

CASE STUDY

A deepening relationship built on trust and measurable results

This mid-sized auto retailer specializing in high-end vehicles has approximately 2,000 employees and is headquartered in Miami, Florida with multiple other US locations.

The challenge

The auto retailer understood the impact a data breach could have on its business and customers and had made significant cybersecurity investments to proactively protect both. Over time, the client had contracted with multiple service providers and deployed a range of solutions from various technology vendors to secure the business.

Despite these investments, the client continued to experience challenges. Because it had invested in a range of tools from various providers, it was dealing with a security environment that not only was complex to manage but also was highly fragmented. With every tool being deployed and managed by a different vendor, there was a lack of integration between the different security products that was causing gaps in reliability and a frustrating lack of visibility for its IT personnel.

Additionally, the client was encountering issues with communication and support that stemmed from a lack of ownership by the different service providers. Oftentimes, when the client reached out to one vendor for technical support, they would be directed to another vendor. These challenges were compounded by the fact that the client had limited in-house IT resources.



The solution

LevelBlue recognized that the client needed an IT security environment with less administrative complexity and more centralized visibility, and that the way to do this was by consolidating some of its security tools. Most importantly, the client needed a managed services provider that was willing to maintain a close, supportive relationship with its IT team and function as a single, trusted point of contact.

The auto retailer had worked with LevelBlue's Cyber Advisory & Transformation team for several years on various projects including:

- Virtual CISO engagements to help meet Federal Trade Commission (FTC) standards for auto dealerships, ie, the FTC Safeguards Rule, as well as providing guidance on achieving strategic cybersecurity goals
- Identifying and addressing vulnerabilities in the company network to work toward a more resilient cybersecurity posture through LevelBlue Penetration Testing
- Addressing the risk of account takeover (ATO) with the LevelBlue Exposure and Vulnerability Management's Dark Web Monitoring solution
- Development of incident response and business continuity plans

The result

The relationship between LevelBlue and the auto retailer has grown and expanded as LevelBlue has continued to demonstrate its capability not only to help the company solve a range of cybersecurity challenges but also as it has proven its willingness to be available 24x7.

LevelBlue helped the client replace its managed security information and event management (SIEM) service with LevelBlue Managed Detection and Response (MDR), working closely with the customer's IT team to ensure a premium onboarding experience. The foundation of this managed service is the LevelBlue USM Anywhere open XDR platform, which centralizes visibility and monitoring across a customer's environment to help security teams connect the dots and uncover threats before they harm the business.

Our team also assisted the customer in moving to a consolidated endpoint detection and response (EDR) strategy. Initially, the customer deployed endpoint technologies from several vendors but with help from LevelBlue, it successfully transitioned to one managed EDR solution, deploying LevelBlue Managed Endpoint Security across all the company locations.

More recently, the customer has deployed LevelBlue's SASE with Palo Alto Networks solution to help reduce the risk of data breach and increase productivity and efficiency. The team was concerned about outdated technology and inadequate access management policies, which potentially placed the business at risk. Not only could a breach result in loss of revenue and productivity, but it could also cause significant damage to a company's reputation.

