TREND MICRO™ Securing Your Web World

Ochsner Health System Automates Threat Mitigation

Hospitals with Trend Micro™ Threat Management Services strengthen protection of patient data.

"Threat Management Services has greatly reduced malicious activity in our environment. Threats are discovered faster—we have much greater visibility—and security is now easier to manage."

— Don Brack, Network Development, Ochsner Health System

EXECUTIVE SUMMARY

Customer Name: Ochsner Health System

Industry: Healthcare

Location: New Orleans, Louisiana

Web Site: www.ochsner.com

Number of Employees: More than 10,000

CHALLENGE:

- Minimize the risks to security from third-party laptops and devices on the network
- Discourage risky employee behavior such as streaming or file sharing that can introduce threats
- Speed the time to discovery for next-generation threats and zero-day attacks

SOLUTION:

- Deploy Trend Micro Threat Management Services to discover and remediate hidden threat infections and provide proactive security planning

BUSINESS RESULTS:

- Saved time for IT, for lower cost of ownership for security
- Greater protection of patient data and help ensuring compliance by reducing risk on the network
- Proactive steps taken with vendors and partners to better secure all devices
- Reduced network traffic, giving doctors faster access to information that enables better patient care

Challenge

Ochsner Health System is a thriving organization with high levels of network traffic. New hospitals and clinics have been added to the network in recent years, and the infrastructure is increasingly important for patient care. The organization's technology team needs to maintain security while managing rapid growth. Ochsner relies on a layered security solution to protect mission-critical assets.

One of the major challenges for the IT organization involves its open network, which supports a broad range of equipment brought in by partners and members of the Ochsner community. "As IT professionals in the healthcare industry, we often face problems with devices that are brought into our network," said Don Brack, a network architect at Ochsner. "We have no control over the antivirus and security solutions on those devices. When they use our network, they represent a risk to our overall environment."

Multiple layers of the Trend Micro™ Enterprise Security solutions provide protection to hospital-owned PCs and servers, and help to block many threats at the gateway. In the past, the IT team relied exclusively on these in-place security solutions and also worked with networked device vendors and partners to quickly identify problems and clean up any newly introduced infections as quickly as possible after detection. Still, this took up valuable IT time, and was not as proactive as desired. The sensitive nature of patient privacy and risk to continuity of care led IT to search for a solution that could more quickly identify and remediate security issues on the network.

Solution

Last year, Ochsner Health System decided to try out Trend Micro Threat Management Services because IT needed the ability to respond much faster to the risk of data loss from malware activities. Threat Management Services includes discovery, remediation, and management functions. Overall, the service monitors the network to catch threats that have evaded detection from the traditional front line security infrastructure and then performs network-wide cleanup.

To fully evaluate the threat discovery and remediation features, Ochsner deployed threat discovery technology at the network layer to monitor for hidden infections. Ochsner then installed the threat remediation technology on a few hundred clients. IT configured the service to manage any network traffic for those devices. The service provided visibility for the non-port 80 traffic and looked for Internet-borne activities and malicious triggers. The healthcare organization has a total of five Internet gateways, and the service picked up all activity across those network connections.

"Threat Management Services gives us daily reports—we can see what devices in the environment are at risk or are already carrying out malicious infections," said Brack. "All three parts of the service—discovery, remediation, and management—are very useful. The service is very proactive and automatic. When the discovery service picks up activity, it triggers the mitigator and any required cleanup is carried out immediately. I can read the reports to see what is going on, and I can also do manual scans."

After the successful trial, Ochsner decided to purchase the Threat Management Services. The solution helps identify and remediate a broad range of next-generation threats including day-zero, targeted attacks, guest laptops, rogue endpoints, infected USB sticks and removable storage devices, and P2P applications such as file-sharing programs that can introduce infections.

"With Threat Management Services, we've discovered which users are streaming from inappropriate sites," said Brack. "If we get a call about an infected machine, we can run a report and see if the user was using file sharing applications or involved in any other risky activities.

"We currently have the service fully deployed—using its entire infection discovery and clean up capabilities. We are now able to detect all types of activity. It shows us streaming activity, users who are instant messaging, and user activity related to all of the network protocols. The agent is very easy to deploy—in just 30 to 40 seconds we can set up a device to be monitored. It has been easy to roll out, and we are cruising along with the service in place."

Results

Since deploying the Trend Micro services and regularly reviewing the associated reports, Ochsner has seen numerous inappropriate activities being eliminated from the network. Automatic cleanup has removed undetected threats; changing employee behavior has accounted for further improvements in security. IT has also used the services to identify unprotected devices, and has extended protection to those endpoints.

With discovery, remediation, and automated cleanup, Ochsner now has increased protection of their patient data. "Threat Management Services has greatly reduced malicious activity in our environment," said Brack. "Threats are discovered faster—we have much greater visibility—and security is now easier to manage. Threat Management Services cuts my time in half for servicing each infected or unprotected device."

Network monitoring and reports increase Ochsner's visibility of the overall security situation. "Reports are emailed to me automatically, and I can forward them to everyone who needs to know," said Brack. "We can also get detailed information through the user interface, including suggestions for each item in the reports. The support from Trend Micro has been very beneficial in our enterprise environment."

As regulations and requirements continually evolve in the healthcare industry, compliance efforts require that IT take advantage of whatever visibility they can. "As part of an audit or routine troubleshooting to maintain compliance, we often have to maintain detailed logs on the security activity in the network as well as research the activity on particular machines," said Brack. "Threat Management Services will certainly help our compliance efforts in this area."

Besides improving overall security, the services have decreased traffic on the network. "We are now saving 5 to 10% of our Internet bandwidth," said Brack. "This means we can give better responsiveness to our users. The Internet is critical for 90% of care delivery—doctors use it for everything from research to treatments. Improving our bandwidth helps doctors get faster results and ultimately provide better care."

DEPLOYMENT ENVIRONMENT

50+ sites

12,000 PCs

400 servers

Trend Micro™ Enterprise Security for Endpoints 10.0

Trend Micro™ InterScan™ Messaging Security Virtual Appliance 5.0

Trend Micro™ InterScan™ Web Security Suite 3.1

Company Profile

Ochsner Health System is a non-profit, academic, multi-specialty healthcare delivery system in Southeast Louisiana. The organization has grown to become the largest healthcare system in the region, with 600 physicians and 80 medical specialties. Eight hospitals, a sub-acute facility, and 40 neighborhood health centers host one of the largest non-university-based physician training centers, and the health system conducts 700 ongoing clinical research trials annually. Ochsner Health System was ranked "The Best Place to Work in New Orleans" in 2005 and 2006.

Trend Micro Security

- **Trend Micro Threat Management Services**
  http://us.trendmicro.com/us/solutions/enterprise/security-solutions/threat-management/key-components/
- **Trend Micro Enterprise Security**
  http://www.trendmicro/go/enterprise
- **Trend Micro Smart Protection Network**
  http://www.trendmicro.com/go/SmartProtectionNetwork
- **Trend Micro Enterprise Security for Endpoints**
  http://us.trendmicro.com/us/products/enterprise/security-for-endpoints/index.html
- **Trend Micro InterScan Messaging Security Virtual Appliance**
  http://us.trendmicro.com/us/products/enterprise/interscan-messaging-security-virtual-appliance/
- **Trend Micro InterScan Web Security Suite**
  http://us.trendmicro.com/us/products/enterprise/interscan-web-security-suite/index.html

www.trendmicro.com