California MSP Turns to Sophos to Provide Enhanced Incident Response and Remediation

Located in Northern California, Endsight is a privately held, founder-led IT managed services provider (MSP) with a team of approximately 140 computer enthusiasts and experts who are deeply committed to helping small and medium-size businesses and organizations with 20 to 200 employees thrive with technology. The company also has a presence in Southern California and in Hawaii.

PARTNER-AT-A-GLANCE

endsight

Endsight

Industry
Managed services

Number of Users
Approximately 140 employees

Sophos Solutions

Next-Generation Endpoint:

- Sophos Intercept X Advanced with XDR and MTR: 4,220 licenses
- Sophos Intercept X Advanced with XDR and MTR for Server: 689 licenses
- Sophos Intercept X: 1,322 licenses
- Sophos Intercept X Advanced for Server: 185 licenses

Next-Generation Firewall:

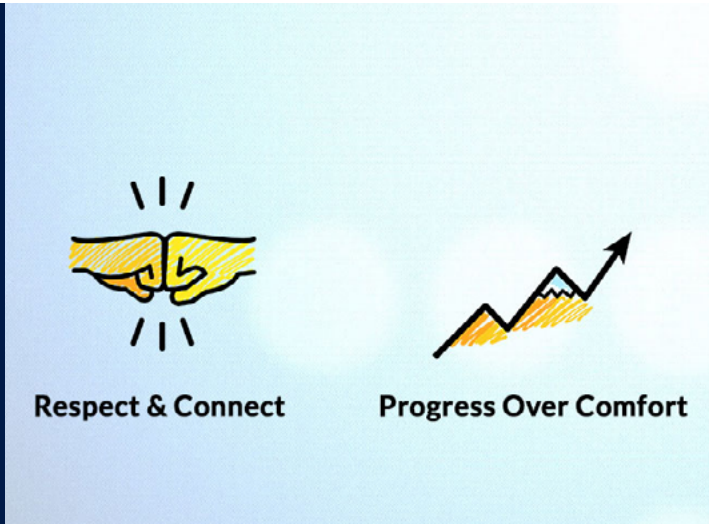
- Sophos XG Firewall XGS430: 17 appliances

Security Awareness Training:

- Sophos Phish Threat: 469 licenses

"Sophos excelled on the partner side. Sophos made it really easy to get started, with no barriers to push through."

Josh Carroll
Chief Operating Officer
Endsight



Challenges

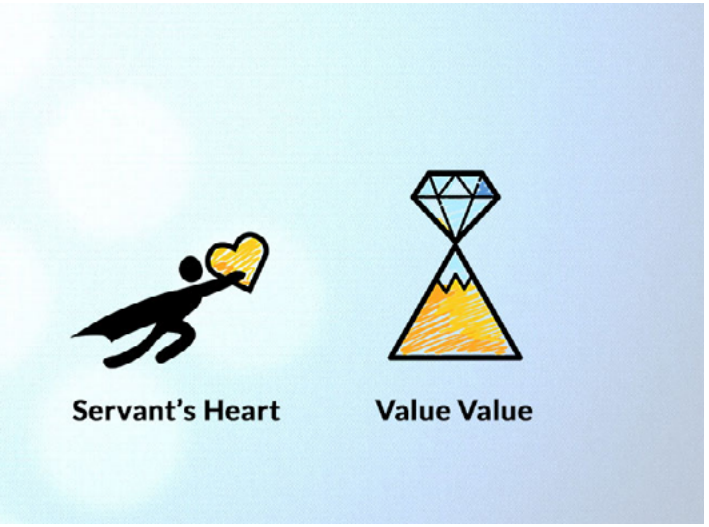
- Deploying advanced solutions that would enable a proactive rather than reactive approach to security
- Extending internal security team capabilities with rapid incident response and threat-hunting
- Finding the right solutions that would help move the business to a 24/7 SOC model
- Establishing an enduring partnership with a trusted security vendor who understands MSPs and helps grow their business

In 2021, Endsight was listed for the 7th time on the Inc. 5000 list, the most prestigious ranking of the fastest-growing private companies in the U.S. Endsight serves more than 400 customers across the commercial and not-for-profit sectors, which amounts to over 10,000 users. While the MSP serves clients across all industries, the primary targeted verticals are law firms and all aspects of the wine business in the Napa and Sonoma regions.

Endsight typically manages the entire IT operation for their clients—from strategy to security to backup and storage. Prior to engaging with Sophos, the MSP's primary security offerings were antivirus, business continuity with backup, anti-spam, firewall, multifactor authentication, and other custom processes.

What recourse does an MSP have when there's a sudden rash of breaches?

In business since 2004, Endsight had an admirable track record. Over a period of 17 years, they were involved in remediating fewer than 10 breach incidents for their clients. Then COVID-19 gripped the world and work-from-home became the norm, opening up a whole new set of security issues. In 2021, Endsight was impacted directly, when four clients experienced major breaches in rapid succession within a three-month timeframe. These breaches sent the MSP down a new path. The team knew it was time to step up their security and started looking into how they could take a more proactive approach. They began by looking at the endpoint solutions offered by five top-tier vendors.



"Sophos Intercept X Advanced with XDR and MTR...makes a lot of noise when it detects things—and this helped us turn the corner and evolve into more of a proactive security group."

Jefferson Dolphin
NOC Manager
Endsight

How does Sophos foster longstanding partnerships with MSPs?

Chief Operating Officer, Josh Carroll, points out that in the course of Endsight's vendor evaluation process, every single vendor met the MSP's technical requirements. But there was another factor that was just as important to them: the ability of a vendor to cultivate a collaborative and productive partnership. That's where Sophos exceeded all expectations.

"Since all the top five providers satisfied us on a technical level, we had to look at the business relationship and ask the question: Will this vendor be easy to work with? Sophos excelled on the partner side. Sophos made it really easy to get started, with no barriers to push through. We didn't have to sign up for long-term contract or purchase a high volume of licenses," remarks Carroll.

When there's a breach and your antivirus fails, what's the alternative?

After signing up with Sophos, Endsight's security team enthusiastically plunged into learning about and experimenting with both the endpoint and server versions of Sophos Intercept X Advanced with XDR and MTR—and that was fortunate for Endsight and its affected clients, who immediately experienced the value of these solutions first-hand.

As Jefferson Dolphin, Senior Systems Engineer, explains, Endsight's legacy antivirus package was based on older technology, and though it was superior to out-of-the-box solutions, it had no intelligence forming the foundation of the technology. Alerting was also generally poor. As a result, it did not detect activities associated with the breaches. Dolphin knew it was time to up the game on endpoint protection by bringing in solutions with advanced detection and response, along a managed service with an expert threat-hunting and remediation team.

Sophos Intercept X Advanced with XDR and MTR turned out to be the right choice. The solution uses artificial intelligence (AI)-driven analysis and rich data sets for automatic detection, investigation, and prioritized response to a broad scope of potential threats—from ransomware to known and unknown malware. Another key component of the solution is managed threat response, a 24/7 service which draws on the knowledge and experience of an elite team of threat hunters and analysts who not only track down security issues but also act swiftly to neutralize threats. These combined capabilities enabled Endsight to augment their capabilities and extend their team.

"What really attracted us to Sophos was its go-to-market strategy. It made a lot of sense to us, allowing us to get the margins we need while enabling us to roll out the solutions in a way that worked for us. Sophos understands the MSP model better than any competing vendors, and this led to a natural partnership."

Mike Chaput, CEO, Endsight

How does Sophos shut down a breach and enable faster recovery?

One of the breaches occurred at an insurance company: it affected nine servers and involved data exfiltration. Once the Sophos MTR team detected the breach, the servers were isolated from the network and shut down, and the threat was contained in just a matter of a few hours—before any more damage was done.

"It was all hands on deck on a Friday afternoon for Endsight and Sophos. Sophos MTR was indispensable, enabling us to isolate, perform forensics, and retrieve files. It opened up a whole new toolset for us." says Dolphin. "As our team rebuilt and restored the servers, we were able to maintain business continuity for our client."

After Endsight completed reconstruction and restoration of the servers, they redeployed Sophos MTR to make sure there were no traces left of the threat.

"When the Hafnium group of threat actors compromised our clients, our existing antivirus was dormant—it didn't detect anything," he says. "Sophos Intercept X Advanced with XDR and MTR, on the other hand, makes a lot of noise when it detects things—and this helped us turn the corner and evolve into more of a proactive security group."

He further points out that Sophos solutions has helped the Endsight security team formulate a response plan. Not only does the team receive meaningful and actionable insights, they have the Sophos MTR team of experts on hand 24/7 to respond to issues when they arise.

"The Sophos MTR managed services team responds much faster than we can. They immediately detect threats and suspicious activities, block them, and then let us know what remediation steps we needed to take," he observes.

How has Sophos reshaped Endsight's business?

Sophos endpoint solutions have enabled Endsight to take a quantum leap toward their goal of scaling up to a 24/7 security operations center (SOC). Thanks to Sophos, Endsight now offers reliable and ongoing incident response, which enables them to fully move their business from an MSP model to a managed security services provider (MSSP) model in the near future.

To promote these new capabilities, Endsight worked closely with the Sophos team to present its clients with a webinar that outlined the benefits of Sophos Intercept X Advanced with XDR and MTR and how it would fit into their organizations. Hundreds of people participated in the live event, and those who missed it, signed up to watch the recording.

"Sophos helped us explain to our clients that this is something we have to do for everybody—and it went over very well. Our client could see the strength of the partnership we have with Sophos, which gave them a high degree of confidence in us and in Sophos solutions. Once the message was communicated, we were able to start deploying the Sophos MTR across the board very quickly. We feel good about that decision—and we haven't had a major breach since," says Carroll.

Carroll further remarks that Sophos MTR is a great fit for clients who are eager to step up their security. They like the idea of Endsight having a third-party component.

"Something we conveyed to customers is that breaches tend to happen after hours or on the weekend when folks aren't working," said Carroll. "The Sophos MTR team works 24/7 to contain threats, and then we come in to clean them up with Sophos Support always in the background to help us."

As Carroll says, times have changed. Threats frequently hit before patches are even released, so it's critical to have the ability to react in real time.

"Before Sophos, I don't think we could responsibly say that we were providing adequate security. Now that 80% of our customers are running Sophos MTR, and 100% are running other components of the Sophos endpoint solution, we don't have those weekend breaches," he adds. "We can execute an immediate response in a client's environment and lock things down as events are occurring to prevent further harm."

How does Sophos keep an MSP's security team productive and prevent burnout?

On the heels of the breaches experienced in 2021, Endsight's internal security team immediately got on board with Sophos and promoted the endpoint solution to clients. Knowing that these serious breaches were thwarted, the team sees that Sophos is doing its job—and that gives them confidence and peace of mind.

"In keeping with our core values, we want everyone to thrive. Our team's stress level is much lower if we can eliminate breaches from occurring rather than having fire drills every weekend, where team members give up family time and clients' businesses are in jeopardy," says CEO Mike Chaput. "We have no interest in churning and burning through the great people on our team. Now, with Sophos, the amount of effort required on the part of our team to get issues corrected is greatly minimized."

Carroll confirms this, noting that internal resources can now spend time on critical preventative activities, such as patching firmware and software in a timely fashion and maintaining infrastructure hygiene, such as ensuring that all tools are running the latest versions in optimal fashion. "Right now, we're in a really happy place—we're on an upward spiral," he says.

How does Sophos support MSP business growth and expansion?

Endsight has always regarded its vendors as long-term partners—and that's especially true for Sophos.

"What really attracted us to Sophos was its go-to-market strategy. It made a lot of sense to us, allowing us to get the margins we need while enabling us to roll out the solutions in a way that worked for us. Sophos understands the MSP model better than any competing vendors, and this led to a natural partnership," asserts Chaput.

He points out that Sophos MTR and EDR technologies provide Endsight with additional revenue—and their clients don't have a problem paying a small premium for the extra assurance. "As a trusted advisor to our clients, we want to keep our clients successful by having a strong security posture from the start. We want to put them in a situation where they actually win."

Sophos has also brought Endsight new business. "No other vendor has given us leads, and there hasn't been much alignment with other vendors on go-to-market. We did not choose Sophos because of this, but as it turns out, we have gotten some

new clients because of Sophos—and this has been awesome. It's been a real gift, an unexpected bonus—and a really good one!" Chaput exclaims.

On the technical side, Dolphin appreciates the value he and his team members derive from the weekly calls with the Sophos Account Manager. These regular check-ins provide him and his team with updates on the Sophos product line-up and future roadmap, along with an opportunity to provide constructive feedback.

"We have a lot of relationships where the account management doesn't add much value. That's not at all the case at Sophos. Our account manager created a relationship unlike any relationship we have with a partner right now. That occurred early on and continues to this day," asserts Carroll.

What's on the table for the near future?

Endsight looks forward to evolving and broadening the scope of its security services and sees immense value in establishing a solid relationship with a vendor like Sophos that offers a comprehensive portfolio of solutions that work together seamlessly.

Sophos Phish Threat is also part of Endsight's security offering. It helps raise awareness among Endsight's clientele about today's highly targeted phishing attacks. Phish Threat enables clients to test their users through customizable phishing attack simulations based on the latest threats. Reporting metrics help clients determine their level of security awareness and identify areas that may need improvement.

"The number one thing we look for when we evaluate a vendor is integrations, as we have several tools we work with. Sophos does integrations really well. On the technical side, there's an opportunity for other tools to make it into our main offering—data loss prevention, web protection, and other Sophos products," says Dolphin. "The more we explore Sophos, the more we discover tools that are useful for us and our clients—and adding those to our security suite has made it even sweeter."

"The more we explore Sophos, the more we discover tools that are useful for us and our clients—and adding those to our security suite has made it even sweeter."

Jefferson Dolphin
NOC Manager
Endsight

Learn more about MTR today.
www.sophos.com/mtr

SOPHOS

2022-06-27 CCS-NA (NP)