Armorblox + box

SOLUTION BRIEF

Stop phishing and data loss on Box

SUMMARY

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

Protect confidential content on Box

Prevent lateral data loss across Box, email, and messaging services

Detect malicious URLs and attachments on Box

COMPATIBILITY

Box

Box Shield

DEPLOYMENT

Connect over APIs

CONTACT US

+1 408 475 8713

info@armorblox.com

https://www.armorblox.com

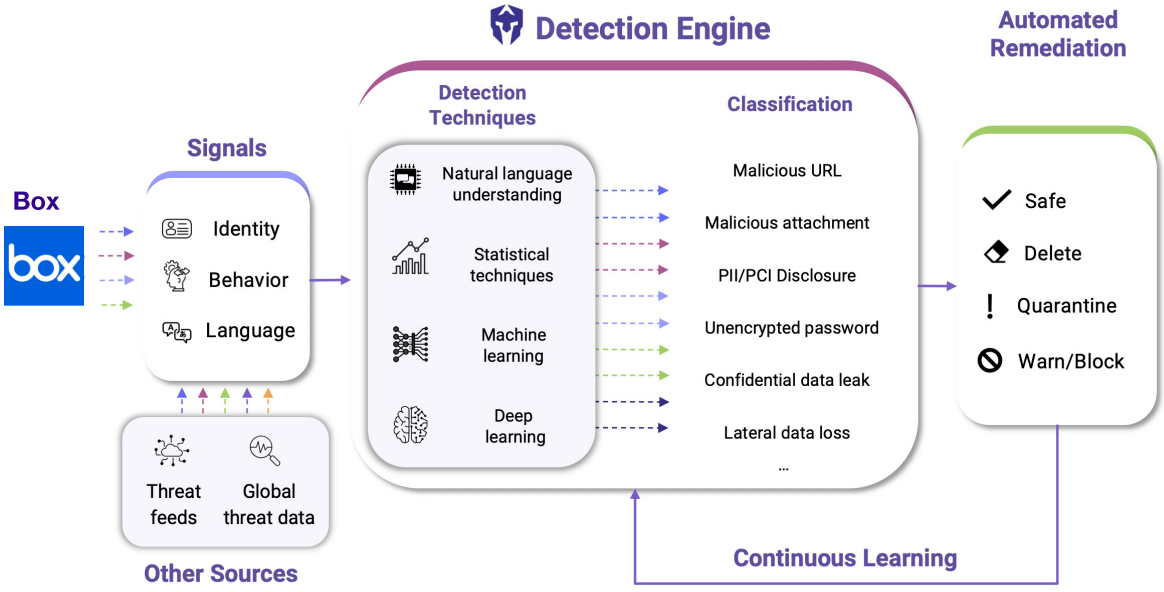
Communications are the lifeblood of any organization. But in a world dominated by remote work and digital workflows, humans don't communicate in silos, whether they're in office or at home. Email might be the true system of business record, but it's supported - and in some cases, supplanted - by file-sharing applications such as Box. While this cross-channel communication and collaboration has done wonders for organizational agility, it has also paved the way for targeted attacks and data loss.

The widespread adoption (and misuse) of cloud-hosted files have caused gaps in data visibility and security. Attackers can get hold of an employee's Box credentials and host malicious URLs or malware on enterprise Box accounts to infect high-value targets such as customers and third-party vendors. Whether accidentally or maliciously, employees can share sensitive PII/PCI information over cloud-hosted documents with noncompliant recipients. With these lapses being stringently penalized under regulations such as GDPR and CCPA, organizations need to safeguard compliance by investing in both native and third-party security controls for file-sharing applications.

While Box Shield effectively secures your Box environment, lateral data loss over applications like email and messaging is prevalent. Since the security solutions analyzing each environment are siloed, organizations lack a unified layer of context to protect their communications. Box customers can augment native Box capabilities with Armorblox for complete protection against targeted attacks and data loss across cloud office applications.

Armorblox for Box

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 Box over APIs to analyze thousands of signals across identity, behavior, and language. Organizations can use pre-configured Armorblox policies to stop malicious URLs and attachments, prevent PII/PCI disclosures, and protect against lateral data loss across cloud applications..



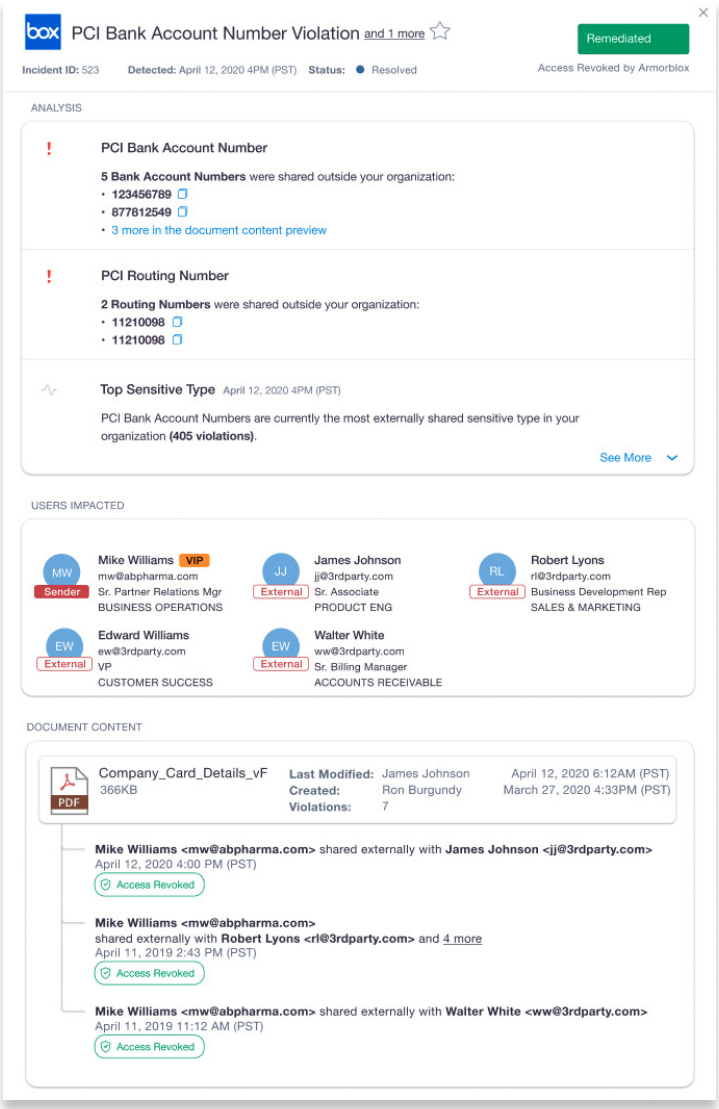
Integration Features

- Detect and delete malicious zero-day URLs and malware shared over Box or stored on Box.
- Detect accidental or malicious data loss over Box files such as SSNs, bank account details, and unencrypted passwords.
- Prevent lateral data leaks across Box, email, and messaging services.
- Study detailed message-specific analysis that draws insights from identity, behavior, and language signals.
- Leverage preconfigured policy actions to automatically warn users of noncompliant actions, delete malicious Box files, and block data leaks.
- Send Armorblox detected Box 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.

Use Case 1: Stop Phishing Attacks Hosted On Box



Problem

The decentralized nature of cloud-hosted files often brings data protection and compliance into question, especially if an employee's Box credentials are compromised. Attackers can host malicious URLs or malware on enterprise Box accounts to attack high-value targets such as customers and third-party vendors. In case these are zero-day attacks, the payload can reach thousands of targets before someone reports it and gets it taken down.

Solution

Armorblox analyzes all unstructured Box files to build baselines around identity, behavior, and language for every organization. Armorblox also leverages threat feed data and global insights from its cross-organizational ML model. These thousands of signals enable the platform to detect zero-day links hosted on or shared over Box files, including links with multiple redirects and lookalike pages. Security teams can set predefined actions that automatically delete or quarantine malicious Box files.

Benefit

Armorblox safeguards your organization's reputation by stopping these attacks before adversaries weaponize public cloud-hosted files to compromise vendors, suppliers, and clients. Detecting every malicious URL enables security leaders to accurately measure and contain risk exposure. Customizable actions (quarantining, deleting) help security teams assign response steps according to the severity of the violation, safeguarding people and data without sacrificing organizational productivity.

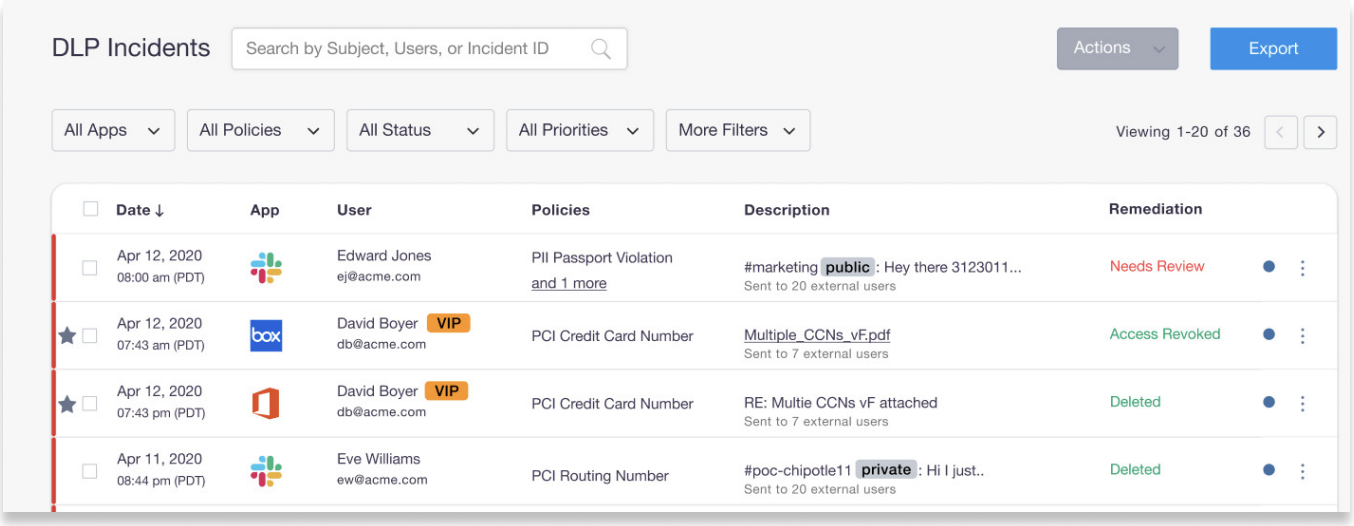
Use Case 2: Prevent Lateral Data Loss Across Box and Email

Problem

The disparate and siloed nature of DLP solutions has made it tougher for security teams to gain visibility over sensitive data, whether at rest or in transit. Since there's no universal context identifying data as sensitive across applications, an employee can easily download sensitive data from Box and share it with noncompliant recipients over email.

Solution

Armoblox connects with email, messaging, and file-sharing services over APIs to build contextual baselines that run across applications. Based on preconfigured policies and user-defined inputs, the Armorblox platform has a universal understanding of what constitutes sensitive and confidential data. Organizations 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 avoid the swivel-chair fatigue that comes from piecing together context across multiple security solutions. Predefined and automated response actions ensure compliance while also minimizing manual, repetitive work. Customizable actions (warning, blocking, deleting) help security teams assign response steps according to the severity of the violation, safeguarding people and data without sacrificing organizational productivity.