CASE STUDY

Overwhelmed and under protected: How a manufacturer took back control with BDVision

Customer Profile

With over a century of history, this family-owned manufacturer has grown into a leader in production and distribution, operating in more than 20 locations. Renowned for their dedication to crafting high-quality products, they also prioritize cultivating an exceptional workplace and giving back to the communities they serve-setting a benchmark for excellence in their industry.

Challenges

The team struggled to manage the flood of alerts from their security tools, lacking resources to investigate them fully and feeling blind to potential threats. Rapid growth and recent acquisitions added strain, making it harder to deploy agents on critical servers and endpoints. They also lacked the expertise to create effective SIEM detection rules and didn't have an EDR with advanced threat detection capabilities.

Solution

Managed Detection & Response
Co-Managed SIEM
MDR Agent - BDVision

Results

- Deployed BDVision on over 2,500 endpoints
- Cost Savings - Implemented 57 targeted filtering rules to significantly reduce log ingestion costs, optimizing resource use for greater cost efficiency
- Custom Detection Power - Over 40 custom detections built by BD Detection Engineers bolstering client defensive capabilities

Challenges

This Manufacturer is no stranger to building a high-quality product, they've been doing it for over a century. But when it came to building a mature security program, they were just getting started. They didn't have a dedicated Security Operations Center (SOC), and their small IT team was handling both IT and security with limited resources and even less time. Their environment was a patchwork of cloud data, on-prem servers, and an EDR tool, all feeding into their SIEM. But without deep expertise or dedicated support, their SIEM quickly became a source of alert overload instead of actionable insight. Worse, their tools weren't fully optimized, and as the company continued to grow through acquisitions, the pressure only mounted. Deploying agents to new systems, developing detection rules, staying on top of potential threats, it was all too much for a small internal team. They knew they needed help. Fast.

Solution

The Manufacturer turned to Binary Defense, not just for a quick fix, but for a long-term partner who could meet them where they were and help them grow. Binary Defense introduced them to BDVision, a lightweight MDR agent designed to enhance Microsoft Defender, not replace it. With BDVision, the Manufacturer gained powerful new capabilities, like behavior-based threat detection, managed containment, deception technology, and EDR bypass protection. Together, BDVision and Microsoft Defender created a layered defense that was both smart and scalable. The Binary Defense team didn't stop there. They helped the Manufacturer move from an on-prem SIEM to a cloud-based one, ensuring they had the visibility and scalability they needed. They provided 24/7 SOC monitoring, alert triage, and threat detection backed by real intelligence, so only highfidelity alerts made it to the internal team.

In Action

Once BDVision was deployed alongside Microsoft Defender across all endpoints and critical servers, the Manufacturer's security program started leveling up fast. Binary Defense didn't just add another tool, they transformed how the team detected, understood, and responded to threats. First, they added deceptive environments and decoy systems to lure attackers away from real assets. Every interaction with these decoys generated detailed telemetry, instantly converted into actionable intel by Binary Defense SOC analysts. Instead of just hoping an attack would get flagged, the Manufacturer now had an early warning system built right into the network. One standout moment? An alert triggered by activity on one of the honeyports. These ports were set up to catch unauthorized scanning or probing attempts. BDVision flagged the activity, a Binary Defense analyst triaged it, and within minutes, the Manufacturer's security team had all the context they needed to take action and shut it down. No guesswork. No delay. Even better, BDVision wasn't just watching for trouble; it was built to stand strong if Microsoft Defender ever failed. With EDR bypass techniques becoming more common among threat actor groups, having a second line of defense mattered. BDVision's EDR bypass resilience gave the Manufacturer peace of mind, knowing that if attackers slipped past one layer, they wouldn't get far. This multi-layered approach meant the Manufacturer wasn't just detecting threats, they were staying ahead of them.

Results

The impact of partnering with Binary Defense, and rolling out BDVision, was significant. Here's what changed:

2,500+ endpoints and critical servers secured: BDVision was successfully deployed across the board, giving the Manufacturer complete coverage across both IT and OT environments.

Improved threat detection through behavioral analytics: With BDVision's advanced behavior-based detection and deception capabilities, the Manufacturer could catch sophisticated threats that would've previously slipped through the cracks.

Not reliant on a single tool: BDVision's EDR bypass protection ensured that Microsoft Defender wasn't the sole line of defense. Even if one solution was disabled or evaded, the other stepped in, creating true layered security.

Custom threat detection tuned to their environment: During onboarding, Binary Defense detection engineers worked closely with the internal team to build 40 custom detections, activating 28 that directly strengthened threat coverage.

More meaningful alerts, less noise: Through continuous tuning and client feedback, Binary Defense reduced alarm volume and false positives by refining rulesets and deploying the proprietary BD standard rules. Analysts only escalated high-fidelity alerts, meaning the internal team could focus on what really mattered.

Smooth SIEM optimization and health checks: Binary Defense performed detailed health checks, everything from sensor status and event flow to licensing and connectivity—to make sure everything was running at full speed. They even implemented 57 custom log filtering rules to cut down on data volume and reduce ingestion costs without losing visibility.

A framework built for growth: Whether it was strengthening detection, improving response, or building a system that could scale with each new acquisition, Binary Defense didn't just solve problems, they laid the groundwork for long-term success.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

BINARY DEFENSE