Data Retrieval Firm Boosts Productivity while Protecting Customer Data

With HEIT Consulting, DriveSavers deployed a Cisco Self-Defending Network to better protect network assets, employee endpoints, and customer data.

Business Challenge

EXECUTIVE SUMMARY

DriveSavers Data Recovery

- Technology
- Novato, California, United States
- 80 employees

BUSINESS CHALLENGE

- Protect critical applications and customer data from network attacks
- Gain more comprehensive, accessible information for security audits
- Better control local and remote network endpoints

NETWORK SOLUTION

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

BUSINESS RESULTS

- Put in place more robust, comprehensive network security to safeguard customer data
- Boosted protection against viruses and attacks for the network and all endpoints
- Dramatically reduced the time required to respond to security events and comply with customer audit requests

When Michael Hall says that his company, DriveSavers Data Recovery, "We regularly, literally save businesses," he is not exaggerating. Founded two decades ago in a Silicon Valley garage, DriveSavers has become one of the premier data recovery companies in the world—with a track record of rescuing data from hard drives that have been through warehouse fires, bus crashes, and even several days at the bottom of the Amazon River. Recently, the company rescued 33 hard drives that had sat in mud and water for nine months in the wake of Hurricane Katrina. Today, DriveSavers has the highest data-recovery success rate in the industry, and a long and growing list of customers including global enterprises, financial institutions, major film and television companies, and government and military agencies.

Given the nature of DriveSavers' business, the company must worry not only about the security of its own applications, but also the rescued customer data that resides on its network—much of which is highly sensitive data.

"We save e-mail servers, databases, and proprietary information for companies that are developing new product lines," says Hall, director of PC engineering for DriveSavers. "We need to be able to say with 100 percent confidence that we can protect that information."

The need for strong, verifiable security measures has grown as DriveSavers has taken on more large corporate and financial customers, which demand detailed information about network security. Many customers now require any company handling their data to comply with SAS 70 security audits—detailed internal examinations of a company's security processes and systems. However, DriveSavers traditionally relied on security solutions from a variety of vendors, making auditing difficult. To meet customer requests, DriveSavers' engineers frequently had to take time away from their regular duties to retrieve and manually compile information from dozens of different sources in the network.

"I was spending an hour a day checking our infrastructure and the logs, just for our internal records," says Hall. "Providing a consolidated audit for a customer could take an entire day. When I am taken away from my regular work like that, I am not generating revenue for the company."

DriveSavers also suffered from the same security issues that plague all businesses: Employees' desktops and laptops needed to be secured and protected at all times. Remote employees needed to be able to connect to the network securely and easily. And, DriveSavers needed to guard against "day-zero" attacks that strike before antivirus companies have developed virus signatures to thwart them. This threat was particularly acute for DriveSavers, given that the company attaches thousands of customer hard drives to its network each month. "We almost never see a hard drive that does not have some sort of virus on it," says Hall.

Network Solution

DriveSavers had long relied on Cisco® Premier Certified Partner, HEIT Consulting, Inc., to provide managed security services and consultation, and once again turned to its trusted advisor. The firm recommended overhauling the entire security infrastructure and implementing new Cisco security solutions as part of an enhanced managed security service provided by HEIT.

"Given their corporate, financial, and government customers, DriveSavers needs to ensure that their network is fully and proactively protected, and that they can provide comprehensive security information," says Dan Holt, principal consultant for HEIT. "The only true end-to-end solution that can do that is the Cisco Self-Defending Network."

A Versatile Security Platform

At the heart of DriveSavers' Cisco Self-Defending Network is a Cisco ASA 5500 Series Adaptive Security Appliance. The solution provides firewall, intrusion prevention system (IPS) services, and both Secure Socket Layer (SSL) and IP Security (IPSec) virtual private network (VPN) connectivity from a single, manageable platform—replacing several previously separate point solutions.

"Having multiple solutions in a single platform is a major advantage, both for us and for DriveSavers," says Holt. "It is easier to manage, takes up less rack space, and costs a lot less. If we were to deploy separate firewalls, IPS solutions, and VPN concentrators, we would be looking at probably double or even triple the cost."

The ASA appliance's built-in SSL VPN connectivity offers major benefits for managing DriveSavers' remote employees, enabling users to connect securely from any Internet connection, without having to install a VPN client. The integrated IPS and firewall features help make sure the VPN does not become a conduit for malware and hacking activity.

The platform's inline IPS capabilities also offer major advantages. Unlike conventional intrusion detection system (IDS) solutions, which are limited to alerting administrators of attempted intrusions based on previously known attack-types, the ASA appliance's inline IPS functionality identifies possible attacks in real time, based on automated, contextual analysis of traffic.

Robust Access Control

To ensure all local and remote devices connecting to the DriveSaver's network are trusted, the company deployed Cisco Security Agent and the Cisco Network Admission Control (NAC) Appliance. The Cisco Security Agent, deployed on employee PCs and laptops, goes beyond traditional antivirus solutions by detecting and mitigating any unusual OS behavior—protecting against both known and unknown attacks. The solution serves as, in effect, a personal firewall and

Host Intrusion Prevention System (HIPS) for all DriveSavers endpoint devices, protecting them even when, for example, remote laptops are not connected to the DriveSavers network. The Cisco NAC Appliance uses the DriveSavers network itself to enforce security policies on all devices attempting to access network resources. The solution ensures that all devices are properly authenticated and that they meet baseline security requirements (such as having up-to-date antivirus, OS software, and Cisco Security Agent in place) before gaining access.

Comprehensive Security Intelligence

DriveSavers deployed the Cisco Security Monitoring, Analysis, & Response System (MARS) to serve as the "brain" of the entire security infrastructure and the central repository for all auditing information. 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.

"Whenever we have a security event, the Cisco Security MARS solution lets us know right away what is happening, why it is happening, and what is being done about it," says Hall. "It provides a visual representation of where an attack is coming from, where it is going, and how it is trying to access our systems."

"The Cisco Security MARS appliance makes our job as a managed security provider much easier," says Holt. "Instead of looking at dozens of logs for various solutions, we have every event from every server, Cisco Security Agent, IPS, and other device sent to the MARS appliance. The solution correlates all of that information for us, evaluates the threats, and removes a lot of false positives. For DriveSavers' auditing purposes, all of the security information goes into a single, consolidated report, instead of requiring their employees to pull reports from devices all over the network."

Streamlined Integration

Just as important as enhancing network protection for DriveSavers employees and customers, HEIT was able to perform the security overhaul very quickly, with no noticeable impact to normal business operations.

> **"The self-defending capabilities of this network are a huge advantage for us…Now, any strange behavior is blocked—even if it is unidentified."**
>
> **—Michael Hall, director of PC engineering, DriveSavers**

"We went through this whole security transition with zero downtime," says Hall. "I attribute that to the Cisco solutions, because they are so well integrated. Additionally, HEIT's knowledge of the Cisco products and the professionalism that they exhibited in managing the deployment made this a very simple process."

Business Results

With a Cisco Self-Defending Network and expert managed security services from HEIT Consulting, DriveSavers and its customers benefit from greater visibility into network activity, more robust network and endpoint defenses, and more proactive protection against external threats.

"The self-defending capabilities of this network are a huge advantage for us," says Hall. "We had virus protection, but I was always concerned about a new virus hitting us before our antivirus vendors came up with a patch. Now, any strange behavior is blocked—even if it is unidentified."

“Most of the solutions out there will detect an intrusion, but then we would have to go in and manually make a change or figure out what is happening,” says Holt. “The Cisco Self-Defending Network protects itself. If there is an intrusion on an endpoint, that endpoint communicates with the rest of the network, and the network proactively stops it. It provides preventive, rather than reactive security.”

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 4500 Series Switch
- Cisco 2600 Series Router

Security and VPN

- Cisco Security MARS
- Cisco ASA 5500 Adaptive Security Appliance
- Cisco Security Agent
- Cisco NAC Appliance

Having a single, integrated security infrastructure combined with the added intelligence of Cisco Security MARS makes compliance auditing much easier and less time-consuming.

“Financial institutions, government agencies, loan corporations—they all require security audits of their vendors, and we do not want to miss a piece of that market share because we cannot provide that.” says Hall. “With the Cisco Security MARS tracking and consolidating everything that happens in the network, we have an all-inclusive, catch-all solution that provides any information that our customers need, virtually instantly.”

The intelligent security event correlation capabilities of the Cisco Security MARS solution also reduced the number of reported security events requiring attention from an administrator from an average of 1 million per day to about 30. In all, the time savings from more efficient auditing, security event mediation, and other previously manual tasks adds up to enormous productivity gains for both DriveSavers and HEIT Consulting.

“Everything that we have deployed has saved us a tremendous amount of time,” says Hall. “For me personally, I would say these solutions save me a day and a half a week, or about a week’s worth of work every month. I think that is probably a conservative estimate.”

Given the nature of DriveSavers’ business, the evolving threat landscape, and the growing need for organizations to develop disaster recovery strategies, customers frequently ask Hall’s advice on protecting against natural disasters, pandemics, and other major security threats. Hall’s first word of advice always is to constantly back up data. However, he also stresses the importance of strong network security and secure remote connectivity strategies. He frequently cites DriveSaver’s own Cisco network defenses as a model for protecting corporate and customer assets.

For More Information

To find out more about Cisco Security solutions and the Cisco Self-Defending Network, go to: 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

C36-378371-01 03/07