Saint Francis Healthcare stays safe from cyberattacks

Secures thousands of endpoints vital to patient care

THE CHALLENGE

With patients' health at stake, physicians need uninterrupted access to vital medical information. Saint Francis Healthcare System's previous antivirus software, from Trend Micro, made this more challenging because it erroneously blocked critical applications, requiring doctors to call for support at all hours.

The Trend Micro software also created scan storms, dragging virtual desktop sessions to a crawl. This forced the IT team to remove antivirus programs from the virtual desktop infrastructure, leaving thousands of endpoints unprotected.

To fill the gap, IT added protection with Malwarebytes. Still, the infamous CryptoLocker ransomware evaded the protective layer, disrupting productivity. Because policies across Trend Micro and Malwarebytes often conflicted, engineers couldn't keep up with the constant fixes, which further exposed endpoint protection to risk.

THE SOLUTION

To consolidate and strengthen endpoint protection, Saint Francis Healthcare System evaluated solutions from Cisco, Carbon Black, Sophos and Bitdefender. Ultimately, Bitdefender's solution offered the most complete endpoint protection. Specifically, that meant providing strong antivirus and antimalware, along with advanced device control, application blacklisting, and endpoint firewall encryption, all through a single console.

Saint Francis Healthcare System replaced Trend Micro and Malwarebytes with Bitdefender GravityZone Enterprise Security Suite, which includes Security for Virtualized Environments and Security for Endpoints.

Deployed on premises for 3,000 users, GravityZone protects 2,200 Microsoft Windows-based physical PCs, 2,100 virtual desktops delivered through VMware Horizon and Citrix XenApp, and 425 Windows and Linux servers. GravityZone provides physicians, nurses and administrators with secure, reliable access to the provider's Epic electronic medical record (EMR) systems and legacy EMRs such as AllScripts, Mosaic and eClinicalWorks, as well as payroll, asset tracking and other business applications.

THE RESULTS

Since adopting the GravityZone solution, Saint Francis Healthcare System detects and blocks cyberthreats in near real time. In one month, GravityZone caught 44 viruses on endpoints,

SAINT FRANCIS HEALTHCARE SYSTEM

Medicine to the Highest Power

Saint Francis Healthcare System is a 308-bed facility serving more than 713,000 people throughout Missouri, Illinois, Kentucky, Tennessee and Arkansas. The progressive, innovative regional tertiary care referral center has been named one of the top 100 "Best Places to Work in Healthcare" by Modern Healthcare magazine for six consecutive years.

Industry
Healthcare

Headquarters
Cape Girardeau, Missouri, U.S.A

Employees
3,000 (IT staff, 24)

Results

- Detected and eradicated advanced malware in seconds
- Reduced time to execute exclusion policy updates from 60 to five minutes
- Saved $90 per week in security administration
- Decreased security-related trouble calls by at least 10 percent

stopping even sophisticated ransomware such as WannaCry and Petya. And GravityZone performs without any impact on endpoint performance.

"I've seen first-hand how GravityZone detects a virus and gets rid of it within a couple of seconds," says Phillip Yarbro, network systems engineer, Saint Francis Healthcare System. "When the WannaCry and Petya attacks began, we received a proactive email from Bitdefender alerting us that their virus definitions were already updated and we were protected. That gave everyone here a lot more peace of mind, especially with all the breaches happening at other hospitals."

GravityZone also gives IT greater insight through monthly malware reports that help the team spot trends and uncover opportunities to strengthen protective measures.

"The reports let us see things like the top ten infected endpoints and help us determine if users need to change behavior or we need to modify their workflows, or take some other action to address the issue," says TJ Crowden, Saint Francis Healthcare System's assistant manager, IT infrastructure. "That's more proactive than we could ever be with our previous solutions."

With the GravityZone console, IT can manage exclusion policies more easily and effectively. Before, it could take an hour to determine which application was blocked on a particular endpoint. Now, Yarbro says it takes five minutes to troubleshoot and add an application to the exclusion policy. Overall, security administration time has decreased from 2.5 hours to 15 minutes per week, and security-related trouble calls have dropped by at least 10 percent.

"Consolidating onto a single solution managed through one pane of glass essentially cut our software licensing costs in half," says Yarbro. "And the time savings reduced our administration costs by $90 per week. That allows us to spend more time and resources on things like surgery software and other applications that directly impact patient care."

"When the WannaCry and Petya attacks began, we received a proactive email from Bitdefender alerting us that their virus definitions were already updated and we were protected. That gave everyone here a lot more peace of mind, especially with all the breaches happening at other hospitals."
— Phillip Yarbro, Network Systems Engineer, Saint Francis Healthcare System

Bitdefender Footprint
- GravityZone Enterprise Security
- GravityZone On-Premises Management Console

IT Environment
- AllScripts
- Citrix XenApp
- eClinicalWorks
- Mosaic
- VMware Horizon View

Operating Systems
- Linux
- Microsoft Windows

18052020-Bitdefender-CaseStudy-Sfrancis-crea2058-A4-en_EN