tenable network security

Starwood Vacation Ownership

Overview

Starwood Vacation Ownership (SVO), a Florida-based subsidiary of Starwood Hotels & Resorts, is a leading developer and operator of luxury vacation ownership resorts. With a complex and growing network of more than 5,000 devices across 22 resorts worldwide, balancing security, compliance, and IT business goals required a first-class IT security system.

- **Key Business Needs:** SVO needed a more efficient security system that would streamline and improve its PCI compliance initiatives and strengthen overall security — without breaking the bank.
- **Tenable Products Selected:** SVO deployed Tenable SecurityCenter™, the Nessus® vulnerability scanner, and the Tenable Log Correlation Engine™ (LCE) as the foundation for its new security process and key PCI compliance initiatives.
- **Top Benefits:** A streamlined and optimized PCI compliance process that requires significantly less time investment by the security team and ensures that SVO achieves all PCI requirements. To date, SVO has shaved 20 hours per month from its old PCI compliance process and gained significant visibility and intelligence into network activity for its regulated environment.

starwood Vacation Ownership

Business Needs

Destination: PCI Compliance

SVO is one of Starwood Hotels & Resorts' fastest-growing business units, with nearly six million credit card transactions annually and consistent year-over-year growth. As the company's success increased, so did the need to ensure that it was safeguarding sensitive customer information and meeting key regulatory compliance initiatives — particularly the Payment Card Industry Data Security Standard (PCI DSS).

The company needed a security process that balanced its responsibility to protect customer information and meet regulatory standards with key business goals for the IT department, like the need to drive operational and technical efficiency and consistently identify opportunities for cost savings.

Project Goals: Security Housekeeping

There were three key areas where SVO identified an opportunity to improve the efficiency and effectiveness of its security and compliance process — all of which correlated directly with its PCI compliance goals.

- **Vulnerability management and assessment:** The company's "patch every vulnerability equally" approach had become an incredible resource constraint. SVO needed a way to prioritize high-risk versus low-risk vulnerabilities, and develop an effective patch deployment schedule that would keep them ahead of "true" threats and avoid overinvesting in vulnerabilities that presented no real risk to its network.
- **Log data collection and correlation:** SVO's 87 million daily log files were being siloed within several different departments (for example, IT and operations) — making it difficult and time consuming to gain an enterprise-wide snapshot of network activity. Consolidating and correlating network log data would make it easier to pinpoint threats and achieve compliance initiatives.
- **IT infrastructure:** In addition to overhauling its security practices, SVO was looking to modernize its IT infrastructure. This meant the security team would need to integrate the new technology with its new security systems. Phil Lambert, Director of Information Security at Starwood Vacation Ownership, wanted to make sure the process was as seamless and painless as possible.

> "Our number one goal in the IT security department is the safety and privacy of our customers' information. After an initial internal audit, we recognized there were opportunities to improve the efficiency of our security and audit process. By rethinking our approach, we could find new ways to optimize the process that would result in cost savings, faster results, and stronger security."
>
> ***Phil Lambert***
> Director Information Security,
> Starwood Vacation Ownership

The Tenable Solution

Five-star Rating

With management approval, SVO's security team implemented its new, efficient, and cost-effective strategy. The result: A streamlined and optimized PCI compliance process that requires significantly less time investment by the security team and ensures that SVO achieves all PCI requirements. Tenable's contributions to SVO's success were three-fold:

- The team developed an internal vulnerability rating system, and customized the Tenable Nessus vulnerability scanner so that scanning reports would automatically provide a roadmap of which vulnerabilities needed to be patched first. This new process helped SVO identify and prioritize vulnerabilities by criticality – saving 8-12 hours per week by avoiding unnecessary patching.
- The team also deployed the Tenable Log Correlation Engine (LCE) and consolidated its log data into a single repository, making it easier to gain true visibility into network activity and quickly pull critical information necessary for its internal and external audits. By leveraging the robust reporting capabilities of Tenable SecurityCenter, SVO was able to identify patterns, threats, and network problems in real-time, turning existing log data into valuable network intelligence.
- For its new process to be successful, SVO needed security solutions that were dynamic enough to provide fast and easy access to critical network data, but flexible enough to fully integrate with the company's various network-attached devices. SecurityCenter, combined with the Nessus vulnerability scanner, and LCE helped the team achieve real-time, continuous visibility into all network activity.

Next Steps and Bottom Line

Making Reservations for the Cloud

Moving forward, Lambert and his team are looking to reduce additional costs by increasing SVO's virtual and mobile environment. They plan to extend its security process to ensure the transition doesn't create greater risk for the company.

SVO also plans to expand its Tenable deployment over the next 12-18 months beyond its regulated environment to include its back office data center.

By leveraging the flexibility and robust functionality of Tenable's products, SVO has been able to ace its PCI audits, in less time, and has gained complete visibility into network activity and the data the company holds.

> "We have a small security team and this shift in strategy put us in a position to make smarter decisions that save us a significant amount of time and improve our overall security posture," said Lambert. "We're achieving our compliance goals, protecting our customers' information, and turning our existing log data into valuable network intelligence that affords us the opportunity to identify threats, problems, and patterns in real time."

> "Cloud computing and mobility can present a lot of cost savings and efficiencies, but there are challenges with maintaining access and control," Lambert said. "However, the increased visibility we've recently achieved gives us the flexibility to explore new technologies, without compromising our security standards."

For More Information

Questions, purchasing, or evaluation:
sales@tenable.com or 410.872.0555, x500
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™ network security