CUSTOMER CASE STUDY

Why Executech standardized on Sophos Firewall

An MSP's approach to modern firewall security

executech

Company name
Executech

Industry
IT Services

Number of users managed
1,800 clients and
45,000 endpoints

Sophos solutions
Sophos Endpoint

Sophos Managed Detection and Response (MDR)

Sophos Firewall

Sophos Central

Sophos Access Points

Sophos Email

Sophos Switch

SOPHOS

Challenges:

- **Emergency patching on legacy firewalls** forced engineers into repeated "drop everything and fix it" cycles, increasing operational risk and consuming valuable time.
- **Exposure from outdated VPN configurations** — especially legacy SSL VPN setups without MFA — left customers vulnerable to brute-force attempts and credential-based attacks.
- **Fragmented firewall management** across multiple vendors made it harder to maintain visibility, keep firmware consistent, and ensure secure backups, increasing the likelihood that issues would be missed.

When U.S.-based managed service provider (MSP) Executech made the decision to further standardize its security stack, the firewall was one of the last major pieces still fragmented across its customer base. Many clients were still running SonicWall or Fortinet appliances, and the Executech team had grown increasingly uneasy with the operational load, patching requirements, and vulnerability exposure that came with maintaining so many third-party devices.

As Executech Vice President of Cybersecurity Tyler Rasmussen put it: "We know attackers are targeting our customers. The question isn't if something is happening — it's whether it gets caught or goes undetected."

Executech is one of the largest MSPs in the western U.S., serving 1,800 clients and more than 45,000 endpoints across industries ranging from healthcare and financial services to critical infrastructure.

The company has built its reputation on owning the entire IT environment for its customers — from a help desk and infrastructure to cybersecurity — which means every vendor decision directly affects their ability to protect organizations at scale. Sophos has been part of that strategy for nearly a decade. First introduced to Executech in 2017, the partnership has steadily deepened as Executech expanded its managed security offerings and standardized on Sophos tools that offer broad protection and centralized visibility.

Those moves set the stage for the next major step in Executech's evolution: Completing the move to Sophos Firewall across its customer base.

"The question isn't if cybersecurity had to be one of our core strengths, not just for business continuity, but also for client trust."

Tyler Rasmussen
Executech Vice President of Cybersecurity

SOPHOS

A shift motivated by security, not just convenience

According to Executech Vice President of Central Services Andrew Sweeney, the move toward Sophos Firewall was the cumulative effect of recurring | pain points with other vendors.

"We had a lot of SonicWall deployments," he said. "Their licensing, their VPN licensing, the recent security concerns, and how they handled vulnerabilities — it all pushed us to make Sophos Firewall our standard."

He contrasted that experience with Sophos' approach to urgent patches: "With SonicWall or Fortinet, we'd have to drop everything, figure out what was out there, and rush through manual updates. With Sophos, we haven't had to do that in a long time. Sophos can push fixes automatically."

Additionally, the communication between Sophos Firewall and Executech's other Sophos solutions like Managed Detection and Response (MDR) bolstered the threat feeds Executech monitors for their clients, with intelligence from MDR and Extended Detection and Response (XDR) feeding directly back into the firewall platform, according to Rasmussen.

Real-world saves drive confidence

Before the standardization effort to get all their customers onto Sophos Firewall even finished, Executech had several close calls — the kind that could have escalated into major incidents if the right controls weren't in place.

Sweeney shared one example involving legacy SSL VPN configurations without multi-factor authentication (MFA) enabled that still lingered at a few older client sites. Attackers attempted brute-force access in the middle of the night.

"The [Sophos] MDR team hopped right in and blocked those bad actors. It really saved our bacon," he said.

That level of automatic protection was central to Executech's decision.

"We've had situations where attackers get in through VPN," Rasmussen said. "That's exactly why we encourage customers to go with Sophos Firewall — because the monitoring is plug-and-play. We know things are happening. It's about whether [adversaries] get caught."

> "With SonicWall or Fortinet, we'd have to drop everything, figure out what was out there, and rush through manual updates. With Sophos, we haven't had to do that in a long time. Sophos can push fixes automatically."
>
> **Andrew Sweeney**
> Executech Vice President of Central Services

A transition that's 'pretty darn easy'

Migrating hundreds of firewalls is no small lift, but Executech found the process smoother than expected. Sweeney credits Sophos' onboarding experience, Professional Services team, and the product's intuitive user interface.

"Sophos Firewall is pretty darn easy," Sweeney said. "The interface is intuitive, everything's right where you need it, and once our technicians see the full ecosystem, the switch just makes sense."

Executech used an automated migration tool early on and now handles most transitions manually after all their employees gained a mandatory certification on the process. Even without the tool, Sweeney reported few technical surprises.

The bigger lift wasn't engineering — it was adjusting internal habits.

"People are used to what they're used to," Sweeney said. "But once they understand the 'why,' the rest is straightforward."

Single-vendor efficiency becomes a strategic advantage

For an MSP deeply invested in operational efficiency, the move to a consolidated hardware stack paid off quickly.

Rasmussen emphasized the practical impact, saying that "It's easy to maintain a single pane of glass for all your firewalls. With SonicWall, backups were unencrypted or compromised. With Sophos Central, we don't have to worry about that."

Executech now deploys Sophos Firewall, switches, and access points as a full standard hardware stack for new customers.

"The more we can standardize, the more streamlined we are, and the better we can support customers. It's equipment our technicians know and trust," Sweeney said.

> "That's exactly why we encourage customers to go with Sophos Firewall — because the monitoring is plug-and-play. We know things are happening. It's about whether [adversaries] get caught."
>
> **Tyler Rasmussen**
> Executech Vice President of Cybersecurity

Looking ahead: Success measured in stability

When asked what success looks like in 12 months, Sweeney and Rasmussen are looking at a pretty straightforward goal.

“Honestly? Nothing bad happens,” Sweeney said.

“No news is good news — but it’s also heartening when we see threats actually get caught at the firewall. That’s validation,” Rasmussen added.

With Sophos Firewall, Executech expects continued benefit from:

- A maturing firewall model line with long lifespans.
- Seamless MDR and XDR integration.
- Telemetry-driven early warning on vulnerabilities.
- Simpler management at scale through Sophos Central.

“With Sophos more than any other vendor, it feels like a true partnership,” Sweeney said.

Ready to get started with Sophos Firewall? Start your free trial today. And if you need help migrating to Sophos Firewall, we have resources for Partners.

To learn more visit Sophos.com