Large Catholic Diocese Relies on Sophos to Modernize End-to-End Security and Meet Cyber Liability Requirements

The Roman Catholic Diocese of Syracuse is a large evangelical religious organization in upstate New York. Its estate encompasses 116 parishes, 10 missions, and seven oratories. The Catholic diocese also encompasses two hospitals, six area charities, and 21 schools, including four junior and senior high schools.

CUSTOMER-AT-A-GLANCE

DIOCESE OF SYRACUSE

Diocese of Syracuse

Industry
Religious organization

Number of Users
3,000 employees

Sophos Solutions

Next-Generation Endpoint:
Sophos Intercept X Advanced with XDR: 650 licenses
Sophos Intercept X Advanced with XDR for Server: 25 licenses

Next-Generation Firewall:
Sophos XG Firewall XGS430: 2
Sophos XG Firewall XGS230: 14
Sophos XG Firewall XGS136: 106

"I was astounded by the throughput of these devices—even after high levels of scrutiny. Sophos firewalls go above and beyond."

Kory Hopkins
IT Director
Roman Catholic Diocese of Syracuse

Challenges

- Implementing an affordable solution with truly integrated end-to-end protection and advanced capabilities that can adapt to the evolving threat landscape
- Meeting the stringent and changing requirements of their cyber liability insurance provider
- Centralizing and unifying management in the cloud to improve the efficiency and effectiveness of a small team
- Finding a trusted security vendor who could provide expert support and assist with security planning

IT Director, Kory Hopkins, manages a small team consisting of two technology professionals who support approximately 125 locations—a mix of parishes and schools. Each location's network has unique complexities and issues—some have firewalls, others have IP-based security, and still others have access control systems. The diocese has a minimal server footprint on the main campus and is transitioning its operations to the cloud. These disparate technologies have complicated security management and have resulted in an inconsistent security posture across the diocese.

To lighten the burden on the small IT staff, Hopkins has been working closely with Armory 5, a managed service provider that caters to small-to-medium-size organizations and offers everything from Security-as-a-Service to IT support to process improvement. For the Diocese of Syracuse, Armory 5's primary responsibility is front-line help desk management and Microsoft Azure cloud platform support.

How do you meet changing requirements when it's time to renew cyber liability insurance?

When Hopkins was confronted with new and more stringent requirements from the religious organization's cyber liability carrier, he knew it was time to reassess the security infrastructure of the diocese.

"The way the industry is going, if you can't check all the boxes, you get less and less liability coverage and end up paying more. That's what dictated our move from our previous vendor and led us to look at Sophos," he explains.

Prior to engaging with Sophos, Hopkins and his team had incorrectly assumed that their current firewall vendor had a solution that was capable of adapting

to the changing threat landscape and technology trends. They were lured by the convenience and ease of use. Certain functions, such as creating VPN tunnels, were really simple. Over time, however, he came to find out that setting up VPN tunnels was so easy because the vendor left so much unprotected. As he puts it, there were "a lot of unlocked doors and ways into the network."

What convinced Hopkins that Sophos was the right choice?

Hopkins was introduced to Sophos solutions at a security conference two years ago by Sam Heard, owner of Data Integrity Services. Located in Lakeland, Florida, the managed service provider and IT consulting firm has been in business since 1997. Data Integrity Services supports organizations all over the U.S. with their cloud initiatives, cybersecurity, and more. The IT consulting firm holds more than 50 Sophos certifications. Over a period of 16 years, Data Integrity Services has been heavily involved in helping dioceses all over the country unify their security across their pastoral centers, schools, and parishes.

Hopkins knew that the diocese would soon outgrow its existing firewalls due to increasing bandwidth consumption and other factors. After several conversations with Heard, Hopkins was motivated to look at more robust and more secure high-performance firewall appliances and endpoint solutions beyond antivirus.

He began his research in earnest, speaking to IT leaders at other dioceses who had adopted the Sophos XG Firewall. He also delved into industry and analyst reports to determine which vendors were consistently well-positioned and stayed ahead of the security curve.

A key requirement for the small team was the ability to remotely manage the solution from the cloud. Hopkins was also looking to integrate their security from end to end, uniting endpoint security with network security. At the time, the diocese had an antivirus solution, but he realized that it lacked the stronger protections the organization needed at price points the diocese could afford. Hopkins was not just looking for a solution that would fit in the budget, but something that could provide reliable end-to-end protection and reduce the burden on his team.

With its leadership position in multiple Gartner Magic Quadrants over the years, Sophos was a perfect match. "When we demonstrated to Kory how Sophos could bring together firewalls, endpoints, and servers for each individual sub-estate under the Sophos Central enterprise dashboard, he fell in love with it," Heard relates. "It was a win-win-win situation for us, for the diocese, and for Sophos."

For network security, Hopkins decided to implement 122 Sophos XG Firewalls, which provide visibility into risky user behavior, detect unknown and unwanted applications, block ransomware and other advanced threats, and more.

High throughput was another requirement. When Hopkins and his team purchased a 500Mbps bandwidth pipe to accommodate higher usage, they discovered that their legacy firewall topped out at 100Mbps. After switching to a Sophos XG Firewall, they were able to get full bandwidth utilization. "I was astounded by the throughput of these devices—even after high levels of scrutiny. Sophos firewalls go above and beyond," he asserts.

To improve endpoint protection, Hopkins implemented 650 licenses of Sophos Intercept X Advanced with XDR for endpoints and 25 licenses of the server version. These solutions help his team accelerate threat detection and response for ransomware and other attacks. It provides artificial intelligence (AI)-based threat-hunting capabilities that put a halt to the stealthiest threats. Sophos Intercept X Advanced with XDR includes Sophos Managed Threat Response (MTR) managed service, which augments the security team with 24/7 threating-hunting services staffed by a team of seasoned experts. These highly trained professionals not only alert Hopkins of issues they detect, they also act swiftly to neutralize threats.

Additionally, Hopkins was impressed by how Sophos enables automatic incident response by identifying the source of infections on the network. This is made possible through Sophos Synchronized Security; where Sophos endpoints and firewalls communicate with one another and isolate an infected endpoint to prevent malware from spreading laterally.

"To have endpoints and firewalls talk to each other was a big plus—and all this is visible to us in one place, one dashboard, which simplifies management immensely. When we have an outbreak, we just drop a wall over it and contain it," notes Hopkins.

"To have endpoints and firewalls talk to each other was a big plus—and all this is visible to us in one place, one dashboard, which simplifies management immensely. When we have an outbreak, we just drop a wall over it and contain it."

Kory Hopkins
IT Director
Roman Catholic Diocese of Syracuse

All these solutions are unified by the cloud-based Sophos Central management platform, which helps Hopkins and his team work more efficiently and cover the needs of all diocese locations. With cloud management a top priority, having a single, unified console that marries firewall and endpoint saves time and provides real-time data to help Hopkins and his team respond faster and more effectively.

"For people like us who are resource-limited, this is a highly worthwhile solution. Unlike other options out there, this one does not sacrifice cloud access for rich functionality. Sophos was a good value, with a feature set that gives me more confidence that we can protect locations we would likely not be able to visit for several years," he points out. "Sure, there was a learning curve, but I call it a 'pleasant burden.' I would rather have to deal with that than have to pick up the pieces after a breach," he asserts.

How does Sophos Technical Support ease deployment?

The Sophos Technical Support team and Data Integrity Services assisted Hopkins with the planning and execution of a staged deployment. This was critical, as there is a narrow window of permissible downtime at some diocese locations, particularly at schools. By reaching out to his IT consulting firm and to the Sophos team of experts, he was able to seamlessly complete installation of the firewalls and other products while ensuring maximum uptime.

Data Integrity Services initiated the process by having all 122 firewalls shipped to their Florida location. There, the IT consulting firm staged each one and then shipped the appliances to Hopkins, who installed the firewalls with the assistance of Sophos Technical Support.

The project was completed right on schedule. "It was a great partnership because everyone involved on our team and at Sophos helped the diocese lock everything down and tighten up its security footprint. Kory was extremely happy about that," asserts Heard.

Hopkins advises other IT professionals not to do it all at once and to make sure they purchase Sophos Support hours—which he said only adds pennies to the monthly lease. "There's no way my team and I would have been able to complete the deployment ourselves." he says. "There's a lot to get your head wrapped around—and having access to the Sophos Support team was invaluable."

Hopkins believes it was a worthwhile investment, as he and his team could get a Sophos expert on the phone when they needed someone to troubleshoot issues and to ensure smooth and optimal functioning of their Sophos products.

"I would highly recommend Sophos. I've had an excellent experience with the product and with the team—they are extraordinarily knowledgeable and were very flexible and accommodating to our schedule, given our time constraints and responsibilities," he adds.

How has Sophos specifically benefited the diocese overall and the IT team?

Though the diocese is still in the early stages of implementation, it has already realized significant benefits from its Sophos solutions.

For example, directly as a result of Sophos, the diocese was fully approved for its cyber liability insurance. "We were really pleased about that, as it's critical to many business decisions. We have to drive financial protection, and that means driving technological protection," affirmed Hopkins.

Another advantage is the added visibility Sophos provides, which allows Hopkins to step back and be more judicious about what users really need to access and how to plan site-to-site connections. Each location at the diocese has a hub-and-spoke network architecture. When one hub connects to another, it's not confined to the specific hub it needs to communicate with; it essentially connects to all network hubs—and this can potentially open the network up to the lateral spread of attacks.

"Sophos XG Firewalls allow us to carefully review each location and chop down some of the things that were flying under the radar and were not necessarily ideal. Now we can step back and do things a little differently, such as imposing firewall rules that change how people access other locations and completely eliminate certain connections," he explains.

What words of wisdom can the Diocese of Syracuse share with other IT pros?

The advice Hopkins offers to other IT professionals is to be proactive and work on the assumption that "It's not a matter of if you will experience a breach, but when."

In view of recent headlines about national security and financial stability issues, he believes it's critical to orient yourself around how to contain the damage and mitigate loss when infections or attacks occur. "You need good backup solutions and practices. Today's threat actors are now looking beyond ransomware and are performing more data exfiltration—releasing data rather than just holding it ransom. It's a constant game of escalation. We need to design strategies that help us stay many steps ahead of bad actors and anticipate their next moves," he observes.

There are two fundamental architectural principles that Hopkins recommends to help manage user behavior. First, he believes that it's crucial to deploy a solution like Sophos that provides comprehensive visibility at a glance, along with proper alerting when suspicious behavior is detected. The second principle is to keep user access restricted and segmented—and then to revisit that every year and make any necessary modifications.

"You don't have to grant users access to the entire network or to your database. The more segmented the disparate pots of information and key assets are, the better. And make sure that, if someone doesn't need it, they don't have it," he summarizes.

What is the vision going forward?

Looking to the future, Hopkins sees tremendous value in growing the partnership with Sophos and Data Integrity Services.

"In the past, we became experts in the legacy firewall because it was so simple, but I don't see us going there with Sophos because of the complexity of today's threat landscape. I really see the need to lean on a vendor partner for these larger responsibilities. And that's not necessarily a bad thing. I'm grateful that Sophos is there for us when we need them," he says.

He also finds a great deal of value in the questionnaires provided by cyber insurance agencies as part of the annual renewal process. This means cultivating a closer relationship with security partners like Sophos for planning purposes and being more proactive rather than reactive. "I can take those questions to our security partners and ask them, 'Where does this put us?', 'How are we prepared to deal with these requirements?'" he asserts. "We want to show our insurers that we are ahead of the curve and in an even better position than what they asked for."

Over time, Hopkins foresees that cybersecurity insurer questionnaires will coalesce around a standard security framework, such as the one put forth by the National Institute of Standards and Technology (NIST). The expectation to have certain controls in place will be helpful to the diocese from a planning perspective, as the IT team will know that they have 12 months to get these in place.

"Partnering with a good security partner like Sophos and trying to apply a security framework is very helpful. All the Catholic churches in the U.S. would benefit if they adopted NIST as our security framework under the auspices of our governing body, the United States Conference of Catholic Bishops (USCCB). For institutions like ours that include healthcare and education—segments that have potentially sensitive information—it makes sense to adopt some kind of security framework. We have a legal and moral duty to do so," points out Hopkins.

Heard sees a great deal of potential for other Sophos products at dioceses all over the country. For those embracing the cloud, he highly recommends Sophos Cloud Optix to provide expanded visibility and security for the cloud environment. Since most dioceses use Microsoft Office 365, Sophos Email is also a must, as it integrates directly with Microsoft Outlook and similar products. He also believes that encryption is critical because many parochial schools and vocational facilities need to protect confidential student identification data. And Sophos Phish Threat would be another wise addition, especially as cybersecurity insurance companies are offering preferential rates to organizations that have security awareness programs.

What would you say to others who are considering Sophos?

"Call up a reseller, get an appliance, get a demo copy of the endpoint protection, and walk through it. The feature sets of these products were something I was expecting from an appliance well above the price point. You'll be pleasantly surprised by how feature-rich the firewall is," concludes Hopkins.

"I really see the need to lean on a vendor partner... I'm grateful that Sophos is there for us when we need them."

Kory Hopkins
IT Director
Roman Catholic Diocese of Syracuse

Learn more about
Sophos Central today.
www.sophos.com/central

SOPHOS

2022-05-11 CCS-EN (NP)