Real-World Healthcare Case Studies:

Data Security and Compliance in the Age of Advanced Cyber Threats
Table of Contents

INTRODUCTION ............................................................................................................................................ 3

CASE STUDIES
Rush University Medical Center ................................................................................................................. 4
DCI Donor Services ..................................................................................................................................... 7
Beaumont Hospital ........................................................................................................................................ 9
Navicent Health ........................................................................................................................................... 10
Aomori Hospital .......................................................................................................................................... 12
Adventist Health System ............................................................................................................................. 14
Ochsner Health System ............................................................................................................................... 16

CONCLUSION .............................................................................................................................................. 18
Introduction

Healthcare organizations—from national or regional hospital networks to small local clinics and private practices—are dedicated above all to caring for individuals and families, to providing personal services that improve patients’ quality of life, and to extending lives.

In the era of digital, online information, these organizations also have a responsibility to protect highly confidential and sensitive medical and financial information about their patients. Unlike medical care, however, data security is often outside these organizations’ area of expertise. Given the sensitive data that is required to be collected and stored for purposes of caring for human lives, healthcare organizations also need to be diligent in protecting the digital lives of their patients.

Understanding the Threat Landscape

There is a growing awareness throughout the healthcare industry that the threat of a major data breach is real and increasing. Recent highly publicized breaches and warnings from the FBI directed at US healthcare organizations demonstrate that the risk of a breach of patients’ confidential data is a major concern.

Because healthcare organizations collect some of the most valuable and sensitive information—identity data, financial data (such as credit card information), and health information—they are being actively targeted by sophisticated cyber criminals. Recent attacks on healthcare organizations have included thefts of identity information, and at least one case of “data blackmail” in which criminals threatened to release patient data unless the hospital paid a substantial ransom.

The fact is, mounting a major cyber attack is no longer difficult—it does not require highly skilled and talented hackers with substantial funding. The technology required for an attack has become a commodity, easily available from underground online sources.

In addition to malware, a vast array of services and support can be found at bargain prices. For well under $400, an individual with moderate to low programming skills can acquire what they need to launch a successful attack, steal critical data, and then sell it on the black market for profit. Even a relatively small number of patient records is worth attacking and stealing, because the costs are much lower than the potential profits.

Meanwhile, the costs to organizations that fall victim to these criminals can be dramatic. In an industry in which trust is so critical, loss of reputation can result in massive revenue losses. Fines for regulatory non-compliance, compensation to victims, and other associated costs can be significant—not to mention the potential career impacts for senior IT personnel and executives alike. Among enterprise-scale organizations, the average total cost of a major breach is an estimated $5.9M US, and several high-level resignations have followed some of the recent wave of targeted attacks.

Within the pages of this book, you’ll learn the stories of how various healthcare organizations chose to fulfill their responsibility to protect the digital lives of their patients with Trend Micro. You’ll learn about the challenges they faced, the solutions they considered, why they ended up choosing Trend Micro solutions, and how their decisions helped them to protect patients’ digital lives and meet regulatory requirements—letting them focus on their core mission of caring for human lives.

For more client successes, watch these videos:

- Rush University Medical Center
- Adventist Health System
- DCI Donor Services

---

1 “FBI Notice: Healthcare security not as mature as other verticals”, Searchsecurity.com, Brandan Bievins, April 24, 2014
2 “Hospital network hacked, 4.5 million records stolen”, CNN Money, Jose Pagliery, August 18, 2014
4 “Your medical record is worth more to hackers than your credit card”, Reuters, Caroline Humer and Jim Finkle, Sept 24, 2014
5 Ponemon Institute LLC, May 2014
Rush University Medical Center Creates Safer Environment with End-to-End Protection for Healthcare and Academic Environments

Complete User Protection Solution, Deep Security, and Deep Discovery enable greater visibility to defend against sophisticated attacks.

Overview

**Rush University Medical Center** (Rush) is a not-for-profit healthcare, education, and research enterprise with a 664-bed academic medical center that includes hospital facilities for adults and children. In addition to the University Medical Center, Rush also includes Rush University, Rush Oak Park Hospital, and Rush Health with a total of 8,000 employees. Rush offers residency and fellowship programs in medical and surgical specialties to more than 2,000 students.

With a large and experienced IT team, Rush manages three data centers across its campuses. The organization currently supports approximately 1,600 virtual desktops and 600 virtual servers, along with 10,000 physical desktops. The Rush IT team is tasked with supporting users on all devices, including smartphones and tablets. Rush operates proprietary wireless networks for its doctors, nurses, students, and support staff, while it also provides public Wi-Fi for patients and families. Rush was recently named one of Hospitals and Health Networks Most Wired organizations for 2014. “We cover the gamut of everything you would find in a modern academic medical center, including one of the most advanced electronic medical records systems,” said Jaime Parent, Associate CIO, Vice President IT Operations at Rush University Medical Center.

In addition to being a premier medical facility in Illinois, Rush is also committed to the community it serves. Recently, Rush founded the **EN-Abled Veteran Program**, which trains and prepares transitioning military veterans in healthcare IT. As a result of the program, veterans from conflicts in Iraq and Afghanistan are learning skills that will help them succeed in the healthcare IT marketplace.

Challenges

Rush University Medical Center’s IT leadership knows the importance of providing protection to all levels and types of customers that are on site at the hospital and supporting facilities, such as doctors, nurses, staff, technicians, and patients. To provide that protection, they’re always looking for the very best in IT security. However, in 2011 Rush realized their former security vendor did not have the tools or the capabilities to defend against a new breed of advanced threats.

In one attack, Rush was hit hard by the Conficker virus, a computer worm that targets Microsoft Windows environments and creates botnets that can steal valuable network data. Their existing security system could not identify and resolve the virus. This was a major concern for Rush, because their network holds information on patient, research, and other hospital related data. “Like any major medical facility, Rush operates 24/7/365, so we could not simply shut down the system and search for a solution,” said Parent.

Another issue for Rush was dealing with unknown and zero-day attacks that were assaulting its network on a regular basis. “We were challenged in balancing a growing security architecture against emerging persistent threats,” said Alex Radenkovic, Information Security Engineer at Rush University Medical Center. “An attacker can deploy new attack techniques when capable defenses have not yet been deployed, leaving the attacker with the upper hand.”

Daily scanning presented another challenge for the medical facility. The scanning by its previous endpoint security provider was impacting performance of users across its network. Because scanning was scheduled for mid-day, the solution caused processing delays that reduced user productivity for all levels of users. As a result, some Rush employees would work on their own personal laptops, smartphones, and tablets to avoid the scan, leaving Rush with a mix of managed and unmanaged endpoints. “As a medical center, we have to make sure we have the monitoring and security to ensure compliance across all of our users’ many devices,” said Parent.

Some of the primary compliance regulations that Rush needs to meet include: the Health Information Portability Act (HIPAA) on the medical side, the Family Educational Privacy Act (FERPA), which protects the privacy of student education records, state regulations, and Public Health Information (PHI).
Challenges  Continued
As if zero-day attacks, scanning issues, and compliance problems weren’t enough, Rush was concerned that its current solution could not meet the demands of its modern data center. Rush was looking for a solution that would protect its virtual desktop infrastructure (VDI) and virtual servers, and provide virtual patching that shields potential vulnerabilities before attackers can take advantage of them.
Finally, Rush IT was concerned with malware entering the system via unauthorized USB devices being brought onto campus. “Once we learned about the sophisticated nature of the new threat landscape, we knew we had to protect the entire hospital network,” said Parent. “And we had to handle the scanning issue that was impacting user performance.”

Why Trend Micro?
After evaluating several leading security vendor solutions, Rush was most impressed with Trend Micro because of the quality and effectiveness of their solutions. The Rush IT leadership was also swayed by the level of engagement from the Trend Micro account team who took the time to understand the complexity of Rush’s IT challenges and tailor an end-to-end security solution for their unique environment.

“The Trend Micro team was great to work with. The camaraderie and level of discussion between the members of our organizations was the first step in our win-win relationship,” said Parent. “They provided excellent support, came on-site for strategy sessions, and really made a significant effort to understand our security requirements.”

While Trend Micro was working to tailor a solution, Rush experienced another malware attack that made it appear as though some of their files were disappearing. However, with Trend Micro’s help, this time Rush was prepared to defend its environment. The virus was eradicated and a strategy provided to prevent the virus from being retransmitted. “We all pitched in and collaborated to eliminate the virus,” said Parent. “Even though Trend Micro had only seen this virus at one or two other sites, they were able to stop it.”

When a 30-day Proof of Concept for Trend Micro™ OfficeScan™ was completed, Rush IT recognized not only the number of threats they were facing, but where the threats were coming from. “Once we understood how much traffic we had to manage, how much malicious traffic to block, and the magnitude of the threats, it was easy to make the case for Trend Micro,” said Parent.

The Solution
Impressed with the results of the OfficeScan endpoint protection solution, Rush decided to switch to Trend Micro and deploy the Trend Micro™ Complete User Protection solution in 2012. The solution includes OfficeScan, as well as email and collaboration security, web security, mobile security, and integrated data loss prevention. The result is a protective shield that is extremely difficult for cyber criminals to penetrate.

In addition to providing protection across Rush endpoints, OfficeScan uncovered far more malware than Rush’s previous security solution and delivered much faster virus scans that did not impact user productivity. “The technology used by Trend Micro was much less intrusive on the CPU, so scans were completed much faster and users stopped complaining,” said Parent. “And the scans were identifying viruses and Trojans that our previous solution did not detect. Put all that together and it’s pretty clear that Trend Micro’s solution was a superior product.”

While having regular strategy sessions with the Trend Micro team, Rush IT leadership quickly recognized that today’s threats require multi-layered protection, particularly in the highly-regulated healthcare and academic environments. After a successful Proof of Concept, Rush deployed Trend Micro™ Deep Security™ and Trend Micro™ Deep Discovery™ solutions.

“We use Deep Security to protect our VDI and virtual servers. The solution provides a comprehensive, agentless security platform for our virtual environment, and we plan to use it for our cloud server implementation,” said Radenkovic. “In addition to maximizing protection for our VDI environment, Deep Security provides virtual patching that shields vulnerabilities before they can be exploited, eliminates emergency patching, frequent patch cycles, and costly system downtime.”

“With Deep Discovery, Rush can monitor the entire network for attacks, analyze malware using sandboxing, and quickly assess and react to the threat,” said Radenkovic. “Deep Discovery is a virtual powerhouse. In the last 90 days Deep Discovery has examined and investigated over 100,000 samples and more than half-a-million million viruses and other malware were blocked using OfficeScan.”

“Once we understood how much traffic we had to manage, how much malicious traffic to block, and the magnitude of the threats, it was easy to make the case for Trend Micro.”

Jaime Parent,
Associate CIO, Vice President IT Operations at Rush University Medical Center

Deep Discovery is a virtual powerhouse. In the last 90 days Deep Discovery has examined and investigated over 100,000 samples, and more than 500,000 viruses and other malware were blocked using OfficeScan.

Alex Radenkovic,
Information Security Engineer at Rush University Medical Center
One example of the multi-layered support that Trend Micro provides to Rush was when a user downloaded zero-day malware to a PC within the Rush network. Deep Discovery inspected the suspicious malware and ran the threat through its sandbox technology to see what harm it could do and what type of system it could infect. “We actually were able to watch the malware trying to contact its Command and Control servers to get new code and steal our data,” said Parent. “We would have had an outbreak if it wasn’t for Deep Discovery.”

The solution’s centralized management also offers significant benefits. It allows Rush to monitor the health and status of servers, workstations, laptops, compliance—all from a single screen. “Trend Micro’s Control Manager” solution gives you incredible user-based visibility into what’s going on in your computing environment. It also gives you everything you want from a reporting device—data ranges, graphs, advanced views, and extremely detailed logs,” said Radenkovic. Trend Micro’s support team also played an important role in helping Rush quickly realize the solution’s benefits. “With Trend Micro’s Premium Support Program, the support team not only helped us install and configure software, they taught us how to use their products just like they do,” said Radenkovic. “The level of professionalism and expertise was very impressive—it feels like we’re all on the same team—it’s a fantastic collaboration.”

Since switching to Trend Micro in 2012, Rush University Medical Center has recognized several significant benefits in both the level of network protection and increased user performance. Trend Micro’s Complete User Protection allows the Rush IT team to manage users from a single console, giving Rush complete visibility into security across their IT environment. “Since switching to Trend Micro, our computing environments are now stable. Once we deployed Deep Discovery we have not had any major outbreaks—they helped us identify the infection source and attack vector, so we could address the threat right away,” said Radenkovic.

“Switching to Trend Micro from our previous vendor, it would sometimes take us a day to two to figure out where the attack was coming from, involving lots of resources to correlate that data. After switching to Trend Micro, we’ve been able to identify the attack and the sources almost instantaneously.

Trend Micro OfficeScan has improved user satisfaction with faster and more effective scanning, while making it easy to manage security. “From an overall environment perspective, the number of threats have decreased significantly since we installed Trend Micro solutions,” said Parent. “We can see from the logs provided by the solution that it’s really working.”

With Trend Micro now protecting their entire IT environment, Rush has peace of mind that their valuable healthcare, academic, and other sensitive information is always protected. For healthcare organizations facing ongoing attacks as well as HIPAA compliance regulations, this is very important. “With Trend Micro solutions, we have the tools to see which types of threats we are facing, and quickly resolve them before they affect our system,” said Parent. “This makes us very confident with our compliance audits.”

Rush realizes that there is no shortage of security challenges for medical centers, so they value Trend Micro as an ongoing partner and member of the strategy team. “We currently use Trend Micro encryption for our laptops, but I’d like to deploy Trend Micro encryption for all of our endpoints,” said Parent. “We’ve enjoyed a true partnership with Trend Micro and we may even develop a security solution together someday.”

“We have taken the next step in protecting our data, safeguarding our data, we are now at the next level. The threat landscape has changed and evolved here at Rush and Trend Micro has evolved with us,” said Radenkovic.

For More Information
For more information, please go to: http://www.trendmicro.com
DCI Donor Services Focuses More Time on Saving and Enhancing Lives Thanks to a Secure IT Environment

Trend Micro™ Deep Security, Trend Micro™ OfficeScan™, and Trend Micro™ ScanMail™ protect physical and virtual server environments, user endpoints, and email.

Overview
Few organizations have the capacity to impact life more than organ, eye, and tissue donor services, which connect the donors who make transplantation possible with patients whose lives are saved or enhanced by these gifts. DCI Donor Services (DCIDS) is a family of companies founded in 1971 that includes a tissue bank, eye bank, and organ procurement locations with 11 offices in Tennessee, California, and New Mexico. DCIDS supports potential donor families and provides care for them throughout the donor process.

DCIDS’s mission, vision, and values are summed up through their commitment to save and enhance lives. They connect people through organ donation and transplantation, as well as through their commitment to science, health, and hope. DCIDS’s mission is realized by mobilizing the power of people and the potential of technology to extend the reach of each donor’s gift.

Challenge
Given the sensitive nature of its lifesaving and life-enhancing operations, DCIDS is available for donors and patients around the clock, 365 days a year. In order to support an always-on network and protect the safety of patient information, DCIDS uses a traditional on-site IT environment. This includes a mix of physical and virtual servers, with plans to virtualize the majority of its servers in the future. However, supporting 300 users across the nation, operating between 400-500 computers, laptops, and other mobile devices in the field without central security management was becoming challenging and costly for the IT team.

Without a high level of visibility, DCIDS wasn’t confident its security vendor was automatically updating the machines with the latest security patches, leaving the organization vulnerable to attacks. “Our time wasn’t being put to good use because our security was consistently outdated and overmatched,” said Greg Bell, IT director of DCIDS. “We were constantly checking it.”

That made detecting attacks a big issue for DCIDS. “Given the poor performance of our machines, we realized our previous vendor wasn’t detecting as many threats as they should have,” said Taylor Atkins, System administrator for DCIDS. “We needed a far more effective and flexible solution for our environment.”

In addition to protecting its IT environment, DCIDS must also comply with strict healthcare regulations. Processing and distributing donor tissue and organs follows stringent safety guidelines and government mandates such as HIPAA. “We’re committed to maintaining public trust by providing the best possible security for all patient health information, including donors and recipients,” said Bell. “We wanted a solution that would help us ensure compliance and public trust.”

In addition to ensuring compliance, DCIDS wanted a security vendor that would support its planned virtual desktop infrastructure (VDI) implementation and keep its costs in check. “Our IT security costs were beginning to rise, and as we moved closer to a VDI environment, it was clear our previous vendor could not provide an effective solution at an affordable price point,” said Bell.

Finally, because organ donation is stressful for families, DCIDS is committed to providing exemplary customer service to its donors and patients. DCIDS wanted this level of customer service from its security vendor. Unfortunately, support from its prior vendor was inconsistent.

“We experienced a ransomware attack on a machine that had our prior security vendor installed on it. Fortunately, Trend Micro not only detected the attack, they protected the rest of the network and helped us quickly resolve the issue.”

Taylor Atkins,
System administrator, DCIDS

Why Trend Micro
After reviewing security solutions from a number of vendors, DCIDS selected Trend Micro for a number of reasons. “We’re a small company but we have enterprise-size security requirements. Trend Micro was the only vendor that understood our needs,” said Bell. “They helped us see how their solutions would solve our security challenges and support our business for the long term.”
It’s our policy to go the extra mile to protect patient information. After reviewing several competing solutions, it was clear that Trend Micro would provide the comprehensive security and central management we needed.

Greg Bell, IT director, DCIDS

Our reputation is very important to our public trust. Securing patient health information across all IT environments is a top priority for us.

Greg Bell, IT director, DCIDS

One of the deciding factors for Bell was the broad range of security services that Trend Micro offered, including the centralized management that protected DCIDS’s endpoints and physical and virtual servers with powerful cloud-based protection from viruses, malware, and advanced threats. Another factor was Trend Micro had VDI security that could support DCIDS’s ongoing move towards virtualization.

“We found Trend Micro solutions easy to use and they provided advanced security capabilities that our prior vendor lacked,” said Atkins. “And because Trend Micro was an authorized VMware solution provider and we planned to deploy VDI on a VMware platform, the choice for us was easy.”

Solutions

Today, DCIDS uses Trend Micro to protect its entire IT environment. Trend Micro Deep Security provides a comprehensive security platform that protects the company’s physical and virtual servers from data breaches and business disruptions—and achieves cost-effective compliance across these environments.

Trend Micro Deep Security also offers DCIDS the flexibility it needs to respond in an evolving threat environment with tightly integrated modules for anti-malware, web reputation, firewall, intrusion prevention, integrity monitoring, and log inspection. “Deep Security’s agentless security is a big advantage for us. It doesn’t hinder the performance of our servers, shields us from attacks, and secures our virtual desktop environment,” said Bell.

To protect its end users against the latest threats, DCIDS deployed Trend Micro OfficeScan for endpoint protection. OfficeScan protects physical and virtual desktops, laptops, and mobile devices with cloud-based global intelligence, integrated data loss prevention, and a virtualization-aware agent that improves endpoint performance across the organization.

For DCIDS, one important feature of OfficeScan was the centralized security management that enables enhanced visibility and control. “Central management of IT security was essential for us because it let us monitor our endpoints and users, and gave us back the time to focus our attention on more important, customer-facing projects,” said Bell.

To get mail server protection for inbound and outbound data that covers their entire internal and mobile workforce, DCIDS deployed Trend Micro ScanMail for Microsoft® Exchange®. ScanMail provides document exploit detection, enhanced web reputation, and sandboxing to protect DCIDS from malware and other security breaches. “Our email environment covers thousands of miles from Tennessee to California,” said Atkins. “It requires comprehensive security like ScanMail to stop spam, malicious URLs, and advanced threats.”

Results

DCIDS feels confident that by choosing Trend Micro to protect its IT environment and patient information, it can focus on its mission of saving and enhancing lives. By installing a centrally-managed solution for their virtual, physical, and email exchange environments, DCIDS was able to protect and monitor their IT environment to ensure patient and company data was always safe.

DCIDS has been particularly pleased with its end-user experience, which was enhanced with an easy-to-use solution that protects against threats and malware and operates behind the scenes without hindering performance. “Before Trend Micro, 50% of our serious virus problems required a complete re-install. This impacted user performance and ate up valuable IT time,” said Atkins. “With Trend Micro, we’ve had no re-installs as the result of a virus attack.”

Another area of value to DCIDS is the increased detection of malware that had previously gone undetected and could have put patient data in jeopardy. This helps DCIDS feel confident that their network is safe and they are compliant with HIPAA and other regulatory requirements.

“Our reputation is very important to our public trust,” said Bell. “Securing patient health information across all IT environments is a top priority for us.”

With OfficeScan, DCIDS is able to protect its endpoints while managing and monitoring security from a single central management console. “With a network like ours, spread across the entire country, being able to secure mobile and desktop devices under one platform simplifies the security for our network and improves our team’s productivity,” said Bell.

DCIDS has already seen the value of ScanMail which ensures DCIDS’ email is secured from attacks, with email alerts providing real-time threat detection and visibility. “ScanMail provides us with updates that integrate with other security layers to prevent attacks using a singular command,” said Atkins. “That integration is a huge time saver for us.”

The bottom line for DCIDS is having end-to-end security from a trusted partner that also helps DCIDS stay within its IT budgets. “Trend Micro’s solutions have reduced our overall security costs by 15%,” said Bell. “We haven’t had to reduce our IT staff, and our system administrators can now focus their time on more important projects.” It seems that saving security costs and saving lives now go hand in hand at DCIDS.
Deep Security is an IT life-saver at Ireland’s renowned Beaumont Hospital

**Overview**

With 3,000 staff and 820 beds, Dublin’s Beaumont Hospital is the second largest hospital in the Republic of Ireland. It is the National Referral Centre for Neurosurgery and Neurology, Renal Transplantation, and Cochlear Implantation, the principal teaching hospital for the Royal College of Surgeons in Ireland, and is closely linked with Dublin City University in the area of nurse training.

The Beaumont operates a VMware environment of vCenter servers managing ESX hypervisors, running over 260 virtual machines. This infrastructure enables the IT team to deliver virtual servers and desktops to senior clinical staff off-site in a highly efficient manner, with all the attendant benefits of VDI including rapid deployment of updates, ease of management, lower power usage, lower hardware expenditure and a unified desktop environment.

The team is currently in the process of upgrading its infrastructure to ESX 5.1 on vCenter 5.5 servers, including upgrades to the fibre switching.

**Challenges**

The IT team discovered servers were sluggish and slow to respond at certain times of the night. After consulting with IT partner Triangle Computer Services to assist with diagnosis, the Antivirus (AV) solution used by Beaumont was found to be the root cause. Put simply, the AV tool’s server scans were eating up resources, causing huge CPU spikes which led to unusably slow network speeds. Virtual machines even lost connectivity for periods.

The challenge is a common one for security products which are simply not designed for virtual environments and treat VMs as physical machines, causing these so-called “security storms”.

**Solution**

Based on their experience with other clients, Triangle suggested a hypervisor based security solution. After seeing a demo of Trend Micro Deep Security, the IT team proceeded to a proof of concept, running alongside their existing provider. This delivered an immediate improvement, and the decision was made to proceed to rollout with the assistance of Triangle. Deep Security features an agentless architecture for VMware virtual machines, handing over resource-intensive tasks like antivirus and other security scans to a dedicated, security-hardened virtual appliance. It also offers virtual patching, integrity monitoring, log inspection, firewalling, web security, plus it also deploys policy and scans any new VMs automatically to address instant-on gaps and inter-VM attacks.

**Benefits**

Installing Trend Micro Deep Security caused a noticeable improvement in the Beaumont Hospital’s VMware environment. Operationally there was no discernible hit to performance or any related network problems. In short, clinical staff was able to reap all the rewards of desktop virtualisation with no risk of a technology malfunction impeding their productivity.

For the IT department it has also improved troubleshooting—allowing the team to rule out their AV product as the cause of any future performance problems. They have also been impressed with the customisable dashboard interface of Deep Security, which allows admins to manage the entire virtual security environment from a single pane of glass.

“‘For us, Trend Micro is at the top of its game when it comes to security virtualisation—I believe no one can touch them.”

David Kelly, Virtualisation Manager at Beaumont Hospital

“Beaumont Hospital, Dublin
Region
EMEA-Ireland
Sector
Healthcare
Employees
3000
Trend Micro Solutions
- Deep Security
Business Benefits
- Noticeable improvement in the hospital’s VMware Environment
- Improved troubleshooting
- Ability to manage the entire virtual environment from a single pane of glass

"For us, Trend Micro is at the top of its game when it comes to security virtualisation—I believe no one can touch them.”

David Kelly, Virtualisation Manager at Beaumont Hospital
Navicent Health operates a designated Level I Trauma Center and one of 42 twice-designated Magnet® hospitals for nursing excellence nationwide. It provides a broad range of community-based, outpatient diagnostic and primary care; extensive home health and hospice care; and comprehensive cancer and rehabilitation services.

The Medical Center, Navicent Health is a 501(c)(3) private, not-for-profit corporation. The hospital is owned by the Macon-Bibb Hospital Authority and maintains an active affiliation with Secure Health Plans of Georgia, a network of central Georgia hospitals and physician providers.

**Challenges**

Within health systems such as Navicent Health, the already serious risk of targeted threats is compounded. Besides laptops, notebook computers, and smartphones, the hospital’s network hosts numerous biomedical devices that are not under the control of the in-house technology team, and do not run standard antivirus protection.

Medical devices with embedded processors are vulnerable to viruses and other malware threats. However, due to FDA regulations, memory limitations, or proprietary issues, these devices are typically not able to run antivirus or other security protection, and Navicent Health had no way to monitor or control the status of these devices without impacting performance or processes. Such unprotected and unmanaged biomedical devices pose serious risks, since any malfunctioning device can put patient care at risk. An infected device can also act as the source of network-wide infections, causing disruption and/or repeated cleanup costs.

When the Navicent Health security team began to see an alarming increase in time being spent on threat remediation across the health system’s infrastructure, they called on Trend Micro to help them assess end-to-end security, including security for their networked medical devices. While reducing costs and increasing productivity are always priorities, Navicent Health puts patient care first and therefore wanted to maximize the protection of private healthcare information and avoid any malware that could compromise the quality of patient care or privacy.

**Why Trend Micro**

Ten years ago, Navicent Health switched to Trend Micro AV solutions, including Office Scan and Control Manager. When the time came to evaluate advanced threat protection, they required a Best of Suite solution—right price, and right vendor, with proven technology, and leading-edge capabilities.

To minimize their risk exposure on non-managed systems and medical devices, Navicent Health implemented Trend Micro’s Deep Discovery Inspector. It offered a cost-efficient solution to track down malware and mitigate its risks, and minimized the IT time required to monitor security. With 360-degree monitoring of network traffic, all ports and over 80 protocols, Deep Discovery Inspector provides network-wide visibility and intelligence to detect and respond to targeted attacks and advanced threats.

It also provides a Web Services API to allow integration with other Trend Micro and third-party products, and a manual submission feature for threat research. Its custom sandboxing environments precisely match target desktop software configurations—resulting in more accurate detections and fewer false positives.
“From a strategic standpoint, we made a decision about 5 years ago to go with a security vendor that provided a competent ‘Best in Suite’ portfolio, so we standardized on Trend Micro for all of our security requirements. This led to our deployment of Deep Discovery Inspector, which protects the organization from targeted attacks and APTs.”

Ty Smallwood, Information Services Security Officer, Navicent Health

“Deep Discovery quickly paid for itself. In the first 48 hours, it detected viruses on vendor owned and maintained biomedical devices from several manufacturers that have traditionally not been as secure as they should be. We now had the visibility on the inside that we had on our perimeter. We are now adding Deep Discovery Analyzer to our portfolio which will provide us with even better visibility than before and allow us to scale.”

Ty Smallwood, Information Services Security Officer, Navicent Health

**Solution**

A security assessment identified several challenges with the previous levels of protection built into Navicent Health’s infrastructure, including vulnerable, non-managed medical equipment and public kiosks. As a first step, Navicent Health updated the previously deployed Trend Micro endpoint and mobility device solutions, and took advantage of many new security advancements, including enhanced control over USB devices and file, email, and web reputation checks.

However, even with strengthened endpoint security, Navicent Health still needed a better way to oversee medical devices, registration kiosks, and other thin-client devices on the health system’s network. The local Trend Micro team recommended the introduction of Trend Micro™ Threat Management System, the predecessor of Trend Micro Deep Discovery.

This additional layer of security gave the hospital automatic 24x7 threat monitoring, and gave IT increased visibility of the overall state of security. Ty Smallwood, Information Services Security Officer for Navicent Health, said, “Our first deployment gave us the tools we needed to approach the medical equipment manufacturers, and push them to patch their machines. It was about improving the quality of care we provide. The threat management solution helps us avoid legal liability issues by maintaining high standards with our partners.”

“Deep Discovery gives us an extra layer of security at a time when we are entering into Stage 2 Meaningful Use. This phase of HIPAA compliance calls for more stringent measures. Deep Discovery increases our ability to act quickly—it enhances our compliance position.”

Navicent Health has also taken advantage of Deep Discovery’s enhanced customization capabilities. “Deep Discovery gives us a lot more widgets—we can set up the console so that we get an at-a-glance look at what we are most interested in. Plus we get a sandbox architecture—Deep Discovery goes beyond threat detection to eliminate a lot of false positives with this capability. Now when I get an alert, I know it is something I need to carefully evaluate. This is a definite time saver.”

**Results**

Before strengthening on-premises security solutions and introducing a threat management solution, Navicent Health was spending valuable resources troubleshooting malware. Upgrading to the latest versions of Trend Micro™ Enterprise Security for Endpoints and Trend Micro Deep Discovery helped them simultaneously improve security and lower the cost of protection by minimizing risks.

“Our first deployment of the Trend Micro solution quickly paid for itself,” said Smallwood. “In the first 48 hours, it detected viruses on vendor owned and maintained biomedical devices from several manufacturers. Since upgrading to Deep Discovery, we have even better visibility than before. The rules and filters are much more fine-grained. We can more effectively focus on our hot spots and prevent risks from escalating into problems. I have a higher level of comfort—Deep Discovery has proved that it can catch critical threats in our areas of importance.”

“The visibility that we gain from Deep Discovery helps IT focus in the right places, and it also gives me compelling information to share with executives. I can show them exactly which threats we face—the sources, the destinations, and the details. The visual dashboard is a great tool for enlightening management about threats. I really like the dashboard and the meaningful reports because now everyone—not just IT—can understand the big picture.”

**What’s next?**

Navicent Health’s network structure includes multiple VLANs. Therefore, to allow them to scale and have all of their VLAN traffic go through one server, they have made the decision to expand their Deep Discovery deployment with Deep Discovery Analyzer. Deep Discovery Analyzer is a custom sandbox analysis server that will augment the capabilities of Deep Discovery Inspector.

Deep Discovery is helping Navicent Health prevent risks at the gateways. “Trend Micro solutions have successfully mitigated risks on our endpoints. Now our email and proxy gateways have the added sandboxing technology,” said Smallwood.

**For More Information**


To speak with a representative, contact us: [http://www.trendmicro.com/us/business/have-sales-contact-me/index.html](http://www.trendmicro.com/us/business/have-sales-contact-me/index.html)
Aomori Prefectural Central Hospital ensured safety with security optimized for a virtualized environment

Before
The hospital was worried that running several systems on a single server in a virtualized environment would result in wide-ranging damages if an incident occurred.

After
The hospital implemented the optimum security countermeasures for a virtualized environment. In particular, a VDI which used tablets swept away fears regarding performance.

Challenge
In recent years, Aomori Prefectural Central Hospital has pushed forward organizational reforms and reorganized wards, establishing treatment centers for each of four major illnesses, including cancer, heart disease, strokes, and diabetes. “In order to provide the best treatment and care for patients’ illnesses, we have a policy in which doctors and technicians from a number of departments, not just the department of treatment, come together to decide the best methods for treatment,” says Shigeaki Yoshida, Director General of the hospital.
In order to support such advanced medical services, the hospital actively engages with IT. However, a number of problems surrounding the hospital’s internal IT environment had surfaced recently.
First, there had been a shortage of PCs for electronic medical records. Because the PCs at nurse stations were shared, staff had to queue to use them in the evening and other busy periods. “Because of the waiting, work got held up and our operating efficiency deteriorated. Staff worked overtime, which led to an increase in personnel costs, so we had to work out a solution promptly,” explains the hospital’s Shigeaki Murakami.
The second problem was the way that servers were dispersed. Because each individual medical department had a variety of systems, servers were scattered throughout the hospital. In addition to putting pressure on limited space resources, it was difficult for the Medical Information Department to ascertain the type of IT resources used within the hospital, and where they were located. “When trouble arose we would contact the Medical Information Department. However, because of the on-site nature of day-to-day operations, it would take a lot of time to determine the cause of the problem. We felt that we had to reduce waste and also make improvements to governance,” says the hospital’s Hidaki Miura.
Consequently, it was virtualization technology that caught the eye of the hospital.
The hospital consulted with the company in charge of the project, NEC, used VMware® Horizon View™ (to construct a VDI (Virtual Desktop Infrastructure) to virtualize its desktops, and then distributed tablets to each member of the nursing staff. As a result, it became possible to access electronic medical records at any time, without the need to wait. “Tables have a superior cost-performance ratio over PCs, and don’t take up any space. We decided that providing a device for each staff member was the best method to increase operational efficiency at the optimum cost,” explains NEC’s Junichi Ono.
Due to improved integration rates and operating stability, the hospital decided to adopt VMware vSphere® to consolidate the servers dispersed in each department in the virtualized environment. “The Medical Information Department wanted to manage server resources centrally and migrate to a system which provided resources to each department as they were needed,” says Miura.
Although the hospital decided to migrate from a physical environment to a virtual one in this manner, a problem still remained - security.

**Solutions**

The hospital was worried that the scope of damage that resulted from an occurrence of an incident would be wider in a virtual environment in which a single server was running a number of virtual machines than in a physical environment. Furthermore, from the perspective of safe treatment, medical institutions such as hospitals demand advanced security countermeasures.

The hospital adopted Trend Micro’s Deep Security™. In addition to the proven track record of Trend Micro as a security vendor, the fact that Deep Security is optimized for VDI also supported the adoption.

Traditional antivirus solutions can easily cause a degradation in the performance of VDI. If an agent is installed in each virtual PC, the processing load on servers will increase when distributing pattern files and performing virus scans. “We were worried about performance because the VDI combined tablets and wireless LANs. If response times were slow and it wasn’t easy to use, the benefits of the deployment would be reduced by half,” reflects Murakami.

However, Deep Security coordinates with VMware vShield Endpoint, the security optimizer of the hospital’s VDI platform VMware vSphere, and the virtual appliance protection modules of Deep Security provide antivirus protection for each virtual PC. This controls sudden increases on server load, and maintains the appropriate responsiveness for the VDI.

Additionally, in regards to the hospital’s aim to consolidate department servers, Deep Security supported the adoption due to its compatibility with multiple types of server OS, including Windows and Linux. After evaluating these benefits, Aomori Prefectural Central Hospital decided to apply Deep Security to the entirety of its virtualized environment.

**Results**

There are now 410 virtual PCs running in Aomori Prefectural Central Hospital’s VDI. “Performance has been excellent. We feel that it is even quicker than our former setup,” says Miura. In the past, information from multiple patients was collected and entered into the system, meaning that there was a risk of mixing up patient information. However, because data entry operations can now be performed at any time, the hospital expects that medical safety will also be strengthened.

The unique ways in which tablets can be used continue to expand. For example, when explaining the medical conditions of patients to them at their bedside, tablets can display materials which enable the explanation to be easily understood. “Not only has operating efficiency improved, the deployment has also increased the quality of medical services,” explains Murakami.

The hospital is continuing to consolidate and unify the servers of each department into the virtualized environment. Specifically, almost 30 systems including pharmaceutical systems, device control systems, and meal provision systems are already running in the virtualized environment. “We want to push the consolidation forward even further, and we hope to eventually migrate core systems such as electronic medical records to the virtualized environment,” says Kenichi Takahashi, indicating his vision for the future.

Deep Security has maintained the safety of the virtualized environment and has also provided the benefits of an agentless solution.

One such example is a reduction of the time required for testing when migrating to a virtualized environment. “When migrating, you have to perform tests to ensure that the client software and each system that you had been using previously will run without problems in the virtualized environment. There is a natural risk that security products may interfere with your systems, but because Deep Security is agentless, we never had to worry about that possibility. This led to reduced testing times,” says NEC Fielding’s Hiroaki Sato.

This benefit has also proved useful for quickly isolating problems whenever trouble has arisen since starting operation of the VDI. This is because we can instantly eliminate the possibility that “it might be the security product” when we are investigating the cause of the problem. Consequently, Deep Security has contributed to stable operation of the virtualized environment, as well as providing antivirus functions.

Deployment of virtualization technologies has broadened the possible ways that Aomori Prefectural Central Hospital is able to apply IT to health care. “We wish to pursue new standards for health care by continually strengthening our IT environment,” concludes Yoshida firmly.
Adventist Health System Selects Trend Micro for Web Application Security

Trend Micro™ Deep Security for Web Apps provides a single, easy-to-manage solution for SSL certificates and application scanning

Overview

Today’s healthcare organizations in the United States face a growing number of challenges that require innovative solutions. From implementing the Affordable Care Act, to compliance with HIPAA and other regulations, healthcare providers are looking for ways to increase the quality of care, increase meaningful use of technology, and reduce costs.

Adventist Health System is a faith-based health care organization headquartered in Altamonte Springs, Florida. A national leader in quality, safety and patient satisfaction, Adventist Health System’s nearly 70,000 employees maintain a tradition of whole-person health by caring for the physical, emotional and spiritual needs of every patient.

With 45 hospital campuses and nearly 8,300 licensed beds in ten states, Adventist Health System facilities incorporate the latest technological advancements and clinical research to serve more than 4.5 million patients annually. The full continuum of integrated care also includes urgent care centers, home health and hospice agencies, and skilled nursing facilities.

Each Adventist Health System facility operates independently in delivering care and services to best meet the needs of the local communities they serve. While each entity is unique, all remain united in one mission: to extend the healing ministry of Christ.

AHS Information Services (AHS-IS) is a 695-person department of Adventist Health System that manages data centers, business applications, and IT applications across 32 of the 45 campuses. AHS-IS also acts as an information security provider for the corporate headquarters and individual campus operations. AHS works hard to maintain a high level of security and protection for patient health information accessed via web applications by both patients and healthcare staff.

Challenges

To help secure its web applications and portals, AHS-IS requires Secure Socket Layer (SSL) licenses for hundreds of domains. Their previous certificate provider required them to sign a yearly contract for a set number of licenses, but the frequent addition of new domains made it difficult for the IT team to accurately predict the number of licenses required in a given year. As a result, they often ran out of licenses part way into their yearly contract and had to open a new purchase order.

Managing licenses was also a challenge. With so many divisions using licenses, the process required to accurately track when SSL certificates were issued and when they would expire was time-consuming and labor-intensive.

“When we needed more licenses, we’d have to buy more at the last minute,” said Mark Dunkerley, Messaging and domain services team lead for AHS-IS. “The inability to predict how many SSL certificates were needed created a budget issue for our annual SSL purchases.”

Another challenge that AHS-IS faced was a lack of centralized management of their application security. With many web applications across their campuses, AHS-IS needed an application security solution that simplified monitoring and management across multiple locations.

For example, AHS-IS used a combination of Public-key Infrastructure (PKI) for internal apps and SSL certificates for external apps, forcing AHS-IS to monitor and manage multiple systems. “Trying to manage our PKI, SSL, and security for all of our websites and applications was very inefficient without a central management system,” said Dunkerley.

AHS also needed to make sure patient information was secure, encrypted, and HIPAA compliant across hundreds of domains. This meant securing operating systems, web servers, and applications throughout its AHS divisions. “Providing PHI (Patient Health Information) electronically and through the web requires us to be extremely cautious. We have to ensure that information is always secured at the highest of levels,” said Dunkerley.

“...When we needed additional credits for new domains, with our previous SSL vendor it could take days to get them published. With Trend Micro, all it takes is a simple email to the account team and it’s done, which is significant for us.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services
To find the right application security solution, AHS-IS initially focused on analyzing certificate authority vendors and considered analyst and peer recommendations. They selected Trend Micro Deep Security for Web Apps, which includes unlimited SSL certificates as well as application vulnerability detection and protection for a low, flat yearly fee.

Dunkerley says that his team at AHS-IS is looking forward to reducing the multiple vendors and their separate application security solutions with the centralized management provided by Deep Security for Web Apps. “The ability to track all of our SSLs and monitor them on one console will dramatically increase our IT productivity,” said Dunkerley.

AHS-IS has started to leverage the solution’s application and platform vulnerability scanning capabilities to increase the team’s confidence in the security of their web applications. They are also planning to test and compare some of the protection capabilities like intrusion prevention and web application firewall (WAF) rule generation.

“Overall, we strive to be as proactive as possible with security,” said Dunkerley. “Deep Security for Web Apps gives us greater visibility into our vulnerabilities and allows us to quickly address those issues and focus our IT efforts more efficiently.”

To comply with regulations and protect patient information, AHS-IS needs to continually scan applications and platforms for vulnerabilities and mitigate those issues quickly. Deep Security for Web Apps meets those needs by continuously detecting vulnerabilities at the app and platform layer and automatically protecting them with virtual patching of platform vulnerabilities or WAF rules.

The solution also removes distracting false positives found during web application scanning. “Trend Micro’s vulnerability scanning solution provides a proactive solution instead of a reactive one,” said Dunkerley. “It’s important to protect both internal and external portals and comply with HIPAA regulations. Protecting personal health information for our patients is a very serious matter that demands our highest scrutiny.”

Trend Micro Deep Security for Web Apps simplified Adventist Health System’s SSL purchases and delivered 70% in cost savings. AHS-IS no longer faces unnecessary and unpredictable purchase orders for SSLs thanks to the unlimited certificate model, including extended validation (EV) certificate capabilities found in Deep Security for Web Apps. “With Trend Micro’s unlimited SSL model, we no longer have to worry about how many licenses we might need for an entire year, or scrutinize decisions about SSL because of the cost,” said Dunkerley.

The Trend Micro solution also dramatically reduced the time AHS-IS had to wait for domain approvals. Prior to Trend Micro, AHS-IS would have to reach out to their different locations and collect paperwork in order to validate that they owned specific domains, a process that has taken up to two weeks in the past. “With Trend Micro, we’ve reduced our domain approval time from up to two weeks down to minutes,” said Dunkerley.

Using Deep Security for Web Apps, AHS-IS can manage application security, including SSL certificates in a single, integrated web-based console. This eliminates unnecessary tasks and gives AHS-IS greater administrative access and flexibility. “The ability to manage multiple divisions under one account has given us significant cost savings,” said Dunkerley.

With automated, continuous application and platform vulnerability scanning, and elimination of false positives, AHS-IS increased their confidence in the health of their web applications.

Dunkerley has also been impressed by the excellent customer support provided by Trend Micro throughout the entire implementation process. For example, Trend Micro detected an incorrectly issued 1024 bit SSL, and informed AHS-IS to help them resolve the issue the same day. “1024 bit SSLs were no longer going to be supported, so Trend Micro recommended we reissue it as a 2048 bit SSL. We quickly resolved what could have been an end-of-the-year problem,” said Dunkerley.

Looking ahead, AHS-IS hopes to address mobile security issues and bring your own device (BYOD) trends, and to continue providing the best possible protection for its systems and patient information. “We look forward to working with Trend Micro to help solve challenges posed by consumerization and mobility,” said Dunkerley.

“Trend Micro Deep Security for Web Apps gives us greater visibility into our vulnerabilities and allows us to quickly address those issues and focus our IT efforts more efficiently.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services

“With the Trend Micro solution, we reduced our domain approval time from up to two weeks down to minutes.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services

Solution

Results

With the Trend Micro solution, we reduced our domain approval time from up to two weeks down to minutes.

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services

“With the Trend Micro solution, we reduced our domain approval time from up to two weeks down to minutes.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services

“With the Trend Micro solution, we reduced our domain approval time from up to two weeks down to minutes.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services

“With the Trend Micro solution, we reduced our domain approval time from up to two weeks down to minutes.”

Mark Dunkerley,
Messaging and domain services team lead,
AHS Information Services
Ochsner Health System Helps Maintain the Vitality of 15,000 Users and 1,000 Servers with Trend Micro Security Solutions

Maintains stable platform to support delivery of high-quality healthcare.

Overview
Delivering high quality healthcare in a region that’s vulnerable to large-scale disasters is critical. Founded in 1942 in Southwest Louisiana, Ochsner Health System is a non-profit healthcare provider that delivered key support to the victims of hurricane Katrina. It hosts one of the largest non-university based physician training centers, and conducts approximately 300 ongoing clinical research trials annually.

To help bring stability to this region in the aftermath of hurricane Katrina in 2005, Ochsner stepped up to acquire four additional hospitals that were closing. Ochsner is now the largest healthcare system in the area with 900 physicians, 90 medical specialties, 10 hospitals and 45+ neighborhood health centers. Ochsner employs an IT team of 280 technicians, which oversees 15,000 workstations and 1,000 servers. They have a primary data center in Jefferson Parish, Louisiana, and a disaster recovery center in Tennessee.

Challenges
As a significant healthcare provider in the region, Ochsner must protect patient data as well as proprietary business information. With the awareness that comes with an increasingly sophisticated threat landscape, Ochsner wanted to provide a predictable IT environment for 24/7 compliance, rock-solid security, and improved customer satisfaction. “The five pillars of Ochsner’s mission are to serve, heal, lead, educate, and innovate,” said William Schley, IT Director for Ochsner Health System. “We take the stewardship of healthcare data very seriously. In order to uphold our pillars of excellence, we go beyond regulatory requirements to protect our patient information.”

Having quadrupled in size through acquisitions since hurricane Katrina, Ochsner also acquired a variety of disparate systems that had to be integrated and protected. In 2001, Ochsner operated 200 servers. Today, their network uses over 1,000 servers. “As we expanded our services, it was important to maintain our reputation,” said Schley. “To do so, we needed to protect our growing IT environment with a reliable security solution.”

With a data center environment that was 80% virtualized and a non-virtualized desktop environment, Ochsner wanted a solution that could efficiently manage their private cloud, desktop, and virtualized ecosystems. “We have a diverse network that requires multiple layers of protection,” said Schley. “Keeping our IT environment secure is one of our biggest concerns.”

In addition to simplifying the management of their core services, Ochsner required a comprehensive system that managed security from a single pane of glass. “After hurricane Katrina, we acquired a handful of hospitals with disparate systems, some virtualized, some not,” said Schley. “We wanted a solution with sophisticated yet simple capabilities that would allow us to manage the system from a single console.”

Why Trend Micro
A satisfied Trend Micro customer for well over a decade, Ochsner chose not to explore solutions from other competing security vendors. “Other security vendors would take days to respond to our service needs, while Trend Micro was always just a call away and very responsive,” said Schley. “We really appreciate our close relationship with Trend Micro, and the knowledge provided by their Premium Support Services—they have been an excellent security partner.”

“Our goal is to maintain a stable platform to support the delivery of high-quality healthcare in our region. Trend Micro allows us to do that at the highest of levels.”

William Schley,
IT Director, Ochsner Health System
Ochsner turned to Trend Micro for a Complete User Protection solution in order to provide 24/7 compliance, end-to-end security, and customer satisfaction. The solution includes Trend Micro™ OfficeScan™, ServerProtect™, and Trend Micro™ Control Manager™. With familiar tools that protect its wide-spread IT environment and valuable customer data, Ochsner is able to manage all security from a single console.

To deliver real-time protection for Ochsner against the latest threats, OfficeScan was deployed for both physical and virtual endpoint environments. OfficeScan enhances Ochsner’s endpoint protection with cloud-based global threat intelligence, integrated data loss prevention, and a virtualization-aware client that reduces the endpoint footprint, protects sensitive data, and improves endpoint performance across the organization. “OfficeScan has been an excellent tool for our IT department,” said Schley. “Its flexibility provides us with the capabilities we need to adapt in a complex environment.”

While simplifying and automating security operations on Ochsner’s 1,000+ servers, Trend Micro ServerProtect solution delivers reliable virus, spyware, and tool kit protection. The solution scans and detects malware in real time and helps remove malicious code and repair system damage. “The virus containment capabilities of ServerProtect have been very effective at preventing the spread of malware,” said Schley. “We rely on Trend Micro’s prompt protection and clean-up capabilities to the fullest. Their automated approach keeps viral threats off our radar and turns security into a non-issue for management.”

With multiple Trend Micro solutions to manage, Ochsner uses the end-to-end visibility of Trend Micro Control Manager to monitor their entire security environment, enable centralized policy management for data and threat protection, and quickly identify issues. “Control Manager makes it so easy to assess status and respond to security events. We use the quarterly reports to keep our entire organization updated on security issues and requirements,” said Schley.

The Ochsner IT team realizes that vital patient information flows throughout their systems, and takes the responsibility to protect that data very seriously. Ochsner looks to Trend Micro to keep their environment protected and allow their IT team to focus on more important issues. “Instead of dealing with malware, we can work on value-added activities that directly benefit the business,” said Schley. “Trend Micro provides a secure IT environment that earns the trust of our patients. That’s big.”

Ochsner has enjoyed dramatically improved physical and virtual endpoint protection from OfficeScan with capabilities like virtual patching against zero-day threats. “When we found a zero day problem, we sent Trend Micro the information,” said Schley. “They promptly issued a new signature to avoid the threat.”

With ServerProtect in place, we can easily deploy security to new physical or virtual servers and enable policy enforcement,” said Schley. “The solution downloads scan engine updates automatically, making it much more efficient and effective compared to manually updating the scan engine for a thousand servers.”

A high level of security protection at Ochsner is confirmed by recent reports. “According to those reports, 99% of our products are protected, and 97% of attempts to access the system were detected and quarantined,” said Schley. “Those are exceptional numbers that we are very pleased with.”

The cherry on the top has been the Trend Micro Control Manager central console. It has given Ochsner improved visibility across the IT environment, providing peace of mind that its systems and private information are always protected. “Trend Micro makes it easy to forget about the numbers. We don’t need to worry about IT threats—Control Manager makes it easy for us to see problems and fix them before they impact users,” said Schley.

What’s next?

While pleased with the depth and breadth of Trend Micro security solutions, Ochsner knows that it must continue to prepare for the future. Ochsner is considering Trend Micro™ Deep Security™, which would support desktop virtualization and further enhance Ochsner’s IT security profile. “We plan to continue innovating and providing a high-quality IT environment to support Ochsner’s medical environment,” said Schley. “As we grow, we will look to Trend Micro for solutions that can help us protect that environment. Our goal is to maintain a stable platform to support the delivery of high-quality healthcare in our region. Trend Micro allows us to do that at the highest of levels.”

For More Information

For more information, please visit www.trendmicro.com/switch
Conclusion

As you’ve seen in the preceding pages, healthcare organizations are choosing Trend Micro to help them improve security and meet compliance needs. Each of their stories—their real-world experiences, challenges, and successes—is unique. However, they all share the need to focus on caring for their patients’ real lives, without letting the job of protecting their digital lives burden their resources.

In addition, they all see the value in deploying a solution powered by the world’s most advanced global threat intelligence system. The Trend Micro Smart Protection Network enables rapid and reliable threat analysis to speed detection of, and response to, targeted attacks.

Organizations that are challenged by complex, incomplete security systems—difficult and time-consuming to configure and manage—find that Trend Micro solutions provide comprehensive, layered protection that is fully integrated across the network, along with simple, centralized management to speed operations.

Now that you’ve learned how Trend Micro’s smart, simple, security that fits is helping your peers to secure endpoints, data centers, and networks, you may want to learn more about how we can help you meet your organization’s security and compliance challenges. If so, the next step is to contact us. You’ll find we’re eager to learn about your needs and concerns, and to help craft a solution that makes it easy for you to protect your patients’ digital lives—so you can focus your resources on your primary mission to care for human lives.

Learn more about Trend Micro Healthcare security solutions.