Ranking Email Security Solutions

A Data Analysis of Cyber Insurance Claims

Author: Adam Tyra

Contributors: Ayelet Kutner, Eric Murphy, Ido Lev, Matt Actipes

at bay

A NOTE FROM OUR CEO

Choosing which security products to buy is a challenging task for an organization, especially with limited resources or security expertise. It is easy to believe that security products help, but to what extent are they worth the investment, and which product within a category is the most effective? Those questions are really difficult to answer by experts, let alone customers.

But the issue runs deeper than that. Security solutions are layered on top of IT choices with products and configurations that can create wildly different security challenges for organizations. Some software products are more prone to becoming vulnerable to attacks, while others lack security controls that highly impact the risk of the organization. Without a clear analysis of the risk associated with IT choices, insureds are left to make a choice based solely on functionality, inadvertently putting themselves in a riskier position.

The reality is that all software products can become vulnerable to a cyber attack, but some are more vulnerable than others. Still, there is little accountability or incentive for software vendors to prioritize security — especially since enhanced security features often come at the expense of a “seamless” or more straightforward user experience with the product.

What’s needed is an objective, statistically significant financial analysis of the relationship between software and software security choices as well as the financial loss and business impact from cyber attacks associated with each product choice. Such analysis would also make it possible to measure the return on investment for different security products and product categories, which is essential for organizations with limited budgets.

In pursuit of our mission to bring clarity to cyber security and empower businesses to embrace technology with confidence, we have created this report to help provide a benchmark for the expected losses, according to our portfolio, associated with several of today’s popular email solutions and email security solutions.

As an insurance company, we are less interested in the theoretical capabilities of a product and more interested in statistically significant results from real-world incidents in our portfolio. We use these findings to guide our insurance pricing decisions, incentivizing our customers to choose better-performing products in order to unlock better rates on their policies.

Thanks to our first-party data on attacks and losses, At-Bay can reveal the real-world relationship between product choices and corresponding financial risks for each major product category in software and software security. This provides valuable insight into both product performance and prioritization of solutions.

We trust that this report — and those that follow — will serve as a valuable resource to the security community, providing vendors with an opportunity to improve their own intelligence on their product performance and decisioning, while empowering customers to make better decisions in choosing secure software.

Rotem Iram

At-Bay Co-founder and CEO

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In this research analysis, At-Bay's Cyber Research team investigates the frequency of email-related cyber incidents among customers who use email security solutions to protect their organizations from cyber criminals, in addition to those who don't use any third-party solutions at all.

The output of the analysis is a ranked list of the "Email Security Solutions" and "Email Solutions" that have the highest and lowest frequency of successful email-originated attacks according to At-Bay's customer data, which includes cyber insurance claims and breach notifications filed from mid-2018 through to May 2022.

The dataset used for the analysis includes details from the mid-to-small size businesses that held an At-Bay policy since 2018 and also had a security incident where the attack vector included a malicious email or a network security attack against a local email server. Over the four-year period we issued ~40,000 individual policies to businesses, and this makes the population sample meaningful in our opinion.

Top findings

Email Security Solutions

- There's a significant difference between the frequency of incident-related claims that included email as a factor among the most prevalent email security solutions within our book. The gap between the best and the worst email security solutions is 53%.
- The email security solution associated with the lowest number of security incidents involving email is Mimecast.
- On average, At-Bay customers using Mimecast experience 22% fewer incidents compared to all organizations in the email security solutions category.
- Other high-performing email security solutions, in order of effectiveness after Mimecast, were, Sophos, Intermedia, Appriver, and then Proofpoint.

Email Solution

- Organizations using cloud-based email solutions like Microsoft 365 and Google Workspace experience significantly fewer security incidents compared to those that operate an on-premises email infrastructure (e.g., Microsoft Exchange).
- The email solution that was correlated with the lowest number of security incidents involving email was Google Workspace.
- On average, Google Workspace customers saw about 40% fewer security incidents compared to all organizations analyzed in the email solutions category.

Potential Cost Savings

- Based on a cost analysis done on our portfolio, a typical company could have saved as much as 50% on their premium prices if they used the best email solution or email security solution in their category (i.e., Mimecast or Google Workspace).

METHODOLOGY

At-Bay's analysis included claims and breach notification information from mid-2018 through the end of May 2022. Selected claims included those covering breaches of email solutions themselves as well as claims for other incident types that had email as a significant factor in the incident (such as via network attacks of an email server). For each relevant cyber incident, At-Bay's Cyber Research team evaluated the historical data to determine:

1. Did the insured have an email security solution in place at the time of the claim? Note that the term "Email Security Solution" as used throughout this report includes any identifiable product or service with a primary purpose of detecting and containing potentially malicious emails.
2. If there was an email security solution in place, what was the name and vendor for the solution?
3. For insureds who reported a cyber incident but didn't have an Email Security Solution, At-Bay's cyber research team documented the name of the "Email Solution" used by the insured for further analysis instead. Email solution includes on-prem email servers whether operated and maintained by the insured themselves or by a third party hired by the insured. Email solution also includes cloud-based email providers such as Google Workspace and Microsoft 365.

Data about insureds' email systems was collected as part of the initial underwriting process (i.e., via written policy applications and automated scans) and updated throughout the lifecycle of each policy via periodic and ongoing external scans initiated by At-Bay.

To establish the set of "Email Security Solutions" that were worth investigating, we identified more than a dozen providers that were prevalent enough within our customer population to warrant further analysis. For the selected solutions, our researchers established a normalized claims frequency to identify potential correlations with incident occurrences. After further analysis, six email security solutions were considered prevalent enough to provide statistically

significant results. The same was done for the “Email Solution” category.

By identifying the solutions that have a high or low claims frequency compared to the average, we believe that we can assess the relative effectiveness of email security solutions in mitigating the risk of security incidents stemming from email usage.

We infer from this that the email security solutions which appear less frequently in our dataset are more effective at mitigating email risk. The same goes for the customers who don’t use any incident and didn’t have an email security solution in place, that the relative claims frequency is indicative of the effectiveness of the native security capabilities that come built-in for today’s email solutions.

INTRODUCTION

Email is still the most critical gap in the perimeter for all businesses regardless of size, industry, or security maturity.

Regardless of industry, email has emerged as the indispensable technology service for businesses of all types. In addition to enabling communications between employees, many companies rely on email as their indispensable tool for key functions including customer relationship management, file storage, memorialization of key business decisions, control of financial transactions and even to enable elements of other platforms (e.g., usage of email for multi-factor authentication (MFA)). Because of this, email is often the top priority for restoration in the wake of disasters and IT outages.

Email incidents accounted for 41% of our customer claims in the first half of 2022.

Unfortunately, email remains extremely difficult to secure. Fundamentally lacking security by design, email solutions require users to accept unsolicited messages from almost anyone at any time. Although email standards and protocols have evolved over the past five decades[1], native email security features have been somewhat of an afterthought for many email solution providers until recently. Because of this, an overwhelming number of computer intrusions originate via email, and it is also the most common source of fraud incidents experienced by businesses.

1 Email And The Evolution Of Technology Standards, Lila Kee, Forbes Technology Council, September 24, 2021.

Increasing security around business email usage is a reliable way to mitigate cyber risk. Businesses that host their email servers entirely in the cloud experience far fewer incidents than those that operate on-premise solutions without additional security. An email security solution will also generally help to lower risk among businesses that use an on-premise solution or operate their email in a hybrid IT environment. However, there exists significant variation in effectiveness among the solutions most used by our customers in lowering email risk. The negative correlation is so reliable that we feel confident in drawing conclusions about the relative effectiveness of email security solutions.

60% of those email-originated claims were attributed to financial fraud.

Before we detail our findings, a few caveats should be noted:

- First, our data does not include details about the configuration of email security solutions that our insureds have in place. Our rankings do not reflect the optimal potential performance of a solution but rather its actual results in the field, which is based on a variety of factors. While we normalized the data to exclude factors like size of company, industry, and geography, we did not account for variations in configuration for the solutions we analyzed. As most IT and security professionals are aware, configuration matters. Even the best security tools struggle to deliver value if they're poorly deployed or maintained. Designing a product that can be effectively used by its customers is as important as any other functionality of the solution. We believe that a solution that excels in controlled security tests when properly configured by its manufacturer yet fails to perform in real life cases due to poor configuration by its customer is not a high performing email solution.
- The second significant caveat we will note is that there may be environmental factors impacting the apparent effectiveness of email security solutions that we can't directly identify or measure. Email security solutions are rarely the only relevant security control that our insureds have in place, and incidents usually result from systemic -ures among multiple controls rather than weaknesses in individual controls. Nevertheless, the statistical significance of the data acts to normalize (or average out) the differences

between environments and allows us to assess the impact of the chosen solution on the overall security ecosystem. We feel confident using it to support decisions on pricing and coverage for our insurance products. It follows that readers should feel confidence in our recommendations that are based on the same data.

- Finally, we haven't included a comparison between the claims frequency of organizations without an email security solution and those that have one, because we believe that it would be both invalid and misleading. Our reasoning for this is that we aren't able to disaggregate an organization's level of risk before they procure an email security solution from the residual risk remaining after the solution is deployed. We believe that the mere presence of an email security solution may provide an indication of the level of cyber risk experienced by the organization that purchases it, and there is a strong positive correlation between revenue and likelihood of an email security solution being present.

We already know (and our pricing models reflect) that organizations with higher revenue experience a higher frequency of claims. So, we weren't surprised to discover that organizations that had an email security solution in place had, overall, a higher frequency of claims than those that didn't have an email security solution. While this might imply that having an email security solution makes an organization more likely to experience a security incident, we believe that the actual explanation is that many organizations that don't have an email security solution are simply too small to be interesting targets for attackers and therefore don't experience a level of risk that would justify investment in an email security solution. Thus, comparing them with organizations that see the need to purchase an email security solution seems inappropriate from a risk perspective.

DATA FINDINGS & ANALYSIS

Email Security Solutions

The table below shows the individual email claims frequencies of the email security solutions providers most used by our customers.

Email Security Solution	Email Claims Frequency	Email Risk Index*
Mimecast Email Security	0.097%	78
Sophos Email	0.106%	85
Intermedia Email Protection	0.112%	89
Appriver Email Threat Protection	0.118%	94
Proofpoint Email Protection	0.133%	106
Barracuda Email Protection	0.148%	118
Avg Frequency of ALL At-Bay Customers with Email Security Solution	**0.125%**	**100**

*Indexed numbers based on email security solution average, which is weighted at 100.

Key Findings

- While most of the email security solutions in our dataset were correlated with some reduction in risk for email-related incidents, organizations using the top performer, Mimecast, experienced an impressive 34% fewer email security incidents than the email security solution that was the least effective at lowering risk, Barracuda.
- Compared to the ALL category average, Mimecast customers experienced 22% fewer email-related cyber incidents.

Analysis

We believe that these findings provide statistical evidence of the difference in effectiveness that exists among market-leading email security solutions.

We believe so strongly in these findings that we have updated our pricing models to reflect the relative risk implied by operating these products. As such, businesses that use email security solutions for which we have effectiveness data have their policies priced to match the implied risk (see the last page of this report for more insight).

It is important to note that this analysis provides a perspective on the relative effectiveness of the leading email security solution that our insureds use to lower their risk of incidents from email usage generally. It does not provide a perspective on the objective effectiveness of any of these platforms at stopping cyber attacks as promoted on their websites. We can't comment on the fitness for purpose or the merits of the respective features of any of these platforms. However, it does appear that some are more effective than others at mitigating the risk of incidents involving emails.

Other Important Call Outs:

1. The presence of an email security solution may be a bellwether for the presence of other security controls or capabilities that are effective at mitigating risks. Organizations with the budget to invest in email security likely have invested in other security controls as well, and they may also be more risk-aware than organizations without email security solutions. Thus, they may be less likely to experience a security incident in general. This idea could

potentially be verified by examining the correlation (if any) between the relative costs of email security solutions and their apparent effectiveness.

2. Organizations that have invested in email security platforms that seem ineffective at mitigating the types of risks that At-Bay studied may be subject to more significant risks that we haven't considered. It's important to note that readers considering how to use our research findings in planning their own security controls should interpret them through the lens of their own circumstances. While At-Bay's claims tend to involve phishing, ransomware, and financial fraud, some of our insureds are likely to experience much higher losses from threat scenarios involving unauthorized disclosure of proprietary data. In these cases, investment in email encryption and data loss prevention technologies may make more sense than investment in anti-phishing and anti-malware technologies.

Email Solutions

Our next analysis includes a comparison of claims frequencies among organizations using cloud email solutions with those using on-premise email. Thus, this chapter is for customers who do not buy email security.

While few organizations opt to migrate to the cloud specifically to realize enhanced security, it's our belief that they likely expect to experience some security benefits by outsourcing part of the responsibility for the security of their email infrastructure to the cloud service providers themselves via the "shared responsibility" model.[1] Thus, an analysis of the security outcomes experienced by these organizations is highly relevant.

We will note that our analysis excludes organizations that have taken a layered approach to their security and paired an email solution with an email security solution. We are only comparing the native security capabilities of cloud email solutions with the native security capabilities of on-premise email servers. We will also caution readers not to compare the average claims frequency by email solution with the average claims frequency among organizations with an email security solution as it results in invalid conclusions for risk-centric reasons previously discussed.

[1] In its simplest terms, CrowdStrike explains that the Shared Responsibility Model dictates that the cloud provider—such as Amazon Web Service (AWS), Microsoft Azure, or Google Cloud Platform (GCP)—must monitor and respond to security threats related to the cloud itself and its underlying infrastructure; meanwhile, end users, including individuals and companies, are responsible for protecting data and other assets they store in any cloud environment. You can read more about Microsoft's view of shared responsibility here.

The table below shows the individual email* claims frequencies of the email solutions most used by our customers. This includes Google Workspace, Microsoft 365 and on-premise Microsoft Exchange.

Email Solutions	Email* Claims Frequency	Email Risk Index
Google Workspace	0.070%	59
Microsoft 365	0.140%	118
Microsoft Exchange	0.189%*	159
Avg Frequency for ALL	**0.119%**	**100**

* Cloud email providers were only evaluated for email-related incidents. However, since Exchange is not only an email service but also an on-premise, publicly facing server that can be compromised, the data also reflects incidents that occurred via network security attacks that may not have involved a malicious email as the initial point of entry specifically.

Key Findings

- Among the configurations for email that At-Bay considered, organizations that used Google Workspace experienced the lowest frequency of incidents on average. Compared to the overall average, Google's claims frequency was, on average, 41% lower.
- Microsoft 365 has a relative claims frequency that's 18% higher than the overall average.
- Organizations operating an on-premise Microsoft Exchange server experienced over 2.5x more security incidents than those with Google Workspace.

Analysis

Cloud-based email solutions provide a lower risk alternative to on-prem email servers.

The burden for maintaining on-premise email servers is on the organizations that own them and as such, businesses who use on-prem solutions experience almost two times as many security incidents as those who use cloud solutions from Google and Microsoft 365 combined. Many small and medium sized businesses don't have the technical knowhow or capacity to credibly maintain their IT infrastructure. Some make up for this shortfall by engaging a managed service provider to do it for them. Nevertheless, security researchers and threat groups continue to discover new vulnerabilities in these products, and vendors struggle to keep pace with patches.[2]

Organizations that operate these products struggle even more. Data collected from At-Bay's Active Risk Management service shows that our insureds required, on average, ~10 weeks to patch high-severity vulnerabilities after notification by At-Bay. While this is twice as fast as organizations that aren't At-Bay insureds[3], it still leaves attackers with more than enough time to find and exploit victims.

For most organizations, operating an on-premise email server no longer makes sense. At-Bay recommends transitioning to a cloud-based email solution whenever possible and certainly before current in-use solutions reach end-of-life status.[4]

In comparing the apparent effectiveness of security embedded in Google's and Microsoft's cloud-based email solutions, we believe additional consideration is needed. While it's possible that Google does offer better security and is therefore less likely to be part of a security incident involving email as compared to other cloud service providers, there are other factors that could create differences in the outcomes experienced by organizations using various email providers. One plausible explanation is that attackers favor Microsoft 365, because it has a higher market share, especially with larger and more lucrative targets. Thus, Microsoft users experience more successful attacks on a relative basis as compared to Google users because they experience more attacks on an absolute basis.

[2] ProxyNotShell was first published by Microsoft on September 30, 2022. The patch release was on November 08, 2022.

[3] Kenna Security: Prioritization to Prediction, Vol 6: Attacker, Defender Divide

[4] End-of-life solutions are those which no longer receive maintenance from their vendors. This means that vulnerabilities identified in these solutions will likely not have patched developed that can remediate them. MS Exchange Server 2016 was the latest version of that product to be deprecated and reached end-of-life status in October 2020. Exchange Server 2019 (the current version) is currently scheduled to reach end-of-life status in January 2024.

In short, we aren't clear if this disparity is a simple case of Google offering better security features than Microsoft. It's in our opinion that both vendors appear to offer a credible and highly robust portfolio of security control options to accompany their email offerings. Instead, it's possible that the outcomes depicted by our data may be more closely related to circumstances surrounding the organizations operating these respective solutions than about the effectiveness of the solutions themselves.

As At-Bay expands its security capabilities, the relative merits of available cloud platforms will continue to be a focus of data collection and research. In the meantime, organizations considering a move away from an on-premise email server to a cloud-centric offering should consider offerings from both Google and Microsoft as strong contenders from which to source their email service.

The Insurance Perspective

By Eric Murphy and Matt Actipes

As pricing actuaries, one of our main goals is to make sure the prices we charge for insurance are as closely tied to the costs we expect to incur as possible. This helps to ensure that our insureds are only paying for the level of risk they are exposed to and incentivizes companies to implement better security practices, which reduces their risk of having a cyber incident and also lowers At-Bay's likelihood of having a claim. As a result, we want today's technology decision makers to understand that their purchasing decisions not only have an impact on their likely risk exposure, but their insurance premiums as well.

An email attack costs businesses an average of approximately $110,000, with those at the top of the range sometimes costing in the millions.

Careful analysis of claims data shows that the likelihood of an insured having a claim (or multiple claims) varies considerably depending on the email services they utilize. Combining the data with insights and knowledge of our cyber research team allows us to gain confidence that the observed differences in the claims data will continue into the future, so much so that we vary our pricing based on it.

The financial risk tradeoff: Adopt a better product now, or pay later in higher premiums and higher risk.

The table below illustrates the average premium a company may expect to pay based on their size and the email solution they employ. For example, an email security solution or an email solution. Each entry represents a different email solution price-point included in our rating plan and gives examples of the email solutions that would lead to that price.

Insurance Pricing Estimates* for Businesses using Low to High Risk Email Solutions Based on At-Bay Claims Analysis

	25 Employees	50 Employees	100 Employees	200 Employees
Google & Mimecast	$5,137	$6,573	$14,045	$16,584
All Other Email Security Solutions	$6,988	$8,902	$19,562	$23,162
Microsoft 365 Customers	$7,603	$9,676	$21,378	$25,324
Microsoft Exchange Customers	$9,783	$12,409	$27,830	$32,997

Based on this portfolio cost analysis, it's possible that a typical company could have saved approximately as much as 50% on their premium prices last year if they used the best email solution or email security solution in their category (i.e., Mimecast or Google Workspace).

* Pricing based on average policy within At-Bay's portfolio with given employee count. Premiums based on rates and policies in force as of October 2022. Actual premiums offered are based on a variety of factors. The values in this table are not indicative of future pricing, nor do they guarantee future coverage offerings.

Based on this portfolio cost analysis, a typical company could have saved as much as 50% on their premium prices last year if they used the best email solution or email security solution in their category (i.e., Mimecast or Google Workspace).

NOTABLE MENTIONS & BACKGROUND

About At-Bay and this Report

At-Bay helps businesses mitigate digital risk and avoid cyber incidents by continuously analyzing data from security scans and collected cyber threat intelligence along with the relevant details of security incidents reported by insureds. Because we can correlate information about a significant number of real-world incidents with data about the victim's technology environment before the incident occurred, this enables us to reliably identify trends and relationships that other companies and security vendors cannot. We're able to clearly identify security controls that mitigate risk, differentiate them from security controls that don't mitigate risk, and prove our case with empirical data from actual incidents where those security controls were in place.

In the past, we have communicated our views on these issues to our insureds indirectly via the terms and conditions of our insurance products. We're making a change. This will be the first in a series of works wherein At-Bay will share its findings on the respective impacts of a range of security controls with the public at large. Our hope is that we can use facts and evidence to cut through the noise of a crowded cybersecurity marketplace and enable organizations to deploy scarce cybersecurity resources for maximum impact. To this end, we will develop and share a slate of statistically provable leading practices for security that can be readily consumed by organizations regardless of headcount or the size of their security budget.

The information is provided for informational purposes only and no warranty is given or liability accepted regarding this information.

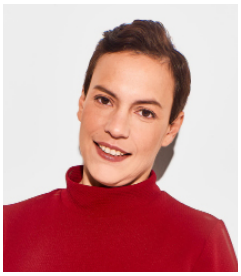
Contributors

Adam Tyra

GM, Security Services

Adam Tyra is a technology professional with over 18 years of experience in security and deep expertise in cyber security operations. He currently serves as At-Bay's General Manager of Security Services.

Prior to joining At-Bay, Adam was a security leader at Kivu Consulting, TalonX, McKinsey & Company, and EY. Before becoming a consultant, he worked as a software developer, architecting and implementing cyber security tools for the U.S. defense and intelligence communities. He also served as a cyber security officer in the U.S. Army.



Ayelet Kutner

Chief Technology Officer

Ayelet Kutner is the Chief Technology Officer and General Manager of At-Bay's Tel Aviv office, leading the R&D, Product, Data Science, and Cyber Research teams. With more than 15 years of experience in the network security field, she was previously VP of Engineering at Forescout Technologies and Head of Platforms, SMB, and Industrial Control Systems Products at Check Point Software Technologies.

Eric Murphy

Senior Actuarial Manager

Eric Murphy is the Senior Actuarial Manager of Pricing at At-Bay, where he oversees the maintenance of the company's pricing model and overall program profitability. He previously worked at Esurance, an Allstate company, where he led a team of actuaries to develop pricing strategies intended to drive long-term profitable growth and improve customer experience.

Ido Lev

Cyber Research Team Lead

Ido Lev leads the Cyber Research team at At-Bay. He previously served as a cyber researcher in the Israeli Defense Force where he utilized his cyber knowledge and big data technologies to defend the IDF networks and detect anomalies.

Matt Actipes

Actuary

Matt Actipes is an Actuary at At-Bay specializing in cyber products. He has over 7 years of pricing and predictive modeling experience in property and casualty insurance, with a focus on personal and commercial lines. Prior to joining At-Bay, Matt worked for Nationwide, as well as Allstate Insurance.