zensar

Industry Leader Boosts Resilience Against Existing and Emerging Threats

Case Study

Overview

Comprehensive cybersecurity consolidation

With a 65-year track record of pioneering and innovating, a medical equipment manufacturer built its industry leadership in respiratory diagnostics, ventilation, anesthesia delivery, and patient monitoring.

The company manufactures and markets more than 27,000 unique products for the diagnosis, treatment, and monitoring of respiratory conditions in every stage of life. As a global leader in respiratory care with operations in USA, Mexico, Brazil, Germany, and China, it needed a transformative security solution to defend against evolving cybersecurity threats.

Zensar's brief:
Enable comprehensive cybersecurity consolidation with these key moves:

- Improve email security by migrating from Tessian to Microsoft Defender for Office 365 (MDO).
- Enhance security information and event management (SIEM) by migrating from IBM QRadar to Azure Sentinel.
- Upgrade endpoint security by migrating from Palo Alto Cortex to Microsoft Defender for Endpoints (MDE).
- Optimize vulnerability management by migrating from Rapid7 Insight Vulnerability Management to Microsoft Defender for Vulnerability Management (MDVM).

Beyond the brief:
We put together a heterogeneous team of specialists for the large-scale Microsoft security transformation, delivered within an uncompromising timeline to avoid the cost impact of extending existing licenses.

Challenges

Responding effectively to sophisticated cyber attacks

In a post-pandemic world where remote and hybrid work have become the norm to ensure business continuity, organizations across the world have become more vulnerable to sophisticated cyber-attacks with the potential to severely disrupt operations.

Incompatible security tools: The client's IT department found that its existing security tools were not compatible with the multi-cloud hybrid environment, with the support teams overwhelmed with rising alert volumes and tool complexity.

Need to cut IT costs: Given that economic uncertainties were mandating IT budget cuts, it was time to re-evaluate the company's existing security tech stack to reduce its IT footprint and move toward adopting a mature cyber risk management framework.

Lean in-house team: The company's internal IT team did not have the required specialist resources to deliver a major cybersecurity consolidation project seamlessly. It needed a technology partner to transform the company's security landscape with a holistic and innovative approach.

Solution

Steering large-scale security transformation

In the interest of enabling cybersecurity consolidation, a strategic decision was made to migrate the client's existing siloed security system to the Microsoft security tech stack and upgrading the Microsoft Enterprise Mobility and Security license from E3 to E5. After performing a thorough technical due diligence of the proposed solution and its compatibility with the existing environment, we carried out deployment in four phases:

Phase 1: Improving email security with MDO

- **Assessment and configuration:** We started with a detailed assessment of the capabilities and gaps between Tessian and MDO. We then configured MDO, including Exchange Online Protection (EOP) for spam, malware, and email threat filtering, and set up enterprise policies for anti-malware, anti-phishing, and anti-spam. Advanced features such as Safe Links, Safe Attachments, and Zero-Hour Auto Purge (ZAP) were also enabled to extend the protection beyond emails, covering SharePoint Online, OneDrive, and Teams.
- **Integration and roll-out:** We integrated Azure Sentinel and rolled out the solution in different stages with thorough user testing to ensure smooth implementation. The integration helped provide a unified view of all security alerts and enhance overall SecOps functionality, providing real-time insights and a single pane of glass for monitoring security incidents across all devices.
- **Security enhancement and automation:** Leveraging industry-led AI and automation, we built email security capabilities to process trillions of signals globally each month. With the goal of enhancing overall SecOps functionality, we adopted a comprehensive approach that included multi-layer protection for all email IDs, improved blocking of malicious links and domains, and automated investigations to expedite response times.

Phase 2: Enhancing security operations with Azure Sentinel

- **Assessment and architecture design:** We began with a detailed assessment of the capabilities and gaps between IBM QRadar and Azure Sentinel. Based on this analysis, we designed and implemented the architecture of Azure Sentinel, integrating critical infrastructure, security solutions, and custom logs for comprehensive event correlation and detection of malicious activities.

.

- **Configuration and integration:** We configured security use cases according to the MITRE ATT&CK framework and integrated Azure Sentinel with the organization's ticketing tool for automated SLmanagement. Subsequently, we developed custom dashboards to monitor SecOps efficiency, traffic, and cost utilization; enabled enterprise-wide threat hunting to proactively search for threat actors; and carried out data archival from the old solution to ensure regulatory compliance.
- **Security enhancement and automation:** Leveraging Azure Sentinel's automation and SOAR capabilities, we reduced alert fatigue and false positive alerts, expedited incident response, and improved overall SecOps functionality. Next, harnessing the scale of the cloud SIEM and AI capabilities, we delivered in-built threat hunting, threat intelligence, and user and entity behavior analytics (UEBA) services. Also, the support from the SIEM community and Microsoft security experts enabled continuous information sharing and robust protection against emerging threats.

Phase 3: Upgrading endpoint security with MDE

- **Assessment and configuration:** We began with a detailed assessment of the capabilities and gaps between Cortex XDR and MDE. Subsequently, we moved endpoints and servers to Hybrid Azure AD Join to ensure MDE onboarding; configured MDE policies, including antivirus, file and folder inclusion/exclusion, attack surface reduction, and automated investigation; and made group policy object (GPO) changes to enable MDE services without impacting the existing antivirus solution.
- **Threat hunting upgradation and automation:** We enabled enterprise-wide threat hunting, based on the MITRE ATT&CK framework, to proactively search for threat actors on endpoints. By automating investigations, we helped detect and prevent sophisticated attacks within minutes. Leveraging OS native services, the cloud-enabled agentless solution enabled strong security AI and behavioral monitoring of users, files, and processes. As a result, the threat intelligence from trillions of signals globally enhanced detection and response capabilities.
- **Integration and SecOps efficiency:** We integrated Azure Sentinel to provide a unified view of all security alerts and improve overall SecOps efficiency. Moreover, we ensured comprehensive protection and enhanced security management with multiple options to expedite incident response and initiate remediation actions, in-built threat hunting and threat intelligence services, and security posture status and scores for each endpoint.

Phase 4: Optimizing vulnerability management with MDVM

- **Assessment and configuration:** We began with a detailed assessment of the capabilities and gaps between Rapid7 and MDVM. Next, we enabled the relevant permissions in the Defender portals to capture vulnerability and recommendation data for each endpoint and server. Lastly, we activated remediation actions such as remediation handling, exception handling, and application handling.
- **Enablement of interactive dashboards and insights:** We deployed interactive dashboards to provide insights into the software inventory, top vulnerability systems, most exploited CVEs, zero-day vulnerabilities, and best practices for prioritizing remediation. With this setup, we enabled real-time and deep insights into vulnerabilities and threats across devices, along with recommendations for remediation.
- **Automation and remediation:** We automated and prioritized zero-day and exploitable vulnerabilities for remediation, based on applicable risks. Next, we created an independent software usage inventory to help identify non-applicable enterprise software. Lastly, we initiated a remediation program to track progress, block vulnerable applications, and manage security exceptions, EOL/EOS devices, and applications. Overall, our approach was aimed at defining the overall security posture of each endpoint.

Throughout the four phases of deployment, we enabled seamless data movement and decommissioning of the existing solution; UAT, pre-pilot/pilot, and production rollouts; and documentation of standard operating procedures.

Impact

Enhanced security posture

- **Speed:** Built the capability to quickly detect, analyze, and respond to security incidents, minimizing the time between threat detection and mitigation.
- **Preparedness:** Leveraged intelligent technologies to not only detect known threats but also predict and adapt to new, emerging threats.
- **Optimization:** Adopted a consolidated approach to security management to ensure comprehensive protection across diverse cloud environments and platforms.

Business outcomes: By enabling greater threat visibility across the entire IT ecosystem and enhanced protection for both infrastructure and end users, the solution increased the organization's overall security posture and resilience against existing and emerging threats.

zensar

An RPG Company

At Zensar, we're 'experience-led everything.' We are committed to conceptualizing, designing, engineering, marketing, and managing digital solutions and experiences for over 145 leading enterprises. Using our 3Es of experience, engineering, and engagement, we harness the power of technology, creativity, and insight to deliver impact.

Part of the $4.8 billion RPG Group, we are headquartered in Pune, India. Our 10,000+ employees work across 30+ locations worldwide, including Milpitas, Seattle, Princeton, Cape Town, London, Zurich, Singapore, and Mexico City.

For more information, please contact: **info@zensar.com | www.zensar.com**