Internet Content Provider Safeguards Customer Networks and Services

Synacor used Cisco network infrastructure and security solutions to enhance network protection and streamline compliance.

EXECUTIVE SUMMARY

NAME

Synacor

INDUSTRY

Technology

LOCATION

- Buffalo, New York, United States

SATELLITE LOCATIONS

- Herndon, Virginia
- Santa Monica, California

NUMBER OF EMPLOYEES

133

BUSINESS CHALLENGE

- Protect networks, applications, and customers from data theft and network attacks
- Access more comprehensive, accessible information for audits and compliance activities
- Gain greater insight into the health and performance of all internal and customer networks

NETWORK SOLUTION

- Upgraded network infrastructure and security solutions to implement intelligent, proactive network protection

BUSINESS RESULTS

- Improved ability to identify and respond to security events
- Boosted protection against viruses and attacks for all networks and endpoints
- Created a framework for easy, comprehensive auditing and compliance

Business Challenge

Fast-growing Internet businesses simply cannot afford network failures or security breaches. This is especially true for Synacor, a leading technology company that advances the delivery of meaningful content and technology solutions for multiple system operators (MSOs), telecommunication companies, and Internet service providers (ISPs) around the globe. Through Synacor's private label portals, subscribers can access a broad range of published and premium content, including entertainment, education, and family-oriented offerings from their homepages. Today, through its service providers, Synacor's products and services reach more than 20 million broadband subscribers worldwide.

With Synacor's business built around Internet products and services, network security is essential. The company must meet strict service uptime agreements and cannot afford to have its back-office assets or production networks disabled by a network attack. Additionally, as the company's business evolves, its security exposure has evolved as well.

"As we move to higher-bandwidth media, movies, and especially gaming services, we are opening ourselves up to more threats," says Adam Howell, director of network engineering and systems operations for Synacor. "One of our new accounts launching in 2007 will support more than one million subscribers right out of the gate and host a million e-mail accounts at our headquarters. We need to help ensure that there is no disruption or service degradation because of an attack on our network."

Synacor has heightened internal compliance standards. The company continues to be indirectly and directly involved in content sales, and with this enhanced activity maintains the protection of credit card information and complies with the Payment Card Industry (PCI) data security standard. As the company and systems continue to grow and develop, Synacor's IT team has committed to making the technical infrastructure compliant with the U.S. Sarbanes Oxley Act governing financial and accounting disclosure.

"We have to make sure that everything that we do is absolutely secure," says Howell. "Since our revenue stream is generated by subscriber authentication and log on, we can only get paid for what we know to be accurate. We have to make sure that all of our services are protected and meet strict auditing requirements."

> **"As multiple system operators (MSOs), telecommunications companies, and ISPs, our affiliates reach many people who may attempt to harm their networks. Now, if someone is trying to launch a DDoS or infiltrate one of our customer networks, we know immediately."**
>
> **—Adam Howell, director of network engineering and systems operations, Synacor**

However, Synacor's network and security infrastructure had been designed when the company was a much smaller organization. As of 2004, the network consisted of a variety of equipment from multiple vendors, governed by security policies that were vendor specific, which made monitoring and reporting very difficult and tedious.

"If someone was complaining of latency, significant labor and time were expended to determine the root cause, costing the company revenue, and making Synacor not nearly as efficient in controlling our network and systems as we should have been," says Howell.

Network Solution

Synacor's first task was to re-architect the security policies to cover all of the company's users and applications, and reflect the size and scope of the company. Next, Synacor began planning the network overhaul. The firm was in the process of relocating to new office space, and the move presented an opportunity to rebuild the corporate network infrastructure and defenses from the ground up. After reviewing several options, Synacor's leaders decided to work with Cisco® Certified Gold Partner IPLogic, and to build the new technology backbone of the company with Cisco solutions.

"I knew that I could rely on Cisco and our Cisco channel partner to do all of the heavy lifting for us," says Howell. "I could say, 'These are my concerns, this is where our company is going, this is what we need from a feature and scalability standpoint,' and I knew that they would help us deploy the right solution."

Through a phased rollout, Synacor deployed a Cisco routing, switching, unified communications, and wireless solution, as well as comprehensive Cisco network defenses. To protect the company's internal assets and upgrade the production networks, Synacor deployed Cisco ASA 5500 Series Adaptive Security Appliances at the network edge. The Cisco ASA appliances combine firewall, intrusion prevention system (IPS) services, and virtual private network (VPN) connectivity in a single, manageable platform, eliminating the need for multiple point solutions.

"Synacor pays for power and floor space in the co-location facility where we host our network services, so equipment rack space is at a premium," says Howell. "This solution, including a redundant failover bundle, takes up just two rack units, while our old solution required eight."

The Cisco ASA platforms allow Synacor to tightly control the network edge while allowing partners and customers to securely access needed resources. The platform supports both IP Security (IPSec) and Secure Socket Layer (SSL) VPN. Synacor uses IPSec VPN connections for their customers' support organizations and customer relationship management (CRM) systems, while using SSL connections between content servers.

"We use the VPN functionality of the ASA appliances to support our customers' billing and customer service requirements," says Howell. "This allows us to conduct business with each other live and create a positive end-user experience with our affiliates and broadband subscribers."

In addition to VPN connectivity with partners, Synacor also needed to provide remote voice and data connectivity for a significant portion of its workforce. Nearly a quarter of the company's employees work frequently from customer sites and remotely, and several members of the executive leadership team work full-time from small remote offices dispersed across the United States and the United Kingdom. "Synacor is a 24-hour company with customers that span six time zones worldwide. We were able to increase productivity as Synacor employees were no longer restricted to their desks, but could work from anywhere at anytime without creating a security risk," says Howell. "We have executives who travel frequently around the globe, working on very sensitive information, including funding and contracts," says Howell. "Now, all of our users are encrypted and working securely, no matter where they are located."

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 6500 Series Switches
- Cisco 7300 Series Router
- Cisco 7600 Series Routers
- Cisco 2800 Series Integrated Services Routers
- Cisco 3750 Series Switches
- Cisco 2950 Series Switches
- Cisco 4500 Series Switches

Network Management

- CiscoWorks LAN Management Solution
- Cisco Network Analysis Modules
- Cisco Performance View

Security and VPN

- Cisco Security MARS
- Cisco ASA 5500 Adaptive Security Appliances
- Cisco Guard XT 5650
- Cisco Traffic Anomaly Detector XT 5600
- Cisco PIX 500 Series Security Appliances
- Cisco VPN 3005 Concentrator

Voice and IP Communications

- Cisco Unified CallManager
- Cisco Unified Contact Center Express
- Cisco IP Communicator

Wireless

- Cisco Wireless LAN Controller
- Cisco Aironet® Access Points

To tie all of the infrastructure and security solutions together and serve as the nerve center of Synacor network defenses, the company deployed the Cisco Security Monitoring, Analysis, & Response System (MARS). Cisco Security MARS appliances efficiently aggregate and synthesize massive amounts of network and security data and use sophisticated event correlation and validation intelligence to help administrators more effectively identify and respond to threats. The solution also serves as a central repository for all auditing and compliance information.

"The Cisco Security MARS provides us with trend analysis and reporting that gives us a snapshot of the health of all of our networks at any time," says Howell. "When something goes wrong, we can identify it in minutes, if not seconds, and understand exactly what the issue is and how it will affect our services."

Business Results

Today, Synacor and its global broadband affiliates are benefiting from Synacor's state-of-the-art business network and network defenses. Synacor's partners are able to use Synacor's services to offer published and premium content to their customers, while confident that all subscribers, content, and financial data are protected.

"As multiple system operators, telecommunication companies, and ISPs, our affiliates reach many people who may attempt to harm their networks," says Howell. "Now, if someone is trying to launch a Distributed Denial of Service (DDoS) or infiltrate one of our customer networks, we know immediately. We can keep a close eye on those things, block them, and report back to our customers when we see excessive activity from a specific IP address, or port scanning, or other evidence of an attack. It is much more proactive, versus trying to resolve crises once they have already started."

The Cisco Security MARS and Cisco ASA 5500 appliances also allow Synacor to tightly control access to internal networks and customer resources, and rapidly respond to any potential threats.

"Within the first eight minutes of the Cisco Security MARS coming online, it identified multiple potential threats that Synacor's Network Operations team had identified two weeks previous. The identification of those threats had taken several of Synacor's staff and many labor hours to capture. MARS saw the quarantined threats automatically in minutes," says Howell. "We do not yet have the solution configured to fully automate the response, but we were able to identify the issues immediately and use the Cisco ASA appliances to block them."

The Cisco Security MARS appliance also provides an ideal clearinghouse for compliance and auditing information for the entire network.

"As we work to obtain Level-two PCI merchant status, we will need to make sure that all of our data is protected and encrypted, that we can accurately monitor when we do antivirus updates, and that we can track everything that we do in our network operations center," says Howell. "With the Cisco security solutions, hardware and software are no longer a factor in my concerns for becoming compliant. Anything that we need to do, the Cisco solutions will support it."

Howell also believes that Synacor has benefited by building all network and security systems with Cisco solutions.

"For everything we do, from both a sales and support perspective, we have a single point of contact," says Howell. "Instead of having 10 different devices from 10 different vendors, we deal with one person. That gives us a much higher purchasing power and a lower cost of ownership. Additionally, Cisco is leading the market in security. We know that every time there is a new update, our Cisco maintenance contracts give us access to the latest and greatest updates and features."

Next Steps

As Synacor continues to grow and add new partners, the company is continually expanding its Cisco network infrastructure and security solutions. In 2007, Synacor plans to add several more Cisco ASA appliances and Cisco Security MARS solutions to protect new customer networks.

Synacor also recently purchased Cisco Guard XT 5650 and the Cisco Traffic Anomaly Detector XT 5600 solutions. The Cisco Traffic Anomaly Detector XT 5600 will detect DDoS, worm, and even unknown "day zero" attacks in Synacor customer networks, and provide comprehensive reports on their characteristics. The Cisco Guard XT 5650 will then perform per-flow-level attack analysis, identification, and mitigation services to block attack traffic. The solution will block only the specific packets and flows responsible for the attack, while allowing legitimate traffic to pass unimpeded—enabling Synacor to provide the uptime and performance customers expect, even when a network is under attack.

Synacor also plans to deploy the Cisco Network Admission Control (NAC) Appliance in 2007 to help safeguard employee PCs and provide even tighter control over access to internal and customer networks.

“Our core is now worldwide, so if something is contaminated in one of our offices, that virus is likely to spread,” says Howell. “The Cisco NAC Appliance will help ensure that every PC that accesses our network, no matter where it may be located, cannot introduce spyware or malware into our systems.”

For More Information

To find out more about Cisco Security solutions, visit: http://www.cisco.com/go/security.

Americas 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: 408 527-0883

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

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C36-387745-00 1/07