Armorblox + Exchange

SOLUTION BRIEF

Stop targeted attacks and data loss on Exchange

SUMMARY

Stop targeted attacks such as BEC, phishing, and vendor fraud

Automate remediation of threats forwarded to abuse mailbox

Stop sensitive data disclosures (PII, PCI, passwords) over email

Protect confidential content on email

Prevent lateral data loss across email, messaging, and file-sharing

COMPATIBILITY

Exchange

DEPLOYMENT

The Armorblox Exchange Connector can be installed on-premise and connect into the Armorblox cloud

CONTACT US

+1 408 475 8713

info@armorblox.com

https://www.armorblox.com

Although email delivery is rapidly moving towards the cloud, 65% of organizations still utilize on-premise email, at least to some extent. In addition to organizations that are entirely on-premise, many organizations also end up deploying Microsoft Exchange in hybrid mode: hosting the Active Directory (AD) on the cloud but still hosting Exchange servers on-premise. Many modern cloud-delivered email security vendors fail to support such complex email deployments. If organizations just invest in Secure Email Gateways (SEG), they leave the door open for both targeted attacks and data loss.

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.

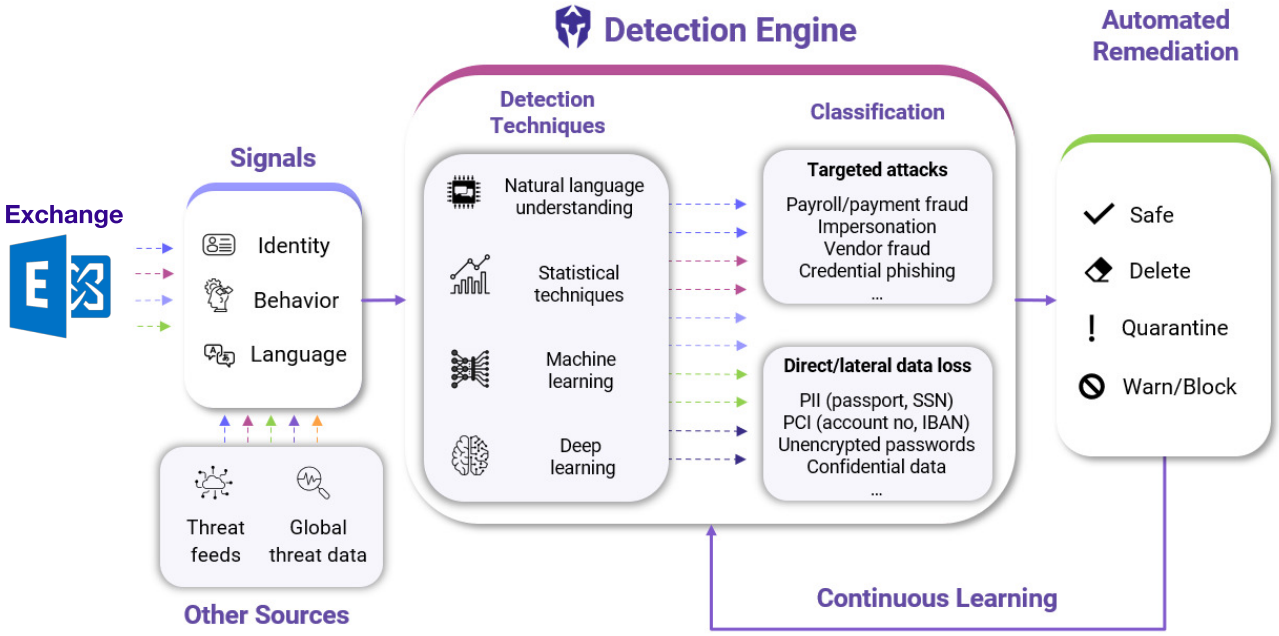
On the outbound front, the sprawl of communication applications has paved the way for direct and lateral data loss. Employees share sensitive PII/PCI information with noncompliant recipients, either within or across communication channels. Since the security solutions analyzing each environment are siloed, organizations lack a unified layer of context to protect their communications.

Armorblox for Exchange

Armorblox is a cloud office security platform that protects enterprise communications across email, messaging, and file-sharing services using natural language understanding. The platform connects with Exchange over APIs using an on-premise Connector to analyze thousands of signals across identity, behavior, and language. Organizations can use pre-configured Armorblox policies to stop targeted email attacks, protect against direct and lateral data loss, and automate remediation of threats reported to the phishing/abuse mailbox.

SOLUTION BRIEF

Stop targeted attacks and data loss on Exchange



Integration Features

- Stop targeted attacks such as business email compromise, payroll fraud, executive impersonation, and credential phishing.
- Connect Armorblox with your enterprise phishing/abuse mailbox for centralized detection and automated remediation.
- Auto-remediate false positives to focus on threats that need human review.
- Remove similar suspicious emails across user mailboxes with one click.
- Detect accidental or malicious data loss over emails such as SSNs, bank account details, and account passwords.
- Prevent lateral data leaks across email, messaging, and file-sharing services.
- Study email-specific analysis that draws insights from identity, behavior, and language signals.
- Leverage preconfigured policy actions to automatically delete or quarantine suspicious emails, warn users of noncompliant actions, and block sensitive data from being accessed by noncompliant recipients.
- Send Armorblox detected email incidents to downstream SIEM and SOAR solutions over APIs.

Gartner COOL VENDOR 2020

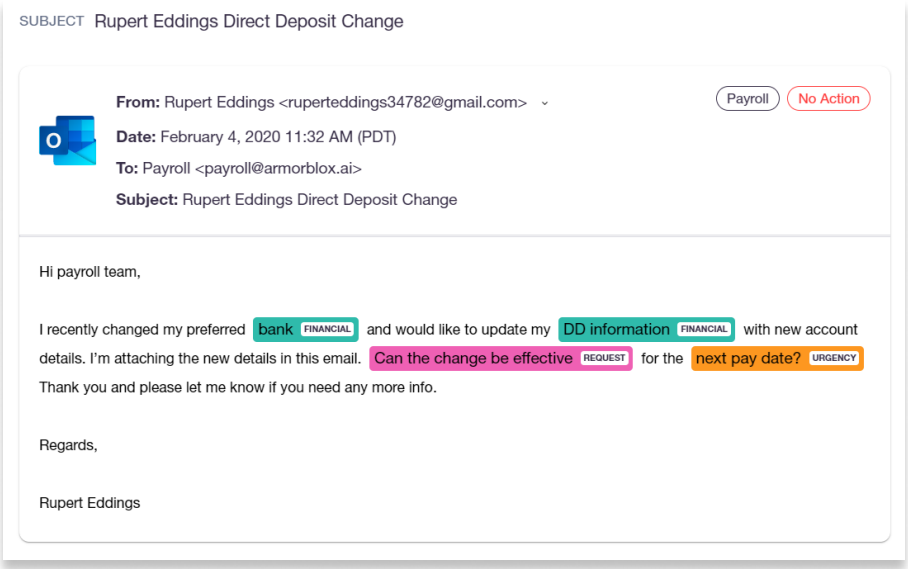
Armorblox is a language-powered cloud office security platform that stops targeted attacks and data loss across email, messaging, and file-sharing services. Armorblox leverages natural language understanding and deep learning to analyze identity, behavior, and language on all enterprise communications. 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.

Stop targeted attacks and data loss on Exchange

Use Case 1: Stop Business Email Compromise

Problem

Business email compromise (BEC) attacks are laser focused and get past traditional detection by targeting human nature. These emails usually forego malicious links and attachments, instead opting for manipulating the target through impersonation tactics and social engineering. Traditional Microsoft email security controls as well as Secure Email Gateways (SEG) lack the context to catch these payloadless attacks.



Solution

Armorblox augments native Microsoft email security capabilities to provide the widest non-overlapping breadth of attack protection. Armorblox analyzes all emails to build baselines around identity, behavior, and language for every organization. The platform detects a broad spectrum of BEC attacks and classifies them into granular attack categories. Security teams can set predefined actions that automatically delete or quarantine malicious emails, revoke user access to compromised accounts, and warn end users of potentially suspicious emails.

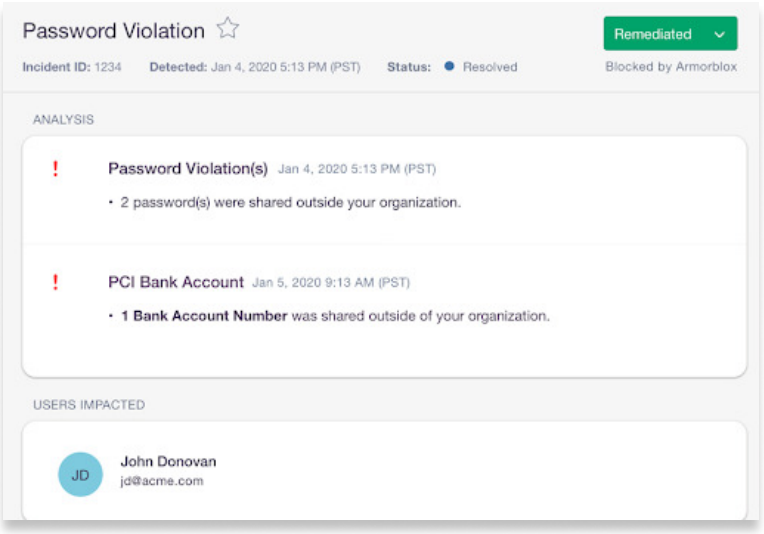
Benefit

Armorblox stops hitherto undetected business email compromise attacks, helping organizations avoid financial loss and reputational damage. Accurate classification and detection highlights within each email threat provides security teams with relevant context for investigation. Automated and customizable remediation actions (deleting, quarantining, revoking access) help security teams assign response steps according to the severity of the violation, safeguarding people and data without sacrificing organizational productivity.

Use Case 2: Prevent Accidental PII/PCI Disclosure Over Email

Problem

The rapid-fire and distributed nature of email often brings data protection and compliance into question. With the aim of speeding up business processes, employees accidentally share sensitive information such as SSNs, bank account details, and passport numbers over email. With stringent fines being imposed for accidental data loss under GDPR and CCPA, compliance is not optional any more.



Solution

The Armorblox platform detects any instance of PII/PCI information being shared on email. Based on preconfigured policies and user-defined inputs, Armorblox has a universal understanding of what constitutes sensitive and confidential data. This enables Armorblox to detect and prevent data loss within and across cloud office applications such as email, messaging, and file-sharing services. Security teams can set predefined actions that warn users of noncompliant actions and block confidential/sensitive data from being shared with unauthorized parties.

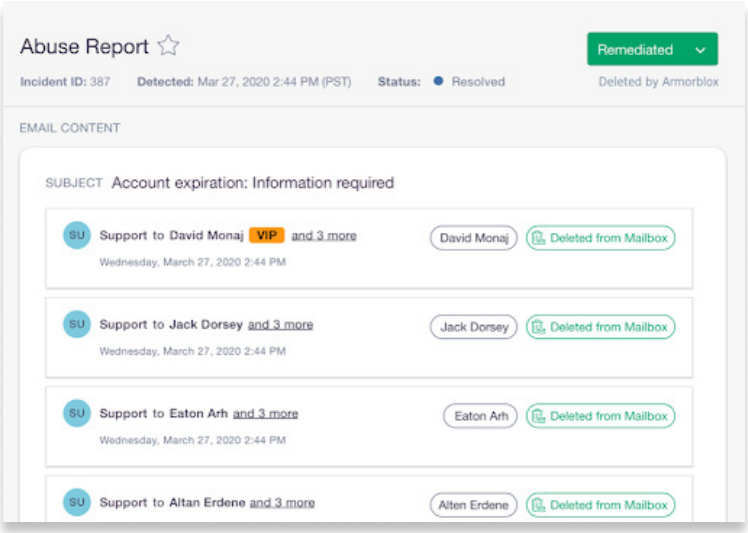
Benefit

Armorblox helps security teams gain control over the hitherto distributed nature of sensitive data residing in email. Detecting every sensitive PII/PCI disclosure enables security leaders to accurately measure risk exposure. Customizable actions (warning, blocking) help security teams assign response steps according to the severity of the violation, safeguarding people and data without sacrificing organizational productivity.

Use Case 3: Automate Abuse Mailbox Remediation

Problem

Large organizations are subject to daily attack campaigns across users, resulting in abuse mailboxes bursting at the seams. Phishing awareness training has helped but sometimes overcorrects the problem, with employees now forwarding safe emails to abuse mailboxes en masse. Security teams struggle with this high email volume, wasting time on false positives and lacking both the context and time to investigate targeted attacks.



Solution

Armoblox can be connected to your enterprise phishing/abuse mailbox for automated remediation of known threats and simplified investigation of unknown threats. Every reported email is analyzed by the Armorblox detection engine, with remediation actions being applied across affected user mailboxes. Manual actions by the security team (eg. mark safe, delete) are also applied across affected user mailboxes. Armorblox ML models learn from every manual action, creating dynamic policies that protect against similar future threats.

Benefit

Armorblox helps security teams avoid the alert fatigue that usually comes from instituting phishing reporting mailboxes. Predefined and automated response actions ensure compliance while also minimizing manual, repetitive work. Customizable actions (marking safe, deleting, quarantining) help security teams assign response steps according to the severity of the violation, safeguarding people and data without sacrificing organizational productivity.