Synoptek

IT and Security Assessment Services Enable a Premier Car Rental Company to Improve Security Posture

CASE STUDY

Customer: A premier car rental service company

Size: 201-500 employees

Location: Newport Beach, CA

Industry: Hospitality

Profile: The company provides luxury vehicle rental services across 80 locations in the US and is focused on the high-end travel segment.

Services: IT and Security Assessment

Business Need

Due to the expansion of the business, the rental company had grown significantly over the last couple of years. However, the IT environment had not been able to keep pace with the needs of the company and the level of impending risk – especially with respect to risk management, security and high availability.

Since the client manages confidential personal information that is very intimate and personal for its high-profile customers, the security of their business data and customer data is fundamental to their success and existence. Yet, the client had an inadequate security posture relative to the level of risk to its business.

Basic standard security practices were not followed and a complicated suite of vendors and technology partners had created a situation where access control had become difficult to manage.

At the same time, the rental company was undergoing a fundamental transformation in terms of business systems and IT infrastructure capabilities and was looking to develop new business applications to enable exceptional customer service as well as transition to a modern cloud environment to increase cloud presence.

In addition, the client organization had been targeted by ransomware, and was looking for a security partner who could identify the threat vectors for the ransomware attack, study their existing infrastructure, evaluate and assess any gaps and issues, and establish a security evolution roadmap outlining the critical milestones in enhancing their security posture.

The client partnered with Synoptek to overcome their security challenges, act on recommendations, and strengthen their security posture.

Solution and Approach

> *Synoptek partnered with the client through a two-fold engagement: we looked into the breach that caused the ransomware attack and reviewed their existing infrastructure, applications, and identity and access management procedures as well as their business and IT strategy, people, and processes.*

Through our assessment, we observed the following:

- Many tools and technologies were available to secure the environment, but standard security processes, procedures and protocols were not configured.
- General security awareness and long-term strategy were absent; there was lack of training on tools in use, lack of appropriate roles to own and maintain an appropriate security posture as well as lack of real-time monitoring alerts; audit logs.
- The lack of network segmentation made it easy for attackers to penetrate easily throughout the client environment.
- Production Active Directory was replicated to the Sandbox environment, which enabled domain admin access to be used to attack the production environment.
- In addition, external entities were provided generic user accounts to access network resources.
- The client did not have the staff to manage and secure the current environment with a high degree of confidence.
- The fact that the company was undergoing a dramatic IT transformation only made matters worse.

Post evaluation, we offered the client recommendations and outlined the different steps they had to take to improve the security of their business. As part of the IT Security Risk Management engagement, Synoptek:

- Provided a list of security posture best practices for the client to implement and follow.
- Established an 18-month security evolution roadmap that included:
  - Security gaps remediation, stabilization, and hardening
  - Vulnerability management
  - Security policies development
  - Network architecture re-design
  - Network monitoring and access control development
  - Data loss prevention policies deployment
  - SIEM deployment and integration
- Offered to provide a dedicated security engineer to overlook the security of the organization.
- Provided recommendations across
  - Security breach detection and prevention
  - Replication of data and restoration of services in the event of a disaster.
  - General security auditing and forensics
  - Security awareness training
  - Automation of tasks, proactive monitoring and change management

Business Results

> *As a team of professionals providing strategic IT leadership and IT management for hundreds of businesses, Synoptek carried out timely and accurate assessment of the client's existing infrastructure and offered an array of pragmatic recommendations.*

Through our services, the client was able to:

- Identify the cause for the ransomware attack and implement policies to reduce the probability and impact of future attacks.
- Build a long-term roadmap to evolve their IT and enable security, risk management, reliability, and high availability.
- Create a comprehensive security program to address challenges and protect the confidentiality, integrity, and availability of data.
- Develop and enforce a policy for change management to minimize downtime and ensure that changes are in accordance with their security and information technology practices.
- Review configurations for servers, workstations, and network devices and develop standards in accordance with industry best practices.

Synoptek's services helped the client improve reliability and availability of services, efficiently manage risk, and improve profitability. Today, the client is able to minimize IT complexity, improve flexibility and reduce cost of operations.

About Synoptek

Synoptek is a global systems integrator and managed IT services provider offering comprehensive IT management and consultancy services to organizations worldwide. Founded in 2001; headquartered in Irvine, CA, we have offices and resources across North America and delivery centers in Asia.

Synoptek

19520 Jamboree Road #110 Irvine, CA 92612

888.796.6783

www.synoptek.com