SOPHOS

Benedictine Monks Streamline Security Management and Boost Their Defense with Sophos Synchronized Security

Customer-at-a-Glance

Benedictine Order of Cleveland

Industry
Religious organization

Number of Users
23

Sophos Solutions
Sophos Synchronized Security
Sophos Central Endpoint Protection Advanced
Sophos Central Server Protection Advanced
Sophos Intercept X
Sophos XG Firewall

The Benedictine monks of St. Andrew Abbey in Cleveland provide multiple services for their community: Catholic education, parish ministry, upkeep of St. Andrews Abbey, and pastoral service. In addition to operating Benedictine High School for young men in Cleveland and leading Assumption Parish in Ohio's Broadview Heights, they also offer resident chaplain services and assist the staff at the Loyola Retreat House near Akron.

Like many modern monastic orders, the St. Andrew monks use both desktops and laptops to help them fulfill their religious duties and mission. To ensure that online activities are secure inside and outside of the monastery, the monks chose Sophos Synchronized Security for unified, coordinated protection, easy management and improved visibility, and efficient, automated incident response.

'Sophos Synchronized Security is an easy way to protect our users and their devices — and it's completely transparent. For example, the Sophos XG Firewall component of the system automatically puts the bad files into quarantine without any instructions from the user.'

Brother Philip Petrow
Benedictine Monks of Cleveland

Challenges

‣ Need for easier, more manageable security

‣ Coverage gaps and lack of coordination among existing point products

‣ Lack of real-time endpoint and network visibility across devices and user locations

‣ Acceleration and automation of incident response processes

‣ Protection for non-technical users and their devices on-site and on the go from zero-day attacks, advanced threats, and ransomware

How do you simplify security management while protecting against sophisticated attacks?

For some time, the monastery had been using Barracuda Networks for email protection and SonicWall firewall technology for network protection, but they were dissatisfied with these solutions for several reasons. Brother Philip Petrow, who manages IT for the Benedictine Order, explained that the point products worked in isolation and required him to juggle multiple administrative consoles.

'Since we've deployed Synchronized Security, it will be so easy to integrate Sophos Intercept X into our system. It's exciting to know our security can truly grow with us.'

Brother Philip Petrow
Benedictine Monks of Cleveland

As a result, they were difficult to manage and unable to quickly and effectively counter today's coordinated attacks. Additionally, these tools were not all-inclusive and required expensive add-ons and upgrades.

"I was looking for something that provided a full spectrum of protection against today's threats, offered better visibility, and was easier to manage," says Brother Philip. "I've seen the tactics of hackers get more sophisticated and complex over time. So I felt it was essential to our operation to have a solution that would enable us to detect, respond, and remediate issues faster."

Prior to introducing Sophos security solutions to the monastery, Brother Philip had successfully deployed Sophos Home on his personal Mac and found it to be both highly effective and simple to use. Brother Philip concluded that Sophos was the right vendor.

He chose a configuration consisting of the next-generation Sophos Synchronized Security platform with Sophos XG Firewall and the Sophos Central management platform. The solution provides the breadth and depth of protection Brother Philip believes the monastery needs to detect and defeat today's advanced threats, zero-day attacks, and ransomware.

Switching over to Sophos was a simple process — it was just a matter of unplugging the previous solutions, plugging in the Sophos XG Firewall appliance, and configuring the Synchronized Security system.

"Not only was it easy, but it's working great and is providing our network and endpoints with a truly effective and consistent defense," he points out.

How do you safeguard users onsite and on the go?

"Some of our monks rely on technology to carry out their mission, but they are nontechnical users. At times,

they may unintentionally engage in risky behaviors, like clicking on a malicious link," he explains. "Sophos Synchronized Security is an easy way to protect our users and their devices — and it's completely transparent. For example, the Sophos XG Firewall component of the system automatically puts the bad files into quarantine without any instructions from the user."

Because their important work frequently takes them to other cities, the monastery needed a solution that would protect users and devices everywhere they go. Brother Philip appreciates the on-the-go security provided by Sophos, which helps support the activities of the monks at different locations.

"The laptops travel, so I like that the protection goes with them and isn't just here at the monastery," remarks Brother Philip.

How does Sophos Synchronized Security enhance visibility and incident response time?

As Brother Philip is well aware, hackers can successfully carry out attacks on their intended targets in less than a day — and often in minutes or even seconds. In addition, as he points out, complex and sophisticated attacks are becoming increasingly difficult to detect.

Sophos Synchronized Security has fundamentally changed the way the monastery approaches security. Rather than relying on individual components acting in isolation with no communication among them, the organization now has Sophos Synchronized Security working for it around the clock.

The Security Heartbeat™ technology that drives Sophos Synchronized Security ensures that the monastery's endpoint security and the firewall are talking to each other. Through the Sophos Central platform, Sophos

XG Firewall and Sophos Endpoint Security can share threat information and respond automatically to prevent advanced attacks from spreading. For example, Sophos Endpoint pinpoints a system that has been compromised by malware. Then, the firewall isolates the machine and limits network access. The endpoint then automatically undergoes cleanup and remediation, and patches or upgrades are added as needed. For the Abbey and its users, Sophos Endpoint pinpoints a system that has been compromised – for example, when a user is tricked into clicking a phishing link.

"It's much like having our own team of intelligent robots. When something goes wrong, they spring into action and work together to resolve the problem," explains Brother Philip.

Sophos Synchronized Security also provides real-time insights and control all in one place, which helps Brother Philip quickly identify issues and take action immediately — across endpoints, the network, email, and beyond.

"If there's a problem, Sophos sends me a notification. Then I get on the Sophos Central platform to track down the problem. If I have to do anything in-house to clean the malware or virus, then I can respond to issues in a timely fashion. Sophos Synchronized Security offers us the kind of protection we've been looking for, and I can confidently say that I sleep better at night because of it."

What's the best way to integrate ransomware protection?

Lately, Brother Philip discovered that the monastery's Administrative Assistants were receiving quite a number of ransomware emails, a type of malicious software that blocks access to a computer system until money or some other type of ransom is paid. Ransomware is the most prevalent malware attack affecting today's organizations.

"With the increase in terrorist attacks on religious organizations like churches, ransomware is top of mind for us at the monastery. We want to be sure that we're fully protected against this rising threat. We think that Sophos Intercept X is a valuable addition to our to security toolbox," he suggests.

Brother Philip has now deployed Sophos Intercept X, which uses CryptoGuard technology to block the malicious, spontaneous encryption of data by ransomware. Through Sophos Synchronized Security, ransomware-infected devices are assigned a status indicating they are at risk. This information is then shared with Sophos XG Firewall, which isolates these devices from the network. By doing so, ransomware attacks are unable to communicate to command-and-control servers, so the attack cannot infect other systems.

"Since we've deployed Synchronized Security, it was so easy to integrate Sophos Intercept X into our system. It's exciting to know our security can truly grow with us," he asserts.

Start your free trial of Sophos XG Firewall today to get started with Synchronized Security.

SOPHOS