DATA SHEET

Armorblox

Inbound and Outbound Email Protection

Email Security Lacks Understanding

Over 70% of all enterprise data is textual. Without the security controls in place to analyze the content and context of enterprise communications, organizations are left to fend off targeted email attacks and outbound data loss.

Targeted Email Attacks

Email attacks today are laser targeted and evade traditional detection by preying on human nature. Moving beyond mass-phishing and malicious payloads, attackers are now researching their targets before impersonating trusted parties or taking over legitimate email accounts to induce actions that cause financial loss. Over **$26 billion** has been lost to business email compromise (BEC) attacks over the last three years according to the FBI.

Data Loss

The desire for speed and productivity usually comes at the expense of data privacy and security, with employees inadvertently sharing sensitive PII/PCI data with external parties, or maliciously sharing confidential data outside the organization.

Armorblox Overview

Armorblox brings understanding to security to protect the most attacked layer in enterprises today: the human layer. Armorblox is a cloud-native and content-aware email security platform that protects against targeted attacks such as business email compromise, account takeover, and executive impersonation. The Armorblox detection engine analyzes identity, behavior, and language across all email communications to detect attacks that other products miss. Organizations use Armorblox to deploy pre-configured policies that block suspicious emails, automate abuse mailbox remediation, and prevent outbound data loss.

SUMMARY

- Stop targeted email attacks
- Prevent outbound data loss
- Automate abuse mailbox remediation

EMAIL INTEGRATIONS

- Office 365
- G Suite
- Exchange

USE CASES

Inbound:

- Payroll Fraud
- Vendor Invoice Fraud
- Payment Fraud
- Executive Impersonation
- Account Takeover

Outbound:

- PII/PCI Compliance
- Confidential Content Protection

Armorblox Product Capabilities

Inbound Email Protection

- Stop targeted attacks such as business email compromise, account takeover, executive impersonation, and spear phishing.
- Study detailed email-specific analysis that draws insights from identity, behavior, and language signals.
- Leverage threat-specific policy actions that automatically block, quarantine, or label suspicious emails.

Outbound Data Loss Prevention

- Detect accidental or malicious data loss over email such as SSNs, bank account details, and account passwords.
- Leverage policy actions that automatically block emails containing sensitive data from leaving the organization.
- Protect confidential content from being accessed by unauthorized parties over email.

Abuse Mailbox Remediation

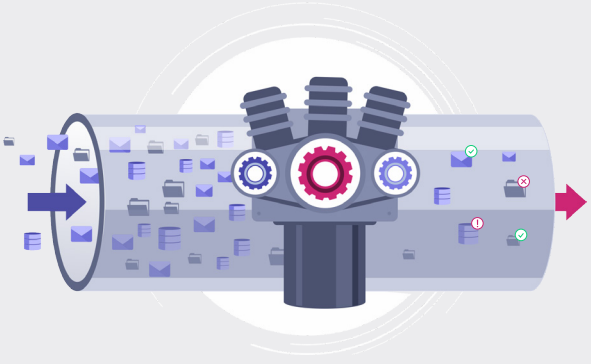
- Connect Armorblox with enterprise phishing/abuse mailbox for centralized management with intuitive search and query.
- Auto-remediate safe emails and known threats to focus on reported emails that need human review.
- Remove similar suspicious emails across user mailboxes with one click.
- Apply forward-looking remediation actions that automatically protect against similar attacks in the future.

Policy Framework

- Utilize pre-configured policies for every threat type that automatically block, quarantine, or label suspicious emails.
- Leverage continuously updated policies as attacks evolve with time.
- Customize actions per policy and add multiple actions for a single policy (per AD group, per VIP list, and so on).

Armorblox Detection Engine

Armorblox uses a broad spectrum of detection techniques to analyze identity, behavior, and language on all email communications. The detection engine leverages natural language understanding, deep learning, machine learning, and statistical techniques to cover thousands of signals that lend unprecedented accuracy to detecting targeted email attacks.



Armorblox Platform Features

API-first Architecture

The Armorblox platform is cloud-native and integrates with email clients over APIs to deploy and protect within minutes. An API-based approach minimizes deployment complexity and ensures rapid, real-time attack detection.

Extensible Integrations

The Armorblox platform is built to be extensible across both data sources and incident response solutions. Armorblox integrates with Office 365, G Suite, and Exchange, offering comprehensive email security support and protection against data loss. Integrations with SIEM and SOAR solutions over RESTful APIs gets threats detected by Armorblox to any preferred source of alert aggregation.

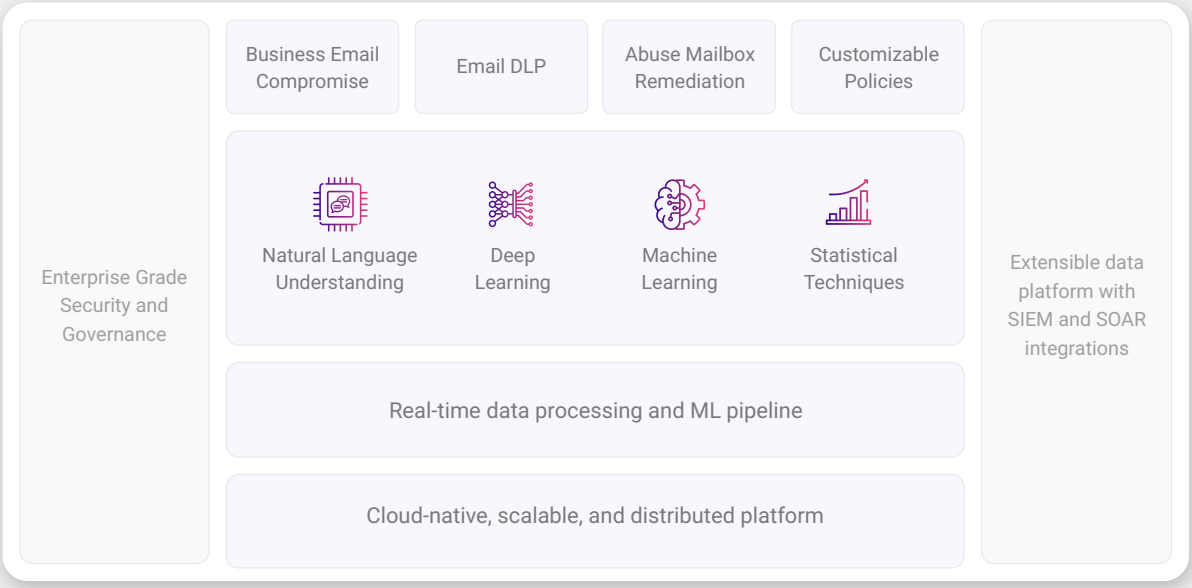
Enterprise Grade

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 1 certified, highlighting the commitment to upholding the integrity, confidentiality, and privacy of customer data.

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.

Armorblox Architecture



Armorblox Benefits

Comprehensive Email Security

Protect your business against payment fraud, executive impersonation, credential phishing, account takeovers, and other attacks

Data Loss Prevention

Stay compliant by stopping accidental or malicious disclosure of PII, PCI, and passwords over email

Accelerated Incident Response

Reduce SOC burden with automatic remediation for inbound email threats as well as one-click remediation for abuse mailbox emails

Resource-Light Management

Avoid resource strain with a security solution that's easy to deploy, manage, and use

Increased Analyst Productivity

Reduce investigation time with clearly explained insights and analysis for even the most targeted email attacks

Compounding ROI

Get smarter every second with Armorblox ML models that learn from each email and manual action

An Inbox That Loves Armorblox

CITY OF SAN JOSE
CAPITAL OF SILICON VALLEY

"Cities and counties have seen a startling increase in business email compromise and impersonation attacks. In deploying Armorblox, we have a tool that helps detect and prevent those attacks smartly— it is highly effective and does not interrupt the flow of City business. Armorblox is the type of high-value tool that makes a true difference as these risks continue to grow."

Rob Lloyd - CIO, City of San Jose

Armorblox

Armorblox is a cloud-native and content-aware email security platform that protects against targeted attacks such as business email compromise, account takeover, and executive impersonation. Organizations use Armorblox to deploy pre-configured policies that block suspicious emails, automate abuse mailbox remediation, and prevent outbound data loss.

(408) 475 - 8713 armorblox.com 19200 Stevens Creek Blvd. Suite 100 Cupertino, CA 95014