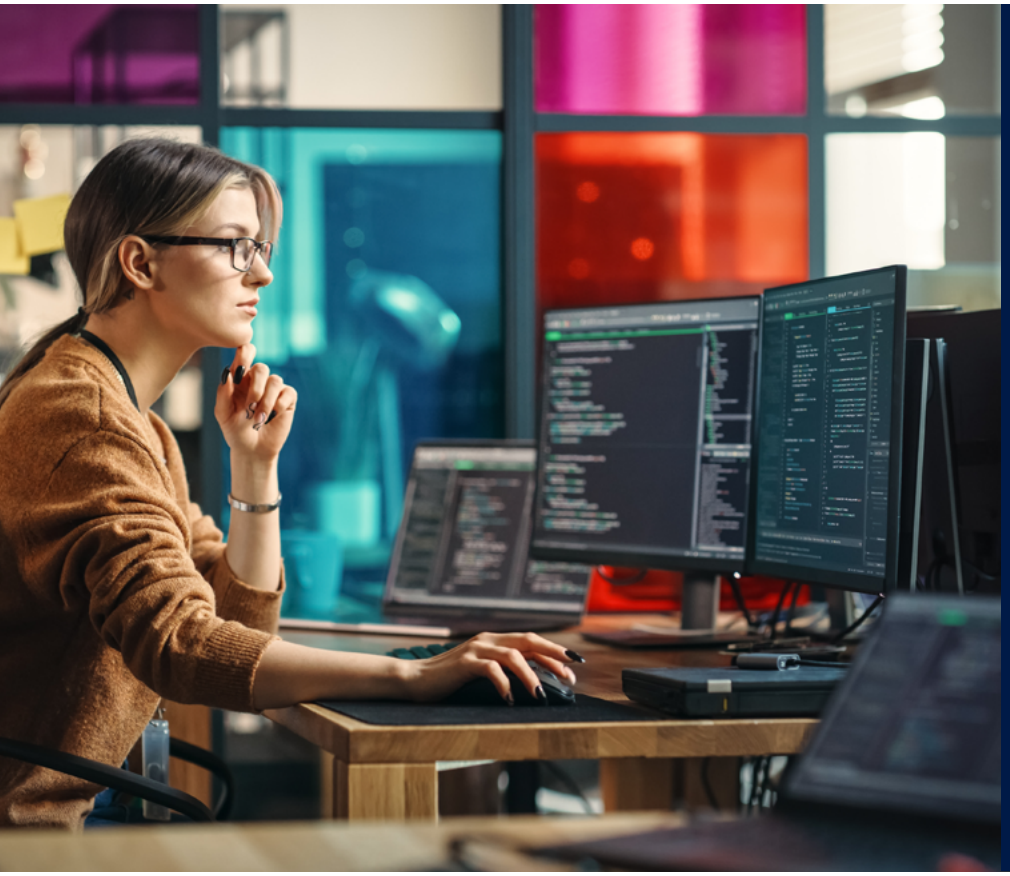

The ITeam Turns to Sophos for Its Small and Mid-Sized Enterprise Clients

The ITeam is a leading provider of comprehensive IT services delivery and management in Calgary and Southern Alberta, Canada. The company's managed security offerings include firewall, network security, business continuity and disaster recovery (BCDR), multi-factor authentication (MFA), threat intelligence, cyber awareness training, and pen testing. For over 25 years, The ITeam has been serving small and mid-sized enterprises (SME) as well as organizations in oil and gas, finance, healthcare, construction, and the legal sector.

PARTNER-AT-A-GLANCE

The ITeam

Industry
Managed IT Services

Website
theiteam.ca

Number of Users

Small and mid-sized enterprises in Calgary and Southern Alberta, Canada

Sophos Solutions
Sophos Intercept X Advanced with Managed Detection and Response (MDR)
Sophos Central
Evaluating Sophos Network Detection and Response (NDR)

"We selected Sophos MDR Complete over Sophos MDR Essentials because we know we can rely on Sophos to be our SOC rather than creating our own. Knowing that we have direct call-in support, a dedicated incident response team, and breach protection warranty (up to $1 million) helps us sleep better at night."

James Wagner, President of The ITeam

Challenges

- Replacing next-generation antivirus with a managed service to increase protection for the company and its clients
- Remediating issues outside business hours with a 24/7/365 outsourced security operations center (SOC)
- Partnering with a trusted vendor's knowledgeable sales and service team to ensure mutual success
- Increasing peace of mind and profitability with the right solution set
- Expanding offerings to include network security products

As with most managed service providers (MSPs), partnering with the right security vendor is critical for success. Recently, The ITeam realized that its vendor's next-generation antivirus was no longer sufficient to protect clients. It was time to begin the search for a new vendor with proven solutions that could keep up with the ever-evolving threat landscape. The security group's due diligence led them to evaluate several vendors based on specific criteria: a reliable 24/7/365 SOC, a trusted endpoint security agent with a light footprint, responsive teams, and Canadian representation.

What happens if, during new vendor evaluation, a threat is discovered at one of the MSP's largest clients?

All vendors evaluated met the technology criteria, but Sophos stood out by going above and beyond and actually addressing a threat discovered during the assessment process. The threat was found at one of their largest clients, where the client had decided to managed their own security through their in-house IT team instead of opting for The ITeam's managed security services.

As it turned out, the client's PC was communicating with an active command and control (C&C) server, relaying proprietary information. The ITeam sought guidance from the Sophos Managed Detection and Response (Sophos MDR) team on how to tackle the threat.

Despite Sophos not being fully engaged yet, Sophos promptly involved senior MDR experts. Upon reviewing the event, the MDR team determined that the attackers had controlled the PC for almost a year, awaiting the opportunity to strike. Had Sophos been engaged before the incident, Sophos Intercept X, with its comprehensive endpoint protection, would have been installed and the root cause would have been identified. However, due to the extended period without a Sophos agent installed on the endpoint, this was not possible. Nevertheless, the desktop was immediately disconnected from the network. Ultimately, the Sophos recommendations were swiftly implemented, saving the client from further harm.

This impressive response at a critical time made it clear that Sophos was the right partner to help The ITeam protect existing clients and open doors to new ones.

What benefits has The ITeam seen with Sophos MDR Complete so far?

Having decided that Sophos was the right partner, the next question was which solutions to onboard first. The assessment experience clearly demonstrated the value of the Sophos MDR team. And Sophos MDR met the criteria of 24/7/365 fully managed protection with full-scale incident response and top-rated endpoint protection. The next question was which Sophos MDR tier was best for The ITeam.

James Wagner, President of The ITeam, explains why Sophos MDR Complete was chosen: "We selected Sophos MDR Complete over Sophos MDR Essentials because we know we can rely on Sophos to be our SOC rather than creating our own. Knowing that we have direct call-in support, a dedicated incident response team, and breach protection warranty (up to $1 million) helps us sleep better at night."

Sophos Intercept X was also onboarded as a result of lessons learned during the assessment process. Sophos Intercept X, with patented CryptoGuard, is now enabling The ITeam to protect endpoints with a comprehensive approach that doesn't rely on just one security technique. Sophos Intercept X helps The ITeam achieve its goal of keeping up with the evolving threat landscape by building on basic protections in Microsoft Windows and protecting against fileless attacks, as well as zero-day exploits.

Sophos Central was also onboarded as the unified cloud-based platform that manages Sophos next-generation technologies. The centralized management hub is designed to let teams scale their security without scaling resources, and that is a key benefit for The ITeam.

In a short time, the new set of Sophos solutions, particularly Sophos MDR Complete, has already made a big impact on The ITeam and its clients. "Sophos MDR saved several clients from potentially catastrophic business failures. We couldn't be more pleased to have selected a solution provider that both protects our clients and improves our business processes, enabling us to better serve our customers," Wagner asserted.

While the business impact is easily quantified, the relief that Sophos solutions bring to the team is beyond measure. According to Wagner, "Security events are among the most stressful situations we encounter. Now, the Sophos global SOC does the heavy lifting when issues arise so our teams can stay off the critical path, be productive, and avoid burnout. It also allows them to learn, observe, and complement Sophos and our service options for our clients."

How do culture and business processes change for MSPs who become Sophos partners?

Intercept X, with extended detection response (XDR) and endpoint detection response (EDR), has been a game changer for The ITeam. XDR helps them hunt down and respond to suspicious activity across Sophos and third-party security controls while EDR performs the same functions across endpoints and servers. Sophos Central puts key information at the team's fingertips with consolidated views, robust reporting, and actionable insights. Together with MDR Complete, these powerful tools help The ITeam take cybersecurity and productivity to the next level.

"With these solutions, we can now speak firsthand about how we've been able to leverage next-generation security technologies to help new clients. We can discuss how we've prevented client environments from being compromised and saved those that were already compromised too," Wagner said.

But the changes within The ITeam don't stop there. The Sophos partnership has also raised internal awareness of the security landscape and strengthened the security culture. "These internal shifts keep us more secure and help us speak more confidently about the security tools and services we use to support our clients," remarked Wagner.

What's next for the Sophos partnership?

With nothing but positive experience and results so far, the sky is the limit for The ITeam partnership with Sophos. The ITeam plans to go full speed ahead.

The next step involves implementing Sophos Network Detection and Response (Sophos NDR) as an in-house proof of concept (PoC). The ITeam recognizes the value that Sophos NDR brings, with its ability to identify unprotected devices, rogue assets, insider threats, and zero-day attacks. The security group believes that the way Sophos NDR works with managed endpoints and firewalls benefits existing clients and opens the door to conversations with new ones. Soon, it's likely that Sophos NDR will become a standard offering. This addition will help The ITeam continue its long-standing tradition of keeping clients secure and delivering peace of mind.

"Sophos MDR saved several clients from potentially catastrophic business failures. We couldn't be more pleased to have selected a solution provider that both protects our clients and improves our business processes, enabling us to better serve our customers."

James Wagner, President of The ITeam

To learn more about Sophos solutions, please visit sophos.com

SOPHOS

2024-01-26 CCS-EN (NP)