WHITEPAPER

Supercharge your Microsoft Email Protection with Armorblox
Contents

Armorblox is Built to Augment Microsoft Security

Armorblox Stops Targeted Attacks that Slip Past Microsoft Native Email Security

Armorblox Enables Proactive Threat Investigation for Security Operations Teams

Armorblox Saves Time for Security Teams with Automated Threat Remediation

Armorblox Integrates with Microsoft Azure Sentinel

Armorblox Prevents Accidental or Malicious Data Exposure

Armorblox Connects with Microsoft Exchange

Armorblox is Available on Azure Marketplace

Armorblox is a Proud Member of Microsoft Intelligent Security Association

Customers Trust Armorblox to Complement Microsoft Office 365
Armorblox is Built to Augment Native Microsoft Security

Armorblox helps 58,000+ organizations stop business email compromise and targeted phishing attacks, protect sensitive PII, PCI, and PHI, and automate the remediation of user-reported email threats. Armorblox connects over APIs without needing any MX record changes, and analyzes emails after Exchange Online Protection and Microsoft Defender. Using Natural Language Understanding, Armorblox analyzes thousands of signals across user identities, user behavior, and language in emails to stop targeted email attacks, protect against direct and lateral data loss, and automate security response.

Armorblox is built to learn from every customer’s data to stop advanced threats that cannot be caught by filters, blocklists, and other binary detection techniques. Custom ML models are built for every organization to provide better detections; trained across organization and user-specific communication patterns, known vendor associations, and common business workflows like receiving invoices or payment requests. It is because of this that Armorblox extends past both Microsoft Exchange Online Protection and Defender plans, complementing Microsoft’s capabilities for threat prevention, investigation, and response.

---

**Armorblox Advanced Threat Prevention**

- Advanced Phishing
- Financial Fraud
- Wire Fraud
- Payroll Fraud
- Payment Fraud/Invoice Fraud
- Socially Engineered Attacks
- Supplier/Vendor Attacks
- Malicious Internal User
- Brand Impersonation
- VIP Impersonation

**EOP License**

- Anti-Spam
- Anti-Malware

**ATP License**

- Anti-Phishing
- Link/Attachment checks

---

Spam + Malware

- Phishing

**Targeted Email Attacks**

- Breadth of Email Attacks
Armorblox Stops Targeted Attacks that Slip Past Microsoft Native Email Security

Microsoft security controls are effective at stopping spam, known malware, and phishing—so effective that organizations are discontinuing their investments in Secure Email Gateways (SEGs). However, many targeted email attacks like business email compromise and spear phishing still get past Microsoft security controls.

### Armorblox Complements Microsoft Email Security for Threat Prevention

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>Exchange Online Protection</th>
<th>Defender Plan 1</th>
<th>Armorblox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-spam, anti-malware, mass email attacks</td>
<td>✓</td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Impersonation detection</td>
<td>✓</td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Admin quarantine / false positive, negative submission</td>
<td>✓</td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Allow / block for URLs and files</td>
<td>✓</td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Anti-phishing</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Safe attachments and safe links</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Time-of-click protection in email, office clients, teams</td>
<td>✓</td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>User and domain impersonation protection</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Alerts and SIEM integration</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Targeted spear phishing attacks</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Dynamic malware scanning</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Vendor fraud and third-party risk protection</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Payment fraud</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Payroll fraud</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Invoice fraud</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Image analysis within emails</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
<tr>
<td>Dynamic selective URL rewriting</td>
<td></td>
<td></td>
<td>✓+</td>
</tr>
</tbody>
</table>

Armorblox complements Microsoft EOP with protection against a wide range of targeted email attacks that bypass Microsoft security layers. Armorblox provides capabilities that exist in MSDD Plan 1, for organizations that wish to extend EOP without purchasing this plan.

---

**Targeted Spear Phishing Attacks**

Armorblox understands the content and context of email communications necessary to stop sophisticated and targeted email attacks, such as spear phishing attacks. These threats are specific, tailored to the victim, and can easily slip past native email security controls that do not use language or behavior as a signal.

**Dynamic Malware Scanning**

Armorblox provides static and dynamic analysis of attachments for malware and advanced persistent threats, without interrupting business email workflows. Identified attachments that need further analysis are isolated within Armorblox cloud sandbox; expediting remediation through AI-based analysis by targeting only suspicious attachments. Multi-layered scanning technology of attachment signatures enables quick identification of malicious and zero-day links, as well as potential vendor fraud attempts.

---

Copyright © 2023 Armorblox Inc. All rights reserved.
Vendor Fraud and Third-Party Risk Protection

Armorblox analyzes historical emails and automatically identifies the vendors and third-parties conducting business within your organization. Armorblox continuously monitors and assesses the risk of each vendor based on communication patterns to identify whether communications from a vendor are safe or compromised, protecting organizations from the loss of money or sensitive credentials. Armorblox detects vendor accounts that have been compromised and prevents your organization from engaging with these malicious actors, protecting organizations from vendor fraud attempts such as invoice fraud, look alike domains, and hijacking payment-related email threads.

Payment Fraud

Armorblox stops emails impersonating external entities in attempts to defraud organizations (fraudulent invoices, fake routing numbers, or bank accounts), through custom models trained specifically around identifying potentially compromised financial communication workflows. According to a recent FBI IC3 report, targeted BEC attacks led to more than $43B in exposed business loss. Armorblox helps organizations protect themselves against these attacks by using machine learning techniques to detect malicious emails that target financial business workflows.

Payroll Fraud

Armorblox understands the content and context of email communications to protect against fraudulent financial transactions. This protects customers from targeted email attacks impersonating employees in order to steal money or initiate payroll-related change requests.

Dynamic Selective URL Rewriting

Microsoft and legacy SEG vendors rewrite all URLs in emails. This means that for an end user to know if a link is safe they must click into the URL, which encourages the opposite behavior that security teams desire. Armorblox follows a very different approach – only malicious URLs are rewritten and safe URLs show up as is. This educates end users in exercising caution whenever they see a rewritten URL, and to easily know that URLs not rewritten by Armorblox are safe to click. If an end user clicks on a rewritten URL, Armorblox can track click statistics, and prevent that user from being directed to the malicious page. This provides additional analytics for further user security awareness and training.
Armorblox Enables Proactive Threat Investigation for Security Operation Teams

Security teams can save time and better protect end users across the organization with Armorblox product capabilities that enable proactive threat investigation. Armorblox complements Microsoft email security with greater precision and integrated insights, leading to a reduction in false positives and time to respond for threats that need human review.

Armorblox Complements Microsoft Email Security for Threat Investigation

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>Exchange Online Protection</th>
<th>Defender Plan 1</th>
<th>Defender Plan 2</th>
<th>Armorblox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit log search</td>
<td>✓</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Search by email</td>
<td>✓</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Search by email sender, tag, incident number</td>
<td>✓</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Message trace</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEM integration for detections</td>
<td>✓</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Real-time threat detections</td>
<td>✓</td>
<td></td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>URL trace</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat explorer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat trackers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Campaign views</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account compromise protection</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>User risk profile</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>End user threat engagement</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Armorblox complements Microsoft EOP with proactive threat investigation for security teams. Armorblox provides capabilities that exist in MSDO Plans 1 and 2, for organizations that wish to extend EOP without purchasing these plans.

Account Compromise Protection

Armorblox helps organizations prevent account compromise by analyzing a broad array of signals such as sign-in logs, risk alerts, security alerts, IP addresses, and account configurations, to determine if a particular account access or behavior was legitimate or not. Account compromise signals are then presented in a timeline view so analysts can see the sequence of events with detail, before determining if an account can be unlocked and returned to normal status.

This provides security teams a comprehensive view of account compromise attempts before, during, and after an EAC attack. Armorblox has preconfigured categories, automatically identified, with the ability to apply automated remediation actions to compromised accounts or suspicious user activity at the touch of a button. Some of the signal categories Armorblox identifies are:

- Unusual mail forwarding rule detection - Quickly detect and remove unusual mail forwarding rules set up by attackers or malicious insiders.
Anomalous login detection – Armorblox reduces false positive rates through improved detection and alerts on anomalous logins into user accounts.

Impossible travel detection – Detailed alerts and increased precision from Armorblox allows security teams to take quick action on accounts with simultaneous logins from geographically disparate locations.

Detection of unusual password reset requests – Armorblox goes beyond Microsoft capabilities to monitor and detect unusual password reset requests via email.

Detection of user logins from atypical devices – Monitor and detect logins from new devices with better precision and identify logins from atypical devices to improve security posture.

Credential phishing protection – Microsoft relies predominantly on threat feeds that flag known bad links, so recently registered domains and recently compromised sites hosting bad links slip through the defenses of Microsoft and legacy SEGs. Armorblox complements Microsoft’s capabilities by providing accurate credential phishing protection. Armorblox decodes rewritten URLs and follows all redirects to the destination page. Pages are analyzed by custom vision models to detect brand impersonation attempts (Microsoft, Google, DocuSign, Okta, Adobe, Zoom), and these URLs are defanged to prevent credential phishing attempts.

User Risk Profile

See which users within your organization are most at risk, based on continuous monitoring and attack trends automatically curated, updated, and maintained by Armorblox. This gives you insights into which users need more protection and tailor auto-remediation actions or security trainings accordingly.

End User Threat Engagement

Be notified in real time even if a user engages with an email from a threat actor that was deleted or quarantined. Track these reply and forward actions to provide targeted training for employees.
Armorblox Saves Time for Security Teams with Automated Threat Remediation

Armorblox helps security teams avoid the alert fatigue that usually comes from threat review and remediation. With predefined and automated response actions for user-reported threats, Armorblox enables continued compliance while minimizing manual, repetitive work. Armorblox increases end-user education and awareness of malicious threats, through contextual warning banners that clearly state why a remediation action was applied.

Armorblox Complements Microsoft Email Security for Threat Remediation

<table>
<thead>
<tr>
<th>CAPABILITIES</th>
<th>Exchange Online Protection</th>
<th>Defender Plan 2</th>
<th>Armorblox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero-hour auto purge (ZAP)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Refinement and testing of allow and block lists</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Automated Investigation and Response (AIR)</td>
<td>✓</td>
<td>✓</td>
<td>✓⁺</td>
</tr>
<tr>
<td>AIR from threat explorer</td>
<td></td>
<td></td>
<td>✓⁺</td>
</tr>
<tr>
<td>SIEM integration for automated investigations</td>
<td>✓</td>
<td></td>
<td>✓⁺</td>
</tr>
<tr>
<td>Abuse mailbox remediation</td>
<td></td>
<td></td>
<td>✓⁺</td>
</tr>
<tr>
<td>M-SOAR</td>
<td></td>
<td></td>
<td>✓⁺</td>
</tr>
<tr>
<td>Contextual warning banners</td>
<td></td>
<td></td>
<td>✓⁺</td>
</tr>
<tr>
<td>Automated scheduled reports</td>
<td></td>
<td></td>
<td>✓⁺</td>
</tr>
<tr>
<td>Safe email detection in spam</td>
<td></td>
<td></td>
<td>✓⁺</td>
</tr>
</tbody>
</table>

+ Armorblox complements Microsoft EOP with automated threat remediation for a wide range of targeted email attacks that bypass Microsoft security layers. Armorblox provides capabilities that exist in M365 Plan 2, for organizations that wish to extend EOP without purchasing this plan.

Abuse Mailbox Remediation

Extending beyond Microsoft’s capabilities, Armorblox analyzes every user-reported email to remediate known threats, isolate false positives, and escalate more sophisticated email threats to the security team. Armorblox protects end users from similar emails within a campaign by automatically identifying and applying remediation actions across all user inboxes, without the need for human intervention. Armorblox learns from every manual action taken to automatically remediate future threats with custom models built for every organization to automatically block emails from attackers.

M-SOAR

Armorblox automated remediation capabilities provide simplified email security automation and response (M-SOAR) of incidents. Customizable actions (marking safe, deleting, quarantining) help security teams assign response steps according to the severity of the violation.
**Contextual Warning Banners**

Microsoft allows organizations to set up EXTERNAL tags for external emails coming into the organization. Users very quickly learn to ignore these, leaving them susceptible to impersonation emails and other targeted attacks. The warning banners that Microsoft and other legacy providers insert are generic and exclude context about the attack that end users find useful. Unlike legacy options, Armorblox can be configured to add contextual warning banners within suspicious emails, specifically calling out why an email is malicious with easy to read tags such as Invoice Fraud or Executive Impersonation. This educates end users with real examples on why a particular email was quarantined or deleted, and increases awareness on how to detect suspicious emails in the future – improving the organization’s security posture.

**Automated Scheduled Reports**

Schedule the automated email delivery of detailed reports, and analyze targeted attack trends for threats that bypassed your organization’s native security tools and were stopped by Armorblox.

**Safe Email Detection in Spam**

Easily review and undo errors made by Microsoft, such as incorrectly labeling safe emails as spam. User-specific and organizational behavior models undo damage done by email provider spam filters that trap genuine internal emails and disrupt business workflows. With Armorblox, security teams improve overall email hygiene with the ability to easily move emails misclassified as spam by Microsoft back into end users’ inboxes.

“We are always looking to complement the security technologies that we have in order to make them better. That’s why we selected Armorblox because it integrated so well with our existing Microsoft technology. Armorblox helps us contextualize the messages and helps us better see what types of issues are going to be cropping up with our employees.”

**BRIAN WILSON**

CISO, SAS
Armorblox Integrates with Microsoft Azure Sentinel

As a partner of Microsoft Intelligent Security Association (MISA), Armorblox has integrated its platform with Microsoft Azure Sentinel. Customers can save time on security operations by routing threats detected by Armorblox to Azure Sentinel environment and reduce mean time to respond to threats. The Microsoft validated solution drives the following efficiencies and benefits to Security Operations teams.

- Improve threat detection, investigation, and response across endpoints, network applications, and business communications
- Automate away 75-97% of manual work associated with user-reported phishing emails without creating any rules; remove malicious emails across mailboxes with one click
- Apply forward-looking remediation actions that automatically protect against similar attacks in the future, focusing on reported emails that need human review

Armorblox NLU powered Threat Prevention feeds threat intel including:
- Financial fraud
- Payment fraud
- Targeted phishing attacks
- Wire fraud
- Socially engineered attacks
- Sophisticated vendor/supply chain attacks

Microsoft 365 feeds threat intel including:
- Spam emails
- Basic phishing attacks
- Impersonation attacks
- DKIM and other protocol check violations
- Malware checks

Benefits of Armorblox/MS-Sentinel integration:
- Share email threat intel with SecOps
- Create playbooks to take remediation actions on emails (delete, quarantine, hard delete)
- Improve threat hunting and investigation with additional intel
- Reduce mean time to resolution on attacks that span multiple infrastructure (email, endpoint, apps, etc.)

Copyright © 2023 Armorblox Inc. All rights reserved.
**Armorblox Prevents Accidental or Malicious Data Exposure**

Armorblox is built to learn from every customer’s data and prevent data leakage that cannot be caught by filters, blocklists, and other binary detection techniques. The biggest challenge with Microsoft Office 365 email data loss prevention is the large number of false positive alerts, diminishing the ability to block or encrypt all non-compliant emails.

Armorblox helps security teams gain control over the hitherto distributed nature of sensitive data residing in email. Detecting every sensitive PII, PCI, PHI disclosure, Armorblox enables security leaders to accurately measure risk exposure, while reducing false positives for DLP-related alerts by 10x. Based on preconfigured policies and user-defined inputs, Armorblox immediately detects and prevents data loss within and across cloud office applications such as email, messaging, and file-sharing services. Customizable actions (block, encrypt, delete) help security teams assign automated response steps according to the severity of the violation, safeguarding people and data without sacrificing organizational productivity.
Armorblox Complements Microsoft Purview for Precise Data Protection

---

**CAPABILITIES**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Microsoft Azure Purview</th>
<th>Armorblox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect PII / PCI / PHI data loss over email</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Support for custom regexes</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Support for custom identifiers</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Automatic encryption of sensitive data within emails</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Support for policy creation with custom identifiers</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Auto-policy generator based on machine learning</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>DLP detections integrated across business workflows</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Protect organization-specific sensitive PII / PCI / PHI data</td>
<td>✓</td>
<td>✓+</td>
</tr>
</tbody>
</table>

* Armorblox complements Microsoft Purview and extends beyond its capabilities with increased precision for email data loss prevention.

---

**Protect Organization–Specific Sensitive PII / PCI / PHI Data**

Armorblox helps security teams gain control over the distributed nature of sensitive data residing in email – with better precision and automated remediation actions (block, encrypt, delete), protection across all types of organization-specific data is attainable. Armorblox language models automatically support PII, PCI, and PHI policies and custom identifiers to reduce false positive rates, often seen with Microsoft solutions, by 10x. Accurately detecting sensitive data disclosures enables security leaders to measure risk exposure, safeguarding people and data without sacrificing organizational productivity.

---

**Armorblox Complements Microsoft Purview for Faster Incident Review**

---

**CAPABILITIES**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Microsoft Azure Purview</th>
<th>Armorblox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block / Delete outbound emails</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Reduce false positives on alerts using content analysis</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Automatic DLP policy violation remediation</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>DLP signals integrated within account compromise alerts</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Comprehensive DLP dashboards</td>
<td>✓</td>
<td>✓+</td>
</tr>
<tr>
<td>Sensitive and confidential label detection</td>
<td>✓</td>
<td>✓+</td>
</tr>
</tbody>
</table>

* Armorblox complements Microsoft Purview and extends beyond its capabilities with faster incident review for proactive data loss prevention.

---

**Automatic DLP Policy Violation Remediation**

Remediation actions are automatically taken across DLP incidents (block, encrypt, delete) for proactive data loss prevention. Armorblox combines NLU and custom identifiers to detect and prevent the sharing of sensitive data with unauthorized recipients. DLP admins directly benefit from Armorblox’s precision and accuracy with 10x reduction in false positives and fewer DLP-related alerts that need human review or verification.
DLP Signals Integrated within Account Compromise Alerts

Armorblox provides security teams a comprehensive view of account compromise attempts before, during, and after an EAC attack. This EAC Timeline View includes DLP incident signals, bringing the entire sequence of events for each compromise attempt into a single view for better identification of potential data loss. DLP admins are alerted of potential data loss in real time, with the ability to review each DLP incident within the account compromise view, and see the automated remediation action that Armorblox took to prevent the exfiltration of sensitive data through a compromised account.

Comprehensive DLP Dashboards

Comprehensive dashboards provide DLP admins and security teams the metrics needed for better reporting. Armorblox provides the number of DLP policy violations by data type as well as department, so you can track which type of sensitive data is being sent out the most and by which department. Armorblox also automatically tracks the top non-compliant individuals across the organization, so that specific remediation actions or tailored security training can be applied for these employees.

Sensitive and Confidential Label Detection

Armorblox extends beyond Microsoft with the ability to identify both MIP labels and sensitive and confidential label detection within emails, attachments, and metadata – regardless of email provider or sharing platform. Data labels applied by rules or manually applied by individual users are identified and automatically remediated by Armorblox, with actions such as block, encrypt, or delete to prevent the sharing of sensitive or confidential data. Unlike email providers limited by the ability to only identify sensitive or confidential data labels within their own email solution, Armorblox provides organizations data loss prevention across all file sharing platforms.

“Protecting our users and email systems from social engineering and hacking is critical to protecting our business and also our customers . . . This is Armorblox’s sweet spot.”

Bob Thibodeaux
CISO, DefenseStorm
Armorblox Connects with Microsoft Exchange

Armorblox brings the same set of product features that help with threat prevention, data loss prevention, and security operations irrespective of the deployment option. The Armorblox platform connects with Microsoft Exchange over APIs using an on-premise connector to analyze thousands of signals across identity, behavior, and language.

Organizations can use preconfigured Armorblox policies to stop targeted email attacks, protect against direct and lateral data loss, and automate remediation of threats reported to the phishing or abuse mailbox. This provides customers that have made a business choice to deploy Exchange servers the same capabilities to fight attacks that are targeted and sophisticated. Our support for multiple deployment methods allows customers to plan their migration between on-premise Exchange servers and cloud-based Office 365 solutions.

Armorblox is Available on Azure Marketplace

The Azure Marketplace is an online market for buying and selling cloud solutions certified to run on Azure. The Azure Marketplace helps connect companies seeking innovative, cloud-based solutions with partners like Armorblox who have solutions that are ready to use.

Armorblox is a marketplace transactable and MACC eligible partner of Microsoft. Microsoft Azure Consumption Commitment (MACC), refers to the contractual commitment customers make with Microsoft for specific amounts of Azure spend over time. By deploying Armorblox customers can get credit towards their MACC obligations.

Armorblox is an IP co-sell incentivized and PRACR-enabled ISV vendor. This ensures that both Microsoft and Armorblox go-to-market teams are aligned to serve our joint customers.
Armorblox is a Proud Member of Microsoft Intelligent Security Association

Microsoft Intelligent Security Association (MISA) is a partner program from Microsoft that is established to foster an ecosystem of vendors that can complement Microsoft products to better protect customers. The MISA program is composed of ISV and MSSP vendors that have built integrations with specific Microsoft products. Armorblox is honored to be part of this invitation-only program and reflects the importance we place on protecting our joint customers from sophisticated email threats.

As a member of this program, Armorblox has benefited from access to the APIs, in-depth technical sessions with Microsoft experts, documentation and guidance on best practices to build the product integration. Our solution is validated and certified by this program, as Microsoft and Armorblox are jointly committed to fighting cyberthreats together.

Customers Trust Armorblox to Complement Microsoft Office 365

Armorblox Advanced Threat Prevention complements Microsoft Office 365 to stop targeted attacks that bypass Microsoft security layers, enable proactive threat investigation, and provide automated threat remediation for security teams. Security teams and DLP admins get precise data protection with Armorblox Advanced Data Loss Prevention that complements and extends the capabilities of Microsoft Purview.

The benefit for Microsoft customers goes beyond the sophisticated threat and data loss prevention capabilities Armorblox cloud-delivered platform provides. As a MACC eligible partner, IP co-sell and PRACR-enabled ISV vendor, and MISA member, joint customers benefit from the close alignment of the go-to-market teams and commitment to fighting today’s ever changing cyberthreats.