



End-to-end security services redesign enhances operations for leading risk management brokers

 **Case study**



Overview

A security overhaul

Our client was looking to streamline its security architecture in incident and problem management, change management, capacity management, log management, and security information and event management (SIEM). First, we thoroughly analyzed the security threats and provided a remediation plan. As a result, we implemented end-to-end security services that included cross-compliance mapping and improved network security and system security. We implemented all the solutions in just six months.



Challenges

Security at stake

The client's existing environment was running on legacy systems with unmanaged firewalls and servers. Many critical tools were not present, which led to mismanagement in event auditing and operational security. Lack of operational security management proliferated the security issues. There was also a risk of unauthorized access due to interception of credentials or access from non-approved management workstations.



Solution

Re-aligning the IT architecture

After analyzing the client's information technology (IT) landscape, we moved to a world-class and agile infrastructure — managed service-oriented architecture. This helped the client align its business goals with the IT architecture.

We redesigned the security services and deployed the following security components within three months:

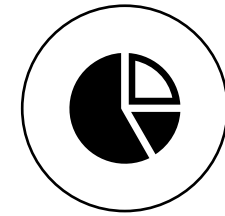
- Zscaler — for effective application of corporate and security policies
- Forcepoint Data Loss Prevention (DLP) Suite
- Cisco Managed Threat Defense (MTD)
- Palo Alto Firewalls
- Cisco AnyConnect
- Netskope Web Protection Suite

In addition, for database encryption, we implemented Thales data encryption. We also built the customized parser and playbooks as per the client's security norms. With the SailPoint identity and access management (IAM) solution, we ensured that the right employees of the client had access for the right reasons.

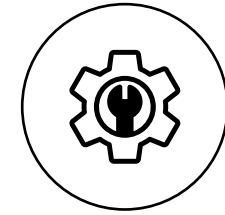


Impact

Secured environment and improved productivity



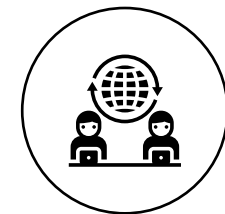
Transition and business as usual (BAU) in parallel



Service level agreements (SLAs) for infrastructure with no service level objective (SLO) period



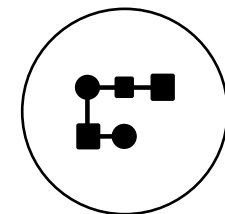
24x7 security operation center (SOC) through managed SIEM-cum-SOAR as a service platform



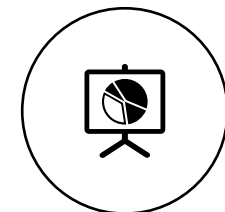
More than 70 percent of users started working remotely



Cost reduction due to effort optimization



Unified workflow with a defined framework for the problem, change, and configuration management



Dashboard and reports for analysis



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

