

Rockford Health Systems Prescribes IPS To Build Immunity Against Cyber Attacks

Summary

Industry: Health care

Challenge: Protect critical patient care systems and business networks and assets from worms and other malicious attacks. Help meet HIPAA information security requirements.

Solution: Corero's IPS

Results: Corero's IPS secures Rockford's networks and helps ensure HIPAA compliance. Patient care systems, such as surgical PCs, are protected from attack and can remain securely in use and patched later.

Key Benefits

- Stops advanced threats out of the box
- Outstanding performance; lowest latency, superior throughput
- Reliable, purpose-built hardware
- Fast, easy deployment
- Blocks, malware, spyware, viruses and botnets
- Compatible with distributed networking architecture

Located in Rockford, Illinois, Rockford Health Systems is the largest health system serving northern Illinois and southern Wisconsin. Rockford Health System has a long tradition of care, built on a commitment to clinical excellence, cutting-edge technology and meeting the health care needs of the region. Consisting of more than 3,500 health care professionals, the system includes Rockford Memorial Hospital, Rockford Clinic, Can Matre HealthSouth Rehabilitation Hospital, Visiting Nurses Association, Rockford Health Plans and Rockford Memorial Development Foundation. As an organization committed to providing employees and patients with a solid technology interface, the availability and protection of the network is fundamental to the success of their business.

The Challenge

Rockford Health Systems had experienced a severe Distributed Denial of Service (DDoS) attack resulting from worm attacks. The DDoS attack crippled the Rockford firewall and infected the network that controls the patient care computers, the critical systems that are connected to patients to monitor and record levels of medications and procedural outcome. While none of the patient care systems were affected by the attack, the idea that such a situation could arise was cause enough for alarm and action.

"We had to act fast, since so much of our organization is now based on solid network availability," says Joe Granneman, Rockford's PC and network manager. "Given the nature of our business and the data that is transmitted, the integrity and security of our network has always been of the utmost importance."

Rockford Health Systems has been moving aggressively toward putting the Internet at the backbone of their business process, and had recently moved patient scheduling to an online, outsourced ASP model.

Additionally, the organization's PCs are all connected to the Rockford network, giving healthcare providers, doctors, nurses, and other personnel instant access to patient care records, real-time medical information, etc. For example, each surgical patient is connected directly to a PC, which in turn is connected to the network, to record and regulate the levels of medications, such as anesthesia.

Performance and reliability are of the utmost importance as the organization continues to move more business processes to its network. Network downtime directly impacts the level of patient care.

"Given the increasingly distributed nature of our organization, our employees are becoming more mobile, working from laptops as they travel from our various buildings, and logging into the network from various open ports," says Granneman. "Unfortunately, we've had instances of employees logging into the network and unknowingly releasing worms, helping the worm bypass the firewall that had previously stopped it."

Released into the network, the worms infected machines and began incessantly pinging and, eventually crashing the firewall. As the worms propagated throughout the network, Granneman was forced to reallocate resources from his department to stop the spread and mitigate the damage. PCs that are used in patient care were particularly vulnerable, because they cannot be patched until they are not in use.

The Solution

As the worms spread through Rockford's network, vital business processes became inaccessible and the costs associated with chasing them down and fixing infected systems began to mount.

"We simply cannot afford to have network downtime. We have too many processes tied to the network to make that an option," says Granneman. "We needed to reevaluate our security policies and take the steps to make sure that we're doing everything possible to protect our network."

Seeing the damage and the potential for more havoc, it was clear that a solution was needed that could actively block all malicious activity, particularly from inside the firewall.

After exhaustive review of information from industry publications and analyst reports, Granneman came to the conclusion that Corero's IPS [formerly Top Layer Security] was the best solution on the market.

"We had to act fast, since so much of our organization is now based on solid network availability."

*Joe Granneman, Rockford Health Systems
Network and PC Manager*

"The implementation was surprisingly simple, I put the box in by myself and had it up and running in no time," says Granneman. "The IDS was telling me where the problems were, I just couldn't do anything about them until now. With the IPS in place, I was able to shut down the trouble spots immediately."

The Results

Granneman noticed a huge difference in his network, and more important, a new sense of security and relief.

"The IPS made the act of cleaning up and securing the network much easier. Previously, we were unable to work on infected

patient care PCs while they were in use. Now we can block the activity of the infected machine while the physicians still use it, and then repair the machine at the end of the day. This enables us to keep productivity excellent while not compromising network security or patient care."

"The protection [Corero's IPS] provides helps us avoid downtime; there is no other defense for that."

Joe Granneman, Rockford Health Systems

Rockford has maintained its commitment to providing its organizations with leading edge technology by undertaking innovative organizational projects, including making customer patient scheduling Internet-based. Corero's IPS supports Rockford's business goals by ensuring that its networks are protected from downtime in the face of malicious attacks, and its online services remain responsive and available to staff and clients.

As the healthcare provider continues to grow, so does the need to migrate traditional paper systems to an electronic format, driven by the HITECH Act mandate requiring conversion of patient information to electronic health records (EHR). The implementation of the IPS marked an important step towards HIPAA compliance, securing electronic health records.

The Corero IPS effectively protects Rockford from worms, such as the damaging attacks released inside the firewall by mobile workers. Its ability to handle malicious traffic that may lurk on a network is a must for any health care organization that relies on its network for patient care information and for conducting standard business functions.

"Implementing the IPS as like providing us with a network insurance policy," says Granneman. "The protection it provides helps us avoid downtime; there is no other defense for that. Without protection like this, no matter what else you do, you're still vulnerable."

About Corero Network Security

Corero Network Security (CNS:LN) is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) defense solutions. Enterprise organizations rely on Corero to protect their critical online assets against risks associated with network-borne cyber threats. Corero, formerly Top Layer Security, is headquartered in Massachusetts, U.S. with offices worldwide. www.corero.com.

Corporate Headquarters

1 Cabot Road
Hudson, MA 01749
Telephone: +1.978.212.1500
Fax: +1.978.212.1600
www.corero.com

EMEA Headquarters

169 High Street
Rickmansworth
Hertfordshire WD3 1AY
Telephone: +44.0.1923.897333

To purchase Corero Network Security solutions, please contact your Corero representative at **1.978.212.1500** or authorized reseller.