



## Memorial Hermann:

### Healthcare Organization Eliminates Security Vulnerabilities Step-By-Step.

#### Background

Worms and viruses can affect the computer networks of any business sector if they are not routinely patched to protect against such threats. In the event of a computer exploit that slows or shuts down their systems, businesses face financial loss and a public relations nightmare, and healthcare organizations face an even bigger challenge. While many other businesses can shut down their operations while they reconfigure their networks, healthcare organizations cannot. Healthcare staff must still have access to patient files in order to continue proper treatment. This puts the burden on the staff while systems administrators work feverishly to minimize damage and restore the security of their systems.

Healthcare organizations must take extra steps to ensure their networks are secure from computer exploits that can cause a threat to the treatment, care and privacy of their patients. Memorial Hermann, a healthcare organization based in Houston, Tex., recognized the necessity to outline a specific timeline to efficiently respond to security breaches and maintain a secure network.

Memorial Hermann is one of the largest not-for-profit healthcare organizations in the country. It serves the greater Houston and southeast Texas communities with nine acute care hospitals, three long-term acute care hospitals, a physician network for primary and specialty care, retirement living and nursing homes, wellness programs, rehabilitation and home health

*"We didn't run across a single problem with Shavlik HFNetChkPro™ when chaining patches together," said Steve Guistwite, director of network solutions at Memorial Hermann.*

programs, and an air ambulance service.

With approximately 16,000 employees spread out within a 160 mile radius of the Houston city limits, the Memorial Hermann network includes 8,300 desktops and 500 Windows®, Novell and Linux® servers. The information systems department within Memorial Hermann consists of approximately 325 people dedicated to network solutions, network engineering, desktop solutions, AIX/database management, mainframe support and VMS operating system management.

Steve Guistwite, director of network solutions for Memorial Hermann, is responsible for all 500 servers, the 18,000 mailboxes in the corporate exchange system, Web services, an extensive Citrix environment, and the network systems monitoring suite.

"I have 12 FTE's on my staff, and we essentially own the entire lifecycle of a server," said Guistwite. "We build the server, install all security software on the server, put it on the network, monitor its performance, fix any hardware, help with application installations—and manage anything else along the path of its lifecycle."

# Memorial Hermann



## The Challenge

While network security has always been a priority for Memorial Hermann, the first time all servers were updated to a specified security level was for Y2K.

"Prior to 2000, we simply made sure everything was updated to Microsoft Service Pack 5, and we thought we were covered," said Guistwite. "If we could update a server, we did, but if one server was patched higher than another, it was not a big deal."

This casual security method came to a quick end when the "I Love You" virus hit in May 2000. Four major hospitals near Memorial Hermann were affected by the virus. While Memorial Hermann was lucky enough to avoid it, the network solutions team went through a painstaking process in order to get the servers updated.

As one of the first viruses written to expose a known Microsoft flaw, the "I Love You" virus linked patch management and anti-virus software in the minds of network security personnel. "We've always been up-to-date on our anti-virus software, but patch management was lagging behind," said Guistwite. "Since the 'I Love You' virus exposed a known Microsoft flaw that could have been fixed with a security patch, we saw our lack of patch management policies as a huge vulnerability."

## The Solution

Memorial Hermann was already using Microsoft Systems Management Server (SMS) for some security patching, but Guistwite and his colleagues determined that there still were vulnerabilities. They began to search for an automated patch management product to meet the needs of the Memorial Hermann

With the click of a button, the Memorial Hermann network solutions group scanned all servers for patch status, and Shavlik HFNetChkPro™ immediately sent status reports indicating where patch updates are needed.

network.

"We did a head-to-head test with Shavlik HFNetChkPro™ and a patch management tool from another vendor," said Guistwite. "We chose Shavlik over the other tool because we ran into some problems when deploying a chain of six or seven patches with the other software. We didn't run across a single problem with Shavlik HFNetChkPro™ when chaining patches together."

Along with the ability to chain multiple patches together, Guistwite and his colleagues wanted their patch management solution to provide a crisp line of reporting. It was important that they had the ability to go back to the Memorial Hermann security officers and CIO and report on which patches are installed on each server.

"We also appreciated that the president and CEO of Shavlik Technologies, Mark Shavlik, used to work for Microsoft," said Guistwite. "That gave us a level of trust, so to speak. And the product spoke for itself."

Memorial Hermann purchased Shavlik HFNetChkPro™ in March 2002.

## The Results

After purchasing Shavlik HFNetChkPro™, Guistwite's team goal was to push patches out across all 500

# Memorial Hermann



servers within six months. Their first initiative was with the demilitarized zone (DMZ)—the most vulnerable area on the Memorial Hermann network because it is the only part that is exposed to the open Internet.

With the click of a button, the Memorial Hermann network solutions group scanned all servers for patch status, and Shavlik HFNetChkPro™ immediately sent status reports indicating where patch updates are needed. Plus, the solution's PatchPush™ capabilities made automatic patch deployment fast and easy. Through a drag-and-drop interface, patches were deployed to individual servers or to groups.

In just over a month, Shavlik HFNetChkPro™ was fully implemented in the DMZ—an extremely short timeframe, according to Guistwite.

"We tested Shavlik HFNetChkPro™ to ensure that all the patches were being deployed correctly, and that we could quickly chain patches together and protect the operating system," said Guistwite. "After confirming this, I drafted a policy that dramatically reduced the deployment time to DMZ servers to 72 hours."

In just 45 days, Memorial Hermann went from having no formal patch management policy to requiring that all DMZ servers are patched with 100 percent accuracy within 72 hours of Microsoft's release of a security patch.

## Patching Plan Timeline

Because worm and virus threats have completely changed in the past two years, Memorial Hermann's current patching policy and timeline has become even more stringent than their first policy. The current goal is to have all 500 Memorial Hermann servers patched within two weeks of the release of a critical update

In just 45 days, Memorial Hermann went from having no formal patch management policy to requiring that all DMZ servers are patched with 100 percent accuracy within 72 hours of Microsoft's release of a security patch.

from Microsoft.

"The first 72 hours are still dedicated to patching nothing but the DMZ, and we've met that goal with every patch in the last two years. From there, the remaining 475 servers are all patched within two weeks of the release," said Guistwite. "We've literally gone from one end of the spectrum to the other, and we do it all with Shavlik."

### Memorial Hermann's patching timeline is as follows:

**Patch Tuesday:** When Microsoft releases security bulletins on the second Tuesday of each month, Memorial Hermann receives an automated notification of the newly released patches from Shavlik's XML notification email service. If any of the patches are classified as "important" or "critical," Guistwite's team generates a ticket for the patch using Remedy resource management software. The Remedy ticket is sent to the Memorial Hermann Web development group, who have 24 hours to test the new patch on Web servers in their lab. This testing validates whether or not the patch is acceptable to install on the network.

**Days Two and Three:** In the next 48 hours, all 30 servers in the Memorial Hermann DMZ are scanned, patched and rebooted with no exceptions. Memorial Hermann has a standing change control time every

# Memorial Hermann



night from 12 a.m. to 1 a.m. If a server needs to be patched, it can be safely taken down and rebooted during this time.

**Days Four, Five and Six:** During the next three days, internal application owners are given a window of time when they can come to the lab to have their applications tested with the new security patches. The testing policy is that if an application owner does not express concern about the patch, patching acceptance is assumed.

**Week Two:** The final week is spent using Shavlik HFNetChkPro™ to patch all the remaining servers. The network solutions group assigns one or two people to work nights during this time to supervise patching.

**End of Week Two:** After all patches are deployed, Memorial Hermann runs a final report using Shavlik HFNetChkPro™ and Nexantis SecureScout™ software. While Shavlik is capable of running its own report, using SecureScout enables Guistwite to provide an independent, third-party assessment of Shavlik HFNetChkPro™. The report outlines all the servers that are patched and is sent to the Memorial Hermann associate vice president of network solutions, director of security and CIO.

## Benefits

According to Guistwite, manually deploying security patches to servers is not feasible given its geographical scope, and Memorial Hermann realized even more savings than expected with Shavlik HFNetChkPro™.

“There are a lot of application servers out there that were built by ‘mom and pop shops’, particularly in healthcare organizations. This means there are often

very elaborate start up and shut down procedures,” says Guistwite. “One significant benefit achieved using the Shavlik tool is that we were able to schedule scans before and after the patch process. The missing patches are deployed using Shavlik HFNetChkPro™, which significantly frees up administrative time for other IT projects.”

While patching all 500 servers in two weeks is an aggressive timeline for Memorial Hermann, without Shavlik HFNetChkPro™, Guistwite estimates it would take closer to eight weeks to patch all servers.

“Using Shavlik HFNetChkPro™ saves us both time and money,” said Guistwite. “By automating patch management, we are able to more accurately patch more servers in a shorter amount of time. This increases the uptime of all our systems and enables Memorial Hermann to access its network systems to deliver top quality care to patients, secure sensitive patient information and generate income for our business.”

Memorial Hermann currently uses 750 licenses to protect its network server system, and is considering expanding their use of Shavlik HFNetChkPro™ to include all 8,300 desktop computers on their network.