LevelBlue

LevelBlue Helps Large Non-Profit Organization Level Up Their Endpoint Security

Overview

A large non-profit organization was looking for a cost-effective endpoint detection and response (EDR) solution to combat emerging cyberthreats. This non-profit provides resources and assistance programs for residents across many different counties. With a small IT team and a modest budget, they were in search of a reliable security expert who could help them safeguard their endpoints and mitigate breaches. This case study discusses how LevelBlue helped the organization successfully enhance its endpoint security posture by identifying and providing swift remediation to threats.

Challenges

The non-profit customer had a small internal security team, and did not have an existing EDR solution in place. They wanted a trusted advisor to fill in the cybersecurity knowledge gaps on their internal team and help with proactive threat hunting and response. With minimal resources, finding a cost-effective solution without sacrificing security was a challenge. They scheduled demos and assessed the capabilities of multiple MSSPs before landing on LevelBlue.

After a live demo, which featured advanced EDR capabilities—including rollback, the non-profit decided to move forward with LevelBlue Managed Endpoint Security (MES) with SentinelOne. SentinelOne's unique "rollback" feature was a key contributing factor in their decision, as they did not have trust in their previous rollback solutions.

The organization was also impressed by the level of expertise LevelBlue had to offer. It was important for them to find a reliable technical expert to mitigate risks in the event of a breach. LevelBlue's proactive monitoring and incident response services would help prevent attacks from compromising business operations.

Solution

LevelBlue MES provided the non-profit with a robust, cost-effective solution, with professional expertise to combat emergent cyberattacks. The organization has benefitted from increased visibility across all their

Solutions

- LevelBlue Managed Endpoint Security with SentinelOne (MES)

endpoints, and they can now easily track activity at the application and device levels. LevelBlue provided the non-profit with a dedicated threat hunter to identify real threats in their environment. The customer was impressed by their ability to find true positives with SentinelOne.

LevelBlue analysts continue to proactively monitor their endpoints to identify and isolate malicious behavior. The non-profit is also working in conjunction with cybersecurity professionals to create custom STAR rules for improved detections.

The organization's positive experience with LevelBlue's active threat hunting has led them to consider expanding their security services. As a non-profit, the customer is price sensitive but has discussed moving towards a bundled MES and MTDR solution. This would strengthen their defenses beyond the endpoint to help secure their entire attack surface. The bundled value through LevelBlue makes this an attractive possibility for organizations with strict budgets and advanced security needs.

Highlights

- The customer's existing IT team was small and they sought to fill their cybersecurity skills gap
- Relevant expertise and competitive pricing were key factors in the decision to choose LevelBlue as their Managed Security Services Provider (MSSP)
- Features such as rollback, customizable STAR rules, and application visibility helped LevelBlue Managed Endpoint Security (MES) with SentinelOne stand out amongst other MSSPs and platforms

Conclusion

As a large non-profit with locations across 29 different counties, the customer was challenged with finding a cost-effective way to secure their endpoints. LevelBlue provided the organization with a comprehensive, fully managed endpoint security solution to thwart cyberattacks, all at a competitive price point. LevelBlue was instrumental in providing the company with reliable threat hunting services to identify true positives in their environment, and provide guidance for threat remediation.

About LevelBlue

LevelB/ue

We simplify cybersecurity through award-winning managed security services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence. This enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.