Armorblox

Measuring the ROI of Your Email Security Platform

Contents

Armorblox

Executive Summary

As budgets tighten, security leaders are required to demonstrate tangible returns on every security investment. However, short of using in-product telemetry and machine-obtained numbers, no ROI model can be truly scientific. For organizations without the time, personnel, or data-capturing maturity to create detailed ROI models, there is value in calculating ROI based on industry estimates and output-oriented data points. Insights from these models can help organizations make quick but informed decisions on their security stack.

This whitepaper will focus on email security and highlight how the market is in a state of transformation given recent drivers and evolved adversarial techniques. Using anonymized Armorblox customer data, the whitepaper will then cover three models that look at email security ROI through different but equally valuable lenses. You can use these models as templates to measure the ROI of your incumbent email security solutions.

Time savings model: Estimate the time the security team spent on email security before deploying a particular product, and then compare it with the time their team spends on email security post-deployment. This model can be used as validation for email security products that claim to reduce friction and free up time for the security team's ongoing operations.

Abuse mailbox automation model: For organizations with existing phishing/abuse mailbox processes, security leaders can estimate incident volumes, triage times, and remediation times before and after deploying an email security product. This model can be used as validation for email security products that claim to simplify the phishing response process, reduce alert volumes, and shorten response times.

Breach cost avoidance model: This theoretical model uses breach cost and breach likelihood estimates from IBM and Ponemon's Cost of a Data Breach Report, 2020. Organizations can then create scenarios (optimistic, realistic, pessimistic) with different levels of risk reduction attribution assigned to their email security product. These numbers can be further refined by applying an abstract risk adjustment number that takes into account organizational nuances not covered by the rest of the model.

Evaluating the ROI of an email security solution should lead organizations towards some interesting questions. How much time are they spending on email security? What other things could they be doing with that time? Is the security team looking at threats that matter? This whitepaper aims to get organizations start asking these questions of their incumbent email security solution.

Armorblox

Email Security Drivers and Challenges

When someone mentions 'email security', one would be forgiven for thinking it's a market that has been around for a long time and is more suited to marginal innovations rather than being a fertile ground for transformation. However, recent industry trends and new email attack techniques paint a different picture.

Email attacks, email delivery, and built-in email security have all changed in the past few years. While some security challenges within this space have existed since email itself has existed, other new challenges have reared their head in response to the changing face of this market.

Industry drivers

- **The move to cloud-delivered email:** According to Gartner, around 71% of organizations now use cloud or hybrid cloud email. This trend has continued to gather pace with the rise in remote work, and it's now a question of 'when' and not 'if' organizations will have at least some part of their email delivery through the cloud.
- **Effective built-in email security:** Microsoft and Google have improved their built-in email security capabilities by leaps and bounds over the past few years. With good spam and malware protection now bundled in with email providers' offerings, organizations are moving away from legacy Secure Email Gateways (SEGs) and now look for augments to built-in email security that do not overlap with what they have already paid for with Microsoft and Google.
- **Increased comfort with email business workflows:** When the world went into lockdown in 2020, our screens became our offices, and that development doesn't seem to be going away any time soon even if there's light at the end of the COVID pandemic tunnel. As a result, employees are now more comfortable than ever with email being the vehicle for critical business workflows. Password resets, fulfilling vendor invoices, granting app access, reviewing security alerts - all of these processes and more involve email and are easy for cybercriminals to replicate and exploit.
- **The rise in targeted email attacks:** Email attacks have evolved and moved beyond the mass spam and phishing scams of old. Today's attacks are targeted, impersonate known people and entities, hijack business workflows, and use social engineering techniques to compromise the human layer of organizations. Business Email Compromise (BEC) and Email Account Compromise (EAC) attacks accounted for $1.86 billion in reported losses in 2020, according to the FBI.

Armorblox

Email Security Drivers and Challenges

Given these drivers, organizations have to deal with a smorgasbord of email security challenges today. Some of these challenges have been around for years, some have grown in impact recently, and others are brand-new problems that security teams have to navigate in a cloud-first, ever-connected world.

Questions of cost

- **The cost of time:** How much time is your lean (probably overworked) security team spending on email security? How much of that time do they actually need to spend on email security, and how much of that time is better spent on other critical cybersecurity priorities for your business?

- **The cost of alert fatigue:** With email threats being forwarded to your company's abuse mailbox in droves, how much effort is your security team expending on manual triage and remediation?

- **The cost of data breaches and increased risk:** The human layer is the most attacked and most vulnerable layer of your organization. What are the financial, regulatory, and reputational implications of a data breach stemming from targeted email attacks or human error?

- **The cost of a duplicative email security stack:** If you've already invested in Office 365 or Google Workspace security, what are the merits and costs of also investing in a SEG? What is the opportunity cost of not investing in third-party augments that stop targeted email attacks without overlapping with built-in email security?

The subsequent sections of this whitepaper will go through various ROI models that help answer the cost and ROI questions posed above. While these models used anonymized Armorblox customer data, they can be used as templates for organizations to insert their own data and evaluate the ROI of their incumbent email security solutions.

Armorblox

Time Savings Model

This section will go through a fairly straightforward but effective model Armorblox uses to quantify time savings that our customers experience after deploying and using the platform. The key to making this model consistent and useful is jointly working with the customers to collect data, present results, and iterate based on their feedback. Every model is subjective beyond a point, but if the customer thinks the model is a fair representation, then the model is useful.

The questions this model tries to answer are:
How much time is your security team spending on email security?
What other things can your security team do with that time?

- **Collect estimates for time spent on email security** (as hours/week) before Armorblox. If the customer agrees, also collect data on the number of employees responsible for email security and their compensation details.
- **Collect user estimates** for time spent on email security after Armorblox.
- **Compare analyst effort before and after Armorblox deployment.** To maintain the integrity of the model, the 'after' times are recorded a few months after Armorblox deployment to ensure there are no short-term bumps that skew the figures.
- **Prepare and present final metrics**: time saved (in hours or days per week) and budget available for redeployment ($).

These tables show anonymized data from an Armorblox customer, highlighting their security resources dedicated to email security, and how much time they spent on email security before and after Armorblox deployment.

Security resources dedicated to email security

Security Resources Dedicated to Email Security			
FTEs	Salary	$/hr	Hrs/Wk
1	$100,000	$48	40
2	$100,000	$48	40
3	$100,000	$48	40
4	$100,000	$48	40
5	$100,000	$48	40
6	$60,000	$29	40
7	$60,000	$29	40
Total	$620,000	$298	280

Savings of 30 hours per week (3.7 days) due to Armorblox

Net Time Savings		
Hrs/Wk	Hrs/Year	Savings
16	832	$40,000
6	312	$15,000
6	312	$15,000
5	250	$12,000
5	250	$12,000
-4	-208	-$6,000
-4	-208	-$6,000
30	1,539	$82,000

Armorblox

Time Savings Model

Time Spent on Email Security Before Armorblox			
% Time/Wk	Hrs/Wk	Hrs/Yr	Cost/Yr
50%	20	1,040	$50,000
20%	8	416	$20,000
20%	8	416	$20,000
20%	8	416	$20,000
20%	8	416	$20,000
0%	0	0	$0
0%	0	0	$0
19%	52	2,704	$130,000

Time Spent on Email Security After Armorblox			
% Time/Wk	Hrs/Wk	Hrs/Yr	Cost/Yr
10%	4	208	$10,000
5%	2	104	$5,000
5%	2	104	$5,000
8%	3	166	$8,000
8%	3	166	$8,000
10%	4	208	$6,000
10%	4	208	$6,000
8%	22	1,165	$48,000

Results and Benefits

For this customer, Armorblox was able to reduce the time spent on email security by 57% or 3.7 days/week. Rather than spending this time triaging inbound email attacks and responding to user-reported email threats, the team can now spend the time conducting deeper investigations and pursuing other cybersecurity goals for the organization.

- **Happier workforce:** Security practitioners don't spend as much time on manual and repetitive tasks and can instead do more stimulating work during those hours (often the things they were hired to do before getting sidetracked with email security busywork).
- **Proactive security operations:** Security personnel can be redeployed to more proactive security activities such as penetration testing, vulnerability management and patching, analyzing metrics to check their organization's security posture, and so on.
- **More secure business:** A happy, proactive, and productive security team has positive effects on other business unit operations. Fulfilled and motivated security employees play a key role in turning your organization's security function from a blocker (or being perceived as a blocker) to an enabler of the business.

The time savings case study presented in this section also found that $82,000 of the customer's security budget was now freed up and available for redeployment. We know this is not literally the case, and that not every organization is comfortable attaching a monetary value to employees' time. The metric has been shared in this whitepaper in case you'd like to include it in your version of the model.

Armorblox

Abuse Mailbox Automation Model

This section will cover a model that Armorblox uses to quantify reduction in incident response times to user-reported email threats for our customers. Phishing triage and response processes today are beset by a large volume of alerts, collecting information across disparate sources, and manual and repetitive actions to weed out false positives and remediate threats. This model provides supporting evidence of how Armorblox streamlines and accelerates abuse mailbox remediation processes for customers.

The Process

- **Collect user data or estimates** on incident volumes and triage/response times for user-reported emails before Armorblox.
- **Collect user data or estimates** on incident volumes and triage/response times for user-reported emails after Armorblox
- **Compare reported email volumes** and response times before and after Armorblox.
- **Prepare and present final metrics:** % reduction in user reported email threats, % reduction in triage and response times.

These tables show anonymized data from an Armorblox customer, highlighting their incident volumes of user-reported email threats as well as the time taken to remediate these threats.

	Before armorblox	After armorblox	Net Change	% Change
On average, how many user-reported emails does your team receive per month?	100	15	-85	-85%
Of the reported emails that were reviewed, what percentage of them are identified as malicious or emails that require additional remediation steps?	90%	50%	-40%	-44%
How much time (in minutes) does it take to remediate user-reported email threaths? For example, finding and deleting all matching emails, creating new policies to stop similiar threats in the future, etc	60	2	-58	-97%
Total Time Spent (hrs/month)	115	4	-111	-97%

Abuse mailbox automation model showing 97% reduction in response times to user-reported email threats

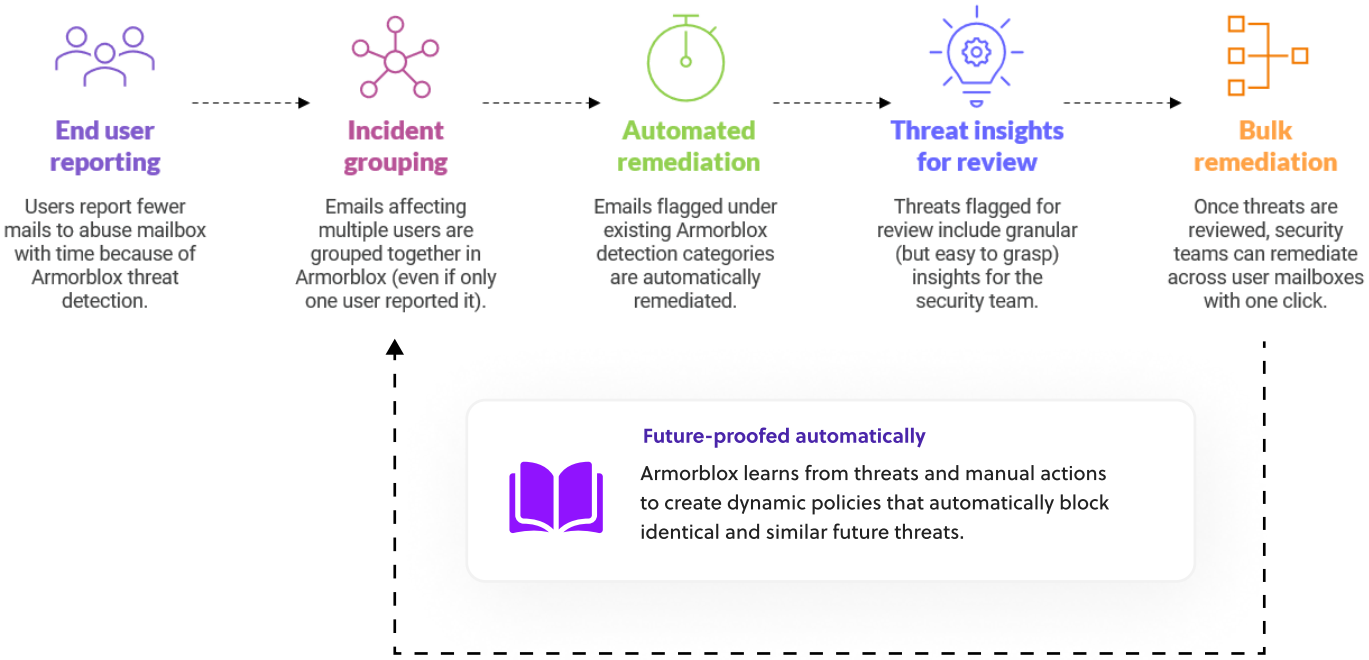
Armorblox

Abuse Mailbox Automation Model

Results and Benefits

For this customer, **user-reported email threats reduced by 85%** after deploying Armorblox because these threats had already been detected and removed from user mailboxes. Moreover, **response times for reported threats reduced by 97%**, freeing up this time for the security team to carry out deeper investigations and other proactive activities.

Armorblox simplifies the abuse mailbox remediation process at every stage of the phishing incident lifecycle:



Armorblox eliminates friction for both the security team and end users with end-to-end automation that gets better with time

Armorblox

Breach Cost Avoidance Model

This section will cover a model that Armorblox uses to quantify reduction in incident response times to user-reported email threats for our customers. Phishing triage and response processes today are beset by a large volume of alerts, collecting information across disparate sources, and manual and repetitive actions to weed out false positives and remediate threats. This model provides supporting evidence of how Armorblox streamlines and accelerates abuse mailbox remediation processes for customers.

The Process

- **Find cost and likelihood of data breach** based on the organization's geography and industry. For this case study, the source data is taken from the 2020 Cost of Data Breach Report by IBM and Ponemon Institute, which analyzed 524 recent breaches across 17 geographies.
- **Calculate Armorblox contribution** to the overall cost avoidance by analyzing root cause categories for malicious attacks in the report. As the table below shows, Armorblox protects against 41% of all breach root causes for malicious attacks.
- **Bundle assumptions and risk factors** into an adjustment rate number for more accurate final estimates. Risk factors that skew the model numbers might include organizational size, existing tools and training, corrections for location and industry, macroeconomic trends, and so on. The table below assumes a risk adjustment rate of 15%.

Average cost of data breach per year	
Industry	**Technology**
Average cost of data breach ($)	**$5,040,000**
Average Risk of data breach (%)	**29.60%**
Root cause due to malicious attack (%)	**52.00%**
Risk value	**$775,757**
Breakdown of malicious data breach root causes by threat vector	
Compromised credentials	**19.00%**
Cloud misconfiguration	**19%**
Vulnerability of third-party software	**16%**
Phishing	**14%**
Phyical security compromise	**10%**
Malicious insider	**7%**
Other misconfiguration or system error	**6%**
Business email compromise	**5%**
Social engineering	**3%**
Other	**1%**
Armorblox Protects Against	**41%**
Breach cost avoidance with Armorblox ($)	
Breach cost avoided ($)	**$318,060**
Adjusted breach cost avoidance with Armorblox ($)	
Adjustment Rate	15.00%
Breach cost avoided ($)	**$270,351**

Armorblox

Breach Cost Avoidance Model

Results and Benefits

For this customer, deploying Armorblox resulted in **$270,351** per year in avoided breach cost due to reduced risk and impact from data breaches. These numbers translate to multiple qualitative benefits for organizations:

- **Protect brand reputation:** Avoid reputational damage stemming from compromised accounts, security breaches, or paid ransoms.
- **Ensure regulatory compliance:** Uphold and enforce mandates to protect your organization's confidential and sensitive data (customers, employees, partners).
- **Safeguard assets and personnel:** Guard your human assets against breach fallouts like overwork and anxiety for the security team, negative publicity, firefighting effort, and so on.

How is the cost of a data breach calculated?

To calculate the average cost of a data breach, Ponemon Institute collected both the direct and indirect expenses incurred by organizations. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services.

Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

To learn more about the Cost of Data Breach Report, you can **visit this link**.

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. Thousands of 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.

How Armorblox saves time

- **Rapid deployment:** Armorblox connects over APIs in minutes without any MX record changes or email rerouting.
- **Predefined detection categories:** Armorblox automatically classifies threats under detection categories (payroll fraud, payment fraud, email account compromise, VIP impersonation etc.) without the need for creating or maintaining custom policies.
- **Threat insights built for human eyes:** Armorblox algorithms aren't just mysterious forces working behind the scenes. The platform clearly explains why each email threat is safe or suspicious. Displaying these threat insights simplifies investigation and enables your security team to mark rare false positives with greater confidence.
- **Automated and configurable remediation:** Armorblox automatically remediates targeted email attacks (delete, quarantine, lock user account) with customization options for exceptions, Active Directory group membership etc.
- **Abuse mailbox remediation:** Connects with your company's abuse mailbox to automatically investigate and remediate emails reported by end users.
- **Bulk remediation of reported threats:** Remediates reported emails across affected users without the need to manually check other mailboxes.
- **Lower alert volumes:** With time, end users will report fewer emails to the abuse mailbox because Armorblox automatically detects and responds to threats in user mailboxes.

Read more stories from happy Armorblox customers **here.**
Request a demo with an Armorblox email security expert **here.**