Customer Case Study

Global Resort Operator Continues to Protect Vacationers' Data and Helps Ensure Smooth Trips

Hilton Grand Vacations deployed Cisco security solutions to further safeguard the business network and protect customer information.

EXECUTIVE SUMMARY

Hilton Grand Vacations®

- Hospitality
- Worldwide, Headquartered in Orlando, Florida, United States
- 3200 employees

BUSINESS CHALLENGE

- Protect critical applications and customer data from network attacks
- Help ensure network availability
- Increase visibility into the network
- Better control network access provided to partners and vendors

NETWORK SOLUTION

- Upgraded network security solutions to implement integrated, multilayered network protection

BUSINESS RESULTS

- More robust, comprehensive network security to safeguard business assets and applications and help ensure network uptime
- Greater insight and granularity into network and security services
- Enhanced control over partner and vendor access

BUSINESS CHALLENGE

Hilton Grand Vacations Company, a wholly owned subsidiary of Hilton Hotels Corporation, is a leading operator of time-share resorts. The company administers 27 properties around the globe, as well as sales offices, data centers, and three call centers, serving more than 90,000 customers.

To keep this large, dynamic organization running smoothly, employees rely on a variety of centralized network applications including corporate financial systems, sales systems, and the basic business applications used to manage resort guests and services. With so much depending on the network, the company cannot afford a major virus outbreak or network attack.

"Obviously, a successful attack would be catastrophic," says Stephen Escher, network security manager for Hilton Grand Vacations. "We always worry about outages, but our top priority is protecting our customer's sensitive data, and preventing intruders from entering the network."

Hilton Grand Vacations had network security systems in place, but most of the solutions had been deployed several years previously, and had not been implemented as part of an overarching security effort.

"We needed a product that would give us better visibility into our systems. We did not always know if infected PCs were logging onto our network," says Escher. "Like many companies, we have been hit by the Sasser and Blaster worms in the past, and I wanted to have a stronger defense in place to protect against future virus outbreaks."

Escher also wanted to lock down the network's remote access links that outside vendors used to support various applications and services. "My biggest concern was our limiting anyone from inappropriately accessing sensitive areas of our network," says Escher. "With legacy systems, an external user who had a virus could have spread it throughout our network."

NETWORK SOLUTION

Upon reviewing the systems in place, Escher decided that Hilton Grand Vacations needed to take a more comprehensive, strategic approach to network defense. The company needed multilayered security, in which security services extend throughout the entire network, instead of just patrolling the perimeter. Escher turned to Cisco Systems®. Hilton Grand Vacations had recently upgraded its network infrastructure to Cisco routers and switches, and Escher believed that Cisco security solutions would support a more integrated, comprehensive security approach.

"I strongly believe in integrated security," says Escher. "I want to be confident that even if one security system is compromised, an attack will have to get through other defenses. Cisco has a comprehensive blueprint for implementing layered security that I try to emulate as much as possible."

Hilton Grand Vacations outfitted its Cisco Catalyst® 6500 Series core switch with a second-generation Cisco Intrusion Detection System Services Module (ISDM-2). The solution integrates full-featured intrusion prevention system (IPS) functions into the network infrastructure itself. The company also took advantage of the security features embedded within the Cisco IOS® Software that controls the network routers and switches.

> **"I want to be confident that even if one security system is compromised, an attack will have to get through other defenses. Our strategy was to deploy a multilayered security platform. Cisco had the most comprehensive blueprint and solution to meet our needs."**
> **—Stephen Escher, Network Security Manager, Hilton Grand Vacations**

"It is very convenient to have so many security features integrated into Cisco IOS Software," says Escher. "I can do inline IPS, turn on the firewall features, and support strong virtual private network [VPN] encryption. I can really lock down our network."

To efficiently collect and synthesize the large amounts of network and security data produced by the upgraded defense systems, Hilton Grand Vacations deployed the Cisco Security Monitoring, Analysis, and Response System (MARS). The solution provides much greater insight into network security events, and allows Escher's IT team to quickly identify and cut off any suspicious traffic.

"MARS is a very comprehensive solution," says Escher. "I am able to use the solution to collect netflow data for our local office and see which hosts are generating the most traffic, where that traffic is going, and more. I find it extremely useful."

At the company headquarters, Cisco VPN technology provides secure remote connectivity for the company's 200 mobile employees, as well as much more robust, manageable connections to the company's partners and vendors. Hilton Grand Vacations deployed Cisco ASA 5500 Series Adaptive Security Appliances at the company's Orlando office and at several remote sites. The solution combines firewall, VPN, IPS, and anti-X capabilities into a single, manageable platform.

"I am using the Cisco ASA solution to provide network address translation, Web content filtering, port blocking, and protocol and application inspection," says Escher. "At our remote sites, I can turn on the solution's Secure Sockets Layer (SSL) VPN capabilities and provide remote access to local employees. Without this solution, I probably would have had to deploy a separate VPN concentrator. It is nice to have all of that in one device."

BUSINESS RESULTS

In the year since Hilton Grand Vacation's upgraded security systems have been in place, the company has not had any major virus outbreaks or security issues. Escher believes that the integrated, multilayered network defenses have made the company more secure than ever before.

"I feel very good about the firewall and security features that are integrated within our routers, as well as the other solutions that we have in place," says Escher. "Each acts as one layer in our defenses, and any attack would have to get through five or six layers. I take comfort in knowing that the Cisco security solutions are protecting our network."

Escher also has been impressed with the wide range of capabilities of the Cisco solutions. “The recent upgrades to the Cisco IOS firewall and the Cisco VPN Concentrator have really increased the capabilities of those solutions,” he says. “I can not only block a port, I can block an application—no matter which port it tries to use. It makes it very easy to lock down things like peer-to-peer traffic.”

The Cisco Security MARS solution also provides much greater visibility into the network. “I can track the direction of any attack signature that we see, and find out where the attack is coming from—even across multiple sites that may be four or five hops away,” says Escher. “The way that the solution synthesizes all security incidents into a short, manageable view also is a real time-saver.”

Escher believes that Cisco VPN technology provides Hilton Grand Vacations with a much more secure way to integrate partners and vendors. “We are able to control outside access to our network at a very granular level. For auditing purposes, we can tell when they came in and what they accessed.”

The Cisco VPN capabilities provide operational advantages as well. “Often, we need to bring up a new site or a new partnership very quickly, and we do not have time to wait for a private circuit to be installed,” says Escher. “Now, any site with a DSL connection can access the business applications that they need via VPN. I can build multiple VPN tunnels and make changes as needed. It is like I am doing my own provisioning. I really like that flexibility.”

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6500 Series Switch
- Cisco 2800 Series Router
- Cisco 1800 Series Router

Security and VPN

- Cisco IDSM-2 Module
- Cisco Security MARS
- Cisco ASA 5500 Adaptive Security Appliances
- Cisco VPN 3020 Concentrator
- Cisco IOS Firewall
- Cisco IOS VPN
- Cisco Access Control Server

NEXT STEPS

In the coming months, Hilton Grand Vacations plans to roll out a Cisco network admission control (NAC) initiative that will inspect every host attempting to access the network, and help ensure that all users have up-to-date antivirus and operating system software before gaining access. The company also is considering deploying Cisco Security Agent on all public-facing servers to monitor for suspicious operating system behavior and protect against both known and unknown attacks. To back up critical corporate data and safeguard against major disruptions, Hilton Grand Vacations is also deploying a Cisco storage solution based on Cisco MDS 9500 Series Multilayer Directors.

FOR MORE INFORMATION

To find out more about Cisco Security solutions and the Cisco vision of the Self-Defending Network, go to: http://www.cisco.com/go/security.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C36-360890-00 08/06