Securing The Human Layer of Healthcare

Human error continues to dominate healthcare security breaches

For healthcare organizations to deliver on the trust placed in them, keeping sensitive data secure and protecting users from phishing attacks are critical. But the frenetic pace and increasingly remote nature of work in healthcare have made the human layer vulnerable.

Whether it’s accidentally clicking on phishing links, sending sensitive data to the wrong person, or paying invoices on spoofed vendor emails, humans are involved in the vast majority of healthcare data breaches. These breaches have also begun to go after the lower-hanging fruit of personal data (66%) rather than medical data (35%) according to the Verizon 2021 DBIR.

$1.86 B
Reported losses from BEC and EAC attacks in 2020 according to the FBI Internet Crime Report

66%
Percent of breaches in 2020 in the Healthcare sector that involved compromised personal data according to the Verizon DBIR

36%
Percent of breaches in 2020 that involved phishing as a tactic, up from 25% last year according to the Verizon DBIR

Healthcare’s unique email security challenges

Lean IT and Security Teams
Healthcare security teams have a lot on their plate and often lack the time and resources to triage and respond to high-volume email threats.

Device and Email Sprawl
Doctors and staff can have email accounts with multiple hospitals and often access these accounts remotely on mobile devices – making it tougher to spot targeted attacks.

Compliance Mandates
Using best-in-class inbound and outbound email security controls is a key part of ensuring compliance with HIPAA and other regulations.

Ransomware Risk
Cybercriminals know that impeding patient care is a strong incentive for paying ransoms, and thus target critical healthcare services with ransomware and extortion attacks.

WHY ARMORBLOX

More than 56,000 organizations across industries and sizes trust Armorblox to secure their human layer against targeted attacks and data loss.

Stop BEC, impersonation, extortion, and other sophisticated email threats that get past Microsoft, Google, and SEG security controls.

Prevent your clinician and healthcare staff accounts from being compromised by cybercriminals and used to launch follow-on phishing attacks against stakeholders.

Safeguard your personal, medical, research, and intellectual property data from cybercriminals without hampering your daily work.

Reduce the burden on strained IT / security teams with prebuilt detection policies and automatable response workflows.

Improve investigation quality with detailed email threat insights that are built for human eyes.

Reassign your security team to higher-value activities by reducing phishing triage and response times by 75-97%.

Quick time to value with deployment over APIs that takes minutes and works with Office 365, Google Workspace, Exchange, and hybrid email environments.
How Armorblox Secures The Human Layer of Healthcare

Armorblox helps healthcare organizations communicate more securely over email using the power of Natural Language Understanding (NLU). Armorblox connects over APIs to understand the content and context of communications and secures the human layer from compromise. Healthcare organizations use Armorblox to stop BEC and targeted email attacks, ensure compliance by protecting sensitive data, and reduce phishing response times for user-reported threats.

Inbound Email Protection
Stop a wide range of targeted email attacks - whether they have malicious links, 0-day links, or no links at all.

Email Account Compromise Detection
Stop cybercriminals from taking over clinician and staff email accounts to launch attacks and exfiltrate sensitive data.

Outbound Email Protection
Safeguard sensitive PII, PCI, research, and IP data against accidental or deliberate exposure over email.

Abuse Mailbox Remediation
Reassign your security team’s time and expertise by automating triage and remediation of user-reported email threats.

How It Works
- Connects over APIs in 5 minutes
- Builds communication baselines for your organization and users
- Automatically flags targeted email attacks - no custom policy creation needed
- Automated and configurable remediation actions (delete, quarantine, lock user account) across affected mailboxes

Capabilities

Inbound Email Protection
- Stop targeted attacks such as BEC, spear phishing, impersonation, and extortion.
- Use detailed threat intelligence and IOCs that draw from 1000s of signals across identity, behavior, and language.
- Simplify email security operations with pre-built detection policies and automated remediation actions.

Email Account Compromise Detection
- Detect and block emails that try to phish for account credentials e.g. fake O365 login portals, fake medical portals.
- Identify anomalous email behavioral patterns and remotely lock suspicious user accounts.
- Prevent data exfiltration by detecting anomalous mail forwarding rules, suspicious email forwards.

Outbound Email Protection
- Detect loss of sensitive PII/PCI over email e.g. SSNs, bank account details.
- Configure in compliance mode (only monitoring and detection) or block mode (applying enforcement actions to noncompliant emails).
- Increase accuracy with language-based models that identify PII/PCI within email context e.g. differentiating between SSNs and Zoom meeting IDs.

Abuse Mailbox Remediation
- Automatically monitor and analyze every user-reported email threat.
- Auto-remediate safe emails and known threats to focus on reported emails that need human review.
- Remove identical and similar suspicious emails across user mailboxes with one click.

Hear From Others Like You
Security in healthcare requires rethinking the fundamentals at a foundational level. Email is as basic as it gets, and at TeamHealth, we were very impressed by the ability of Armorblox to protect us against targeted attacks, and automate triage and remediation of threats.

Tom Perrine, CIO and CISO, TeamHealth

Copyright © 2021 Armorblox Inc. All rights reserved.
Armorblox Benefits and Value

For IT and Security Teams

- Secure the organization against targeted email attacks like BEC, spear phishing, impersonation, extortion, vendor fraud, and other threats that steal money and sensitive data.
- Prevent doctor and staff email accounts from getting compromised and being used to launch follow-on phishing attacks against external stakeholders.
- Ensure compliance by protecting sensitive data like PII, PCI, and unencrypted passwords from falling into the wrong hands over email.
- Shift the perception of ‘security as a blocker’ to ‘security as an enabler’ with in-context email threat education for your end users.

For Doctors and Healthcare Staff

- Communicate over email and other cloud applications with confidence.
- Reduce the likelihood of your email account being compromised and used as a vehicle for phishing attacks against people you know.
- Safeguard your personal, medical, and research data from cybercriminals without hampering your daily work.
- Learn about suspicious email threats within the context of your regular email workflows with warning banners.

56,000
organizations protected

5 minutes
to deploy over API

75–97%
reduction in phishing response times

Why Armorblox for Healthcare?

Algorithms That Understand Hidden Threats

Armorblox algorithms understand the content and context of communications to stop targeted phishing attacks and payloadless threats.

Detection & Response That Saves Time

Armorblox has out-of-the-box detection policies and automatable response actions that take email security busywork out of your hands.

Machine Learning Tailored to Your Business

We don’t have all the answers, but you do. Armorblox builds custom ML models for every customer and end user to keep learning and get better with time.