Product Review

Protecting Your Cloud Office Inbox

Written by Matt Bromiley
May 2022
Email is an integral and necessary part of business communications. With more than 300 billion emails sent daily around the globe, it’s easy to see why organizations rely on email to drive business and keep in touch with customers and employees.

Given its popularity and use amongst organizations, email has also become a preferred entry/delivery vector for adversaries. According to a 2021 survey from Ivanti, 74% of organizations fell prey to phishing in the previous 12 months, with 40% becoming victims in the month prior to the survey.¹

To protect their email infrastructure, security teams rely on defense systems to detect malicious emails and prevent them from entering the environment. However, year after year, phishing numbers grow—and adversaries continue to find success. In 2021, the FBI disclosed that business email compromise (BEC) ranked as the top attack vector overall in 2020.² These payloadless attacks were responsible for $2.4 billion in BEC and email account compromise (EAC) losses in that year alone, yet losses have grown year over year. BEC and EAC attacks have presented challenges to email defenses because attackers often use language and context as weapons to trick victims into fraud.

Do these ever-rising statistics mean that email defenses simply don’t work? We think not. Instead, we think it’s time to look at new approaches and uses of technology to defend against email attacks.

In this product review, we spent some time with a platform designed to do exactly that: Armorblox. Purposely built to integrate with modern email systems, Armorblox provides security teams with advanced capabilities to prevent email-based attacks and put a dent in adversary success rates.

In this product review, we got hands-on with the Armorblox platform, discovering how it can assist security teams and secure email infrastructure(s). Here are some of the key takeaways from our experience with Armorblox:

- It’s a simple yet highly capable and powerful platform that enables malicious email detection and prevention.
- The easy, API-based integration with a myriad of email providers allows for fast product deployment.
- We appreciated its use of advanced technologies, such as natural language understanding (NLU), machine learning (ML), URL protection, and malware sandboxing, to detect and block malicious emails from entering the environment.
- It helps organizations stop attacks (including financial fraud and email account takeovers), protect sensitive data, and shorten security teams’ response times.

¹ “Companies are losing the war against phishing as attacks increase in number and sophistication,” TechRepublic, July 2021, www.techrepublic.com/article/companies-are-losing-the-war-against-phishing-as-attacks-increase-in-number-and-sophistication
• Armorblox maintains a Global Machine Learning Model based on malicious emails observed across its entire customer base, allowing all customers to benefit from detections and put a dent in widespread phishing campaigns.

• Overall, it is a rich, analyst-friendly platform that provides deep investigative capabilities into malicious email traffic.

As you read this product review, consider your current email defenses. What do you have in place, and how well are your defenses integrated into your security stack? Can your analysts detect and investigate malicious emails effectively? Consider any email-related incidents you may have experienced in the past six months. What techniques did adversaries use to defeat your email defenses? How did they find success? These factors, and more, require constant testing and evaluation of controls to ensure that they are optimizing protection of your environment.

**Hands-On with Armorblox**

Our review of Armorblox begins with the initial dashboard. The first screen that any analyst, manager, or stakeholder will encounter is key. The platform’s Overview dashboard, shown in Figure 1, is packed with statistics that offer immediate insight into threats to the environment.

As seen in Figure 1, Armorblox provides insight into the threats the platform detected and/or prevented. The platform does a great job of breaking threats down into various consumable categories that allow for an easy “what’s going on” assessment within the environment. Scrolling down, as shown in Figure 2 on the next page, the platform also provides top threat stats, including most attacked VIPs and persons based on email and title, as well as organizationwide stats as observed by the platform. The dashboard presents data via a trending timeline, showing the number of incidents and titles to enable security operations teams to identify quickly who is being targeted in an organization.

**Figure 1. Snippet of the Threats Overview Dashboard**

Integrating Armorblox into your mail environment is entirely API-driven and does not require a DNS MX record change for implementation. This allows for rapid deployment, with some customers up and running in a matter of hours.
Protecting Your Cloud Office Inbox

Detection Models

The power of the Armorblox platform lies within its various detection models. Instead of relying on malicious—but often static and old—indicators, Armorblox incorporates advanced technologies such as natural language understanding (NLU) and AI/ML (machine learning) concepts to detect suspicious and/or malicious emails. The platform can achieve high efficiency rates by integrating directly with an enterprise’s cloud email environment and “learning” about its email traffic. Let us explore this concept further.

As users within an organization type their emails, there are key characteristics about the way they conduct themselves. These may include:

- Who the user emails frequently
- The types of email being sent
- Whether recipients are internal or external parties
- The expected, or “normal,” content of an email sent to or from an internal user

With these data points and many more, Armorblox builds statistical models of the email traffic flowing in and out of an organization. The platform uses these models to analyze future emails, allowing for precise detection models that only improve with more time and experience. As we can see in Figure 2, Armorblox displays the statistics and maturity of its detection models directly in the platform. We love this level of transparency because it provides insight into exactly how the detection platform is working within a unique environment.

Figure 2. Snippet of the Threats Overview Dashboard
Protecting Your Cloud Office Inbox

Armorblox recognizes that email security is not a one-size-fits-all approach. Its advanced detection capabilities are meant to be honed toward the specific environment it protects through a set of configuration options. Users can also contact the company’s Customer Success team. This approach means a higher level of protection that is tuned to each unique environment. Additionally, Armorblox can integrate other advanced detection techniques via its various telemetries, external threat feeds, and extensible AI/ML capabilities.

**Policies**

Aside from its ability to learn more about your environment via its advanced examination of email traffic, Armorblox also allows organizations to tune and customize the implementation via its extensive use of policies. Figure 3 provides a snippet of a few policies configured for our demo instance.

As seen in Figure 3, myriad possibilities exist when it comes to creating organization-specific policies. The security operations team can create custom policies that are fine-tuned to the needs of the organization. For example, the finance department might need tighter controls to handle credential phishing when compared to the IT department. Such variety should come as no surprise. We’ve already shown that Armorblox uses its technologies to tailor its platform to your organization and needs. The policies are meant to help extend the platform even further, allowing security teams to define custom actions for detected activity. Figure 4 zooms in on the policy for Credential Phishing detections.

![Figure 3. Snippet of the Policies Menu](image)

![Figure 4. Snippet of the Policy for Credential Phishing](image)

---

**Referenced Content**

- [Policy Menu](image)
- [Credential Phishing Policy](image)
The figure illustrates a policy for email traffic coming through Microsoft 365 (M365). The policy looks specifically for emails in which an adversary is trying to steal sensitive data, oftentimes as part of a larger attack. For each policy, the platform provides two key data points:

- Actions to be taken if the policy is tripped. In this case, the email is deleted for employees in the Finance department and quarantined for all other employees. Also, notices are sent out to appropriate security parties.

- How many email(s) have tripped the policy

We can see in this case (Figure 4) that seven incidents were generated because of this policy. Analysts can easily click from policy to incidents, allowing for an examination of effectiveness. Figure 5 provides a subset of the corresponding incidents.

When investigating threats like the ones displayed in Figures 5 and 6, analysts receive a wealth of data, including sender and subject, timestamps, the policies tripped, and the user(s) affected by the email. This is also where the platform shines: by displaying just how easy it is for the security team to consume email alerts and associated actions. In Figure 5, we see that offending emails (1) can trip multiple policies and (2) have two classifications: policies in the system and incident tags (indicated in blue) that are auto-generated by the system. This classification system allows for easier searching or saving. We examine the third email incident—with a subject of “Your Box password was recently changed”—in Figure 6.
Email Analysis

Figure 6 shows the email analysis screen from the Armorblox platform. We’re a big fan of features like this because they allow analysts to stay within the security platform and out of an actual mailbox. This feature also saves analysts from having to retrieve the email from another data source because Armorblox looks up the email from the source (M365 or Gsuite) and makes it available for review.

As you can see in Figure 6, the email was flagged for potential Credential Phishing. However, we’re quick to notice that the platform provides so much more than that information. Key data points include:

- Key email details, such as recipient and sender. Email headers are also easily accessible via a button to the side.
- The detections that Armorblox used to classify this email are also highlighted for ease of review. The detections include:
  - A sense of urgency, often used by adversaries to encourage a victim to act upon a spearphishing email quickly (We see their natural language engine in action here, bringing in the analytics to help customers determine a malicious email threat.)
  - A bad URL, with the text of “Click here to reset password”

Armorblox has also cached a screenshot of the malicious URL for posterity. We love this feature because it saves analysts from having to click through links or set up anonymous sources. Figure 7 provides a screenshot of the malicious URL found in the email.
It’s easy to see why users may fall for this page. It looks like a normal Outlook login. However, Armorblox has correctly identified that the parameters within the email and the URL do not match and has appropriately flagged the email as malicious.

Scrolling down, we can examine further why Armorblox has flagged this email. Figure 8 provides a snippet of the Analysis pane.

We are huge fans of clear and succinct descriptions of why something was flagged as malicious. As seen in Figure 8, Armorblox’s reasoning is straightforward: The email contained a malicious link and has a low communication history. It also provides insight into email authentication details—which, by the way, are all pass!—to provide analysts with even more details about the email exchange.

Navigating back to the main dashboard, we can also examine suspicious or malicious emails from the context of type of detection. Armorblox breaks risks down into two high-level categories:

- **Threats**—Emails that are deemed malicious based on currently active policies
- **Data loss prevention (DLP)**—Emails containing sensitive data that cannot be shared with the intended recipients

The email we examined in the demonstration was classified as a threat, but Armorblox’s detection and analysis capabilities are very similar across DLP. Figure 9, on the next page, provides a screenshot of the DLP Incidents page, which lists emails that tripped DLP rules within the platform.

---

**Figure 8. Snippet of the Analysis Pane for Incident ID 68**

---

**Analysis**

**Credentia Phishing**

**Malicious Link in Mail Body**

Armorblox detected 1 malicious URL(s) in the mail body:

https://urldefense.com...J2lNf6YLQERuavg9v9UW166ujQIQ$

Redirects to:

http://t1-tco.tiffany.com...No2ZVxkb25Ac2Fuam9zZWNhLmdvq==

Number of redirects: 3
Snapshot taken on: May 15, 2020 2:21 AM (CDT)
Detected from Global Model Data: No

**Low Communication History**

Only 1 email has been sent from abhishekiyer52@yahoo.com to bartyc@armorblox.ai until today.
bartyc@armorblox.ai has never written to abhishekiyer52@yahoo.com.

**Email Authentication**

- DKIM: Pass
- SPF: Pass
- DKIM Alignment: Pass
- SPF Alignment: Pass
- DMARC: Pass
Protecting Your Cloud Office Inbox

The DLP functionality within Armorblox prevents users from accidental data leakage and/or exposure. DLP functionality is often one area that can draw mixed reviews; it either works or it doesn’t. However, thanks to the detection engines within the Armorblox platform, its ability to recognize sensitive data amongst email traffic is highly effective. Figure 10 presents an email that is still “Under Review” and suspected of an SSN leak. Armorblox allows for multiple remediation actions for both DLP and threat preventions, including Delete from Mailbox, Quarantine to a Folder, Mark as Safe, or Permanently Delete Email.

Figure 9. Screenshot of the DLP Incidents Page from Armorblox

Figure 10. Snippet of an Email that Tripped a DLP Rule for Social Security Number
Like the threat we examined earlier, Figure 10 shows how Armorblox provides a full rendering of the email chain for analysis. Analysts can easily examine the email headers and view the contents without needing to dig into someone's mailbox. Making analysts' lives easier is a feature we always welcome!

The key differentiator that Armorblox brings to DLP is the integration of its NLU engine to complement what most DLP tools rely on: custom identifiers and regular expressions. Understanding the context and content of the email can help dramatically reduce the false positives. For instance, in the example illustrated in Figure 10, if the email were to contain a Zoom meeting with a nine-digit number (similar to an SSN), it would not be flagged as a DLP incident. The NLU engine can distinguish the context of the email (a Zoom meeting as opposed to an email referring to an SSN). This feature is hugely powerful in reducing false positives from outbound DLP protection.

Also, as it does for threat analysis, Armorblox has highlighted the text(s) that tripped a rule. We’ve blurred out the SSN for the purposes of this product review, but it’s clear that Armorblox has no difficulty recognizing data structures amongst email traffic. DLP rules can also be customized and implemented based on organization specifics (see Figure 11).

Figure 11 shows how the organization specified various product code names that the DLP engine brought into effect. These are custom identifiers that customers can create in the platform based on any specific lists or patterns they want to track. They can establish these patterns using regular expressions and number of occurrences of these identifiers to warrant an alert and take remedial action.

As seen at the bottom of Figure 11, within the Analysis section, the platform clearly calls the product code out as a Custom Identifier. As we’ve mentioned, any chance an organization gets to fine-tune a tool to its own needs, vocabulary, or security requirements benefits the organization. It allows that organization to craft its security infrastructure to its exact needs and ensure that its sensitive data is protected by its controls.

---

Armorblox presents robust email security in a simple, easy-to-use platform. The platform provides analysts with sample decisions and emails in a single place, allowing them to quickly review threats, make decisions, and keep the organization safe from email threats.
The best way to assess the efficacy of any security control is to examine its ability to detect and block threats to the environment. In the following case study, we look at how Armorblox enables analysts to analyze and triage email threats to the organization, all done inside the platform.

**VIP Impersonation**

This case study looks at one of the more significant threats facing organizations today: VIP impersonation, which is also a category of the dreaded BEC email threats. In these types of emails, an adversary will pretend to be a person of importance and request that the recipient perform some action. This action may be sending money to a location, changing wire or ACH instructions, or even passing on a message to another unsuspecting party.

Figure 12 presents quite a few detections and displays the power of Armorblox’s NLU engine. The email has been correctly identified as a VIP impersonation in the form of the sender requesting $2,000 of iTunes gift cards. Notice that Armorblox recognizes this request. The platform continues to analyze the content, detecting the urgency of the request, a deadline listed in the email, as well as the appearance of certain terms. These are classic hallmarks of an impersonation email in which the adversary is attempting to get gift cards purchased for fraudulent use.
**Chain of Trust**

Another key detail unique for analysis is that the email has been crafted to look like it is from the CEO. Notice that the signature is correct (per the company template) and contains no malicious links or attachments. Scrolling down, we can even see that the request email is the latest in a chain—not the first email. See Figure 13.

This is yet another tactic that adversaries use to defeat defenses and wear down unsuspecting users: Establish an email “chain of trust” that can subsequently be abused.

The user obviously “fell” for the first email by informing the adversary that they were at their desk and available. This is a classic technique that sets the victim up for completing the task, all the while thinking they are doing their job. Despite being a step or two in the email chain, Armorblox kept an eye on the email chain and correctly identified the impersonation attempt.

Some of the best spearphishing emails seem simple, innocuous, and innocent enough. That’s exactly the point. Adversaries have discovered what techniques will help them evade email defenses, oftentimes removing links and attachments that bypass email filters. This is where *understanding the conversation* comes into play. The next line of defense looks at context and other key statistics, areas at which Armorblox excels.
Precisely because email is vital to any modern enterprise, it has become a favorite entry point for adversaries. Thus, email security is one of the better investments any organization can make in its security infrastructure. Going beyond basic email protections and protecting against advanced BEC attacks can put a significant dent in adversary success rates as well as protect employees from accidental data leakage and other risks.

In this product review, we examined Armorblox, an email security platform built with the unique, intricate needs of an organization as its priority. With high-powered analytics driven by technologies such as natural language understanding and integrated AI/ML, Armorblox learns and tunes itself to the environment to better protect it. The platform can be used to either complement native email security from Microsoft Office 365 and Google Gmail or add depth in defense to your existing secure email gateway (SEG). Organization-driven policies, highly intuitive analysis, and auto-remediation capabilities also make Armorblox an easy fit with analysts, allowing for robust incident investigation with little overhead.

Adversaries see the value in targeting and exploiting an organization’s email as much as possible. Whether it’s malware delivery, malicious links, credential harvesting, or attempting to reroute ACH funds, adversaries are praying that you don’t have effective email defenses in place. Don’t give them an opening. Ensure that your organization has email security in place and that it is tuned and operational, because an adversary who cannot find a successful entry vector will often give up.