SOPHOS

PARTNER & CUSTOMER CASE STUDY

Midwest IT Services Organization Broadens Its Security Portfolio with Sophos Solutions

Partner-at-a-Glance

Net Activity Inc.

Industry
IT and security solutions provider for multiple sectors

Sophos Solutions
Sophos Central
Sophos Server Protection
Sophos Intercept X
Sophos XG Firewall
Sophos Phish Threat

> *'The Sophos XG Firewall's single-pane-of-glass management interface makes everyone's job easier by offering comprehensive visibility to networked devices. It's really intuitive and easy to use and enables us to set up rules and policies all in one place.'*

Jarret Graver
Technical Services Manager
Net Activity Inc.

In business since 2002, Net Activity is an award-winning IT services and solutions company in Cuyahoga County, Ohio that specializes in cloud migration and support services, managed services to ensure a stable infrastructure, VoIP, backup and disaster recovery, and more. The company has a well-developed security practice that covers email security, vulnerability assessments, antivirus and threat monitoring, IT compliance, and 24/7 security coverage. Net Activity's seasoned staff of technical professionals serves clients in over 380 locations — from two-person offices to companies with 250 employees — across the state of Ohio and beyond. Its customer base encompasses a wide range of sectors: manufacturing, government, accounting and legal, education, and scientific and research labs.

Challenges

- Find security solutions to use internally and recommend with confidence to clients
- Enable customers to take full advantage of the cloud while securing users, systems, and data
- Provide customers with effective tools to block crippling ransomware attacks and other advanced threats
- Offer scalable and customizable security for growing organizations
- Help customers raise employee awareness of phishing threats

Which firewall solution bests serves your customers' network security needs?

With a strong initial focus on network security, Net Activity began its journey with Sophos about a year and half ago. Currently a Sophos gold partner, Net Activity is quickly moving towards their platinum status. Jarret Graver, Technical Services Manager at Net Activity, is at the technical hub of Net Activity. When he and his team were first introduced to Sophos XG Firewall, they fully vetted and tested the product onsite at their own data center. Their goal was to gain hands-on familiarity with Sophos XG Firewall so that they could confidently recommend the product to their valued customers. Net Activity currently runs Sophos XG Firewall in its data center, which has a multi-tenant cloud architecture. The data center houses different server types for its client base — terminal servers, SQL servers, and file servers.

"We found that all the features we've deployed work great," asserts Graver. "The Sophos XG Firewall's single-pane-of-glass management interface makes everyone's job easier by offering comprehensive visibility to networked devices. It's really intuitive and easy to use and enables us to set up rules and policies all in one place."

Sophos XG Firewall has since become a mainstay of Net Activity's security portfolio. Many larger enterprise clients have multiple deployments. The web filtering capability, in particular, is in high demand among customers who are concerned about the security and productivity of their users.

Net Activity is enthusiastic about introducing their customers to the latest version of Sophos XG Firewall, version 17, which has gained recognition from industry experts like NSS Labs, Gartner, and others. One of the next-generation firewall's innovations is breakthrough visibility through Synchronized App Control, which makes it easier to identify, classify, and control custom, evasive, and generic web applications. Additionally, the new control center, which comes complete with enriched on-box reporting, is of great interest to Net Activity because it offers deeper insights into applications, users, and risks to enable improved issue resolution.

When it comes to endpoint security and server protection, what's the best option?

Net Activity has further expanded its security offerings to the endpoint, adding Sophos Intercept X, Sophos Central, and Sophos Server Protection to its security solutions roster. By augmenting its portfolio, Net Activity can now offer customers endpoint protection both on premises and in the cloud. The intuitive, simple-to-use Sophos Central management console enables consistent policy enforcement and comprehensive visibility across the entire infrastructure.

According to Stacy Gay, Director, Government & National Accounts at Net Activity, implementations of Sophos endpoint solutions have been very successful, and this is underscored by the fact that fire drills and support calls to the Net Activity team have been minimal. "We're not hearing any complaints from our customers, which is always a positive thing — it means that Sophos is effective at preventing any type of hacks or malware from getting through," she observes.

Gay proudly points to a new win on the endpoint security side of the business — Cuyahoga County, Ohio, which is among the top 25 counties in the US. The county recently completed a full infrastructure consolidation of over twelve Agencies' IT departments and teams, which added a level of complexity to their infrastructure that required integration of multiple, disparate systems.

Gay was referred to Cuyahoga County Information Security Officer Jeremy Mio, by Officer Trevor from a law enforcement agency to present on cybercrime at a security conference Net Activity was hosting. At the time, the County was in the process of evaluating several vendors, including Sophos, for File Storage Security and potentially the replacement of Microsoft Endpoint Protection, which the county felt they had outgrown.

Following an in-depth presentation by Net Activity, the County reviewed the robust capabilities and extensive feature set of Sophos Server Protection. Cuyahoga County ended up committing to licenses covering their entire Server and File Storage Environment.

"This is an important step forward for us, providing a clear layer of protection for our server environment" states Mio. "We're excited about next-generation Sophos Server Protection and are confident in its ability to safeguard and monitor the county's business-critical data and applications against the latest advanced threats while minimizing performance impact."

Gay emphasizes that the other aspects of Sophos Server Protection that are critical to the fast-growing organization are scalability, the ability to customize the protection based on changing requirements, and server availability. "We want to ensure our customers can work without interruption. It's crucial that we keep our customers safe from the latest attack and that we don't inhibit their productivity," adds Gay.

For customers like Cuyahoga County, server protection should not be underestimated, especially when you consider the type of information kept on various servers. Sophos Server Protection delivers comprehensive protection for Windows, Linux and UNIX Servers against

‘We’re excited about next-generation Sophos Server Protection and are confident in its ability to safeguard and monitor the county’s business-critical data and applications against the latest advanced threats while minimizing performance impact.’

Jeremy Mio
Information Security Officer
Cuyahoga County

the latest threats, regardless of whether those threats are known or zero day. Next generation protection on Sophos Server Protection includes CryptoGuard anti-ransomware, Malicious Traffic Detection, and Server Lockdown for application whitelisting. “As a trusted partner for Cuyahoga County and Jeremy’s team, our goal is to prevent, detect, and remediate malware. We are equally impressed that Sophos Server Protection minimizes any impact on server performance and availability. And that translates to productivity and efficiency for our customers. At the end of the day, we want our customers to be happy with the solutions they have deployed,” describes Gay.

“Availability is a significant concern within any industry, but it is even more critical for government services which are essential to the citizens we serve. Unfortunately, I know some local governments which have learned the hard way, requiring a shut down due to ransomware attacks. Enhanced prevention and detection capabilities, such as CryptoGuard and Intercept X provide vital safeguards to ensure the protection and availability of county services and data. We are looking forward to bringing Intercept X into our organization,” explains Mio.

How do you prevent ransomware from impacting customer business continuity and productivity?

As Graver and this team deepened their knowledge of endpoint security, it became apparent that customers were clamoring for a solution for today’s most widespread and severe threat — ransomware.

A year ago, a manufacturing company that fulfills multiple government contracts, was brought to a standstill by a variant of Crypto-ransomware. The malware spread rapidly from device to device and took over the whole network, encrypting and locking down file shares and databases that contained highly sensitive data related to the company’s government contracts. Operations came to a grinding halt. At the time, the only protection the manufacturing company had in place was Webroot antivirus. Net Activity immediately got in gear and engaged in massive cleanup and recovery of files from backups. With 10 servers on premises to restore, the effort took over one and a half weeks.

Since that incident, Graver and his team transitioned the company to Sophos Intercept X. Just recently, one of the workstations at the customer site was hit with another Crypto virus. Thanks to Sophos Intercept X, the malware was blocked and prevented from communicating with and spreading to other systems. Root cause analysis, which is a key feature of Sophos Intercept X traced the source and trajectory of the ransomware and provided insights that will help forestall future attacks. A major added benefit was significant reduction in downtime. Since the focus of cleanup efforts this time around was only a single workstation, Net Activity had everything back up and running in an hour.

“Sophos Intercept X is almost too good to be true. It’s hard to believe in the technology until you actually see it in action,” relates Graver. “Our customer was very pleased with the results and saw a huge difference in attack recovery time. If it weren’t for Sophos Intercept X, they would have been in a tight spot. Prior to Intercept X, they experienced a significant financial and productivity drain until they were able to get back into production.”

“Prior to Sophos, I clearly recall the process of cleaning 40 PCs and restoring the data from the files shares. It took us approximately 60 hours of support time. In an ideal situation this would have never happened and those support hours could have been used on different IT projects which weren't dedicated solely to clean up. Now with Sophos installed, Intercept X almost immediately identified malicious behavior. Within 3 hours we knew everything was safe and there were no signs left of the virus. We had visibility into the event log from Sophos so we knew exactly when the communication was stopped to the infected PC and when communication was resumed after Sophos cleaned the workstation. This was incredibly efficient and I still think of the hours we saved," explains Net Activity's government contracts customer.

Now, with the rollout of the latest version of Sophos Intercept X with cutting-edge deep learning capabilities, Net Activity will be able to offer their customers an additional level of security through neural network technology. Deep learning provides a better rate of detection for never-before-seen malware detection, fewer false positives, and a smaller footprint than other machine-learning detection systems.

What's the best way to create a security-aware culture?

Always eager to help customers improve their security posture and maintain regulatory compliance, Net Activity found that customers had a growing need to educate users about phishing threats, such as ransomware, credential harvesting, and malicious websites, that use social engineering to take advantage of user trust.

Easy to set up and distribute to users, Sophos Phish Threat provides emulated phishing campaigns to help customers pinpoint weaknesses and train users to become more discerning when faced with potential email threats in their inboxes. Through Sophos Phish Threat's comprehensive reporting, organizations can easily track user susceptibility and performance, along with overall risk scores, to get a better handle on areas that need improvement.

Graver and his team have already implemented multiple Sophos Phish Threat campaigns at customer sites. "Our customers gave us great feedback about how Sophos Phish Threat has helped them get a feel for who is clicking on malicious links," explains Graver. "It provides continued education for users with believable, customizable campaigns and is something we're looking to promote, as it will enable us to round out our security service offering and provide us with a new revenue stream."

Start your free trial of Sophos Intercept X today.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS