

US-based Pharmaceutical Company Expands Collaboration with Zensar to Secure its Digital Transformation Journey

 **Case study**



Client

The client is a US-based major pharmaceutical company manufacturing life support equipment with many remote employees. The client's existing infrastructure comprises 70% of customer devices in data centers across various locations in the United States and about 30% of applications and data in the public cloud. From a security standpoint, the client had a few existing conventional security solutions, including firewalls, identity and access management (IAM), antivirus, and public key infrastructure (PKI) solutions. The client's focus was to improve its threat detection and cost optimization through cloud transition and digital transformation in a secure way.



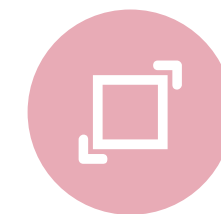
Challenges

- Siloed approach was used for monitoring the logs and alerts generated in multiple sources
- No unified solution was in place to provide comprehensive visibility of security infrastructure across on-prem or cloud environments
- Endpoint security was dependent on the antivirus solution, and advanced threat protection capabilities were missing
- The incident response framework was not in place
- No automation of repetitive tasks caused a very high mean time to remediation (MTTR)
- No threat intelligence solution was implemented to provide proactive intel



Solutions

We conducted a two-week assessment to understand the current monitoring practices. As part of the deliverable, we provided the report on the recent security monitoring coverage, possible improvements (additional integrations, use cases, runbooks, etc.), and multifold saving opportunities in terms of cost after migration to a managed security service provider (MSSP) platform.



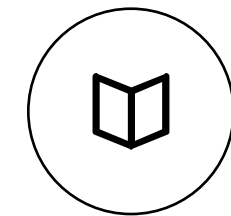
Transformation and Business As Usual Services

The key activities performed by us for the client include:

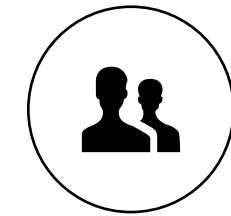
- Advanced endpoint protection solution to mitigate any zero-day attacks
- Integration and configuration of log sources, alerts, reports, threat hunting queries, and playbooks
- Automation of repetitive tasks by building the SOC workflows
- Integration of SIEM and SOAR with ITSM to improve the collaboration between Zensar and customer teams
- 24/7/365 monitoring of security incidents – L1, L2, and L3
- Creation of threat hunting queries and playbooks based on the MITRE TTP to track malicious behavior of threat actors
- Expedition of the overall cloud migration journey, helping reduce operating expenses



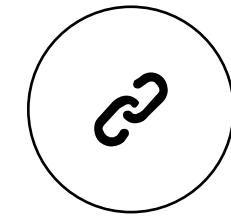
Business Impact:



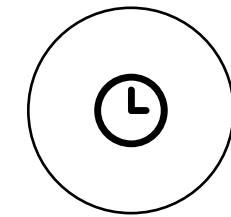
90% reduction of false positives



30% reduction in operating expenses (OPEX)



70% faster incident handling



50% decrease in mean time to remediation (MTTR)



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

