

# Ransomware Defense Validation

Powered By:  blindspot

## Prove Your Security Investments are Protecting You Right Now

You've implemented best-in-class threat prevention, detection, and response solutions, but how can you demonstrate these solutions are effectively safeguarding your organization and continuously delivering a return on investment?

### The Challenge: **Prevention, Detection & Response Failures**

#### ◆ Prevention & Detection Tools (SEG, EDR, SIEM, etc.):

Security tools can fail to prevent or detect due to:

- Tool misconfigurations that prevent attack detection.
- Unintended control changes made by internal teams or 3rd party vendors.
- Evolving adversary tactics that evade and bypass detection mechanisms.
- Security tool disruptions where tool vendors adversely affect tool effectiveness.

#### ◆ Threat Response Providers (MDR, NDR, etc.):

Monitoring teams can fail to respond due to:

- Alerting failures caused by detection telemetry failures and delays.
- Lack of visibility due to incomplete monitoring or access to necessary data.
- Skill and resource limitations due to inadequate training or overwhelmed teams.
- Communication breakdowns due to misaligned priorities and failed procedures.

**7 out of 10 attack simulations identify security tool misconfigurations or exploitable control failures.**

– Data collected from OnDefend red team services (March 2020 – March 2024)

**5 out of 10 attack simulations result in no response or a delayed response outside of SLA requirements.**

– Data collected from OnDefend red team services (March 2020 – March 2024)

As security budgets grow, CEOs and boardrooms are demanding concrete evidence that cybersecurity initiatives deliver value beyond regulation compliance.

– The Hacker News

### Picture This...

*Imagine your home security provider visits your house regularly, opening all the doors and windows to ensure the alarms are successfully alerting their team to ensure they will immediately respond. Wouldn't you sleep better at night?*

This is what OnDefend's Ransomware Defense Validation does for your organization...

# The Solution: Ransomware Defense Validation

OnDefend's Ransomware Defense Validation simulates real-world cyber-attacks to consistently ensure your **secure email gateway** is effectively filtering malicious emails, **threat detection tools** are detecting real-world attacks, and **threat response teams** are neutralizing threats in real-time.

## How it Works: Ransomware Defense Validation Methodology

### SECURE EMAIL GATEWAY (SEG)

**GOAL:** We ensure your email filter is actively preventing malicious emails from reaching employee inboxes and all anti-spoofing configurations are optimized.

#### HOW WE DO IT

- ◆ **Malicious Payload Simulations:**
  - We send simulated malicious emails to test inboxes to evaluate your SEG's effectiveness against real-world threat actor tactics.
- ◆ **SPF, DKIM, DMARC Evaluations:**
  - We assess your email system's setting to successfully authenticate business domain emails through SPF, DKIM, and DMARC testing.

#### IS YOUR EMAIL FILTER BLOCKING EMAILS?



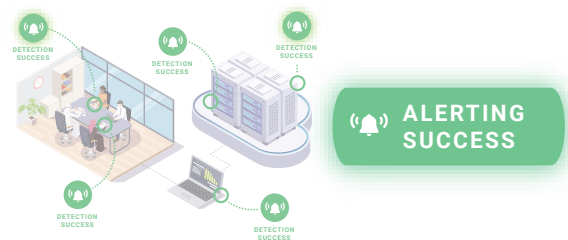
### THREAT DETECTION TOOLS

**GOAL:** We prove your security tools are detecting & alerting your teams to real-world attack activity and lowering your overall Mean Time to Detect (MTTD).

#### HOW WE DO IT

- ◆ **Simulate Cyber Attacks:**
  - We safely simulate real-world attacks on your production network using our assumed beach methodology through BlindSPOT.
- ◆ **Measure Security Tool Response:**
  - Our simulations evaluate the effectiveness of your detection tools (EDR, SIEM, and others) to identifying alerts while measuring your MTTD.
- ◆ **Visualize Security Stack Effectiveness:**
  - We'll show you exactly where your security stack is succeeding, existing gaps, and where further investments might strengthen your defenses.

#### ARE YOUR SECURITY TOOLS DETECTING ATTACKS?



## THREAT RESPONSE TEAMS

**GOAL:** We confirm your internal team and 3rd party response vendors are immediately responding to attacks and lowers your overall Mean Time to Respond (MTTR).

### HOW WE DO IT

- ◆ **Emulate Cyber Incidents:**
  - OnDefend safely emulates real-world cyber incidents on your production network to 'ring the bell' and initiate responses from internal and external response teams.
- ◆ **Demonstrate Response Capability:**
  - OnDefend tracks the MTTR of your team and response vendors (NDR, MDR & others) ensuring they are meeting their Service Level Agreements (SLAs).

WILL YOUR MONITORING PROVIDER RESPOND?



## Easy to Implement: Low Effort, High Value

OnDefend minimizes bandwidth constraints for your team.

### SERVICE SETUP

- ◆ **Secure Email Gateway Validation:** Set up a sample inbox to test if simulated malicious emails with payloads can bypass your secure email gateway and reach the inbox.
- ◆ **Threat Detection Validation:** Deploy the BlindSPOT service on a small sample of endpoints (typically 3–5) where your existing security tools are already operational, validating their ability to detect simulated threats.
- ◆ **Threat Response Validation:** Similar to Threat Detection Validation but only requires one endpoint to assess your internal response team and response vendors' ability to neutralize detected threats effectively.
- ◆ **Total Customer Time:** 2 hours

### PER EXERCISE

- ◆ **Secure Email Gateway Validation:** Set up a sample inbox to test if simulated malicious emails with payloads can bypass your secure email gateway and reach the inbox.
- ◆ **Threat Detection Validation:** After the attack simulation is successfully executed, we simply need your exported logs to correlate the tools response.
- ◆ **Threat Response Validation:** After the simulated incident is successfully executed, we simply need the actual response times of your internal team and response vendors'.
- ◆ **Total Time Per Exercise:** 5 - 8 hours

### COMPREHENSIVE REPORTING

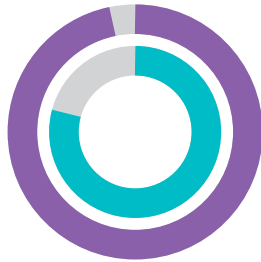
- ◆ You receive comprehensive reporting with detailed insights as well as actionable remediation recommendations.
- ◆ All reporting includes simple graphical representations of outcomes that laypeople in your organization can understand and value.

# Case Study: Prominent Healthcare System (serving over 1 million patients annually)

**CHALLENGE:** This healthcare system needed quantitative proof of defense efficacy and operational readiness against known and emerging threats.

## EMAIL GATEWAY RESULTS

SUCCESSFULLY FILTERED



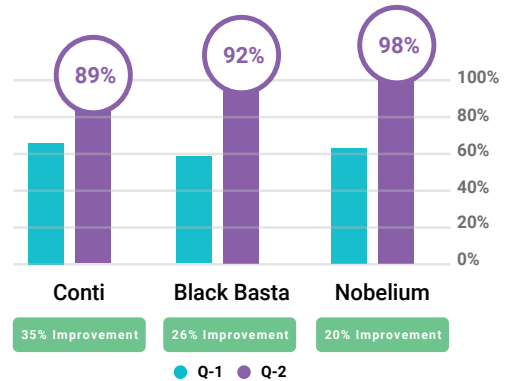
● Q-1 - 78%

● Q-2 - 97%

19% IMPROVEMENT

97% of malicious phishing threats were successfully filtered.

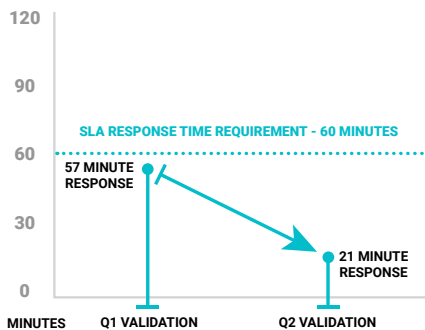
## THREAT DETECTION RESULTS



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

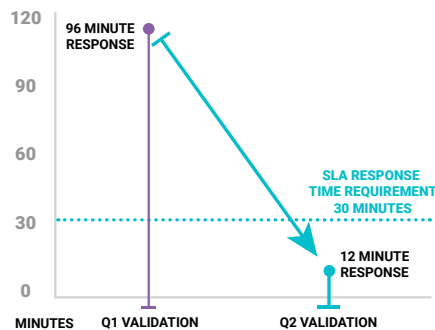
## RESPONSE TIME RESULTS

### NDR Solution



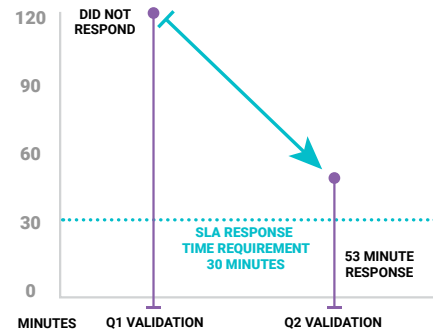
36 Minute Response Improvement

### 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.



## DOWNLOAD THIS CASE STUDY HERE:

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

## Benefits and Outcomes: Bolstering Your Security Program



### Security Operational Assurance

RDV con RDV consistently provides clients with proof that their security controls are optimized and not adversely impacted by their team, third-party monitoring providers, or the security tool providers.



### Proactive Risk Reduction

While eliminating all risk is impossible, RDV empowers security teams with proactive measures that significantly reduces threats, ensuring their defenses remain resilient even in the most critical situations.



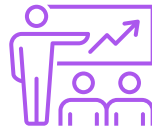
### Security Vendor Accountability

Organizations achieve ongoing assurance that security vendors meet their SLA requirements and consistently deliver the expected level of protection required by the organization to justify investment.



### Demonstrate Preparedness to Leadership

Security teams are frequently asked by leadership about their readiness to defend against advanced threats. RDV provides a reliable way to demonstrate their preparedness and resilience to adversaries targeting their organization or industry.



### Justify Security Investments

RDV enables organizations to ensure their security investments are effective and optimized by providing clear, quantifiable proof of their impact in a way that corporate stakeholders can easily understand and appreciate.



### Lower Cyber Insurance Premiums

RDV helps organizations lower insurance premium costs by providing verifiable proof of security effectiveness, reducing perceived risk, and demonstrating that proactive measures are in place to prevent and mitigate threats.


Are your security controls ready for the next ransomware attack?  
Let's find out.


## Validate Your Defenses Today

Schedule a consultation to learn how to quantify your cyber resilience, demonstrate the ROI of your security resources, and identify gaps before they can be exploited.

**OnDefend**

 [ondefend.com](https://ondefend.com)

 [contact@ondefend.com](mailto:contact@ondefend.com)

 800.214.2107