



Reimagining Ransomware Defense

Protecting Healthcare Systems with
Ransomware Defense Validation

 OnDefend

© OnDefend. All Rights Reserved.

Reimagining Ransomware Defense

Patient care is the #1 priority for this prominent healthcare system and is the driving factor to every decision they make.

Going **beyond** compliance, HIPAA, and regulation standards, delve into how this healthcare system is **reimagining ransomware defense**. Visualize how they are validating their security controls, identifying gaps in defensive coverage, and demonstrating the value of their investments by leveraging OnDefend's Ransomware Defense Validation program.

This allows the healthcare system to focus on what matters most: **caring for patients**.

CONTENTS

<u>The Ransomware Pandemic</u>	3
<hr/>	
<u>Security Control Blind Spots</u>	6
> <u>Email Gateway</u>	8
> <u>Threat Detection Tools</u>	9
> <u>Threat Response Teams</u>	10
<hr/>	
<u>Healthcare System Recognizes Risk</u>	11
<hr/>	
<u>Ransomware Defense Validation</u>	14
<hr/>	
<u>What is Ransomware Defense Validation</u>	15
<hr/>	
<u>Service Delivery, Outcomes and Improvements</u>	16
<hr/>	
<u>Overall Security Program Benefits</u>	32
<hr/>	
<u>Perspectives by OnDefend</u>	35

The Ransomware Pandemic

Lasting Effects on Healthcare
Operations

The healthcare community continues to face a pandemic, a **cyber one**. The alarming rise in ransomware attacks has created a strain on an industry already faced with limited resources.

Industry Sectors Affected by Ransomware



*These numbers are based on 2024 IC3 complaints.

The FBI's Internet Crime & Complaint Center (IC3) received **1,193 complaints** from organizations impacted by ransomware in the critical infrastructure sector.

Healthcare topped that list.

Source: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

2023 Top Five Variants



Source: https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf

Impact of Ransomware

Patient Safety

In its most simplistic form, a healthcare facility's primary job is to care for its patients' health. This is becoming increasingly challenging with looming ransomware threats.

Hospital mortality goes up about 20 to 35% for patients admitted to a hospital during a ransomware attack.

[NPR 2023](#)

Data Loss and Patient Privacy

Ransomware attacks on healthcare companies frequently lead to data loss and violate patient privacy.

In November 2023, the Fred Hutchinson Cancer Center in Seattle experienced a breach where hackers stole the personal information of an estimated **1 million people**. When the medical center refused to pay a ransom, the hackers contacted the patients directly, citing the center "refused to make a deal."

[Health Journalism](#)

Reputation and Trust

Ransomware attacks can inflict severe reputational damage on hospitals, leading patients to seek care elsewhere.

A 2024 attack on a contractor to England's National Health Service forced several major hospitals in London to **cancel operations**, blood tests and appointments and **send patients elsewhere**.

[CNN](#)

Financial Impact & Downtime

Ransomware payments and costs associated with a healthcare system being down grows year after year.

To support affected providers after the 2024 Change Healthcare attack, United Health Group committed **\$2 billion** in addition to paying the ransomware group \$22 million.

[jdsupra.com](#)

These severe consequences frequently arise from exploiting security control failures within healthcare organizations, which makes them prime targets for threat actors.

Security Control Blind Spots



Identifying Exploitable
Failure Points

Security Control Blindspots

Organizations implement security controls to prevent, detect, and respond to ransomware threats. These defenses ensure layers of security are in place to protect against potential breaches.

Below are three defense in depth controls:



Secure Email Gateway (SEG)

This is the frontline defense against malicious phishing emails. SEGs filter out harmful emails before they reach inboxes, reducing the risk of malware infiltration.



Threat Detection Tools

These tools identify and block suspicious activities on endpoints by monitoring unusual behavior, alerting security teams to potential threats, and enabling quick action to mitigate risks.



Threat Response Teams

Comprised of internal security operations and 3rd party detection and response vendors, these teams continuously monitor, respond, and mitigate attacks in real-time.



Secure Email Gateway (SEG)

Why Email Filters Miss Attacks

Misconfigurations & Missed Updates

Misconfigurations can lead to inadequate scanning or filtering settings, allowing malicious attachments to slip through undetected. Similarly, missed updates or lack of regular tuning can prevent SEGs from recognizing new malware signatures and tactics, leaving systems vulnerable.

Policy & Rules Issues

An organization may be at risk if it lacks a comprehensive email security policy or if existing policies are not rigorously enforced. Additionally, outdated security rules can inadvertently create vulnerabilities that allow malicious attachments to bypass these defenses.

Evolving Cyber Threats

Cybercriminals continuously develop new methods to bypass existing security measures, including leveraging the use of Artificial Intelligence (AI). Modern threats often utilize sophisticated social engineering and advanced malware, which SEGs—relying on signature-based or rule-based filtering mechanisms—fail to detect.

The above examples are only some of the potential ways in which this technical control may fail to operate as intended.

On average 24% of malicious emails **bypassed** SEGs.



Data Collected from OnDefend Services (March 2020-March 2024)



Threat Detection Tools

Why Security Tools Miss Attacks

Tool Misconfigurations & Control Changes

Misconfigurations in security settings due to improper setup or maintenance can create vulnerabilities within an organization's network. Adverse control changes—arising from system updates, network adjustments, or administrative errors—can weaken security measures. These changes may originate from internal IT teams, third-party providers, or automatic updates in security tools.

Alerting Delays and Routing Failures

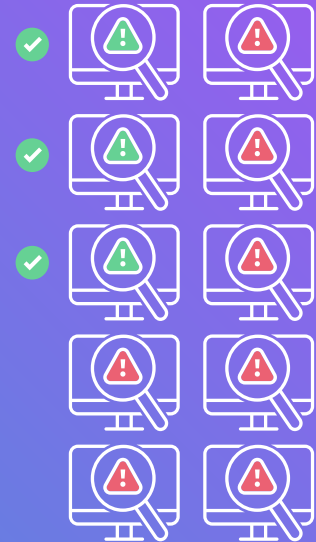
Alerting delays and routing failures in cybersecurity systems can arise from multiple factors, such as the improper routing of detection tool telemetry to the SIEM, ingestion issues that slow down the transfer of endpoint data, or inefficiencies in analyzing and distilling actionable information from large data volumes. Additionally, there may be latency in communication systems that delay the dispatch of alerts based on the analysis, leading to critical lapses in response time.

Evolving Adversarial Tactics

Advanced threat actors continuously refine their tactics to bypass security controls, using techniques like polymorphic malware and zero-day exploits. This ongoing evolution challenges the effectiveness of threat detection tools, creating gaps that can leave organizations vulnerable to sophisticated attacks, even when robust security measures are in place.

The above examples are only some of the potential ways in which this technical control may fail to operate as intended.

7 out of 10 threat detection assessments identify exploitable security tool gaps.



Data Collected from OnDefend Services (March 2020-March 2024)



Threat Response Teams

Why Threat Response Teams Miss Attacks

Skill and Resource Limitations

Response vendors may lack the expertise or resources to handle complex threats, leading to delays or outright failure. Inadequate training and overwhelmed teams can result in missed detections or ineffective responses.

Communication Breakdowns

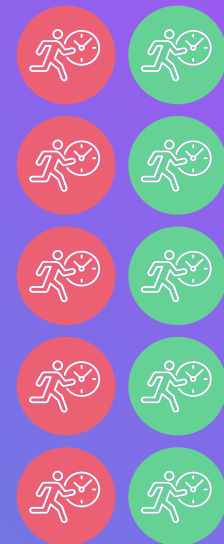
Poor coordination between response vendors and internal teams can lead to delays or critical failures. Misaligned priorities, unclear escalation procedures, or lack of transparency can hinder incident resolution or escalate damage.

Inadequate Response Protocols

Unvalidated or poorly designed response protocols can lead to confusion or failure during incidents. Without proper testing and updates, these protocols may result in missed steps, incomplete containment, or ineffective recovery efforts.

The above examples are only some of the potential ways in which this technical control may fail to operate as intended.

5 in 10 threat response assessments result in a notification response delay or failure.



Data Collected from OnDefend Services (March 2020-March 2024)

Healthcare System Recognizes Risk

—
Why Traditional Testing is No Longer Enough

Prominent Healthcare System Recognizes Risk

This Florida based healthcare system, employs **10,000+ team members** serving more than **1 million patients** a year through primary care facilities, urgent care, and hospitals, including one of the nation's largest children's hospitals.

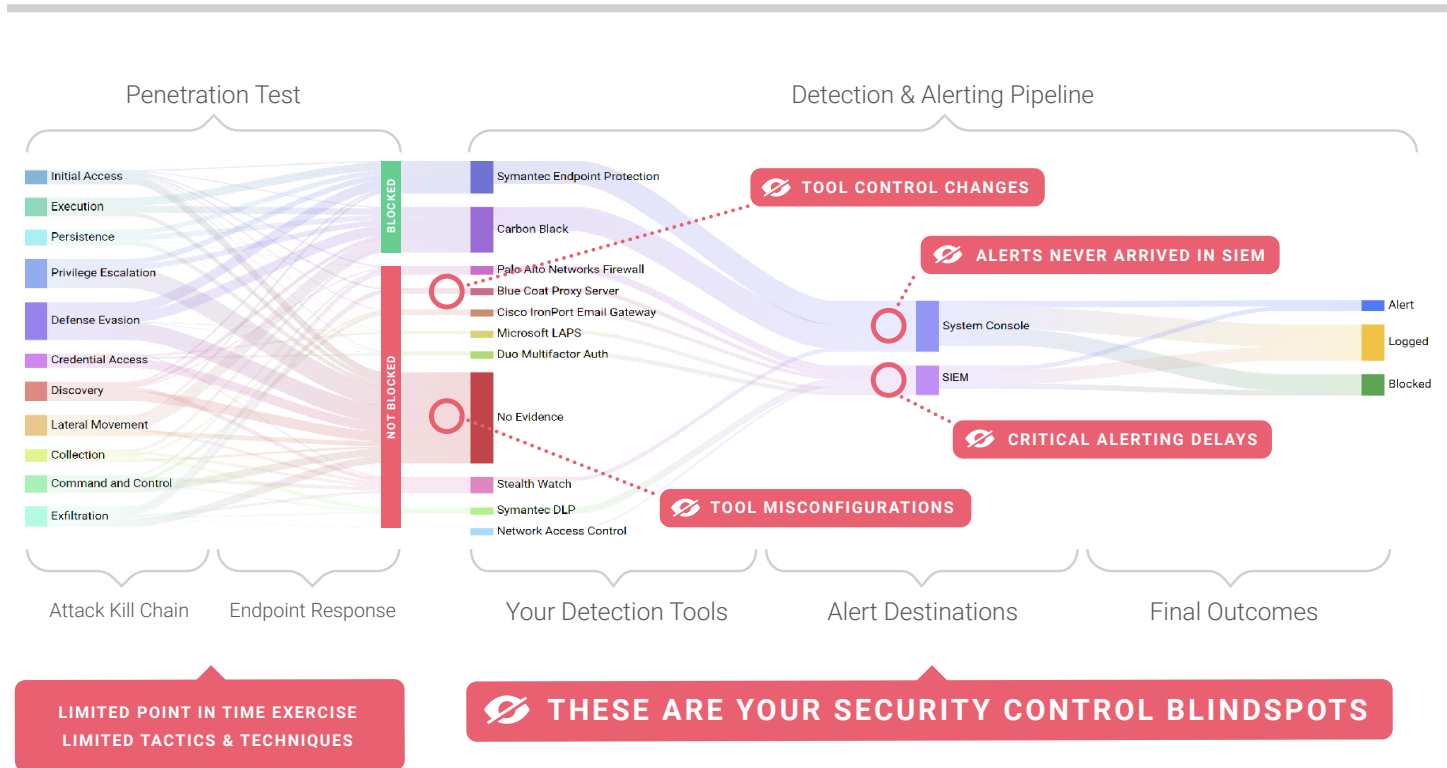


Healthcare system asks: “Are we prepared for ransomware attacks?”

The short answer is: “We think so... but there’s no good way to consistently prove it.”

Traditional cybersecurity services—such as penetration testing, vulnerability assessments, and tabletop exercises—are often conducted only a few times a year, at best. While these methods offer some insights, they don’t emulate the actual Tactics, Techniques, and Procedures (TTPs) of a threat actor and often are not performed enough to properly visualize defense readiness against continuously evolving threats.

This diagram illustrates the gap between traditional penetration testing and the real-world effectiveness of an organization's security controls. It emphasizes the security coverage gaps in detection and alerting pipelines.



“Ransomware is the #1 risk for most hospitals, including ours. We already subscribe to the standard legacy testing practices **but we needed a way to continuously test and validate our defensive controls to prove they are working.**”

Chief Information Security Officer

.....
Prominent Healthcare System

Ransomware Defense Validation

Healthcare System Engages OnDefend to
Validate Security Controls

What is Ransomware Defense Validation (RDV)?

In collaboration with this healthcare system's security team, OnDefend designed a program tailored for the healthcare industry enabled by its breach & attack simulation solution, BlindSPOT. This holistic service offering, run by OnDefend's in-house red team and proprietary BlindSPOT solution, safely simulates real-world healthcare threat actors by consistently testing and validating the following defensive controls:



Secure Email Gateway

To prove malicious emails are being filtered and not reaching employee inboxes.



Threat Detection Tools

To prove security tools are detecting & alerting teams to real-world attack activity.



Threat Response Teams

To prove security teams can respond to threats efficiently and effectively.

Who is OnDefend? What is BlindSPOT? How is it validating controls?

OnDefend empowers organizations to proactively combat real-world cyber threats. BlindSPOT is OnDefend's proprietary Breach and Attack Solution (BAS) that emulates real-world attack activities to identify security control failures and validate the effectiveness of detection and alerting systems. BlindSPOT enables the OnDefend team to deliver Ransomware Defense Validation as a cost-effective, one-time assessment or fully managed service.

[Learn more about OnDefend*](#)

Ransomware Defense Validation

Service Delivery, Outcomes, and Improvements



Email Gateway Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Methodology

OnDefend consistently tests and validates this healthcare system's Secure Email Gateway (SEG) to ensure it is preventing malicious emails from reaching employee inboxes.

This ongoing validation testing includes the following components:

> Malicious Payloads

OnDefend regularly sends simulated malicious emails to the hospital's testing inboxes to assess the effectiveness of their SEG against various simulated threats. These emails contain attachments or embedded content that mimic dangerous scripts capable of exploiting vulnerabilities, executing malicious code, stealing sensitive information, or compromising the integrity of the recipient's system.

This test determines whether the email filter is accurately detecting and blocking emails containing harmful email attachments before they reach corporate inboxes. This testing also verifies the SEG provider will notify the security team of suspicious activity.

> SPF, DKIM, DMARC Evaluations

OnDefend evaluates the email system's capabilities to properly authenticate emails from the business domain.

- > **Sender Policy Framework (SPF) Testing:** Assesses the email system's ability to verify emails are sent from servers authorized by the domain's SPF record and finds instances of email spoofing where the sender's address is forged.
- > **DomainKeys Identified Mail (DKIM) Testing:** These test emails are sent with DKIM signatures to confirm that the email system is checking signatures against the sending domain's public DKIM key, ensuring the email has not been altered during transit and verifies its authenticity.
- > **Domain-based Message Authentication, Reporting, and Conformance (DMARC) Testing:** This testing checks the email system's adherence to the DMARC policy of the sending domain, assessing how well the system enforces its authentication practices to prevent email spoofing.



Email Gateway Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Results

> Validation Testing Overview

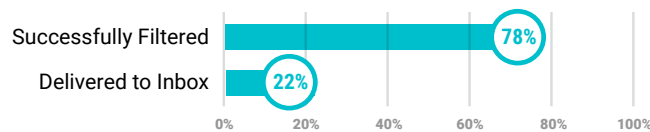
Ransomware Defense Validation is provided to this healthcare system as a quarterly managed service. The **results below are from two quarters of testing**, which evaluated the effectiveness of their Secure Email Gateway (SEG) against real-world threat actor tactics.

During these exercises, OnDefend **deployed 655 emails containing simulated malicious payloads to the healthcare system's testing inboxes**. The objective was to assess whether the email filtering system effectively prevented potentially dangerous emails from reaching employees' inboxes. These emails emulated tactics used by **threat actors such as Qakbot, Alphy/BlackCat, LockBit, Blackbot, Sattered Spider, and others**. Additionally, this test evaluated the healthcare systems **SEG's SPF, DKIM, and DMARC security configurations for vulnerabilities**.

The following visualizes the SEG's response to the validation testing.

> First Quarter Results

Malicious Payload Testing Results:



This healthcare system's filtering system demonstrated a robust initial configuration, **successfully filtering 78%** of the email payloads, with **22% of the emails bypassing the SEG** and being delivered to the testing inbox.

SEG Provider Monitoring Results:

Detection Notification **Success**

The SEG provider was able to accurately identify the malicious emails and **promptly alert the security team within (30) minutes**, demonstrating a responsive and effective threat detection capability.

SPF, DKIM, and DMARC Assessment Results:

Findings **0**

The assessment of the SEG's SPF, DKIM and DMARC security configurations returned **(0) findings**, confirming the email authentication mechanisms were **correctly implemented and functioning as intended**.



Email Gateway Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

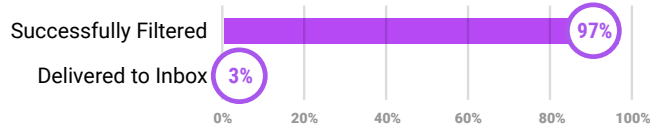
Point-in-Time Validation Result (Continued)

> Second Quarter Results

Following the previous validation assessment, the healthcare system received a comprehensive report detailing how each finding was identified and verified, including severity rankings, actionable remediation recommendations, a full narrative of the engagement, and an executive summary for both the security team and corporate leadership.

Remediation was completed before the second quarter exercise, including tuning and optimizing the SEG.

Malicious Payload Testing Results:



The filtering system demonstrated robust improvements, **successfully filtering 97%** of the email payloads, with **only 3% bypassing the SEG** and arriving in the testing inbox.

SEG Provider Monitoring Results:

Detection Notification **Success**

Once again, the SEG provider was able to accurately identify the malicious emails and **promptly alert the security team within (30) minutes**, demonstrating a responsive and effective threat detection capability.

SPF, DKIM, and DMARC Assessment Results:

Findings **1**

This assessment of the SEG's SPF, DKIM and DMARC security configurations returned **(1) finding** associated with a **policy configuration issue**.

This demonstrates how dynamic environments can experience **unintended control changes that require ongoing testing and validation**.



Email Gateway Validation

VALIDATION TESTING METHODOLOGY

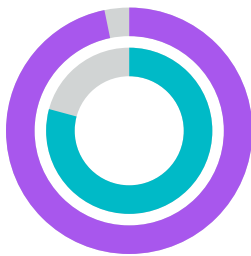
VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Service Outcomes & Improvements

This healthcare system continues making significant strides in strengthening its Secure Email Gateway (SEG) security posture through these ongoing exercises. While the email filtering system was already robust, there were instances where some malicious payloads managed to bypass the email filter solution. Following successful SEG tuning and optimization, the system's effectiveness has seen substantial gains, leading to a marked improvement in threats blocked and a significant reduction in bypasses. These efforts are continuously bolstering the hospitals defenses, ensuring a more secure and reliable email communication environment.

SUCCESSFULLY FILTERED



- Q-1 - 78%
- Q-2 - 97%

19% IMPROVEMENT

The healthcare system improved its email filter effectiveness to 97% of malicious phishing threats were successfully filtered.

With OnDefend's remediation direction, the security program improves in the following key areas:



Detection and Blocking: The healthcare system is able to verify and improve its email system's ability to detect and block emails containing malicious payloads in several ways, like those used by threat actors to gain initial access and gather user credentials. This leads to a reduced number of harmful emails reaching end-user inboxes.



Reduced Spoofing Incidents: Regular testing with SPF, DKIM, and DMARC evaluations continue to enable the security teams to identify and mitigate instances of email spoofing, ensuring that emails received are from legitimate sources.

These SEG validation tests are conducted every quarter in a continuous assessment methodology, regularly adding new and advanced email phishing tactics to regularly test and validate this healthcare systems email filtering system. This method ensures security controls are consistently challenged and refined to prevent control improvements from drifting back into a failure state.



Threat Detection Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Methodology

OnDefend, powered by BlindSPOT's breach and attack simulation technology, safely simulates the same types of activities conducted by threat actors to determine how effective the security controls are at blocking, detecting, and alerting to advanced threat actor activity.

This type of ongoing validation testing includes the following components:

➤ Simulate Cyber Attacks

OnDefend safely emulates real-world attacks on an organization's production network using an "assumed beach" methodology. These attacks are executed via BlindSPOT agents on a sampling of endpoints that represent the customer's security controls. Recurring attacks include ransomware strains, supply chain threats and APT's to simulate the tactics of real-world adversaries.

➤ Measure Security Tool Response

These ongoing attack simulations continuously assess the capabilities of the healthcare systems threat detection tools, including Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) tools. The focus is on evaluating their ability to detect, block, and log attack tactics while promptly alerting security teams, within the thresholds set by the security team and the OnDefend team. Defense effectiveness is regularly measured by comparing successful detections against total attack actions, providing a real-time assessment of the system's resilience to evolving threats.

➤ Visualize Security Stack Effectiveness

Detection, telemetry routing, and alerting results are analyzed to identify threat detection successes, security coverage gaps, and a potential need for further investment.



Threat Detection Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Results

> Validation Testing Overview

Ransomware Defense Validation is provided to this healthcare system as a quarterly managed service. The **results below are from two quarters of testing**, which evaluated the effectiveness of the healthcare systems detection capabilities against real-world threat actor tactics and techniques.

During these exercises, the OnDefend team **emulated three distinct threat actors** specifically targeting the healthcare sector, including **Conti ransomware, Black Basta ransomware, and Nobelium supply chain**, to assess the real-time resilience of the threat detection systems.

These attacks were safely executed by OnDefend's breach and attack simulation solution, BlindSPOT via endpoint agents using an assumed breach methodology.

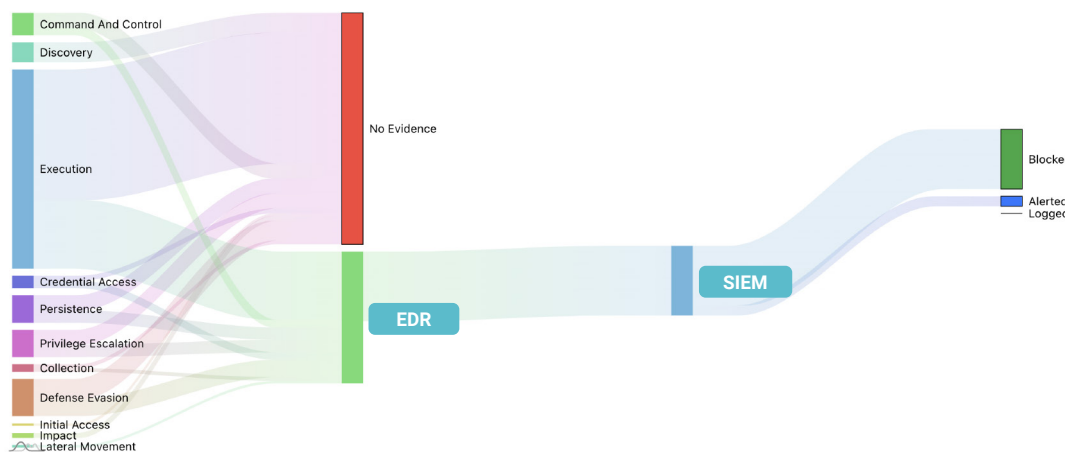
> First Quarter Results

Threat Actor Attack Simulations:

Simulation Name	Expected Block, Alert, or Log	Actual Block, Alert, or Log	READINESS SCORE
Conti Ransomware	54	29	54%
Black Basta Ransomware	64	42	66%
Nobelium Supply Chain	82	64	78%

The initial attack simulations highlighted key areas where the security controls could be strengthened.

Detection & Alerting Pipeline Visibility Results:



This validation assessment revealed areas for detection and alerting pipeline improvements, as telemetry data was mainly directed to its own system console rather than centralized to the SIEM, which reduced the overall visibility needed for a more effective response.

These results highlighted a clear need to enhance this healthcare systems security posture to better defend against these threats.



Threat Detection Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Results (Continued)

> Second Quarter Results

Following the previous validation assessment, the security team received a comprehensive report detailing how each finding was identified and verified, including severity rankings, actionable remediation recommendations, a full narrative of the engagement, and an executive summary for both the security team and corporate leadership.

Remediation was completed before the second quarter exercise, including tuning and optimizing threat detection tools.

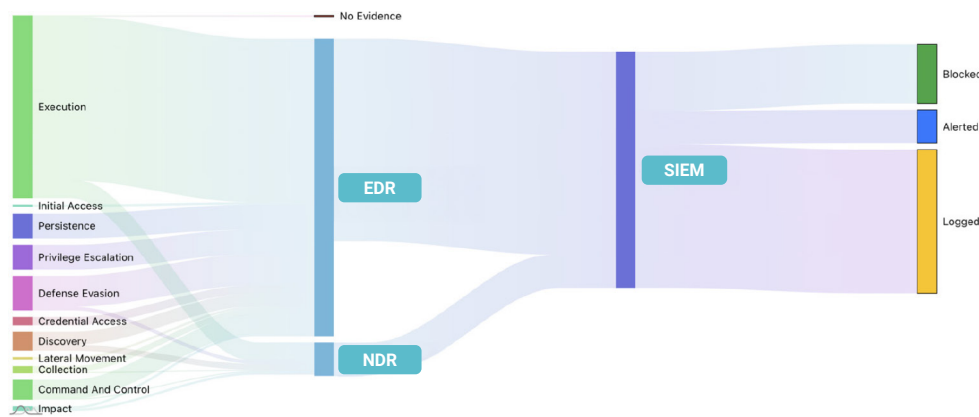
Threat Actor Attack Simulations:

Simulation Name	Expected Block, Alert, or Log	Actual Block, Alert, or Log	READINESS SCORE
Conti Ransomware	54	49	89%
Black Basta Ransomware	64	59	92%
Nobelium Supply Chain	82	80	98%

The second-quarter attack simulations highlighted the significant improvements following the initial validation test.

These results demonstrated a significantly enhanced security posture, enabling this healthcare system to detect and defend against sophisticated threats.

Detection & Alerting Pipeline Visibility Results:



After the initial assessment, the EDR was optimized and additional data sources, including NDR, were integrated. This led to improved attack detection and centralized telemetry routing to the SIEM, resulting in significant enhancements to threat detection capabilities, alerting performance, and overall visibility into organizational threats.



Threat Detection Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

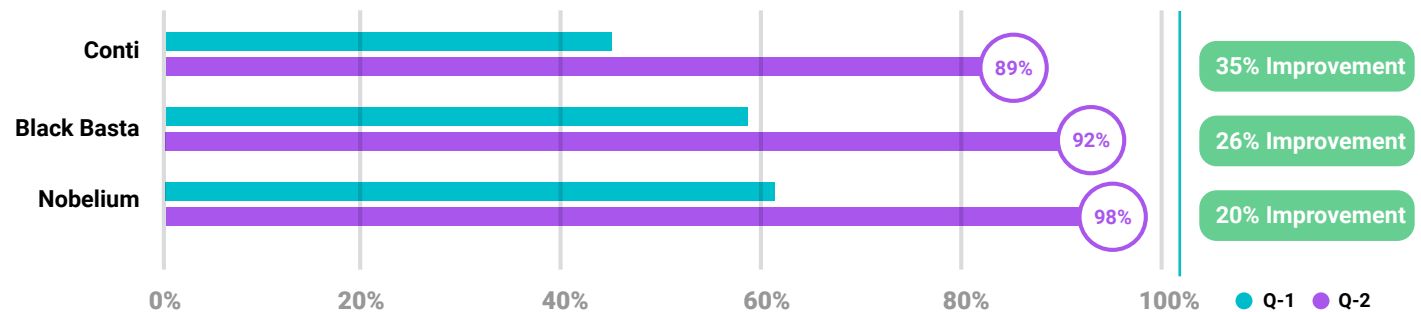
SERVICE OUTCOMES & IMPROVEMENTS

Service Outcomes & Improvements

The healthcare system continues making significant strides in improving its threat detection security posture following targeted remediation efforts. The organization has significantly enhanced its ability to detect sophisticated cyber threats and reduce its Mean Time to Detect (MTTD). These advancements reflect a more robust and resilient threat detection program, positioning the healthcare system to better safeguard its operations against evolving threats.

Key outcomes and improvement trends following these assessments:

Threat Actor Preparedness:



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

Security Tool Improvements:

Additional Events Logged **51**

Additional Alerts Triggered **48**

Additional Attack Blocks **22**

Total Blind Spots Removed **121**

New Detection Rules Created **4**

121 detection blind spots were removed and four advanced detection rules were created.



Threat Detection Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

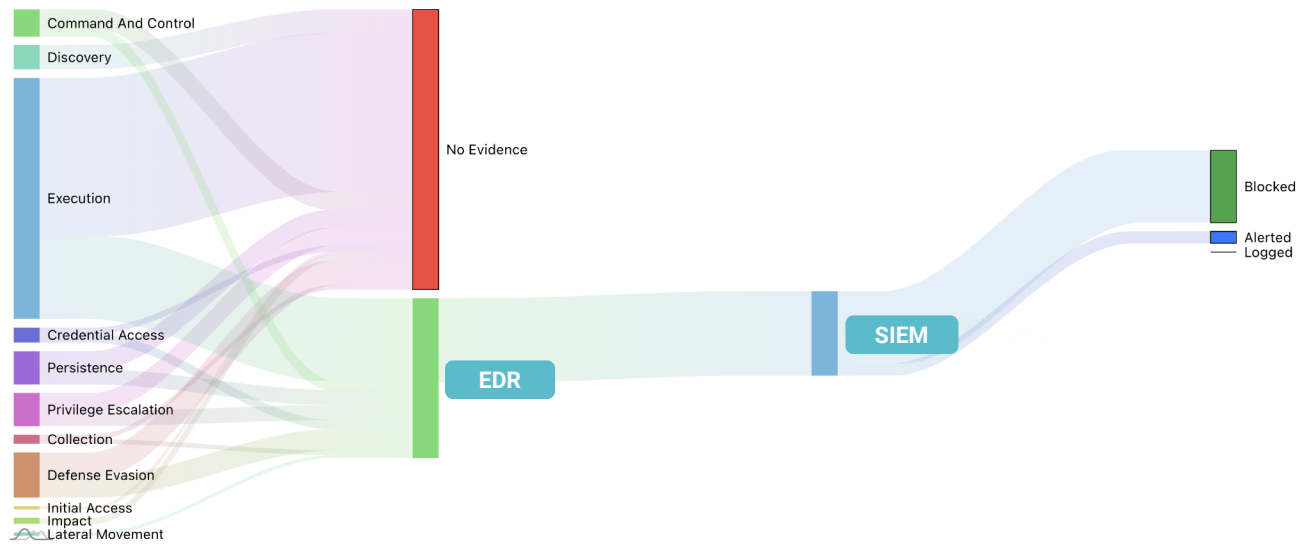
SERVICE OUTCOMES & IMPROVEMENTS

Service Outcomes & Improvements (Continued)

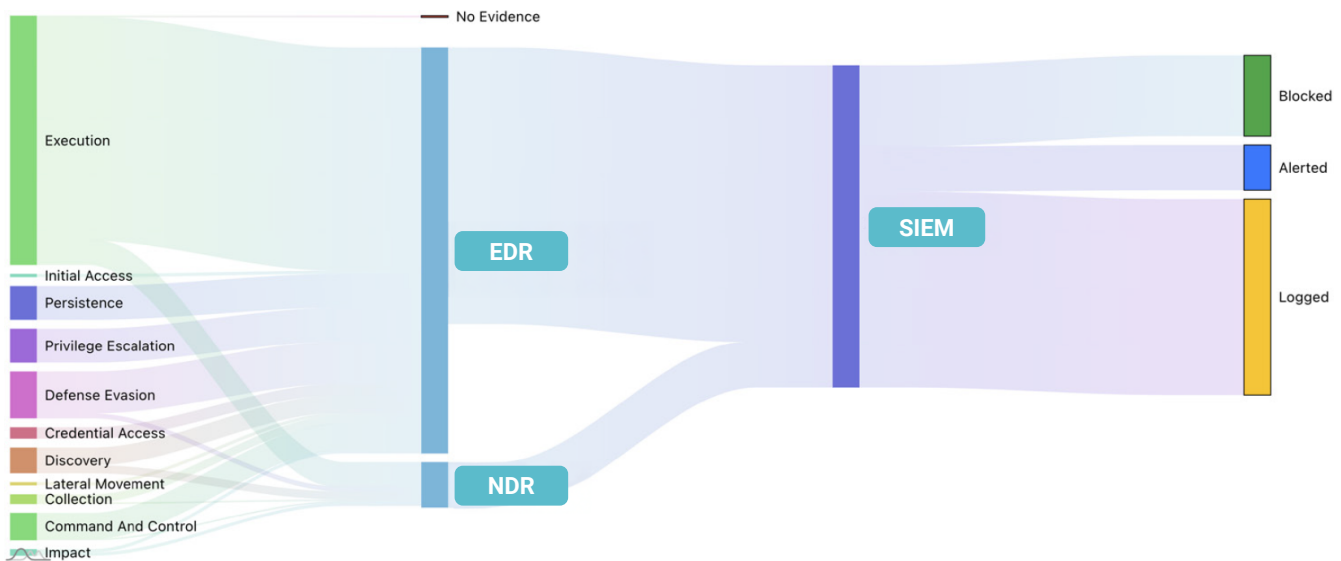
Detection & Alerting Pipeline Visibility Improvements:

The security team achieves 99% visibility into its threat detection pipeline

Q1 RESULTS



Q2 RESULTS





Threat Detection Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Service Outcomes & Improvements (Continued)

With OnDefend's remediation direction the security program improved in the following key areas:



Improved Mean Time to Detect (MTTD): The MTTD continues to improve by optimizing tool configurations and enhancing detection telemetry integration with their Security Information and Event Management (SIEM) system. These enhancements improve the speed and accuracy of threat detection, streamlining the process of identifying and responding to security incidents.



Demonstrated Program Effectiveness: This clear demonstration of the security capabilities provides transparency and reassures stakeholders that the strategic allocation of resources to the cyber security function is safeguarding patient data and hospital operations while also identifying opportunities for enhancement.

These threat detection validation tests are conducted every quarter in a continuous assessment methodology to regularly test against new and emerging threats. As threat actor test scores reach the healthcare systems goals, OnDefend will add new threat actor simulations. This method ensures security controls are consistently challenged, improved, and prevents improvements from drifting back into a failure state.



Threat Response Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Methodology

OnDefend, powered by BlindSPOT's breach and attack simulation technology, safely emulates real-world cyber incidents designed to rigorously test the ability of an organizations internal network defense team and/or third-party providers to detect and respond to threat actor activity. The goal is to confirm if third-party providers are meeting their service level requirements.

This ongoing validation testing includes the following components:

> Emulate Cyber Incidents

OnDefend safely emulates real-world cyber incidents on a production network using an "assumed beach" attack simulation methodology. These attacks 'ring the bell' and initiate responses from internal and external defense teams.

> Demonstrate Response Capability

OnDefend tracks the Mean Time to Respond (MTTR) for an organization's internal security monitoring team, third-party Network Detection and Response (NDR), and Managed Detection and Response (MDR) providers, ensuring the response times align with the established Service Level Agreements (SLAs) and expectations.



Threat Response Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Results

Ransomware Defense Validation is provided to the healthcare system as a quarterly managed service. The **results below are from two quarters of testing**, which evaluated the effectiveness of the threat response teams during a simulated cyber event.

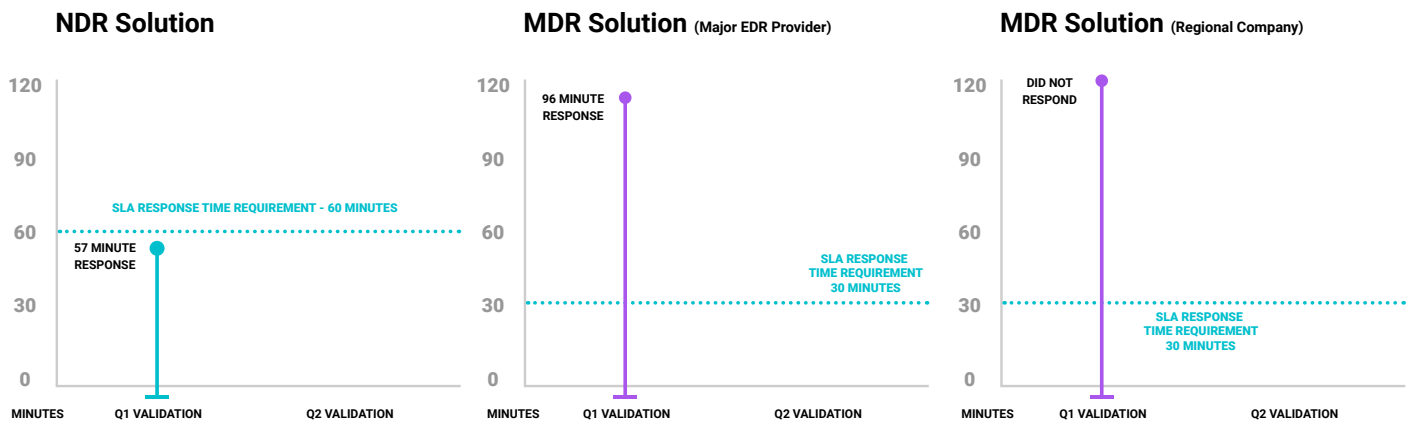
During these exercises, the OnDefend team **simulated a real-world cyber event** to assess the effectiveness of the healthcare systems NDR and two MDR providers, focused on their **response capabilities and MTTR**. The performance was then **compared to the SLA's** and overall customer expectations of these solutions.

This emulated cyber event was safely enabled by OnDefend's breach and attack simulation solution, BlindSPOT via endpoint agents using an assumed breach methodology.

> First Quarter Results

Threat Response Incident Emulation:

The results highlighted concerning disparities in responsiveness among the managed response providers. While the NDR provider met their SLA requirements, both MDR providers failed to meet the healthcare systems expectations for timely and effective incident response.



This validation assessment emphasized the need for the healthcare systems security team to collaborate with its monitoring providers, implement necessary adjustments, and strengthen its incident response program for improved resilience.



Threat Response Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

SERVICE OUTCOMES & IMPROVEMENTS

Validation Testing Results (Continued)

> Second Quarter Results

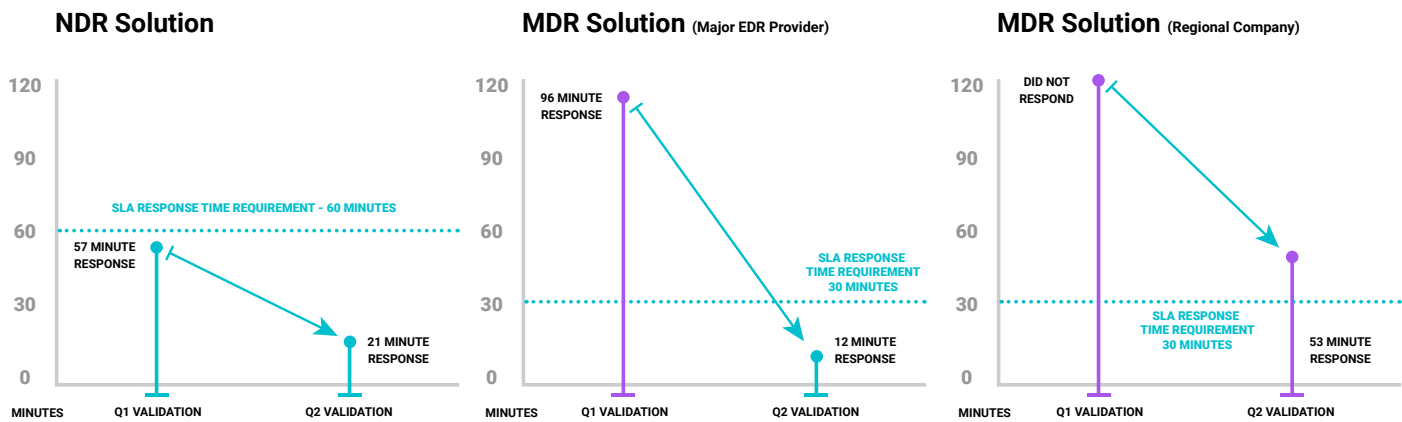
Following the previous validation assessment, the healthcare system's security team received a comprehensive report detailing how each finding was identified and verified, including severity rankings, actionable remediation recommendations, a full narrative of the engagement, and an executive summary for both the security team and corporate leadership.

Remediation was completed before the second quarter exercise, including adjustments made by their third-party NDR and MDR providers for optimized response capabilities.

Threat Response Incident Emulation:

The second round of a cyber incident emulations on the environment demonstrated considerable improvements by the NDR provider and one of the MDR providers.

However, the other MDR solution, a regional company with a 30-minute SLA requirement, once again failed to respond within the SLA requirements, mirroring its performance from the first test.



These results indicated strong performance improvements by the NDR provider and one MDR provider, but persistent issues with the second MDR solution which required the healthcare system's security teams immediate attention.



Threat Response Validation

VALIDATION TESTING METHODOLOGY

VALIDATION TESTING RESULTS

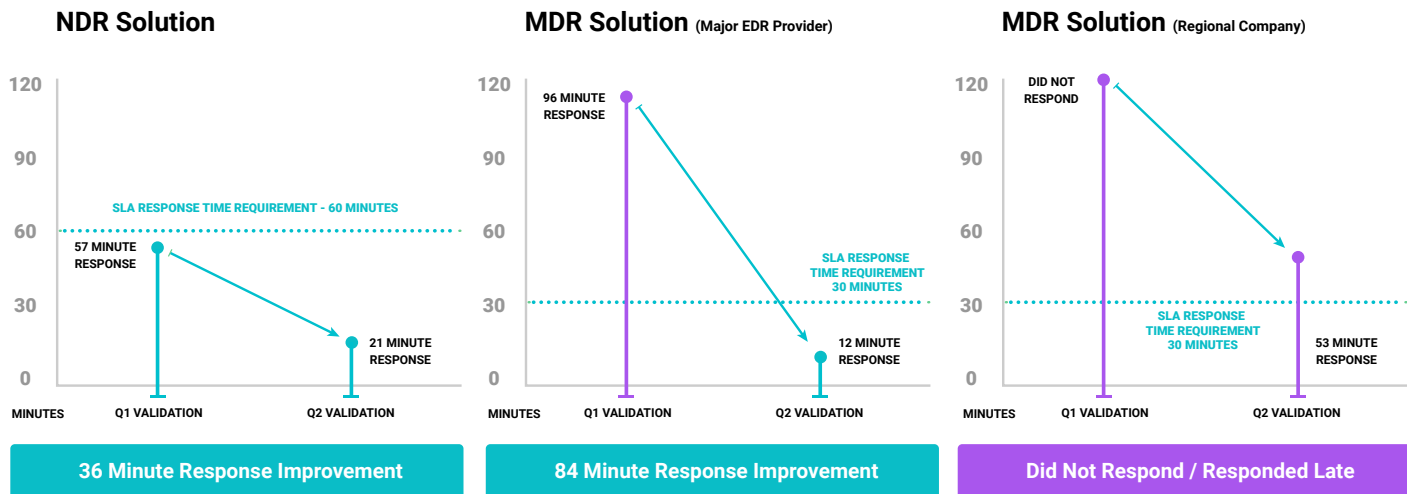
SERVICE OUTCOMES & IMPROVEMENTS

Ongoing Service Outcomes & Improvements

The healthcare system continues demonstrating substantial progress in improving its response capabilities and Mean Time to Respond (MTTR) between validation exercises. These ongoing enhancements result in a more robust and efficient approach to handling potential cyber incidents, ensuring the organization remains responsive and resilient in the face of a cyber event.

Key outcomes and improvement trends following these assessments:

The mean time to respond improved to under 21 minutes



With OnDefend's remediation direction the security program improves in the following key areas:



Response Time Optimization: These assessments reveal delays in detection and response times from the internal team and the MDR provider. As a result, both parties are consistently working to streamline their response protocols to achieve faster reaction times to an attack.



Refinement of Incident Handling Procedures: Insights from the simulations have improved incident handling and escalation procedures with more robust protocols, including clearer roles and responsibilities, ensuring quicker and more effective incident resolution.

These threat response validation tests are conducted quarterly as part of a continuous assessment strategy to ensure that the healthcare systems third-party threat response providers can effectively safeguard the organization. This approach ensures that the investment in these external providers is fully optimized and continuously verifying the effectiveness.

Patient Safety & Security Program Outcomes

The Lasting Impact of
Ransomware Defense Validation

Security Program Improvements & Benefits

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 our 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

Final Thoughts from the CISO: Patient Safety & Data Security

By leveraging Ransomware Defense Validation, our healthcare system reaffirms our ongoing commitment to enhancing patient safety and showcasing our continued dedication to security.

-  **Patient Safety:** Proactively simulating real-world attacks within our environment allows us to find and eliminate vulnerabilities that could jeopardize patient care. Going beyond HIPAA and compliance standards, we've taken this proactive approach to ensure the integrity of our systems and continuous delivery of critical healthcare services.
-  **Patient Data:** Patient safety is our top priority, closely tied with protecting the confidentiality and integrity of medical data. By rigorously testing our security against threats, we ensure that patient information remains secure.
-  **Building a Culture of Security:** By staying ahead of threats, we've fostered a strong culture of security at our hospitals. Our staff is highly aware of potential risks and the importance of following security protocols. This shift helps prevent human error, a critical first line of defense. When patients see our commitment to security, their confidence is reinforced.
-  **Public Trust:** The public's trust in our healthcare system grows when patients see us proactively taking steps to protect them. By thoroughly testing our security program, we're able to show that we go beyond regulatory requirements. This transparency reassures patients that their well-being is safeguarded, and their information is protected to the highest standards.

Ransomware Defense Validation plays 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, their sensitive data, while maintaining their trust so we can focus on what matters most: **patient care**.

Perspectives by OnDefend

Let's Continue the Conversation

Perspectives by OnDefend

Solutions built by security leaders, for security leaders.

By leveraging OnDefend's Ransomware Defense Validation, this healthcare system has fortified its defenses and ensured a higher standard of patient care. But the journey doesn't end here.

Engage with our cybersecurity experts to explore how Ransomware Defense Validation can benefit your organization. Discover actionable insights, customized solutions, and a partnership dedicated to your security success.

Request a Consultation: Schedule a personalized consultation with our experts.

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](#).

Next Steps

 contact@ondefend.com  ondefend.com  800.214.2107 