CASE STUDY

Transforming Email Noise into Actionable Defense with Binary Defense

Customer Profile

With hospitals, health centers, and specialty care facilities spread across the state, this health system provides care to over a million patients each year, driven by a mission to improve lives at scale.

Challenges

Hospitals and health systems are prime targets for phishing attacks, which can lead to ransomware infections, HIPAA violations, and exposure of millions of patient records. For one Healthcare Organization already strained by shrinking budgets, compliance demands, and limited staff, heavy reliance on email made the risk even greater. A small security team was overwhelmed, spending more than 60% of their time chasing SIEM alerts, user submissions, and suspicious emails instead of focusing on critical security initiatives. To protect patient data and reduce risk, the Healthcare Organization needed a way to offload investigations and strengthen their ability to rapidly detect and respond to phishing threats without exhausting scarce resources.

Solution

Phishing Response Service

Results

- 24+ hours saved per week across IT Helpdesk, Cybersecurity, and Server Operations teams
- 2,900+ suspicious emails investigated within the first 90 days, with 181 escalated for action
- Proactive defense that stops phishing emails before a user clicks, instead of reacting to alerts after attackers gain entry

Challenges

Hospitals and health systems remain prime targets for phishing attacks, often leading to ransomware infections or exposure of millions of patient records. For one Healthcare Organization, the challenge was particularly acute. Already stretched thin with shrinking budgets, compliance demands, and limited staff, the organization relied heavily on email to communicate with patients and manage daily operations.

This reliance created a dangerous vulnerability: a single phishing email could trigger financial loss, HIPAA violations, and reputational damage. The Healthcare Organization's small security team found themselves drowning in email investigations from their SIEM alerts and email abuse mailbox, which was consuming more than 60% of their team's time. Tasked with leading strategic security projects, the Healthcare Organization's security team instead found themselves consumed by inbox noise, distracting from critical initiatives and leaving the organization exposed to external threats.

To safeguard patient data and reduce risk, the team needed a way to offload investigations and strengthen their ability to quickly identify and respond to phishing attempts without draining already scarce resources.

Solution

The Healthcare Organization partnered with Binary Defense to lock down one of the most exploited attack vectors—email. Together, they built a phishing response strategy that replaced tedious manual investigations with expert-led email forensics, precision threat detection, and rapid remediation support.

Instead of draining valuable staff time, Binary Defense's Phishing Response service handled rapid triage, IOC extraction, and full-scope investigations of suspicious emails flagged by users or SIEM alerts. Real humans—not rules—reviewed every submission in their abuse mailbox. Each analysis was backed by threat intelligence, deep adversary knowledge, and hands-on analysis from a phishing analyst.

During investigations, Binary Defense analysts go beyond sandboxing. They proactively extract and deliver all known malicious indicators, including domains, hashes, and IPs, for correlation and response. Every report includes concrete next steps: email headers, risk severity, and response guidance tailored to the Healthcare Organization's environment. When threats were confirmed, analysts notified the team, analyzed the root cause, performed malware analysis, and provided incident response context. They also build and fine-tune detection rules, ensuring defenses are continuously strengthened.

For the Healthcare Organization, this partnership translated to faster mean time to response (MTTR), reduced risk of data compromise, and regained focus on high-priority initiatives. With Binary Defense's Phishing analysts providing advanced, skilled, and capabilities, the Healthcare Organization's security team now has the confidence that every email threat is investigated thoroughly, strategically, and with the precision needed to protect the business and patient data.

In Action

A phishing campaign targeted 15 of the Healthcare Organization's employees with an email crafted to look like it came from a trusted supplier's accounting department. The message contained a malicious .svg file that redirected users to a credential harvesting domain. While one employee clicked the file, another quickly reported the suspicious email to the Healthcare Organization's abuse mailbox.

Binary Defense Phishing Response analysts immediately engaged, containing the potentially compromised device and performing a thorough investigation. Endpoint analysis revealed no malicious activity, but Umbrella logs confirmed that the device had connected to a domain hosting a credential harvesting tool.

The analyst escalated findings to the Healthcare Organization's internal team and delivered actionable recommendations. These included purging the phishing email from inboxes, blocking the sender, blocking the hash in Defender, and preventing future access to the malicious domain through Umbrella. The team was also advised to run an antivirus scan, revoke sessions and reset credentials for the impacted user, and enroll that user in phishing awareness training.

Through swift action and clear, strategic guidance, Binary Defense ensured the Healthcare Organization minimized risk, prevented credential theft, and strengthened resilience against future phishing campaigns.

Results

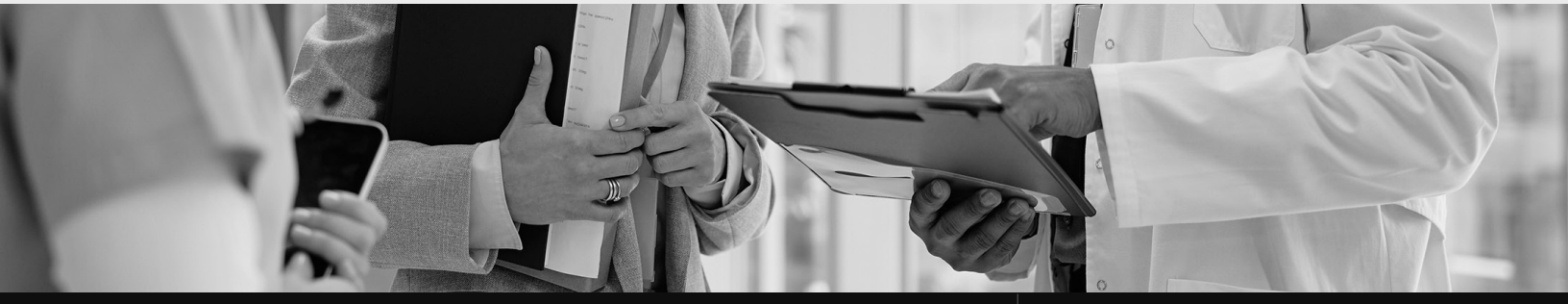
Following onboarding, the Healthcare Organization quickly realized significant time savings across multiple teams, including IT Helpdesk, Cybersecurity, and Server Operations—collectively reclaiming more than 24 hours each week. This efficiency gain allowed teams to focus on higher-priority initiatives while improving the overall security posture of the organization.

24+hours
saved per week across IT Helpdesk, Cybersecurity, and Server Operations teams

For the internal security team, the partnership delivered measurable improvements such as faster campaign email removal, earlier awareness of shifting attacker tactics, actionable visibility into who was being targeted, reduced queue response times, and more effective detection of malicious emails. In addition, tuned rule sets were fed back into their email security tools, strengthening defenses even further. These improvements were not just theoretical, they quickly translated into measurable impact.

Within the first 90 days, Binary Defense Phishing Response analysts investigated more than 2,900 suspicious emails generated from SIEM alerts and user submissions. Of those, 181 were escalated to the Healthcare Organization's security team for action. Beyond these quantitative results, the collaboration produced a qualitative transformation: Binary Defense analysts tailored their processes to align with the Healthcare Organization's workflows, ensuring remediation recommendations were fully adopted and integrated into daily operations.

This proactive approach means the Healthcare Organization is no longer waiting for alerts that signal an attacker has already gained a foothold. With Binary Defense Phishing Response, malicious emails are identified and contained before a user can click, stopping threats at the front door and preventing them from ever becoming full-blown incidents. By shifting from a reactive to a proactive defense model, the Healthcare Organization not only strengthened its resilience but also reinforced its commitment to protecting patient data and maintaining trust.



Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

FORRESTER
WAVE STRONG PERFORMER 2025
Managed Detection And Response Services

BINARY DEFENSE