Armorblox

Email Security Checklist

With the move to cloud-delivered email and evolving adversarial techniques, protecting people and data on email remains a concern for organizations irrespective of industry and size. With 71% of companies now using cloud or hybrid cloud email, enterprise customers are moving away from legacy secure email gateways and now look for augments to built-in email security that are easy to use and take a materially different approach to threat protection.

This checklist is meant as a resource for security leaders responsible for email security operations within their organization. The checklist will help lay a framework for vendor capabilities that security practitioners should seek out in order to achieve the broadest possible threat protection coverage that also aligns with budgetary expectations.

The checklist will have recommended capabilities and tips on:

- **Inbound Email Protection**: Stopping advanced threats like spear phishing, business email compromise, vendor fraud, and socially engineered attacks.

- **Email Account Compromise Protection**: Stopping cybercriminals from taking over your employees' email accounts to launch attacks and exfiltrate sensitive data.

- **Phishing / Abuse Mailbox Remediation:** Simplifying and automating the triage and remediation of user-reported email threats.

- **Outbound Email Protection:** Staying compliant by identifying sensitive or confidential data that falls into wrong hands over email.

- **Detection Controls:** Checking the breadth and depth of detection controls in place to stop the widest possible spectrum of email attacks without duplicating native email security.

- **Remediation Controls:** Achieving a balance between automatable native remediation controls for high-quantity or known threats, and customizable remediation controls with manual overrides for advanced threats.

- **Architecture and Enterprise Capabilities:** Meeting prerequisites related to deployment, privacy, security, and aspects that are critical for enterprise-grade security solutions.

Inbound Email Protection

Protecting against email threats is the proverbial bread and butter of email security solutions, but this section merits a closer look given recent market and threat developments. With Office 365 and Google Workspace having built-in security controls that handle spam and malware, organizations should look for email security augmentations that focus on advanced attacks such as spear phishing, BEC, impersonation, and vendor fraud.

Pro tip

It's great if you can find one email security solution that provides protection against every single type of email attack, but such a situation rarely manifests in reality. Instead, know what your built-in O365 or Google Workspace email security already does, and add non-overlapping layers on top to achieve the broadest possible threat protection.

	Required	Nice-to-have	In place	Comments
Payment fraud protection Stop emails impersonating an external entity to defraud the organization eg. fraudulent invoices.				
Payroll fraud protection Stop emails impersonating an employee to steal money or payroll-related information eg. W-2 or direct deposit.				
Impersonation protection Specific protection against impersonation attacks on VIPs and other key internal staff.				
Extortion and Ransomware protection Stop emails that threaten users with bad consequences unless they take a specific action or pay a ransom e.g. locking a user out of their account, installing malware on their system etc.				
Credential phishing protection Stop emails containing links or redirects to fake login pages attempting to steal account credentials e.g. O365				
BEC and social engineering attack protection Protection against email attacks that try to compromise the user's trust to steal money or data e.g. iTunes gift card purchase.				
URL scanning and decoding Scanning URLs with threat feeds and tracing all redirections down to the URL's final destination.				
Time-of-click protection: URL rewriting Modifying URLs so that they can be checked at time of click.				
Attachment scanning Scanning email attachments for malicious and zero-day links. Scanning attachments to label legitimate vendor invoices.				
Email authentication checks Performing DMARC, DKIM, and SPF authentication on email domains.				
Predefined threat categories Accurate classification of threats under specific categories (eg. payroll fraud, payment fraud, social engineering).				
Automated and customizable remediation Capability to automatically delete, quarantine, or apply other remediation actions to detected threats. Capability to customize actions according to threat category, user roles (AD), and exceptions.				

Email Account Compromise Protection

Email account compromise (or account takeover) deserves its own evaluation section due to the hard-to-catch nature of these attacks. There is usually no telltale email that can be used as evidence - rather, the red flags lie in behavioral anomalies and pattern breaks within login locations, IP addresses, email forwards, and so on. Think user entity and behavioral analytics (UEBA), but for emails.

Pro tip

Email account compromise has three distinct 'Before', 'During', and 'After' phases - when attackers try to gain access to a victim's account, when they try to gain persistence, and when they try to launch follow-on phishing attacks or extract sensitive data from the account, respectively. Look for vendor capabilities that address all three stages of email account compromise.

	Required	Nice-to-have	In place	Comments
Credential phishing protection Stop emails containing links or redirects to fake login pages attempting to steal account credentials eg. O365.				
Anomalous login detection Detect and alert on anomalous login into user accounts.				
Unusual mail forwarding rule detection Detect and remove unusual mail forwarding rules set up by attackers or malicious insiders.				
Impossible travel detection Detect and alert on simultaneous login from geographically disparate locations that are impossible.				
Internal mail protection Scanning of internal emails to prevent lateral movement of attacks.				
Overview dashboard Dashboard displaying an overview of recent threats, auto-remediation stats, commonly attacked employees, and other attack trends.				
Predefined threat categories Accurate and automatic classification of account takeover incidents under a specific threat category.				
Email authentication checks Performing DMARC, DKIM, and SPF authentication on email domains.				
Pre-defined threat categories Accurate classification of threats under specific categories (eg. payroll fraud, payment fraud, social engineering).				
Automated and customizable remediation Capability to revoke user access following suspicious account behaviors. Capability to customize actions according to threat category, user roles (AD), and exceptions.				

Phishing / Abuse Mailbox Remediation

Security awareness programs and phishing mailboxes have a flipside - security teams drowning in a flood of user-reported email threats, wading through endless false positives, and having to manually remediate threats across hundreds of affected user mailboxes. Look for vendor capabilities that leverage automation to tackle all known and high-volume threats, freeing up your security team's time to tackle deeper investigations and other pressing cybersecurity concerns.

Pro tip

Automating low-value tasks in phishing remediation is good, but learning from manual actions to automate remediation of identical and similar future threats is even better. Look for vendor capabilities that automate known threats out of the box, and learn from the security team's actions to get better (and automate more threats) with time.

	Required	Nice-to-have	In place	Comments
Phishing / Abuse Mailbox Remediation Connection with your company's abuse/phishing mailbox to automatically scan all reported emails.				
Automated remediation Capability to configure automated remediation actions for user-reported emails flagged as suspicious or safe.				
Threat insights Threat analysis, IOCs, and in-email highlights for all user-reported threats.				
Bulk remediation across mailboxes Capability to group and automatically remediate identical and similar emails across affected user mailboxes.				
Policies to protect against future threats Self-learning mechanisms that acknowledge manual actions to automatically apply the same actions to similar and identical future threats.				
Overview dashboard Dashboard displaying an overview of recent threats, auto-remediation stats, commonly attacked employees, and other attack trends.				
End user notifications Providing labels and warning banners to end users containing information about the attack with calls-to-action.				
Mail client add-in Add-ins with clients like Outlook to enable end users to report emails to the abuse mailbox.				

Outbound Email Protection

Stopping advanced threats from reaching inboxes goes hand in hand with preventing sensitive data from leaving inboxes. Your chosen email security solution should prevent sensitive data (PII, PCI, passwords) as well as user-marked confidential data from being accessed by unauthorized recipients. Look for vendor capabilities that do not rely on manual rules and policies for data loss detection - that way lies mountains of maintenance.

Pro tip

It's important to walk the tightrope between security and productivity when it comes to blocking outbound emails - you don't want genuinely important emails being blocked from reaching the intended recipient due to an inaccurate DLP detection. Look for solutions that can operate in both 'compliance' mode and 'enforcement' mode, with the former mode resulting in detections to lend visibility to the security team, but without the automated blocking.

	Required	Nice-to-have	In place	Comments
Email DLP - PII protection Stop sensitive personally identifiable information (PII) from being shared with unauthorized recipients over emails eg. SSN, passport number etc.				
Email DLP - PCI protection Stop sensitive PCI (bank account numbers, credit card numbers, etc.) from being shared with unauthorized recipients over emails.				
Email DLP - unencrypted passwords Stop unencrypted account passwords from being shared with unauthorized recipients over email.				
Predefined compliance policies Specific compliance policies to automatically flag sensitive data in emails (SSNs, IBAN, passport number, and so on).				
Accidental data loss Specific techniques to prevent accidental data loss based on the content and/or nature of the communication relationship.				
Automated and customizable remediation Capability to automatically revoke access, delete, or apply other remediation actions to detected data loss violations. Capability to customize remediation according to DLP category, user roles, and exceptions.				
Confidential content protection Preventing confidential content from being accessed by noncompliant recipients.				
Client side add-in A add-in compatible with email clients that allows users to mark confidential content, provides warnings for misaddressed emails, etc.				

Detection Capabilities

Evaluating detection approaches and controls is possibly the most important aspect during vendor selection for email security today. Email attacks today are different from what they were 5 years ago - they eschew the use of links and instead use socially engineered language, they leverage freely available online services to trick reputation-based filters, and they attempt to prey on the nature of the human on the other side of the email. Look for detection controls that solve for today and tomorrow's threats rather than controls that stop yesterday's spam.

Pro tip

Targeted email attacks do not have one clear 'red flag', but rather use a confluence of techniques to evade legacy security controls. To mirror this approach, look for vendors that do not treat any one detection control as a silver bullet, but rather use a combination of best-in-class detection techniques to achieve broad threat protection coverage against advanced email attacks.

	Required	Nice-to-have	In place	Comments
Identity-based detection Analyzing signals based on user identity eg. name, designation, role and hierarchy.				
Behavior-based detection Analyzing signals based on user behavior eg. communication patterns, clients and devices used, common login and IP locations.				
Language-based detection Analyzing signals based on language eg. sentiment and tone, topics discussed, writing styles.				
Threat feed integrations Native integrations into threat feeds for real time threat information. REST API availability for integration with other threat feeds.				
Image analysis Detecting fake login screens and attachments using image analysis techniques.				
ML model per organization Custom ML models or learning mechanisms for every organization to increase contextual relevance of threat detections.				
Continuously trained ML models Models that are trained across organizations, per organization, and per employee.				
Communication baselines Historical analysis of emails to build communication baselines for organizations and mailboxes and enable better anomaly detections.				

Remediation Capabilities

In the race to achieve the best detection, remediation often gets left by the wayside, leaving security teams with a mountain of alerts, false positives to weed through, and a 'Now what?' on their lips. Look for email security solutions that have a good spread of native remediation options that can be customized according to Active Directory groups or user roles. Also look for solutions that are easy to integrate with downstream solutions like SIEM and SOAR, so that their alerts can be routed to your security teams' preferred solution.

Pro tip

'Automation' is a much-used term in email threat remediation. The key is to use automation as an enabler when needed, and automation as a replacement when needed. Look for email security solutions that automate response for all known and high-quantity threats. For unknown and advanced threats, automated response should be balanced with providing threat insights to the security team to make their own decisions, whether or not they align with the decisions taken by the security solution.

	Required	Nice-to-have	In place	Comments
End user quarantine End users can have individual quarantine folders where they can manage and release emails.				
End user feedback Warning banners and inline messages to increase user awareness and empower them to perform triage tasks (mark safe, mark suspicious).				
Automated and bulk remediation Detected threats can be automatically deleted, quarantined, or marked as safe based on predetermined remediation actions. Automated email actions can be applied across user mailboxes.				
Customizable remediation actions Threat remediation allows for customization according to threat category, user roles, group membership, and exceptions.				
Abuse mailbox automation Emails forwarded to the company abuse/phishing mailbox are automatically investigated and remediated across user mailboxes.				
Dynamic policy creation New threat policies are automatically created based on manual actions taken by security teams (marked as safe, deleted) to dynamically protect against similar future threats.				
SIEM and SOAR integrations Capability to route alerts to SIEM, SOAR, and other downstream security solutions via JSON over REST APIs.				

Architecture and Enterprise Capabilities

With most organizations now using cloud or hybrid cloud email, the makeup of the email security stack needs to be different than the SEG-dominated stack of 10 years ago. Organizations should look for email security solutions with modern API-driven architecture that also meet enterprise security, privacy, and compliance prerequisites.

Pro tip

Email security solutions being 'in-line' certainly has some advantages, but organizations have borne the brunt of its challenges over the past few years as well. Namely, this type of deployment duplicates built-in email security from Office 365 and Google Workspace (sometimes reducing their efficacy). Also, being in-line still lets bad emails come through, while inadvertently blocking 'good' or wanted emails and impacting employee productivity. Weigh the pros and cons of in-line vs API-based deployment based on your organizational priorities and what you want your future email security stack to look like.

	Required	Nice-to-have	In place	Comments
Cloud platform The solution is available as a cloud service.				
API-first architecture Capability to connect to mail providers over APIs, obviating the need for MX record modifications or email rerouting.				
Autoscaling Ability to autoscale up or down dynamically depending on data and resource load.				
Exchange support Capability to support on-premise Exchange deployments.				
Hybrid model support Capability to support hybrid deployments (e.g. AD on Office 365, but using Exchange on-premise).				
Multi-tenant support Capability to support multi-tenant deployments.				
Audit logs Providing detailed audit logs to track user activity.				
Role-based access control Providing different roles that govern data visibility and level of access to product capabilities.				
SSO support Access to the solution is protected through single sign-on (SSO).				
Third-party accreditation Accreditation of enterprise readiness such as SOC 2 compliance, ISO 27001, and so on.				
Mobile app support The solution has a mobile application that provides alerts to the security team, warnings to end users, etc.				

Armorblox

About Armorblox

Armorblox secures enterprise communications over email and other cloud office applications with the power of Natural Language Understanding. The Armorblox platform connects over APIs and analyzes thousands of signals to understand the context of communications and protect people and data from compromise. Over 56,000 organizations use Armorblox to stop BEC and targeted phishing attacks, protect sensitive PII and PCI, and automate remediation of user-reported email threats.

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 Sunnyvale, CA and backed by General Catalyst and Next47.

Learn about Armorblox customer success stories here.
Book a demo with one of our email security experts here.

Inboxes that love Armorblox

★★★★★

Holistic platform for mitigating attacks via email

- CIO

Read more

★★★★★

Essential to stop phishing emails that bypass your email filtering solution

- CSO

Read more

★★★★★

Exceptional email and DLP security solution

- CISO

Read more