eSENTIRE

CASE STUDY

QC Holdings

How a leading alternative financial services organization made the move to eSentire MDR to achieve improved threat detection and response and a single pane of glass view across their entire Microsoft environment.

The Organization

QC Holdings is a leading alternative financial services organization that provides short-term lending to small businesses and individuals. The firm offers financial services and products at 250 retail locations across the United States and Canada. With 30+ years in retail consumer finance, QC Holdings has built a reputation as a reliable short-term lender for underserved customers.

- Cloud-native infrastructure built on Microsoft Azure
- 1300+ endpoints
- Cybersecurity program overseen by the Director of IT and two security professionals

Solutions and Results

The eSentire Managed Detection and Response (MDR) solution included:

- **MDR with Microsoft Sentinel** to provide complete attack surface visibility and drive threat investigations with 24/7 log monitoring
- **MDR with Microsoft Defender** for Endpoint to hunt and isolate endpoint threats before they spread
- **Managed Vulnerability Service (MVS)** to identify, investigate, and remediate vulnerabilities under the guidance of eSentire experts

Business and Security Outcomes

- Around-the-clock security event monitoring with 24/7 threat detection, investigation, and response by a dedicated team
- Reduced Mean Time to Detect and Mean Time to Contain
- Moved from MDR competitor to get improved threat detection and response capabilities, powered by proprietary threat intelligence, runbooks, and AI/ML innovations created by the eSentire Threat Response Unit (TRU)
- Maximized ROI on Microsoft investment
- Improved cyber risk profile and alignment with the CIS Framework
- Time to value with rapid service deployment and robust escalation processes to ensure complete response

The Challenge

For financial services organizations, a cyberattack can compromise operational systems and expose clients' sensitive financial data, leading to regulatory fines, lost revenue, and reputational damage. For this reason, continuous improvement of security posture has always been a priority for QC Holdings.

However, with only two in-house cybersecurity staff amidst a team of 30 IT staff, it was impossible for QC Holdings to scale and provide the 24/7 coverage in-house they needed to build a strong security posture. Moreover, budget constraints also meant their IT team would not be able to hire and train additional cybersecurity specialists so outsourcing to an external security provider was a no-brainer.

In addition, the security program at QC Holdings was in its early stages of maturity (i.e., relying on traditional use of firewalls for protection) so they made the decision to implement best practices and controls associated with a specific framework, eventually landing on the CIS Cybersecurity Framework.

"Strategically we knew that we needed to have an MDR provider simply based on the size of our team. The ability to staff a SOC was not in the cards internally coupled with the need to monitor, manage, and respond in real-time when incidents would occur," says Bill Elvin, Chief Information Officer at QC Holdings. "We needed to get 24/7 coverage as part of our CIS alignment. That alignment required us to have a partner that would review all of the logs, identify problems, notify us, and step in to remediate issues in real-time."

To bridge their existing security gaps and fulfill the requirements of aligning with the CIS Framework, QC Holdings initially outsourced 24/7 monitoring, detection, and response capabilities to another MDR provider initially.

However, QC Holdings was not satisfied with the quality of proactive 24/7 threat investigation and response capabilities: "We ran into some struggles, specifically around the feedback loop with the provider we'd chosen. It was taking too long to identify problems and they would not step in to remediate."

In addition to missed alerts and lack of response, the previous MDR provider was not able to integrate with, and manage, the existing technology investments that QC Holdings had made with Microsoft.

"We have significant investment in Microsoft and having to spin up an additional SIEM or storage repository and sending that security data outside of my environment always worried me in our relationship with our previous MDR provider."

After one year, it was clear to Bill and his team that the provider had not helped them achieve their goals, leading QC Holdings to switch MDR providers.

"Strategically we knew that we needed to have an MDR provider simply based on the size of our team. The ability to staff a SOC was not in the cards internally coupled with the need to monitor, manage, and respond in real-time when incidents would occur."

Bill Elvin
Chief Information Officer, QC Holdings

Why QC Holdings Switched to eSentire As Their Proven MDR Partner

When the selection process began once again, Bill and his team knew exactly what they wanted from their new MDR provider:

- 24/7 security monitoring
- 24/7 threat detection, investigation, and complete response
- Immediate live support from a SOC Cyber Analyst
- Seamless integration with their existing Microsoft E5 technology stack
- Expert-level support and guidance from a trusted partner

eSentire MDR fit their bill of requirements exactly: “One of the big things that we looked for when we chose eSentire was a partner that we could rely on to become an extension of our team.”

As a result of partnering with eSentire, QC Holdings benefits from:

- **24/7 threat hunting, deep investigation, and complete response** with MDR with Microsoft Defender for Endpoint to protect against advanced cyber threats and minimize the risk of business disruption
- **Critical threat visibility and 24/7 monitoring** with MDR with Microsoft Sentinel across their 100% cloud-native environment
- **Comprehensive vulnerability management** with Managed Vulnerability Services (MVS) to continuously identify vulnerabilities across their environment and get expert guidance on remediating them

Plus, eSentire was able to leverage QC Holdings’ existing investment in Microsoft Office 365 E5, enabling them to consolidate their cybersecurity spend, be cost-effective, and achieve operational efficiencies. eSentire’s ability to manage their Microsoft tool stack internally meant that Bill’s team could worry about one less threat vector while getting more capabilities than they previously had.

“One of the primary capabilities that eSentire brought to the table was to work within our existing environment. eSentire works with the information that’s within the systems, from inside of your system. They’re leveraging our existing investment, and they have access to do what they need to do and keep us informed without additional infrastructure.”

QC Holdings was looking to execute a swift transition to eSentire as their new MDR provider. Rapid onboarding was essential not only to minimize the vulnerability window but also to accelerate the realization of enhanced threat detection and response capabilities.

eSentire facilitated a seamless onboarding process, quickly integrating endpoint and log data for full attack surface visibility and offering immediate time to value.

The onboarding process, as recounted by the team, was straightforward and simple: “Once we chose eSentire to onboarding was relatively straightforward and simple. We were up and getting feedback within a month.”

One key benefit QC Holdings experienced with eSentire was the ability to achieve centralized visibility into their entire environment with Microsoft. This enabled QC Holdings to have a “single pane of glass” view into the entire environment, simplifying the flow of information and improving the quality of threat detection and response.

Where QC Holdings previously struggled to get detailed and timely information about threats from the previous MDR provider, eSentire's 24/7 SOC became a true extension of their security team, isolating, and remediating threats before they have a chance to disrupt the business.

"When there's something scary happening within the environment, a single phone call starts the process. I usually get the feedback from our CSM within an hour of initiating the ticket and having analysts start evaluating the problem and resolving it very quickly."

Lastly, it was crucial for QC Holdings to see the business value of their security investment. eSentire MDR not only leveraged the firm's existing Microsoft tools but also helped reduce their cyber risk profile and improve their CIS security score, demonstrating a clear ROI.

"One of the things we had to establish early on is the cost-benefit of implementing MDR. We get quarterly business reviews that delve into the business value that eSentire brings to our organization, so it makes the sales job with the executives much easier every year."

Ready to get started?

To learn how eSentire MDR can help your organization reduce your cyber risks and build a resilient security operation, connect with an eSentire cybersecurity specialist today.

CONTACT US

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSENTIRE