OnDefend

CASE STUDY

Prominent Healthcare System Implements Ransomware Defense Validation to Safeguard Patient Safety and Data Security

Learn how a leading U.S.-based healthcare system enhanced its ransomware resilience by validating security controls, ensuring vendor accountability, and strengthening defenses to protect critical patient data and care continuity.

INDUSTRY

Healthcare

CHALLENGE

The healthcare system needed quantitative proof that their defenses in depth remained robust and effective against the rapidly evolving threats targeting the healthcare industry. Having limited confidence in its security controls, detection & response capabilities, and no operational assurance to verify that defenses weren't being compromised, it became challenging to demonstrate continuous risk reduction as well as the value of their security investments.

SOLUTION

The healthcare system engaged OnDefend's managed Ransomware Defense Validation solution to consistently test and validate the following defenses in depth:

- Evaluate their secure email gateway's effectiveness in blocking malicious emails before they reach employee inboxes.
- Measure the accuracy and Mean Time to Detect (MTTD) of their threat detection tools, assessing the reliability of alerting mechanisms and validating efficacy.
- Analyze the performance of their threat response teams, with a focus on the Mean Time to Respond (MTTR) and effectiveness in containing and mitigating cyber incidents.

RESULTS

- ✓ Improved email filter effectiveness, reducing the risk of phishing and spoofing threats.
- ✓ Significantly improved their threat detection capability and MTTD, streamlining the process of identifying and responding to security attacks.
- ✓ Substantial progress in threat response capabilities and MTTR improvement, ensuring the organization remains responsive and resilient to real-world cyber incidents.
- ✓ Validation of vendor performance, providing clear insights into which vendor met operational standards and SLA requirements and which should be reconsidered or replaced.
- ✓ Ensured continuity of critical healthcare operations as well as enhanced patient safety and trust.

The Customer: A Prominent Healthcare System

This leading Florida healthcare system serves over 1 million patients annually through a vast network of facilities, including one of the nation's largest children's hospitals. Committed to high-quality care, they proactively adopt innovative solutions to safeguard patient data, enhance safety, and ensure operational resilience against evolving threats.

Knowing ransomware is a major risk for hospitals, their security team faced a critical challenge: **How can we confidently prove our defenses are prepared to withstand a ransomware attack?** Despite having solid cybersecurity defenses, they lacked a definitive way to validate their resilience against real-world ransomware tactics. Traditional approaches offered some insights but didn't keep up with rapidly evolving ransomware threats.

The Challenge: Do My Security Controls Work?

While traditional cybersecurity services like penetration testing, vulnerability assessments, and tabletop exercises provided some reassurance, these approaches revealed significant limitations that left the team exposed to potential risks:

1. **Limited Frequency of Assessments:** Without continuous testing, the healthcare system lacked visibility into evolving risks that could emerge between scheduled assessments.
2. **Inability to Emulate Real-World Threats:** Conventional methods, such as penetration testing, didn't replicate the actual tactics, techniques, and procedures (TTPs) used by ransomware attackers, reducing the reliability of their threat-readiness insights.
3. **Coverage Gaps in Detection and Alerting:** Changes in threat detection tool configurations, misconfigurations, and alert delivery failures to the Security Information and Event Management (SIEM) meant that potential threats could go unnoticed, weakening their overall response posture.
4. **Dependence on Third-Party Vendors and Service Providers:** The security team had no reliable way to quantitatively validate the efficacy, MTTD, and MTTR claims outlined in their vendor service-level agreements (SLAs), leaving them uncertain about their true detection and response capabilities during an actual ransomware incident.

Recognizing these limitations, the healthcare system sought a more quantitative, proactive, and continuous approach to assessing its resilience against ransomware attacks. It needed a solution that would provide real-world emulation, adapt to evolving threats, and offer continuous validation to reinforce its defenses against these threats targeting their industry.

The Solution: Ransomware Defense Validation

Ransomware Defense Validation was developed in collaboration with OnDefend and this healthcare system's security team. Powered by OnDefend's red team and proprietary BlindSPOT breach and attack simulation solution, this managed service consistently simulates real-world ransomware threat actor tactics and techniques to prove their security investments are optimized and protecting their organization. The goal of this program is to continuously test and validate three key defenses in depth:

- **Secure Email Gateway (SEG):** To prove malicious emails are being effectively filtered and evaluate anti-spoofing configurations, OnDefend's red team deployed hundreds of simulated malicious payload emails to the healthcare system's testing inboxes to validate its SEG capabilities. Additionally, they analyzed the email system for SPF, DKIM & DMARC misconfigurations.
- **Threat Detection Tools:** To prove security controls can detect and alert to real-world attack activity, OnDefend's red team used BlindSPOT to simulate real-world ransomware attacks, supply chain threats, and APTs on the healthcare system's live environment to test their Endpoint Detection and Response (EDR) and SIEM tools' ability to detect, block, log, and alert security teams.
- **Threat Response Teams:** To prove security teams can respond to threats efficiently and effectively, OnDefend's red team used BlindSPOT to simulate a cyber-attack to evaluate, measure, and validate the MTTR of their Network Detection and Response (NDR) and Managed Detection and Response (MDR) providers versus their SLA commitments.

Key Findings and Improvements

Ransomware defense validation is provided to this healthcare system on a quarterly basis. For the initial assessment in Q1, the healthcare system's secure email gateway, threat detection tools, and threat response teams were tested and validated, revealing areas for improvement across all controls.

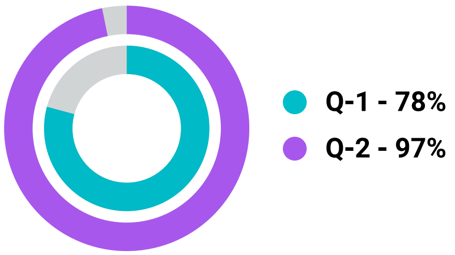
Following the initial assessment, the healthcare system received a comprehensive report with actionable remediation recommendations, a full narrative of the engagement, and an executive summary for the security team and executive leadership.

Remediation, including tool tuning and vendor optimization, was completed before the Q2 exercise. The second quarter attack simulations highlighted significant improvements following the initial assessment.

Test Results

After remediating the **Secure Email Gateway**, the healthcare system improved their ability to detect and block emails containing malicious payloads and reduced spoofing incidents.

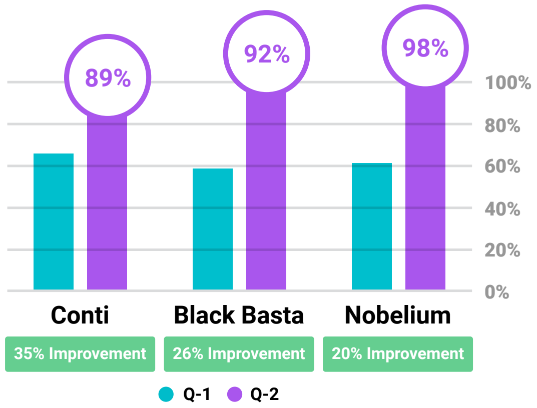
SUCCESSFULLY FILTERED



19% IMPROVEMENT

97% of malicious phishing threats were successfully filtered.

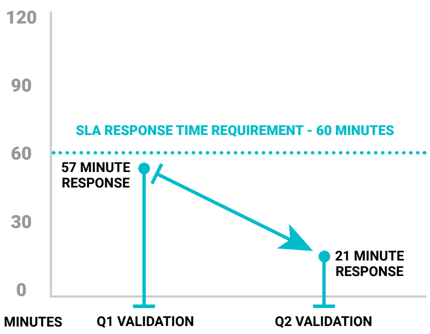
Following the initial assessment, the EDR and NDR were optimized and integrated into the SIEM, resulting in a significant improvement in **Threat Detection Tool** performance.



Improved threat detection capabilities from 66% to 93% against real-world threat actors.

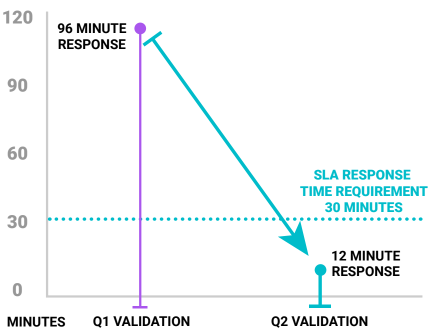
Following the initial assessment, the security team worked alongside their third-party NDR and NDR providers to improve their **Threat Response** handling by implementing more robust protocols, ensuring quicker and more effective incident resolution. However, due to evidence indicating that the regional MDR provider was still unable to meet their SLA, the team decided to replace this provider.

NDR Solution



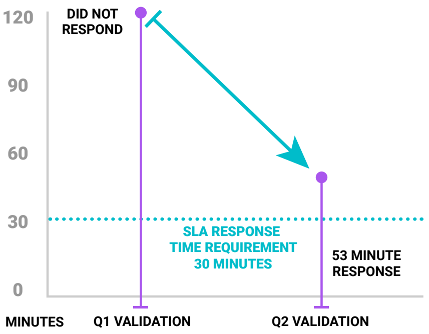
36 Minute Response Improvement

MDR Solution (Major EDR Provider)



84 Minute Response Improvement

MDR Solution (Regional Company)



Did Not Respond / Responded Late

Threat Response Time Improved to Under 21 Minutes. One Provider Replaced.

These exercises are conducted every quarter in a continuous assessment methodology to prepare for new and emerging threats targeting the healthcare industry and to ensure corrected controls do not drift back into a failure state.

> “Ransomware Defense Validation plays a crucial role in building a robust, resilient, and trustworthy healthcare organization. You can’t eliminate all risk, but you can reduce it to safeguard patients and their sensitive data while maintaining their trust so we can focus on what matters most: patient care.”
>
> **Healthcare System CISO**

The Outcome: Security Program Improvements

1 Security Operational Assurance

OnDefend’s Ransomware Defense Validation program consistently provides the healthcare system with proof that their security controls are not adversely impacted by their team, third-party monitoring providers, or the security tool providers.

“Through regular and comprehensive attack simulations, our security team can continuously test and confirm that updates, configurations, and daily operations are not inadvertently weakening the organization’s defenses. This enables us to validate, improve, and adapt our controls in real time against threats.” – Healthcare System CISO

2 Continuous Risk Reduction

The healthcare system recognizes while eliminating all risk is impossible, proactive measures can greatly mitigate them. By staying ahead of potential threats, the security team ensures its defenses can handle even the most critical situations effectively.

“ The Ransomware Defense Validation process is likened to having the answers before taking an exam. While preparation and practice are essential, knowing you are thoroughly prepared instills confidence and readiness. This level of preparedness minimizes risk, allowing our team to uphold the trust of its patients and stakeholders.” – Healthcare System CISO

3 Security Investment Optimization

This healthcare system, wants to ensure their security investments are effective and optimized. Ransomware Defense Validation empowers security teams to regularly demonstrate the value of their defensive investments.

“This program has consistently empowered our security team to showcase the value of our security investments, while also justifying future expenditures to stakeholders by clearly connecting them to measurable improvements in our security posture.” – Healthcare System CISO

4 Executive & BOD Buy-In

The healthcare system’s security team is often asked by leadership about their readiness to defend against advanced threats. Ransomware Defense Validation provides a reliable method to effectively convey their level of preparedness and ensure leadership understands the impact of their security efforts.

“Ransomware Defense Validation allows our team to simulate real-world threats, translating complex security risks into actionable insights. This approach not only validates existing security investments but could also highlight the need for additional support from stakeholders.” – Healthcare System CISO

This case study is based on insights from our comprehensive whitepaper, which includes detailed findings from the Ransomware Defense Validation assessment that gave this healthcare system confidence in its cybersecurity posture. Click here to request your copy and discover how our approach can strengthen your organization’s defenses against a ransomware attack.

About OnDefend

OnDefend, established in 2016, stands at the forefront of preventative cybersecurity testing and advisory services, a reputation further enhanced by the introduction of its advanced Breach and Attack Simulation (BAS) Software as a Service (SaaS) platform, BlindSPOT. OnDefend is a trusted partner, empowering organizations globally to proactively combat real-world cyber threats. From ensuring compliance with industry standards to building out mature security programs, our mission is to ensure that the security resources our customers invest in are well-utilized, effective, and provide tangible results. For more information about their services and solutions, please visit ondefend.com.

✉ contact@ondefend.com 🌐 ondefend.com ☎ 800.214.2107