LevelBlue

CASE STUDY

Temple Health partners with LevelBlue for robust Microsoft E5 cybersecurity transition

Temple Health's transition to a Microsoft E5 cybersecurity environment required partnering with a security vendor capable of supporting the migration, and that is proficient in long-term E5 management. LevelBlue's expertise with Microsoft Sentinel and Defender, along with their 24×7 monitoring, alert triage, and incident investigation services, made them the ideal choice.

Client spotlight

Temple Health is a Philadelphia, Pennsylvania-based, nationally respected academic medical center that offers high-quality care and the latest technology, with about 10,000 skilled faculty members and employees, annually handling hundreds of thousands of patient interactions.

The challenge

Temple Health recently decided to move to a Microsoft E5 cybersecurity environment, utilizing Sentinel and Defender. The organization was generally satisfied with its incumbent MSSPs but noted that while they helped spot an attack, they fell short when responding to the problem.

Additionally, Temple Health felt its vendors were unfamiliar with Microsoft E5, and the healthcare provider did not believe they could properly support Temple Health's switch to the new platform.

Temple Health CISO Hugo Lai noted that his goal was to find an MSSP that looked beyond the endpoint. Which is why he chose LevelBlue.

"For example, LevelBlue can examine logs that we send to Sentinel from the firewalls, from Microsoft 365, or from other security solutions that we think may be relevant to develop a more complete picture of our IT infrastructure and it's vital that we have LevelBlue manage that for us to make sure we have full 100% visibility, not only just the endpoint," said Lai.

The solution

LevelBlue's first step was to build a high level of trust with Temple Health and prove that it was the best choice to help the healthcare facility move to Microsoft E5. This was accomplished with Microsoft Sentinel and Defender engagements and workshops, which were conducted with Microsoft and LevelBlue personnel. The highly professional manner and familiarity the LevelBlue and Microsoft teams exhibited during the workshop boosted Temple Health's confidence that LevelBlue could properly handle the migration to E5.

Lai said, "Going to Microsoft always made sense. It was just a matter of finding the right partner that could help us."

The workshops also helped influence Temple Health's understanding of Microsoft Sentinel and Defender for Endpoint, leading the healthcare facility to opt in favor of several LevelBlue solutions. These included:

- Co-Managed SOC for Microsoft Sentinel
- Managed Detection and Response (MDR) for Microsoft Defender
- Cyber Advisory Services
- Database Security Services: DbProtect

The partnership also places LevelBlue analysts in a position to inspect the massive number of Epic Software logs for indicators of compromise, helping ensure the system's security. Epic is a health information technology company that provides electronic health record software for hospitals and health systems.

Epic software is used to store, access, organize, and share patient medical records. It also helps with administrative tasks, clinical operations, and patient care operations, and patient care.

The result

The shift to Microsoft E5 and the partnership with LevelBlue opened Temple Health to several additional "wins" and stronger security.

Temple Health was able to consolidate its security tech stack by letting the contracts of several previous vendors expire, and having a LevelBlue-managed E5 program resulted, Lai said, in his organization being able to respond faster and gain additional visibility into its system.

"If I'm repeatedly seeing threats coming in from a specific area, even though right now they don't present a problem, I will have that on my radar so I can start planning and work towards a remediation before it becomes an issue," Lai said. "This is a capability I gained with LevelBlue by it telling me, 'It looks like there may be folks who are trying to do a password spray attack.' While they are not successful right now, they may become successful if they continue. So, this type of alert will allow me to start thinking and coming up with a solution before it becomes a problem."

With LevelBlue's expert guidance and deep knowledge, the healthcare organization could fully leverage its E5 license, despite initially having an incomplete understanding of the platform. As Temple Health embarked on its E5 journey, LevelBlue's support was crucial in implementing the full suite of E5 security tools. This strategic move allowed Temple Health to let its existing security vendor contracts expire, resulting in significant financial savings. It also provided a better return on their E5 investment and resolved the challenges of managing multiple proprietary systems.

Why LevelBlue

The client noted that the relationship began with LevelBlue working closely and early with the Microsoft team. Temple Health appreciated LevelBlue's differentiated service offerings, showcasing its expertise and significant advantages over the MSSP incumbents and competitors.

Temple Health deemed LevelBlue's experts more qualified to manage and maintain the client's Microsoft Sentinel instance and onboard, manage, and maintain their new Microsoft Defender licenses. Additionally, LevelBlue Managed Security excelled at 24/7 monitoring, alert triage, and incident investigation. Lai praised LevelBlue's account team, noting their excellence from the start, particularly during the Microsoft workshops delivered by LevelBlue engineers and support teams through the onboarding process.

"The LevelBlue team has been very helpful throughout the process. Before we finalized the deal, they dedicated a significant amount of time discussing my various challenges and how LevelBlue could address them and architect a solution for us," Lai said. "Another important aspect is database – specifically, DbProtect. Although we're not currently leveraging it, I feel confident that it could enhance our visibility into our security posture in the coming years as an additional component to our EDR program."