Sophos Inspires Healthcare Provider to Take Its Security to an Advanced Level of Endpoint and Network Protection

MaineGeneral Health is a not-for-profit healthcare provider serving patients in 88 municipalities throughout the Kennebec Valley, which covers more than 5,000 square miles from central Maine to the Canadian border. MaineGeneral Health offers a broad spectrum of services, including inpatient and outpatient care, at its Medical Center and one comprehensive outpatient center, state-of-the-art outpatient cancer treatment, physician practices, nursing homes, home healthcare, and even retirement living options. It is also the largest private employer in the Kennebec Valley.

Senior Information Systems Security Specialist Joshua Dostie has had a long history with MaineGeneral Health. He initially performed volunteer IT work there when he was in high school and, after completing his computer science degree, joined the company as a systems engineer. For Dostie, security has always been a deep-rooted hobby and a passion. He has always made a point of staying on top of the latest malware and security technologies. When MaineGeneral Health decided to expand its security initiatives in 2017 and assigned him to lead the charge, Dostie had the opportunity to turn his passion into a career.

CUSTOMER-AT-A-GLANCE

MaineGeneral Health

MaineGeneral Health

Industry
Healthcare

Website
mainegeneral.org

Number of Users
3,800

Sophos Solutions
Sophos Intercept X Advanced with EDR
Sophos Intercept X Advanced for Server
Sophos SafeGuard Encryption
Sophos XG Firewall
Sophos Sandstorm for Web Protection Advanced

Challenges

- Attaining buy-in to replace out-of-date security with a modern, integrated solution
- Educating users and stakeholders about the importance of proactive security
- Safeguarding sensitive health data to comply with the Health Insurance Portability and Accountability Act (HIPAA) and protect patient information
- Building an in-depth yet easy-to-manage defense against known and unknown threats
- Bridging the gap between prevention and response with an automated security solution
- Implementing full-coverage network protection

Where do you start when you are faced with outmoded protection and a culture that requires security awareness?

Dostie began by reviewing the state of security in the organization and discovered that there was a general feeling that continuous security improvements within the division was essential. His goal was to bridge that gap to help make it a more comfortable, recurring topic. Dostie finds that, in general, healthcare organizations typically perform a HIPAA risk assessment annually, internal audits for Payment Card Industry (PCI) compliance if needed, and some penetration testing of their existing defenses—but they rarely take a proactive approach to uncover vulnerabilities. This is largely due to the amount of work that comes with the field that is difficult for even a fully staffed team to accomplish.

Dostie took on the role of risk advisor and went deeper, showing IT stakeholders and other departments at MaineGeneral Health the harm that could ensue from a serious ransomware attack or breach. Dostie's motto has always been: "When you are informed, you'll be secure. For me, the best way to make people aware is simply to share knowledge with them." As an example, he brought in the Sophos team to show stakeholders how crippling a ransomware attack could be and how Sophos Intercept X could successfully block the threat and mitigate the damage.

The educational and advisory work initiated by Dostie in 2017 was an eye-opening experience. Once IT and upper management became more aware of the potential impact of cyberattacks, they knew they had to increase funding to include expanding staff and investing in more advanced security solutions.

How does Sophos help defend an organization against known and unknown threats?

Fast forwarding to today, the security program has matured, made great strides, and expanded significantly, with two additional IT staff members and an advanced, comprehensive security solution. MaineGeneral Health now has a full complement of Sophos solutions that cover endpoints and the network. Since his initial call with Sophos, Dostie was convinced. The level of automation and

'Sophos is working 24 hours a day, so I don't have to.'

Joshua Dostie
Senior Information Systems Security Specialist
MaineGeneral Health

'The biggest driver for us was having single-pane-of-glass management to see what's going on. The thing with Sophos is that it is so in-depth – so granular, and yet so simple.'

Joshua Dostie
Senior Information Systems Security Specialist
MaineGeneral Health

integration that Sophos brings to the table is completely in sync with Dostie's mindset.

"People purchase antivirus to protect what they know; we partnered with Sophos to protect what we don't know," says Dostie. "Plus, I can't always be at a user's desk to respond to an incident. Sophos is working 24 hours a day, so I don't have to – whether there's a breach or not. The automated processes bridge that gap between prevention and response."

How does Sophos security management make cloud migration easier and more seamless?

Another big motivation for moving to the Sophos platform was MaineGeneral Health's cloud migration initiative, which has gone so smoothly that users hardly notice the change. Dostie points out that the cloud-based centralized management console, Sophos Central, perfectly complements the new cloud infrastructure. Previously Dostie had to juggle 10 different security consoles, whereas now he can gain immediate visibility into his organization's security posture on premises and in the cloud, along with alerts, all on a single, intuitive dashboard.

"The biggest driver for us was having single-pane-of-glass management to see what's going on. Sophos is so in-depth, so granular, and yet so simple," affirms Dostie.

What are the Sophos endpoint technologies that are instrumental in reducing risk to users, sensitive healthcare data, and systems?

At MaineGeneral Health, endpoints are protected by Sophos Intercept X Advanced with EDR. This solution combines multiple next-generation technologies, including machine learning, a form of artificial intelligence, to combat ransomware, emerging threats, and the latest hacker techniques. It also includes endpoint detection and response (EDR), which provides guided investigations to prioritize threats and enable deep analysis.

Dostie finds that the product accelerates forensics: "What I like about Sophos EDR technology is that, if it detects something like a malicious attachment, I get the alert in minutes and it paints the whole picture for me so I can focus on remediation and preventive measures. I get a snapshot of the affected device right from the screen. It basically offloads the heavy lifting. What would normally take hours is done in less

'Having Sophos here is like having an additional security operations center (SOC) under our control because it's doing so much of the work for us.'

Joshua Dostie
Senior Information Systems Security Specialist
MaineGeneral Health

than five minutes. Realistically, these days, we don't have to respond to that much anymore because Sophos does all that work for us."

When it comes to servers, Dostie and his team operate under the assumption that they house or eventually will house sensitive information, including protected health information (PHI). He ensures that every single server follows HIPAA guidelines. The team has also deployed the server version of Sophos Intercept X Advanced, which has server-specific features and controls to protect applications and data on servers from ransomware, zero-day threats, credential theft and more – all without impacting performance. Dostie has taken all these precautionary measures to reduce risk to MaineGeneral Health.

To further boost endpoint and data security, Dostie also implemented Sophos SafeGuard Encryption, an enterprise-strength, always-on solution that encrypts sensitive data when it's created and ensures seamless, secure collaboration. Sophos SafeGuard Encryption provides both full-disk encryption for Macs and PCs and encryption for individual files. This assures Dostie and his team that, even if files are transferred to a shared folder, removable USB drive, or the cloud, they will stay encrypted.

What are the elements required for complete network security?

For network protection, Dostie recently deployed four Sophos XG Firewalls. These next-generation appliances provide him with expanded visibility into the network. "XG Firewall has provided our entire organization next-generation visibility and protection. Moving to Sophos for our network security allows us to simplify and consolidate. In terms of savings, it's just more efficient for us. Adding in Synchronized Security made sense because we are making the most of what we have on the network and on the endpoint," expresses Dostie. Built-in Sophos Synchronized Security allows endpoints and the firewall to communicate with each other and share information on threats and security posture.

"Sophos Intercept X detects ransomware on a workstation and sends that information to the Sophos XG Firewall, which then blocks internet or network access. Having Sophos here is like having an additional security operations center (SOC) under our control, because it's doing so much of the work for us," observes Dostie.

Sophos Sandstorm, which is available on Sophos XG Firewall, is a cloud-based sandbox

environment that adds an extra layer to MaineGeneral Health's security. Powerful, cloud-based, next-generation sandbox technology and deep learning analysis mean Dostie and his team can quickly and accurately detect, block, and respond to advanced persistent threats (APTs) and zero-day threats.

"Sophos does a great job at protecting what is known, but when you're wondering about how to protect against what we don't know, Sophos Sandstorm is the answer. When it discovers unknown software, Sandstorm looks at its behavior before it even gets to the internet. I believe Sophos Sandstorm is an extra sanity check. It helps us feel more comfortable about giving users access to the web," Dostie explains. "Now pretty much every way into our network is protected by Sophos."

Why is communication so essential in the process of transforming information security?

Throughout this successful journey to the cloud and a modernized security program, Dostie has emphasized the value of communication with the IT team, users, and management.

When it comes to launching a new security initiative or transforming existing practices, Dostie shares these words of wisdom with his peers: "Communication is often the most difficult hurdle. If you can't get buy-in, even the greatest initiative in the world won't go anywhere. Who wants to drive a car they have never been in before? I've learned that it's critical to communicate with people and make them feel safe and comfortable. Before you deploy solutions on your production systems, put them on a test box and let people try them out and learn the process. If your users are invested, they will support you."

For Dostie, communication and close collaboration with vendors is also vitally important. One of the things he likes about Sophos is the availability of informative, quality resources like the Sophos Naked Security blog space and open communication with Sophos Labs. "If I have something I think is potentially malicious and I don't think it's getting detected, I can send the malware sample right over to SophosLabs for analysis, and they get back to me with an assessment. With Sophos, you have that constant stream of communication that you really don't see with other vendors," he notes.

Dostie is eager to share his experiences with others and believes Sophos has provided many benefits that extend beyond securing MaineGeneral Health. "When I have a conversation with somebody from Sophos, I feel truly inspired to do something new or try something different. Not only does Sophos talk the talk, they also walk the walk. Sophos has just made my career so enjoyable. It's gratifying to see how Sophos solutions integrate and how we can make a positive impact on both our company and our community," emphasizes Dostie, with great satisfaction.

SOPHOS

'With Sophos, you have that constant stream of communication that you really don't see with other vendors.'

Joshua Dostie
Senior Information Systems Security Specialist
MaineGeneral Health

Start your free trial of Sophos Intercept X Advanced with EDR today.