

CASE STUDY

Thomas H. Lee Partners

How a Leading Private Equity Firm Uses Managed Detection and Response (MDR) to Standardize Risk Management Across 35+ Portfolio Companies



Solution and Results

eSentire MDR provides 24/7 threat detection and response for 35+ THL portfolio companies to improve their cyber controls, governance, and mitigate the risk of impacting deal valuation.

- ✓ eSentire MDR includes best-in-class tools at a cost-effective price for THL's portfolio companies as part of service delivery.
- ✓ 24/7 threat detection and response across THL's portfolio companies and a team dedicated to identifying and containing threats rapidly so their management teams can focus on growth and scaling.
- ✓ eSentire Managed Phishing and Security Awareness Training helps identify risk areas for employees, test user resilience, and drive behavioral change across all users.



Business and Security Outcomes

- ✓ 24/7 eyes on glass with a dedicated team to identify, contain, and respond to advanced cyber threats on the firm's behalf
- ✓ Trusted guidance prior to investing in a new portfolio company to analyze their security measures and rapidly deploy eSentire MDR services
- ✓ Reduce cyber risk by ensuring complete visibility and a consistent security posture across their portfolio
- ✓ Monthly metrics reporting and a complete overview of cyber resilience across all of the firm's investments to THL's Managing Directors

The Business

Thomas H. Lee Partners (THL) is a Private Equity firm based in Boston, Massachusetts. The firm actively invests in 35+ mid-market growth companies spanning the Business and Financial Services, Consumer and Retail, Healthcare, and Media, Information Services and Technology industries.

With almost 50 years as investors and operators, THL has raised \$35 billion of equity capital, worked with more than 170 partner companies around the world, and fueled more than 600 add-on acquisitions that represent an aggregate enterprise value of over \$250 billion.



The Challenge

Cybersecurity breaches and threats are pervasive concerns for any entity storing valuable data or managing large sums of money: private investment funds are no exception. CIOs have begun to put stronger cybersecurity practices in place to defend against attackers and private equity firms are better defended than ever. But attackers know that the portfolio companies are smaller, growth companies with lean cyber security operations that are less mature.

As a PE firm, THL knows they are a high-value target for threat actors, especially when they announce new investment deals or exit opportunities. This is complicated further since threat actors actively research and target investments, knowing they have cyber insurance.

In THL's case, they needed to ensure that each portfolio company is protected from cyberattacks, but the protection couldn't come at the expense of other objectives like scaling the companies. As Mark Benaquista, a Managing Director who has been with THL since 2011, described the situation, "We want our management teams to focus on things that are going to move the needle and help the company grow."

THL also wanted complete visibility into the cybersecurity posture of each portfolio company in a standardized and easy-to-consume way. "I'm one person, and I have another gentleman on my team, so there's two of us and we have to look after these 35 companies," said Mark.

As a result, THL also wanted a holistic view of the threat landscape impacting their portfolio companies, phishing and security awareness training for their employees, and the ability to identify cyber risks to protect their assets and help them mature.

Given the lack of in-house security expertise, limited access to best-in-class security tools, and ongoing guidance on managing cyber risks, they were looking to outsource 24/7 threat detection and response capabilities to a MDR provider.

Why Thomas H. Lee Partners Chose eSentire

THL was looking for an MDR provider who could become a trusted advisor and partner for not only the firm, but all their portfolio companies as well: "When we were looking at partners, we wanted someone that could be a partner to all of our portfolio companies, not to be wed to any particular technology, and who would use best-in-class tools to help make us aware of the risks that exist, how they're being managed, and where we need to potentially improve," Mark said.

As part of the selection process, THL took a collaborative approach with the CISOs from their portfolio companies to align on the goals and the approach to take prior to partnering with a security provider. The firm eventually chose eSentire to be their trusted security partner to provide:

- ✓ **Managed Detection and Response (MDR)** to safeguard against cyberattacks and deliver 24/7 threat detection, containment, and response, continuous security monitoring, regular threat briefings, and access to world-renowned threat intelligence expertise.
- ✓ **Exposure Management Services** to help each portfolio company steadily progress on their risk management journey and raise cybersecurity awareness with their employees.



The only way we can sleep at night is to have a partner like eSentire at our side.

Mark Benaquista, Managing Director, Thomas H. Lee Partners

Throughout the partnership, eSentire has played a key role in how THL's portfolio companies are protected against the most devastating cyberattacks. As part of its standard playbook, THL has four main priorities upon acquiring a new asset:

- 1. Protect the portfolio company:** From day 1, eSentire is brought in right at close or prior to the deal closing to conduct an analysis on the portfolio company's assets and set expectations with the management team about their security program.
- 2. Mature the program:** As the company grows, their security program and strategy have to scale with it. eSentire supports THL and each portfolio company throughout this process to ensure there are no open security gaps or unaddressed vulnerabilities.
- 3. Educating users:** eSentire plays an integral role in educating their employees on the importance of implementing disciplined patch management, identity and access management policies, or security awareness training.
- 4. Partnering with cyber insurance providers:** THL ensures the portfolio companies partner with the right cyber insurance provider, so their assets are properly insured in case of a cyberattack.

By choosing a partner like eSentire, THL can eliminate certain risks that many portfolio companies may be predisposed to such as high rates of people turnover and travel knowledge moves. This allows THL and their portfolio companies to scale without having to slow down and manage their cyber risks effectively.

Another challenge for THL is maintaining visibility across all their portfolio companies and the status of their security programs. To track performance across THL's portfolio companies, eSentire developed a rolling monthly chart that shows who's live, the components they're live with, where they are in the journey, and if there are any challenges along the way.

"eSentire team has become the arms, legs, and experts that help us understand where we are in the full deployment of MDR and coverage of the attack vectors once the service is deployed. eSentire sees across our whole portfolio and collapses that view so the firm gets a single dashboard view," Mark says.

More importantly, Mark also recommends that portfolio companies leverage the benefits they get as part of Security Network Effects when they partner with a provider like eSentire. "One of the things that we love is that — whether it's a zero day that eSentire discovered or it's something else that's happening fast — when it's brought to eSentire's attention, the entire portfolio gets the benefit of that within seconds or minutes."

Mark characterizes the addition of eSentire as making a night and day difference to how THL manages risk. "My partners ask me all the time, 'How can you be so comfortable?' and I say the only way we can sleep at night is to have a partner like eSentire at our side."

Ready to get started?

Connect with an eSentire cybersecurity specialist to help you build a more resilient security operation.

Contact Us

If you're experiencing a security incident or breach contact us  1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit www.esentire.com and follow @eSentire.