

# USA Health's Journey to Improved Cybersecurity Maturity



## Excessive alert fatigue and siloed security tools

University of South Alabama Health (USA Health) faced a formidable challenge afflicting thousands of healthcare organizations: defending its facilities against increasing cyber threats while operating within budget constraints and limited resources.

After assuming the role of Infrastructure Director and CISO at USA Health, Louis Wright and his team found themselves submerged in a constant stream of security alerts, with new ones rapidly accumulating. Alongside grappling with alert fatigue, the small team also struggled to monitor all the tools they had in place for their security program.

"Our security tech stack was fragmented, with different resources managing Carbon Black and Rapid7. This segmentation led to a lack of holistic visibility, which is crucial for effectively combating the advanced threats we face today. We knew an important step to developing a comprehensive security strategy was conducting a thorough evaluation of all our security tools, particularly those associated with our security operations center (SOC) capabilities," explained Wright.

Wright concluded that the most effective approach to tackle these pressing challenges was to partner with a managed security services provider (MSSP), specifically one that specialized in healthcare and could deliver 24/7 SOC capabilities.



### Health System:

University of South Alabama Health System

### Location:

Mobile, Alabama

### Website:

[www.usahealthsystem.com](http://www.usahealthsystem.com)



## Specialized SOC solutions

After inquiring within his professional network, Louis was encouraged to speak with Fortified Health Security.

As a healthcare-specific cybersecurity provider offering both Advisory and Threat Defense services, Fortified intimately understood USA Health's needs and concerns.

After learning more about their circumstances, environment, and goals, Fortified recommended two essential services to bolster USA Health's SOC:

1. Managed endpoint detection and response (Managed EDR) to streamline 24/7 threat detection and response while reducing alert fatigue, and improving visibility into critical threats
2. Vulnerability threat management (VTM) to reduce their attack surface by identifying, prioritizing, and mitigating vulnerabilities and risks

## Simplifying service delivery

An essential component to incorporating Managed EDR and VTM into USA Health's existing cybersecurity program, without adding to the team's already substantial workload, was Fortified Central Command, a platform that consolidates critical cybersecurity services and tools in one location.

“Central Command has been a missing piece to our complex security puzzle,” shares Wright. “We now have holistic visibility into our Fortified security program. It also prevents our team from having to log into multiple different security tools in order to monitor all these potential threats. Having everything in one place has greatly simplified our ability to identify real risks, quickly respond to incidents, assign and track escalations, and work more efficiently.”

Once Managed EDR and VTM were successfully implemented, Fortified worked with USA Health's IT team to augment their security strategy and team to help alleviate burnout.

Fortified's Threat Defense team also meets regularly with Wright, offering executive insights into USA Health's cybersecurity maturity and the ROI derived from their Managed EDR and VTM services. ultimately helping Wright gain support from leadership.

## Outsourcing positive outcomes

With Fortified's 24/7 Managed EDR and VTM services, USA Health has been able to realize:

- Improved team morale
- Replaced Rapid7 and Carbon Black technologies with a fully managed solution, without increasing costs
- More effective reporting
- Better alert analysis
- Greater knowledge-sharing across teams
- Stronger security for their health system and patient data
- Simplified management of their cybersecurity program



The vast experience and expertise of the Fortified team has given me new perspectives on so many areas of cybersecurity, from conducting a security assessment to strategic planning to remediating vulnerabilities," shares Wright. "I was looking for a partner that would work elbow to elbow with my team and me, and go on this cyber maturity journey with us. Fortified has proven to be that steadfast partner every step of the way."