



CUSTOMER STORIES / QUORUM HEALTHCARE

LevelBlue Helps Quorum Healthcare with a Comprehensive and Fully-Integrated, Custom-Fit Security Stack

Overview

Quorum Health Corporation, based in Nashville, Tennessee, is a quality-focused and clinically driven healthcare organization. This corporation operates 12 hospitals spread across 9 states and has 4,800 employees. They are committed to improving the health and well-being of the communities they serve by maintaining high standards of clinical excellence and patient care. The organization's strategic focus on quality and clinical outcomes is reflected in its operational practices and the dedication of its healthcare professionals.

Challenges

Quorum faced several challenges, beginning with their approach to vulnerability management, which involved generating reports and manually entering data into spreadsheets. This process was time-consuming and lacked the necessary context for effective decision-making and addressing vulnerabilities quickly. Additionally, they were missing logs from crucial assets, highlighting the need for better data integration. This issue created gaps in the log sources, feeding into their Security Information and Event Management (SIEM) system, Sentinel, resulting in incomplete data and an inability to accurately assess their security landscape. Further complicating matters were delays and inefficiencies in upgrading critical assets, such as firewalls. Additionally, inefficient collaboration during the hardening of their environment led to missed opportunities for iterative improvements.

These issues were particularly problematic given the sensitive nature of their operations, where strategic management was crucial to avoid disruptions, especially in a hospital setting. Enhanced collaboration and a more structured approach to managing these upgrades and integrations were essential to overcoming these challenges and strengthening their cybersecurity defenses.

Solutions

- LevelBlue Managed Vulnerability Program with Qualys
- Pen Testing Services with LevelBlue Consulting
- Fully-Managed Microsoft Sentinel SIEM
- Managed Firewalls with Palo Alto
- Technical Support for Managed Endpoint Solution (Microsoft Defender)

Highlights

- LevelBlue improved Quorum's cybersecurity posture and operational efficiency through streamlining their vulnerability management processes, enabling real-time reporting, and prioritization of vulnerabilities.
- LevelBlue provided dedicated technical support, offering expert guidance and tailored solutions during Quorum's software migration project and ongoing security efforts.
- LevelBlue helped Quorum to overcome challenges with addressing log data integration gaps, and firewall upgrade inefficiencies.

"The comprehensive and responsive services provided by LevelBlue have significantly enhanced our cybersecurity capabilities."



Ken Williams
CISSP, Chief Information Security
Officer, Quorum Health Corporation

Solution

Quorum's existing relationship with the LevelBlue team proved invaluable when they sought assistance. LevelBlue quickly understood the challenges Quorum faced and provided a custom integrated solution that allowed Quorum to address their issues promptly.

MVP with Qualys and Quarterly Pen Testing

LevelBlue's Managed Vulnerability Program (MVP), powered by Qualys, enabled Quorum to transition to an agent-based platform, streamlining their vulnerability management process. With real-time reporting on common vulnerabilities and exposures, Quorum's team could quickly prioritize and address vulnerabilities. The dedicated resource from LevelBlue provided expert guidance and support tailored to Quorum's specific needs, ensuring they maintained a robust security posture. Additionally, LevelBlue's customized penetration tests, provided by LevelBlue Consulting, helped Quorum uncover potential vulnerabilities and gain critical insights into their security landscape. This adaptive approach, aligned with their evolving risk profile, ensured their defenses remained current and effective against emerging threats. By adopting this proactive strategy and performing quarterly penetration tests, Quorum significantly enhanced their ability to anticipate and counteract potential security incidents.

Fully Managed Microsoft Sentinel SIEM

The seamless integration of Quorum's Microsoft Sentinel SIEM with LevelBlue and ServiceNow resulted in a fully managed custom solution. This setup included U.S.-based SOC analysts who provided prompt alert reviews, closely aligned with customer-prescribed procedures. This approach ensured more effective and efficient handling of potential security threats and accurate ticket input, enabling the healthcare provider to make better-informed decisions on escalated tickets. Additionally, this integration allowed for custom reporting upon request and facilitated proactive threat discussions with in-depth threat analysis.

Managed Firewalls with Palo Alto

When LevelBlue met with Quorum, the healthcare provider was in the midst of upgrading their existing Palo Alto Networks firewalls. Unfortunately, their previous managed security provider had not stressed the urgency of these upgrades, resulting in an unstable environment where some firewalls had been upgraded while others had not, resulting in unbalanced performance and unpatched vulnerabilities. LevelBlue stepped in to complete the upgrade of the remaining 40 firewalls, delivering quick response times and flexible support to address the dynamic needs of the hospital environment, ensuring a smooth and efficient transition while establishing up-to-date security protocols.

Support for Managed Endpoint, Microsoft Defender Solution

LevelBlue provided U.S. based technical support to the Quorum team, assisting in adjusting their current EDR settings to meet specific requirements, particularly during their software migrations project. The flexibility and responsiveness of the support they received, ensured a smooth transition with minimal disruption, reinforcing the reliability and security of Quorum's current endpoint protection measures.

"This partnership has been a vital component of our overall security strategy, and we are extremely satisfied with the results."



Ken Williams
CISSP, Chief Information Security
Officer, Quorum Health Corporation



Conclusion

Through a strategic partnership with LevelBlue, Quorum Health Corporation successfully overcame significant cybersecurity and operational challenges, enhancing their overall security posture and operational efficiency. By streamlining their vulnerability management processes, Quorum enabled real-time reporting and prioritization of vulnerabilities. With dedicated support from LevelBlue, they received expert guidance and tailored solutions that were critical during their software migration project and ongoing security efforts.

These collaborative efforts and customized solutions allowed Quorum Health Corporation to effectively address their cybersecurity challenges, ensuring a secure, efficient, and reliable operational environment. This partnership highlights the importance of responsive and adaptive support in maintaining high standards of clinical excellence and patient care in the healthcare sector.

“LevelBlue’s expertise, proactive approach, and commitment to excellence have been instrumental in maintaining the security and efficiency of our operations.”



Ken Williams

CISSP, Chief Information Security
Officer, Quorum Health Corporation

About LevelBlue

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.