CASE STUDY

CLOUD ENDPOINT SECURITY MIGRATION ENHANCED SECURITY AND OPERATIONS FOR A LOYALTY SERVICES PROVIDER

Increased ROI and reduced OpEx 25-30% over solution costs with migration of TrendMicro Deep Security solution from SaaS to enterprise cloud

Client Background

A leading provider of Loyalty Services to customers around the world had matured their infrastructure in terms of policies/procedures/standards. To ensure efficient service delivery and data protection, security became the next high-priority initiative.

The client had acquired a company as part of its growth track. Both the client and the acquired company were using TrendMicro Deep Security (TMDS) for their server infrastructures with different architectures and setups. However, limited inhouse skills and experience created challenges in choosing and executing the right TMDS setup and endpoint migration strategy to achieve seamless enterprise operations.

Key Objectives

- Migrate all endpoints from SaaS TMDS solution to enterprise TMDS and deactivate SaaS subscription without any downtime
- Combine all the servers (physical, VM and cloud instances) irrespective of any OS and define the optimal Protection Policies

Xoriant Discovery & Solution

Xoriant team had performed an initial technical assessment of both SaaS and Enterprise setups:

- SaaS-based approach led to issues such as high billing rates for managing a smaller number of endpoints and for endpoint protection hours
- AWS account onboarding process was not defined in the existing SaaS setup
- Client sustained a poor compliance ratio with 7000+ stale endpoint entries, 10+ false positive alerts, unmanaged Windows machines, and limited and untested configuration of protection policies.

KEY BENEFITS

- Increased visibility, management and control of all server infrastructure; 31% increase in fully managed servers
- Improved malware protection from 9 policies to 18 stringent policies with defined actions
- ~ 50% in reduction in false positive alerts ensure better Triage function
- Improved compliance with Enterprise policies and standards – Defined Standard Operating Procedure (SOP) for Security Operations Center (SOC) monitoring to report security alerts and incidents

- Based on the identified SaaS concerns and the availability of better security configurations and policies in Enterprise, Xoriant recommended an Enterprise-level setup as a superior approach in terms of migrating and managing all the endpoints securely.

After reviewing the assessment findings and recommendations for cost-efficiencies shared by Xoriant, the client approved the Enterprise cloud delivery model.

The entire migration was planned and executed successfully in 5 phases:

1. Discovery phase – Deep dive assessment and defining prerequisites
2. Implementation phase – Migration of endpoints and data
3. Policy enforcement – Define protection policies and test
4. Deactivate the SaaS subscription
5. Sign off – Dashboards and compliance report configuration, documentation (Standard Operating Procedures and Knowledge Base articles)

Technology Transformation

AWS Cloud services (EC2, Elastic Load Balancing, VPC and Networking) | TrendMicro Deep Security Manager and Agent