a merger and acquisition, our client needed to ensure the integrity of the acquired company's technology assets before permitting access to their systems.

The Challenge

Data breaches from acquired companies, from subcontractors or partner agencies, can result in the transmission of malicious code, stolen or corrupted data, access interruptions from denial of service attacks, and other network security threats. In addition to the theft of critical assets and intellectual capital, a denial of service attack can completely halt a production line, resulting in significant income and productivity losses.

Our client came to Ensunet after they had completed an in-depth NESSUS security scan that identified multiple security vulnerabilities in the acquired company's servers, workstations, PCs and other devices. The specific goal of our cyber and data security remediation were to:

- Bring the IT assets of the acquired company up to the information security standards of the parent company to minimize the risk of the cyber theft of intellectual property and sensitive business information
- Complete the remediation process quickly and efficiently to enable other post-acquisition initiatives and activities to finally commence

The Strategy

Streamline the process of remediating the servers, workstations and other devices, such as networked printers. Using the results of the NESSUS scan as a starting point, Ensunet proceeded to implement cyber security remediation for two data centers and 10 global offices. The remediation would involve 800 servers and 2,300 workstations, PCs and other devices. We developed a highly detailed, multi-phase plan that enabled us to work simultaneously on different project sites and in parallel with other coding initiatives to make efficient use of our technical teams and analysts.

Our team identified and securely isolated those servers, workstations and devices that could not be successfully brought up to the appropriate security standards. All the IT assets of the acquired company needed to receive new IP addresses that could be associated with the new parent company. Many of these assets had vulnerable systems that needed security patches or were running obsolete applications that needed to be upgraded.

Vulnerable systems that could not be brought up the security standards of the parent company were either placed into isolation VLANs (which would not permit any traffic and which would be subject to specific Internet blocking rules) or were retired from service.

Workstations, PCs or other devices	Servers
We worked on approximately 2,000 PCs and printers, of which:	**We worked on 831 servers, of which:**
• 200 required additional remediation including being placed in isolated VLANs, custom modification of their operating system, and more.	• 484 were resolved (patched or re-IP'ed) • 152 were placed into Isolated VLANs • 195 were retired

Testing

Conduct live tests to ensure that the various business processes worked as expected.

The final stage of our remediation process required us to conduct live end-to-end testing on the day of the rollout. Pre-work involved analyzing terabytes of data and was performed in multiple stages.

The Solution

The remediation process took approximately five months from start to finish, during which time we held daily standup technical meetings with assigned Ensunet personnel and close collaborative meetings with our client to keep them informed of our progress.

Our client had enough confidence with the completeness of our remediation that they were able to take down their internal firewall, allowing unfettered data exchanges between the companies. The ready access to the data, applications, and systems between the companies has permitted our client to finally move forward with several initiatives that capitalize on new synergies and shared intellectual capital.

ENSUNET
TECHNOLOGY GROUP

Ensunet provides technology and consulting services for enterprise level clients in the public and private sectors. From initiatives that support strategic planning, data center design and project resource management, we offer solutions that reduce cyber security risks and mitigate threats to your business operations. Learn more at **ensunet.com.**

ENSUNET® TECHNOLOGY GROUP