Armorblox

DATASHEET

Language-Powered Cloud Office Security

SUMMARY

Stop socially engineered attacks

Prevent outbound data loss across cloud office environments

Automate abuse mailbox remediation

INTEGRATIONS

Office 365

Microsoft Exchange

G Suite

Slack

Microsoft Teams

Box

USE CASES

Inbound Email Protection

Payroll Fraud

Account Takeover

Vendor Invoice Fraud

Advanced Credential Phishing

VIP/Employee Impersonation

Outbound Email DLP

PII/PCI Compliance

Confidential Content Protection

Lateral Data Loss Prevention

Messaging and File-Sharing Protection

Advanced Credential Phishing

PII/PCI Compliance

Lateral Data Loss Prevention

CONTACT US

+1 408 475 8713

info@armorblox.com

https://www.armorblox.com

The Human Layer Challenge

In a world dominated by remote work and digital workflows, humans don't communicate in silos, whether they're in office or at home. Over 70% of all enterprise data is textual and spans email, messaging, and file-sharing channels. This communication sprawl has led to new avenues for targeted attacks and data loss.

Targeted Email Attacks

Email attacks today are laser focused and evade traditional detection by targeting human nature. Moving beyond mass-phishing and malicious payloads, attackers are now researching their targets before sending socially engineered emails. Attackers impersonate trusted parties or take over legitimate email accounts to induce actions that cause financial and data loss. Over $26 billion has been lost to business email compromise (BEC) attacks over the last three years according to the FBI.

Direct and Lateral Data Loss

The desire for speed and productivity usually comes at the expense of data privacy and compliance. Whether inadvertently or maliciously, employees share PII, PCI, passwords, and confidential data - either with outside parties or laterally across email, messaging, and file-sharing services.

Armorblox Overview

Armorblox brings understanding to security to protect the most attacked layer in enterprises today: the human layer.

Armorblox is a cloud office security platform that stops targeted attacks and data loss across email, messaging, and file-sharing services using natural language understanding. The Armorblox detection engine analyzes identity, behavior, and language across all enterprise communications to protect people and data where siloed solutions fall short. Organizations use preconfigured Armorblox policies to stop socially engineered attacks, automate abuse mailbox remediation, and prevent outbound and lateral data loss.

Language-Powered Cloud Office Security

Armorblox Product Capabilities

Inbound Email Protection

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

Outbound Email DLP

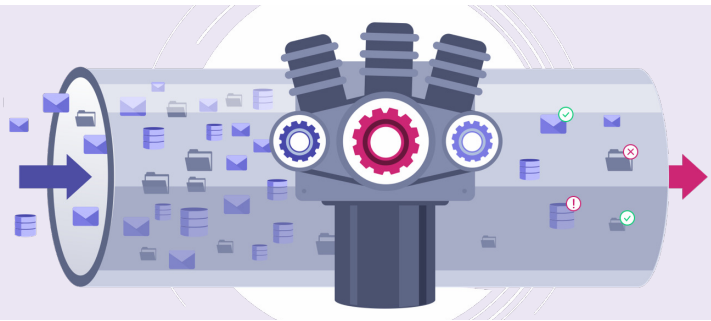
- Detect accidental or malicious data loss over email such as SSNs, bank account details, and account passwords.
- Study detailed email-specific analysis that draws insights from identity, behavior, and language signals.
- Deploy policy actions that automatically block emails containing sensitive data from leaving the organization.
- Prevent lateral data leaks across email, messaging, and file-sharing services.

Abuse Mailbox Remediation

- Connect Armorblox with enterprise 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.

Messaging and File-Sharing Protection

- Detect accidental or malicious sensitive (PII/PCI) data loss over messaging and file-sharing applications.
- Stop malicious URLs and attachments from being shared over messaging and file-sharing applications.
- Prevent lateral data leaks across email, messaging, and file-sharing services.
- Study detailed threat-specific analysis that draws insights from identity, behavior, and language signals.
- Leverage pre-configured policy actions that warn users, delete malicious messages or files, and block data leaks.



Armorblox Detection Engine

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

Language-Powered Cloud Office Security

Armorblox Platform Features

Ease of Deployment

The Armorblox platform is cloud-native and integrates 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, Exchange, Box, and Slack, offering comprehensive threat detection and data loss prevention. Integrations with SIEM and SOAR solutions over RESTful APIs gets threats detected by Armorblox to any preferred source of alert aggregation.

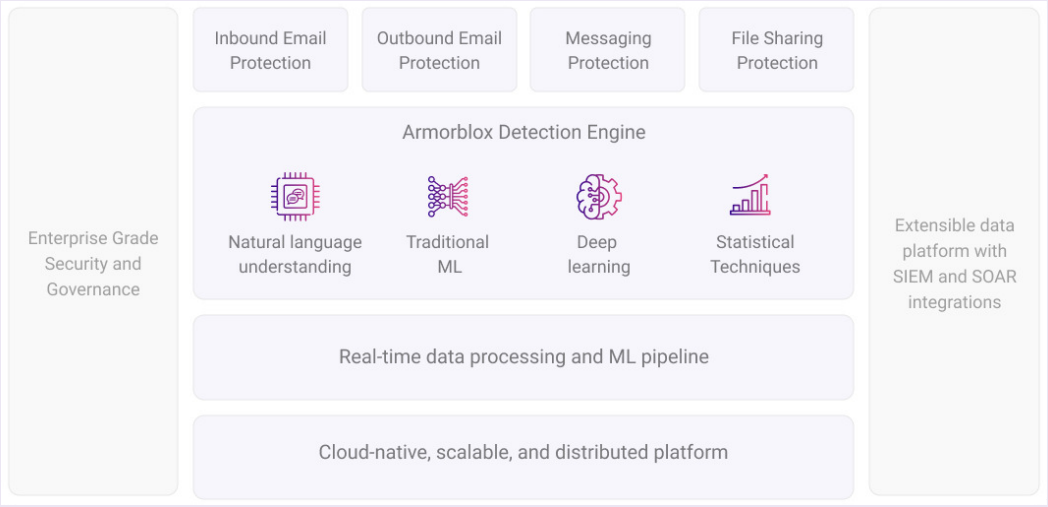
Enterprise Grade

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 2 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



Language-Powered Cloud Office Security

Armorblox Benefits

Complete Cloud Office Security

Protect your business against targeted attacks and data loss across email, messaging, and file-sharing services

Accurate Data Loss Exposure

Track accidental and malicious disclosure of sensitive PII/PCI data across cloud office applications

Accelerated Incident Response

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

Simplified Security Stack

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 attacks

Compounding ROI

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

Inboxes that love 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

Gartner COOL VENDOR 2020

Armorblox is a language-powered cloud office security platform that stops targeted attacks and data loss across email, messaging, and file-sharing services. Armorblox leverages natural language understanding and deep learning to analyze identity, behavior, and language on all enterprise communications. Armorblox integrates seamlessly over APIs without the need for MX record modifications or email rerouting. Organizations use pre-configured Armorblox policies to stop targeted attacks, automate abuse mailbox remediation, and prevent outbound and lateral data loss. Armorblox was featured in the 2019 Forbes AI 50 list and was named a 2020 Gartner Cool Vendor in Cloud Office Security. Founded in 2017, Armorblox is headquartered in Cupertino, CA and backed by General Catalyst.