DATASHEET

Email Security For Your Cloud Office

Armorblox

DATASHEET

Email Security For Your Cloud Office

The Human Layer Challenge

We are entering an age of hybrid work where people can accomplish great things from anywhere and are embedded in scores of digital workflows. Most of those workflows involve email and are being hijacked by cybercriminals to target the human layer of enterprises. Here's how email security has changed over the years:

Email attacks have changed

Phishing attacks have evolved to get past traditional security layers via email, SMS, voice, and so on. The FBI received 110% more phishing-related complaints in 2020 compared to 2019.

Payloadless attacks like Business Email Compromise (BEC) and Email Account Compromise (EAC) use language and context as weapons to cause untold losses. The FBI reported $1.86 billion in BEC and EAC losses in 2020.

Email delivery has changed

With 71% of organizations using cloud or hybrid cloud email, businesses are moving away from legacy Secure Email Gateways (SEGs) and instead seeking API-based email security controls that are easier to deploy and don't require MX record changes.

Native email security has changed

Microsoft and Google now provide good spam and malware protection out-of-the-box with their cloud email suites. This enables organizations to seek out augments to native email security that protect against advanced email attacks without duplicating what they have already paid for.

Armorblox Overview

Armorblox helps organizations communicate more securely over email with the power of Natural Language Understanding (NLU).

The Armorblox platform connects to email providers over APIs to understand the context of communications and protect people and data from compromise. Tens of thousands of organizations use Armorblox to stop BEC and targeted phishing attacks, protect sensitive PII and PCI and reduce triage and response times for user-reported email threats.

SUMMARY

Stop phishing, BEC, and other targeted, socially engineered attacks

Protect PII and PCI from falling into the wrong hands

Automated triage and remediation of user-reported email threats

EMAIL INTEGRATIONS

Microsoft 365

Google Workspace

Exchange

USE CASES

Advanced Threat Prevention

Spear Phishing

Zero-Day Credential Phishing

Payroll / Payment / Invoice Fraud

Executive / Employee Impersonation

Account Compromise Detection

Ransomware

URL Protection

Malware Detection

Advanced Data Loss Prevention

PII / PCI Protection

Password Protection

Custom Policies and Regexes

Security Operations

Vendor Insights

Abuse Mailbox Remediation

EAC Timeline View

Warning Banners

Product Capabilities

ADVANCED THREAT PREVENTION

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

- Stop targeted attacks such as BEC, spear phishing, impersonation, extortion, payroll fraud, vendor fraud and other advanced attacks.
- Use detailed threat intelligence and IOCs that draw from 1000s of signals across identity, behavior and language.
- Simplify email security operations with out-of-the-box detection policies and automated threat remediation actions that delete, quarantine or label malicious emails.
- Uncover communication-focused insights to drive targeted security interventions: e.g. most impersonated VIPs, most attacked employees, most attacked departments.
- Detect and block emails that try to phish for account credentials: e.g. emails linking to fake login portals.
- Identify anomalous email behavioral patterns and remotely lock suspicious user accounts.
- Prevent data exfiltration by detecting anomalous mail forwarding rules, suspicious email forwards.

ADVANCED URL PROTECTION

Block attacks that target your workforce to steal credentials with real-time protection against fraudulent sites and malicious URLs.

- Enforce safe redirects by selectively rewriting bad URLs and preventing end users from navigating to fraudulent sites.
- Block advanced threats that use evasive techniques with Machine Learning-driven analysis: e.g. embedded URLs.
- Increase end-user awareness through pre-click and on-click contextual warning banners.
- Real-time inspection and detection of malicious URLs in emails to stop targeted attacks: e.g. zero day threats.

ADVANCED MALWARE DETECTION

Enhance your email security posture with multi-layered malware protection without interrupting business email workflows.

- Protect your organization against previously unseen, targeted malware and advanced persistent threats using Machine Learning models, static and dynamic analysis to capture both malware attributes and techniques.
- Stop attacks propagated through email attachments with secure environments to test, replay, characterize and document advanced malicious activity.
- Proactively warn end users of threats through contextual banners as files are analyzed without introducing delays in email delivery.

ADVANCED DATA LOSS PREVENTION

Reduce false positives and prevent exposure of sensitive data with natural language understanding and artificial intelligence.

- Reduce false positive rates with language-based models that identify sensitive PII/PCI data within email context: e.g. differentiating between SSNs and Zoom meeting IDs.
- Increase accuracy of data loss detection with custom policies and regexes: e.g. Medical Record Numbers, Vendor or Customer Identification Numbers.
- Configure data loss prevention in compliance mode (monitor and detect occurrences) or block mode (delete and block emails).
- Uncover data exposure insights to drive targeted compliance interventions (most noncompliant individuals, data leakage incidents per department, most common compliance policy violations).

SECURITY OPERATIONS

Reassign your security team's time and expertise by automating triage and remediation of user-reported email threats.

- Connect Armorblox to your organization's phishing/abuse mailbox to automatically monitor and analyze user-reported email threats.
- Auto-remediate safe emails and known threats to focus on reported emails that need human review.
- Faster threat investigation for account compromises with a timeline view that consolidates all events associated with potential takeover.
- Remove identical and similarly suspicious emails across user mailboxes with one click.
- Apply forward-looking remediation actions that automatically protect against similar attacks in the future.
- Quickly search emails by sender, recipient or subject to apply custom remediation actions across user mailboxes.
- Schedule automated reports that share key insights into your organization's threats on the cadence of your choice via email.
- Identify and monitor vendor profiles conducting business with you, create supplier risk assessments to stop vendor fraud attempts: e.g. invoice fraud, look alike domains, hijacking invoice payment conversation threads.

How It Works:

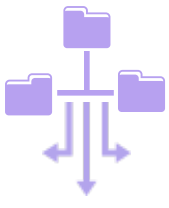
1. Connects over APIs in 5-minutes to MSFT365, Google, and Exchange environments

2. Builds communication baselines for your organization and users

3. Automatically flags targeted email attacks - no custom policy creation needed

4. Automated and configurable remediation actions across affected mailboxes

Armorblox Differentiators



Wealth of Data

We protect tens of thousands of organizations today and learn from attacks across a wide array of industry verticals and company sizes - from Fortune 100 companies to small and medium businesses.

Depth of Models

Armorblox analyzes thousands of signals across identity, behavior, and language using a broad spectrum of techniques like NLU, computer vision, and deep learning to stop advanced attacks that get past other email security layers. Since targeted email attacks don't have any one deterministic 'red flag', the technology to protect against them should consider as many data points as possible.

Transparency and Explainability

Our AI isn't just a mysterious force working behind the scenes. Armorblox clearly explains why each email threat is safe or suspicious. These insights simplify investigation and enable your security team to mark rare false positives with greater confidence. The platform calls out which emails are in the inbox vs spam or deleted folders, and provides activity logs for all actions.

Easy to Deploy and Manage

Armorblox connects over APIs in minutes without any MX modification or email rerouting. Prebuilt policies eliminate the need for manual creation and maintenance or rules. Automated and configurable response actions save time for security teams. Extensible integrations with SIEM and SOAR solutions over RESTful APIs gets Armorblox detected threats to preferred sources of alert aggregation.

Scalable and Cloud-Native

Armorblox leverages a distributed platform built with Kubernetes and Istio that scales across millions of emails and thousands of users instantly. The platform is built on top of Google Cloud, tapping into world-class infrastructure and resource flexibility that makes Armorblox fully enterprise-ready.

Enterprise Grade

Armorblox is built with enterprise scale and security needs in mind. Full role-based access control (RBAC) and detailed audit logs provide users with relevant visibility into activity. Built-in two-factor authentication adds an extra layer of security and protects against compromise. Armorblox is SOC 2 Type 2 certified, highlighting the commitment to upholding the integrity, confidentiality, and privacy of customer data.

Why Armorblox?

Algorithms That Understand Hidden Threats

Armorblox algorithms understand the content and context of BEC attacks to stop advanced 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.

Start Monitoring Threats in Minutes

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.

Inboxes That Love Armorblox

BOB THIBODEAUX, CSO, DEFENSESTORM

"For us, to protect our users and our email systems from social engineering and hacking is critical to protecting our business but also protecting our customers. **We were finding that text based attacks were quarantined right away by Armorblox**. These attacks were not allowed to get to the end users. That is really important to us!"

Learn More ⇢

JONATHAN LEVINE, CTO, INTERMEDIA CLOUD COMMUNICATIONS

"Since implementing Armorblox, we've been able to protect not only Intermedia's corporate users but also over one million customers. We are a hosted Microsoft Exchange Provider and **Armorblox was the only partner who could help us protect our on-premise mailboxes** and was the only decision for our team."

Learn More ⇢

HOWARD MILLER, CIO, UCLA ANDERSON SCHOOL OF MANAGEMENT

"What is really neat for me as a CIO is that whenever I get an email that looks suspicious, I forward it to the email abuse mailbox. **Armorblox then immediately quarantines the threat for everybody else.** As soon as that happens, the magic starts."

Learn More ⇢

58,000
ORGANIZATIONS PROTECTED

5
MINUTES TO DEPLOY OVER API

75-97%
REDUCTION IN PHISHING RESPONSE TIMES

Gartner
COOL VENDOR 2020

Website Blog Customer Success Stories