Xsolis: Leading AI Healthcare Provider Decreases Mean Time to Resolution by 63% with Trend Vision One™

JANUARY 2025

CASE STUDY

Business Impact Results

- **40% reduction** in unresolved vulnerabilities with Trend Vision One™
- **57% reduction** in risk
- **63% decrease** in mean time to resolution (MTTR) in 12 months
- **Enhanced efficiency** with fewer resources
- **More efficient** audits to reach HITRUST compliance
- Cyber-risk **snapshot ready** for the board

Technology Provider: **Trend Micro**

Customer: **Xsolis**

Industry: **Healthcare, Information Technology Solution Provider**

Country: **United States**

Introduction

Xsolis is a healthcare technology company that leverages artificial intelligence (AI) to improve the medical review and decision-making process. It focuses on ensuring medical necessity and the appropriateness of care across the healthcare ecosystem, primarily by helping healthcare providers, payers, and administrators make more informed, data-driven decisions.

Cybersecurity is critical to the success of Xsolis' business. As a healthcare operations service provider, any downtime caused by a cyber event would impact its customers' operating environment, likely impacting patient throughput and potentially exposing sensitive personally identifiable information (PII) data.

These risks further extend to care providers, as regulatory requirements specify that when a healthcare organization suffers a breach, even if it occurs through third-party-vendor or supply-chain compromise, initial disclosure is the responsibility of the healthcare provider, not the business associate.

57% reduction in risk

WE ARE UNDER CONSTANT ATTACK

"It's not a question of if we are going to get attacked—**it's a question about when and how we will respond.**"

Zach Evans, *CTO, Xsolis*

As a third-party healthcare service provider, Xsolis must, therefore, provide transparency into how systems and data are protected from cyber threats, including the ability to prove the entire chain of activities involved in securing the infrastructure.

To deliver on this customer promise, Xsolis needed to architect and operate a secure, 24/7, scalable solution to meet the needs of its rapidly growing customer base.

Zach Evans, CTO for Xsolis, is responsible for architecting and implementing a scalable, secure solution that delivers value for Xsolis' customers. **"Speed and innovation are core to my success formula, but so is the ability to manage risk without slowing down the business,"** says Evans. Protecting PHI data is key for business operations, as industry regulations demand transparency and evidence into how every part of his solution is protected against threats.

Evans saw an opportunity to think differently about security. He focused on strengthening his security posture and consolidating multiple security tools into an integrated security architecture that could grow and scale. **"It needed to be a journey, not a rip-and-replace initiative. This led me on a journey to identify a security partner that would be willing to make a big bet on a small, up-and-coming cloud-based company—a partner willing to embark on the journey with us as a trusted advisor,"** says Evans.

Impressed with both the outcomes from the initial Trend solution and the commitment, honesty, and delivery demonstrated by the company, Evan's team has since deployed additional modules within the Trend Vision One security platform.

"Speed and innovation are core to my success formula, **but so is the ability to manage risk without slowing down the business.**"

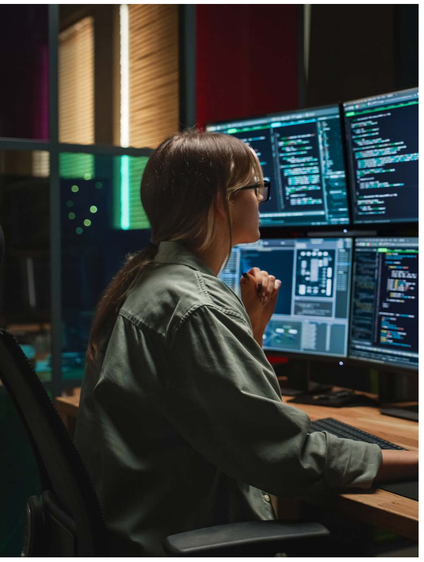
Before Trend Vision One

Prior to Trend Vision One, Xsolis experienced many challenges that touched multiple business areas, including the technical environment, resourcing, culture, and more.

Fragmented visibility, inefficient threat detection, and operational complexity: Monitoring eight different screens to gather data on alerts, logs, and anomalies was a key issue. This fragmented approach made it difficult and time-consuming to correlate security signals from different systems to comprise a comprehensive view of the security landscape. This fragmented approach further made it challenging to detect and respond to malicious activities promptly, leading to delayed response times and increasing the risk of potential successful incidents.

Operational complexity: Managing multiple systems for identifying and addressing issues required significant manual effort. Security personnel had to switch between different platforms to manually piece together information, delaying investigations. The high frequency of false positives further exacerbated the problem, consuming valuable time and diverting attention away from genuine threats.

Talent resource allocation: Without a centralized system, it was difficult to allocate security resources effectively. Multiple teams had to be notified of each alert, leading to frequent personnel overlap and inefficiencies.



Trend Vision One Platform In Action

The Trend Vision One platform provides comprehensive EDR/XDR capabilities with extensive visibility and control over cybersecurity threats. Trend Vision One consolidates, correlates, and analyzes security data from multiple threat vectors within a single platform and through a single security operations user experience. This centralized approach provides a comprehensive view of the security landscape, simplifying the monitoring process and enabling more effective correlation of alerts, logs, and anomalies.

The platform also provides deeper insights into server activities and user behaviors, significantly improving Xsolis' ability to detect and respond to threats in real time. The observed attack techniques feature enabled Xsolis to see how attackers were trying to exploit machines, providing crucial information for writing better detection rules. Additionally, the platform supported the implementation of automated playbooks for common scenarios, reducing the time spent on investigating and resolving false positives. The platform further provided actionable remediation steps within a common workflow, streamlining the response process and ensuring timely mitigation of threats.

Trend's managed XDR service acted as Xsolis' security operations center, providing continuous monitoring and preliminary analysis of alerts. This support enabled Xsolis to allocate local security resources more efficiently and ensured that critical alerts were addressed promptly.

Xsolis reports that the platform helped it **decrease the time to incident resolution by 63% over a 12-month period**, with no additional headcount.

Business Impact

Evans claims that Trend Vision One has had a transformative impact on Xsolis' cybersecurity posture. One of the most significant improvements reported is in the MTTR. Xsolis reports that the platform helped it decrease the time to incident resolution by 63% over a 12-month period, with no additional headcount. This efficiency gain was reported to be critical in ensuring that threats were mitigated promptly, reducing the risk of potential breaches. The decrease in MTTR further enabled the team to operate more efficiently in not only resolving issues, but in focusing on the most critical issues first. The following additional improvements were also reported:

- Trend Vision One™ played a pivotal role in helping Xsolis securely re-platform its solution in the AWS cloud. With the re-platform increasing the number of cloud assets running on AWS by 8 to 10 times, The platform identified and profiled cloud assets, while ensuring proper configuration and security for them all. This capability was seen as vital for managing the expanded attack surface effectively and proactively. "**We are able to pinpoint issues even before they get to production so we're not exposing sensitive data, and it allows us to react quicker,"** said Dr. Andrew Adams, associate manager, information security.

- The platform enabled Xsolis to unearth more vulnerabilities, leading to a 40% reduction in unresolved vulnerabilities in their microservices architecture. This proactive approach to vulnerability management ensured that potential weaknesses were identified and addressed before they could be exploited by malicious actors, helping Xsolis move beyond risk acceptance and mitigation to risk reduction. This results in a more secure environment for clients to house and process their data. It also enables developers a more frictionless approach to security.

A STRATEGIC OPERATING PARTNER

When asked where Trend fits into Xsolis' security program, Evans expressed with confidence that he considers Trend to be a strategic security partner that he looks forward to working with to securely scale and grow the business.

- Enhanced efficiency with fewer resources was another positive impact. Xsolis reported getting more done with the same number of people, scaling up the security program without adding more full-time headcount. **"We've been able to avoid hiring at least one full-time employee (FTE) in 2024,"** said Evans. **"We've also been able to identify our greatest security needs, from a staffing perspective, through the analysis provided and will be making an investment in network security in 2025."** Evans reports that the platform's advanced capabilities further enabled the team to build more confidence, creating a more positive impact on the company's culture and reducing resource risks significantly.

- Asset monitoring saw substantial improvements as well. The Trend Vision One risk score helped Xsolis monitor and track individual categories of assets, ensuring that security for these assets trended in a positive direction. This granular visibility was crucial for maintaining a robust security posture across all assets.

Xsolis was able to quantifiably

reduce overall risk by 57%,

utilizing the Trend Vision One risk index to continuously monitor and report on security posture.

- Xsolis was able to quantifiably reduce overall risk by 57%, utilizing the Trend Vision One risk index to continuously monitor and report on security posture. Utilizing quantifiable data provided by Trend Vision One, Xsolis can now continuously monitor and benchmark against the overall healthcare industry, proving that it is as good or better than its peers on key security metrics and supporting its objective to be at or above the industry benchmark. The risk index is also helping Evans easily communicate this information to Xsolis's board of directors, in addition to enabling him to monitor trends within the operating environment and identify any hot spots that need attention.

- The platform helped Xsolis move through audits and regulatory compliance reporting faster and more efficiently, conservatively reducing the workload by 20% of an FTE, while ensuring that all necessary standards were met without unnecessary delays, especially for HITRUST and HIPAA compliance requirements.

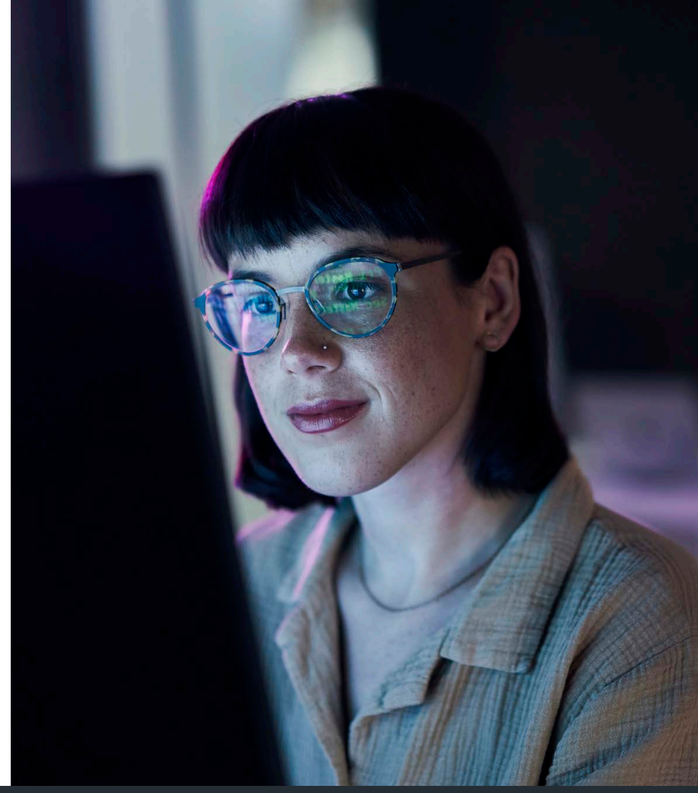
- Time spent investigating false positives was reduced by 65-75%. When pushing out custom code, the risk level is identified. If the score is 70 or higher, the team spends time to review. If it is 69 or lower, it can be a false positive, so it may require further investigation. Data in the alerts enable the security team to recognize that the score was impacted due to a patch being run, saving time from checking multiple systems.

Conclusion

The adoption of Trend Vision One has been a game-changer for Xsolis, providing expanded visibility, centralized control, enhanced threat detection, and streamlined operations. The platform has addressed the key challenges Xsolis faced, transforming its cybersecurity posture and enabling more efficient and proactive threat management.

By continuing to leverage the platform, Xsolis is well-positioned to maintain a low rate of security exposure and enhance its cybersecurity defenses, ensuring robust protection for its critical infrastructure. Xsolis is further able to secure a diverse and expanding attack surface across a hybrid cloud operating environment, supporting both proactive and reactive security strategies, such as attack surface reduction, risk monitoring and assessment, and active threat mitigation.

LEARN MORE



Enterprise Strategy Group™ by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.