Caring for patients and their private information

Recognizing data protection as a key patient service, St. Cloud Orthopedics takes a proactive approach with a Dell solution that improves endpoint security.

“Our providers can work at the clinic or from home because we can allow client devices to leave our network and still stay HIPAA-compliant with Dell data security solutions. If we are audited, we can prove all our devices are always encrypted and protected.”

Jeff Duclos, IT Director of Network Administration, St. Cloud Orthopedics

Business need
To deliver excellent care, St. Cloud Orthopedics must protect patients’ data from cybercriminals, avoid becoming victims of ransomware and comply with increasing regulations.

Solution
The clinic now manages 350 devices with Dell solutions that encrypt drives, protect against advanced persistent threats, and automate endpoint management including event ticketing and software patches.

Benefits
- Stops ransomware and other malware before it can execute
- Protects patients’ health and credit card information
- Simplifies compliance with federal regulations
- Facilitates mobility for clinicians and other employees
- Saves a day of work each month for IT staff

Solutions at a glance
- Data Security
- Endpoint Security

Customer profile

Company  St. Cloud Orthopedics
Industry  Healthcare
Country  United States
Employees  140
Website  stcloudorthopedics.com
Medical records are worth up to 20 times more than credit card numbers and between 2010 and 2015, there was a 125 percent increase in criminal attacks on healthcare systems. But while healthcare organizations must prevent unauthorized data access, avoid being held hostage by ransomware attacks and comply with increasing regulations such as HIPAA and PCI, they still need to devote the majority of resources to helping patients.

St. Cloud Orthopedics is a leading provider of bone and joint care. Its clinicians and physical therapists work from a main office in Sartell, Minnesota, as well as neighboring hospitals and partner sites. Given the alarming upturn in IT security threats — including a ransomware attack that rendered workstations at a Los Angeles hospital inoperable for more than a week — St. Cloud Orthopedics conducted a security audit as a precautionary measure. Jeff Duclos, IT director of network administration at St. Cloud Orthopedics, says, "We’ve never had to deal with any serious malware but I don’t even want to know what ransomware feels like. With the way the world is changing, especially with the increase in cybercrime, we want to be sure we’re doing everything we can to protect our data. And our ability to operate as a clinic is very much dependent on technology functioning at 100 percent."

"It was really eye-opening to see how Endpoint Security Suite Enterprise doesn’t even give malware a chance to run on a system.”

---

Jeff Duclos, IT Director of Network Administration, St. Cloud Orthopedics

---

Protecting patients by increasing endpoint security
The audit yielded one recommendation to reduce risk: add an anti-malware solution that can protect against advanced persistent threats (APT) by immediately detecting changes on the network and devices, including modifications to BIOS settings. This is critical to prevent ransomware, but it also prevents data loss because malware often deletes data or corrupts drives as soon as it runs. “Conventional antivirus programs are only reactive,” Duclos says. "They can only detect a threat after it’s running and then they try to get rid of it.” By then, however, the APT will have damaged files — or worse, hijacked systems or data.

To gain the APT capabilities it sought, St. Cloud Orthopedics implemented Dell Data Protection | Endpoint Security Suite Enterprise. The clinic had already been encrypting its workstations, laptops and USB drives using Dell Data Protection | Encryption (DDP | E) but by upgrading the devices to Endpoint Security Suite Enterprise, it would gain an industry-leading anti-malware solution that includes artificial intelligence technology acquired from Cylance. "We’ve liked DDP | E and we didn’t want to add another vendor, so it made sense to upgrade to Endpoint Security Suite Enterprise,” says Duclos. "Also, we felt confident about the product, and it was really eye-opening to see how Endpoint Security Suite Enterprise doesn’t even give malware a chance to run on a system."
Maintaining continuous patient care while upgrading security
To minimize disruptions to clinicians and patients, St. Cloud Orthopedics engaged Dell Deployment Services to help with the initial installation and configuration of Endpoint Security Suite Enterprise. “We do not pretend to be experts in every area, and we have a very lean IT department,” Duclos explains. “So we rely on outside experts like Dell Deployment Services to help us manage and protect our devices and network as necessary.” In addition to providing a day of training, the Dell technicians worked with Rob Maus, system specialist at St. Cloud Orthopedics, to deploy Endpoint Security Suite Enterprise on a central server so that it interoperates with the clinic’s firewalls and network to meet specific requirements. Technicians also walked through the ESSE installation on some client devices to explain the various settings. “That right there — working with Dell technicians as they installed the product on the server and clients — gave us very good insight into how the whole product works,” says Maus.

After the initial work with Dell technicians, the clinic’s IT staff managed the rest of the deployment. “We upgraded our 350 client devices to Endpoint Security Suite Enterprise over a few months,” Duclos says. “The whole process went very well. We were able to upgrade the server and all our devices without any clinic outages.” Installing the software on each workstation, laptop and thumb drive took about 20 minutes and encrypting a device required about two hours, so IT staff upgraded devices when the clinic was closed, managing a few every day.

Ensuring clinicians and other staff can work where and when they need to
Caring for patients isn’t something that just happens between 8:00 a.m. and 5:00 p.m. in one room, which is why the mobility clinicians and other staff gain with Endpoint Security Suite Enterprise is so important. “Our providers can work at the clinic or from home because we can allow client devices to leave our network and still stay HIPAA-compliant with Dell data security solutions,” says Duclos. “If we are audited, we can prove all our devices are always encrypted and protected.”

This is critical because even though St. Cloud Orthopedics keeps patient data on central servers in a secured data center, cybercriminals often attack client devices. If one becomes infected with malware and then logs on to a virtual private network (VPN), a criminal can infiltrate the VPN. With this solution, St. Cloud Orthopedics protects against such threats because the Endpoint Security Suite Enterprise server communicates with client devices to ensure they are also running Endpoint Security Suite Enterprise. That way, both the client and server monitor for any suspicious activity on devices and the network.

Gaining more time to focus on patient services
Although security is critical, IT staff want to dedicate the bulk of their time to developing new services that can improve patient care. “All the protection that we’ve put in place with Endpoint Security Suite Enterprise has really cut down on issues and management tasks,” says Maus. “We’re saving at least a full workday’s worth of time each month.” Not only are IT employees spending less time manually monitoring client devices, but also they now have one tool for encryption, anti-malware and reports.

“It’s much easier being able to manage encryption and anti-malware from one console,” says Duclos. “We have one less product we need to learn and the console is easy to use. It gives us a lot of information at a glance, and if you want to look at information about potential malware or viruses, you just scroll down and access clickable graphs. It’s also really easy to navigate through the encryption and security policies.” In addition, if IT staff ever have a question
or issue with Endpoint Security Suite Enterprise or their client devices, they can contact Dell Support.

**Taking an extra step to protect patient data and simplify compliance**

Shortly after implementing Endpoint Security Suite Enterprise, the clinic decided to enhance its protection against security threats by increasing insight and control over software on client devices with a Dell KACE K1000 Systems Management Appliance. "We were using a free program for pushing out software updates, but we gain a lot more tools to help manage devices and the network with Dell KACE," explains Duclos. "The ticketing system logs and tracks security incidents, and we can manage software inventory and patching — which are all important for regulatory compliance. We didn’t look too hard at other client management programs in the market. In talking with people who use them, we’ve learned that they have to dedicate a person to manage them because the tools are so difficult to learn. Dell KACE is very straightforward."

Although the K1000 appliance is installed at the clinic’s data center, IT staff are working with Dell Deployment Services to configure all the capabilities over the next few months. In addition, the clinic is having its security consultant perform trial HIPAA and PCI audits to ensure compliance with the latest requirements and to save time if it is audited in the future. "There are many types of reports we need to create for auditors," says Duclos. "We can generate those reports that will help with PCI compliance using KACE — and Endpoint Security Suite Enterprise will help with HIPAA compliance. We will always need to work tirelessly at protecting patient data and meeting regulations, but with all the measures we’ve put in place with Dell, we’re further along than a lot of clinics, so we’re happy about that."

Dell, the Dell logo and KACE are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others. Availability and terms of Dell Software, Solutions and Services vary by region. This case study is for informational purposes only. Dell makes no warranties — expressed or implied — in this case study. Reference Number: 10022974 © September 2016, Dell Inc. All Rights Reserved.