Zivver

EBOOK

Outbound Email Security Best Practices

Measuring the Effectiveness of your Email Data Leak Prevention

Table of Contents

Introduction

Sending sensitive data such as financial information, customer records, patient details or intellectual property to the wrong person could spell disaster for your company. An incorrectly addressed email could result in significant fines, bad publicity, brand reputation damage and customers moving to your competition due to a lack of trust in your organization.

Protecting sensitive and confidential data is critical to the success of your organization.

Organizations using Zivver prevent sensitive information leaks due to senders trying to:

- Send emails addressed incorrectly,
- Attach the wrong files to an email,
- Copy an unnecessarily wide audience, or
- Send unencrypted messages and attachments that could be intercepted in transit.

As well as implementing outbound email security to prevent data leaks, it is critical that organizations constantly monitor the effectiveness of the measures they put in place to ensure they are continually protected.

Insights for Zivver Secure Email provides administrators and security experts with visibility allowing them to monitor user adoption, verify the security awareness of their employees, assess how often users are adopting recommendations, and determine whether securing emails is affecting the email open rate by receivers. Overall, Insights helps administrators determine how successful their Zivver Secure Email implementation is in protecting against email data leaks and advises where administrators can make continuous improvements.

Without this level of visibility, it is challenging for administrators to determine user adoption and where they can make configuration improvements. Constant monitoring of the solution's effectiveness means that changes in business requirements can be detected and addressed quickly - whether particular users are suddenly sending out more sensitive information or other changes in the business that security administrators need to address.

This eBook provides Zivver Secure Email administrators with best practice guidelines to help them optimize their email data leak prevention strategy.

Insights for Zivver Secure Email

There are several key areas that we need to consider when looking at how well Zivver Secure Email is protecting against email data leaks:

- Do we have sufficiently high user adoption?
  If all users that we'd expect to be sending sensitive information are not doing so securely then there is an increased risk of a data leak compromising confidentiality.

- Are users protecting their sensitive emails effectively?
  An email data leak prevention solution is only effective if users follow security recommendations involving sending sensitive information.

- Is sensitive information being secured using strong second-factor authentication?
  Users should use the strongest authentication method possible to ensure that only the intended recipients can access emails.

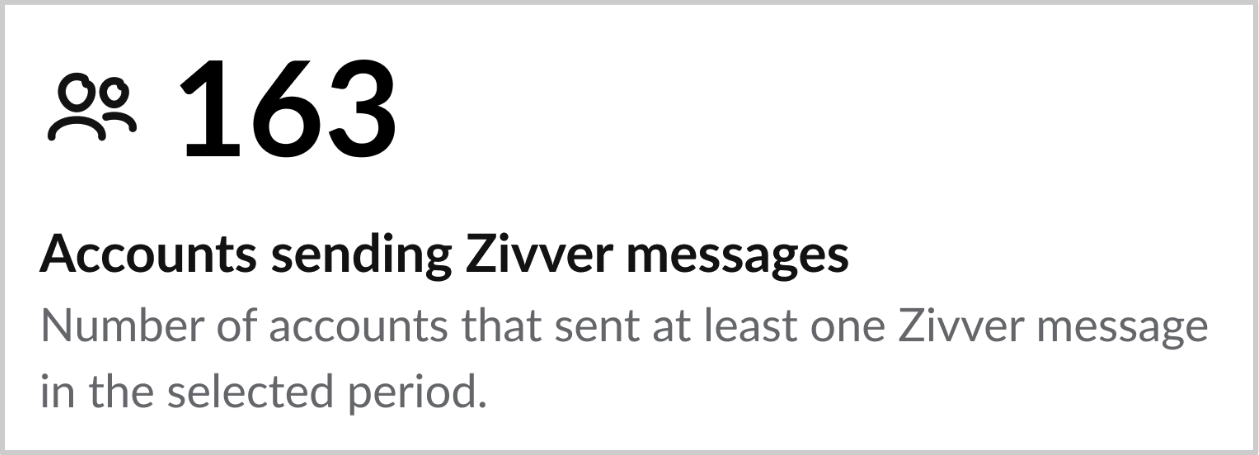
- Are email open rates affected?
  It is important to ensure that email usability is not negatively affected and that recipients are comfortable opening secure emails.

- What type of information is Zivver flagging as sensitive?
  It is important to ensure that the types of information Zivver flags matches what is expected based on the company's business operations. For example, if we were a bank, we would expect to see Zivver flagging a lot of emails containing financial information.

Let's now look at how we can use Insights to monitor the ongoing effectiveness of our email data leak prevention to prevent email data leaks.

Assessing User Adoption

The first step in determining whether Zivver is effective is to assess the number of users sending messages via Zivver. The dashboard in Figure 1 shows us that 163 users have sent at least one secured message in the period in question.



163

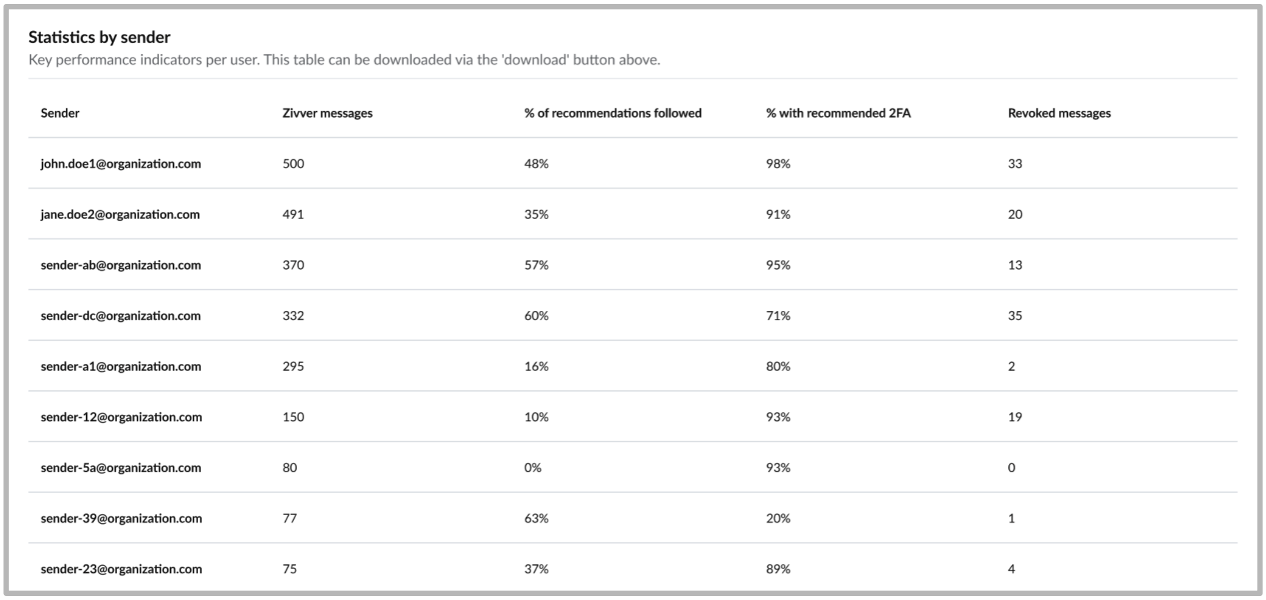
Accounts sending Zivver messages

Number of accounts that sent at least one Zivver message in the selected period.

Figure 1: Dashboard showing the adoption of Zivver to send messages

While this is a useful indicator of how many users have used Zivver in the chosen timeframe, we can't use it in isolation. We need to determine how many users *should* be sending secure messages, which may not be as simple as saying "all of our employees." We need to consider how many employees have access to sensitive data and therefore *could* cause a data leak by sending it out via unsecured email.

If the number reported in our dashboard matches the number of employees we expect, we should still drill down to ensure that all of the right employees we anticipate are on the list.



Statistics by sender

Key performance indicators per user. This table can be downloaded via the 'download' button above.

Sender	Zivver messages	% of recommendations followed	% with recommended 2FA	Revoked messages
john.doe1@organization.com	500	48%	98%	33
jane.doe2@organization.com	491	35%	91%	20
sender-ab@organization.com	370	57%	95%	13
sender-dc@organization.com	332	60%	71%	35
sender-a1@organization.com	295	16%	80%	2
sender-12@organization.com	150	10%	93%	19
sender-5a@organization.com	80	0%	93%	0
sender-39@organization.com	77	63%	20%	1
sender-23@organization.com	75	37%	89%	4

Figure 2: Dashboard showing sent message details by sender

Figure 2 shows a breakdown of our email users and how many Zivver messages they have sent.

If all the users shown in this report match the list of employees who could email sensitive information, then we can be confident that we have a good degree of user adoption within the organization.

Next, it is important to consider the number of messages they have sent. If, say, a user has only sent a few Zivver messages and we'd expect them to send more, there may be a need for additional awareness training. This also applies to the users we'd expect to see who don't appear in this report at all.

Over time, we'd expect user adoption to grow as employees learn the kinds of information that they should send securely. Figures 3 and 4 show how the number of accounts and messages suddenly increased in January and then stabilized. This stabilization indicates users becoming comfortable using Zivver to protect their messages.

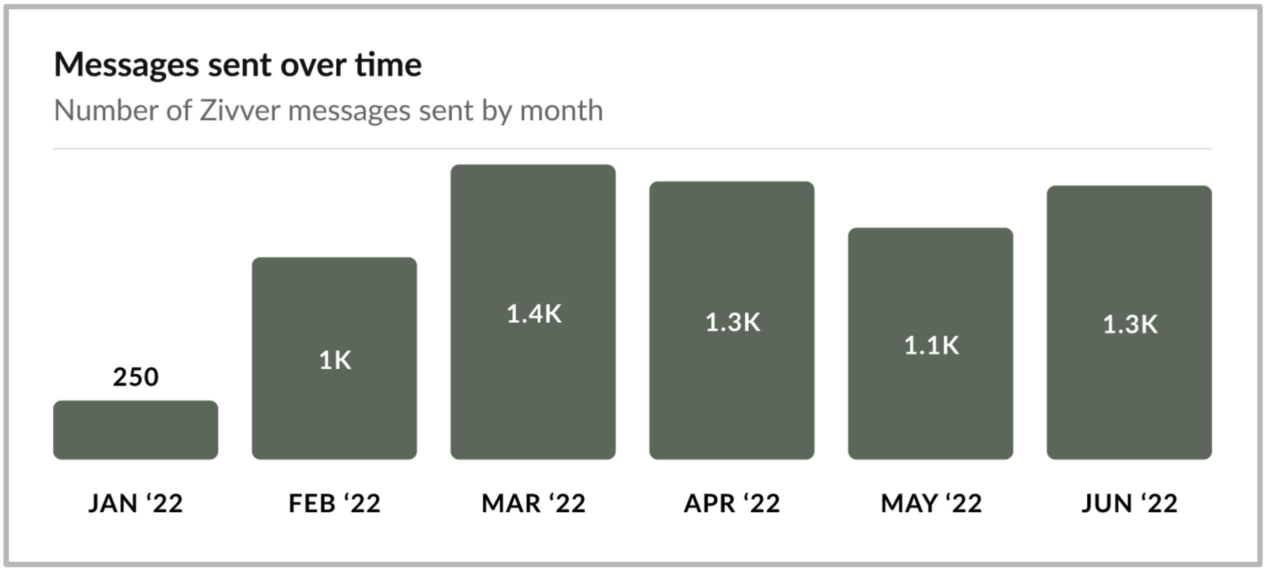


Figure 3: Dashboard showing Zivver messages sent per month

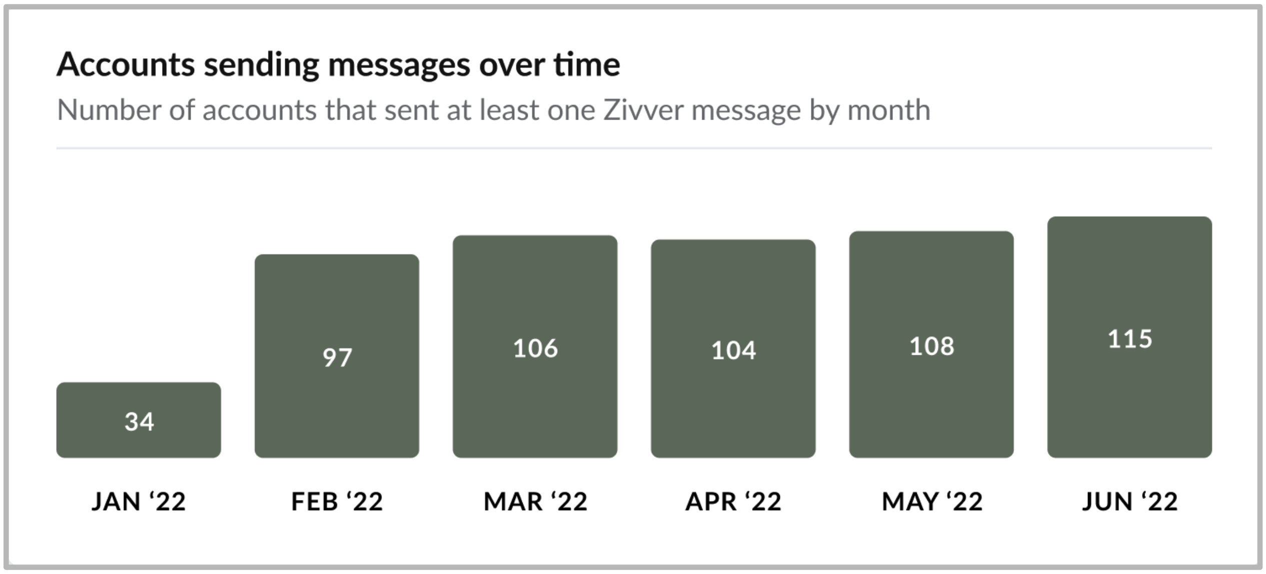


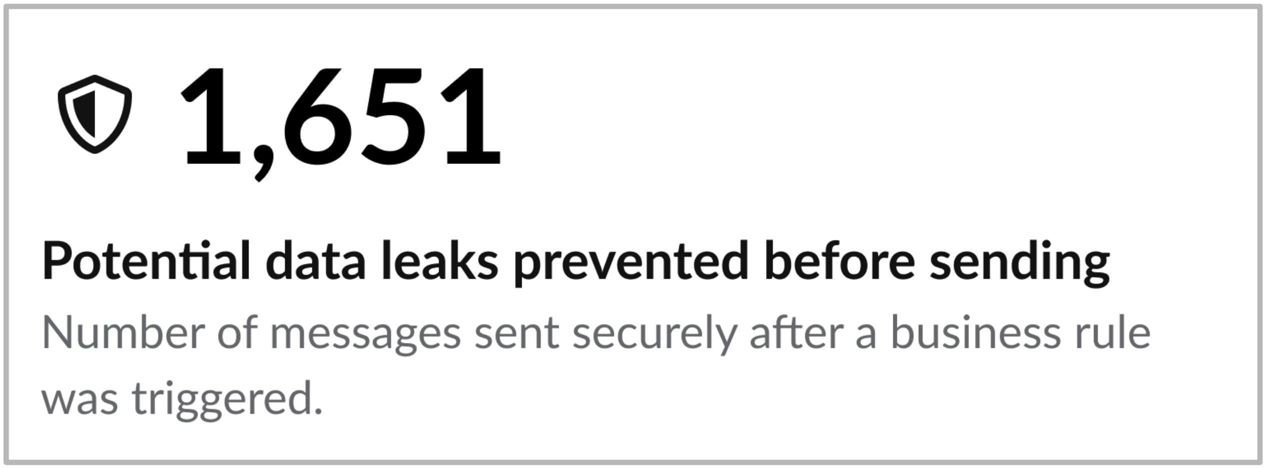
Figure 4: Dashboard showing Zivver users per month

Even though user adoption has stabilized, it is crucial to monitor these two dashboards regularly. We need to ensure that the numbers in these dashboards only change when the business changes. Business changes may include users may become complacent and ignore security recommendations, changes in business requirements may mean that a group of users suddenly start sending out sensitive information, or a significant number of new employees may join the company.

Employee Security Awareness

Once we are confident that user adoption is at the right level for our organization, we can start reporting on how successfully we are preventing data leaks.

The first thing to look at is how many messages users have sent securely after their email draft has triggered a business rule warning of a potential leak. Figure 5 shows users sent 1,651 messages securely after the user received a recommendation, thus preventing a possible data leak.



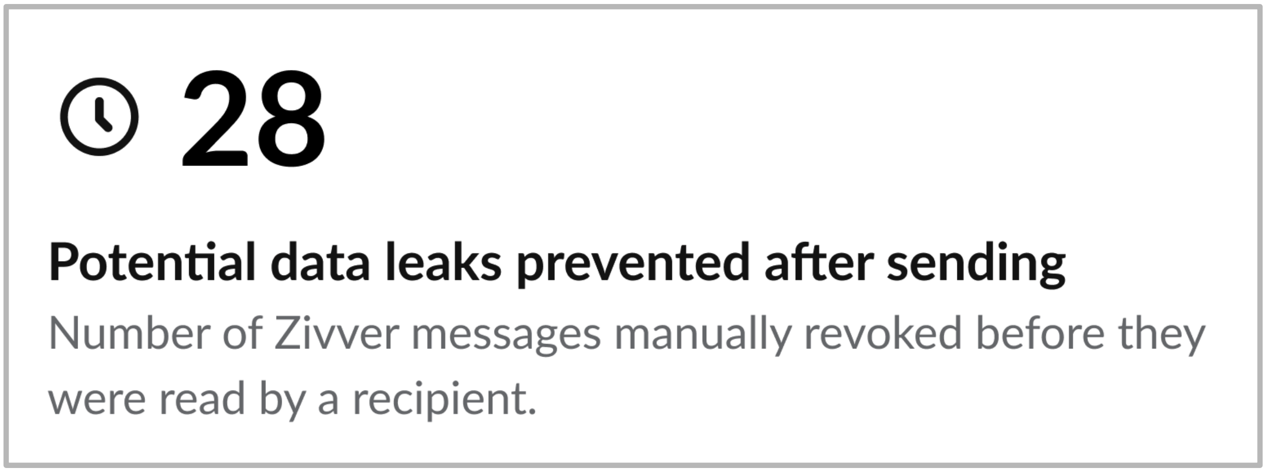
1,651

Potential data leaks prevented before sending

Number of messages sent securely after a business rule was triggered.

Figure 5: Dashboard showing the number of potential data leaks prevented before sending

In addition, users may realize that they have sent an email in error either due to the compromised content falling outside of the business rule detection or because they chose to ignore business rule recommendations and subsequently changed their minds. In these cases, if the recipient hasn’t opened the message, the sender can prevent it from being read by revoking it. Figure 6 indicates that 28 messages were successfully revoked thus preventing potential data leaks.



28

Potential data leaks prevented after sending

Number of Zivver messages manually revoked before they were read by a recipient.

Figure 6: Number of leaks prevented as a result of the sender revoking an email

Together, the number of potential data leaks prevented before and after sending metrics (Figures 5 and 6) indicate how well we have configured our implementation.

When considering revoked messages, we should also look at the number of messages that recipients opened before the sender revoked them and how this metric changes over time. In Figure 7, we can see that the number of revoke attempts and the percentage of successfully revoked emails (i.e. those that senders revoked before recipients opened them) is increasing. It is important to monitor this dashboard on an ongoing basis. If the number of unsuccessfully revoked emails starts to grow, it could indicate that employee security awareness is low and that the organization needs to implement additional measures such as user training and optimization of the business rules.

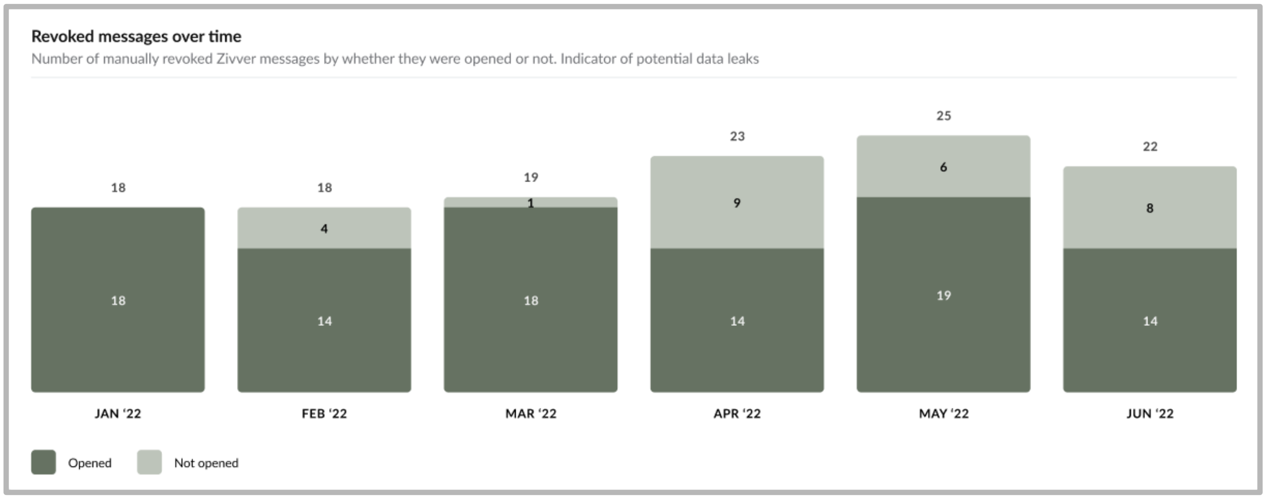


Figure 7: Success of messages revoked over time

This, along with drill-down data available in the Zivver communication logs, is critical to show auditors and authorities how successful the procedures we have in place are to help protect against email data leaks.

Are Users Following the Rules?

As well as considering user adoption and the effectiveness of the solution, it is essential to consider what kind of sensitive information users are sending, how often it triggers business rules and whether senders are adopting the recommendations.

Using the dashboard in Figure 8, we can track the percentage of recommendations followed after a business rule has been triggered. While this may vary slightly over time due to business conditions changing, we need to watch out for and investigate any major changes.

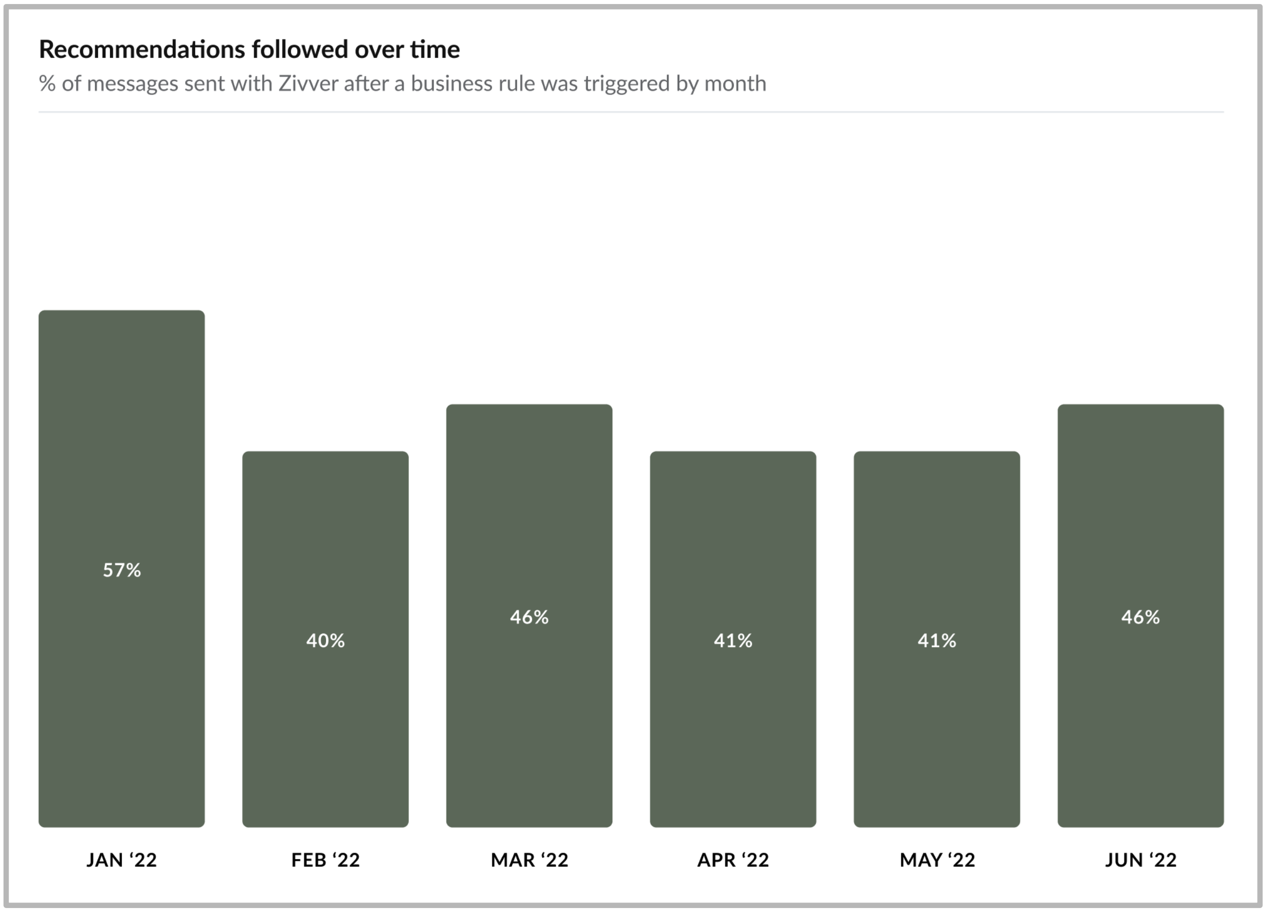


Figure 8: Percentage of recommendations followed by users.

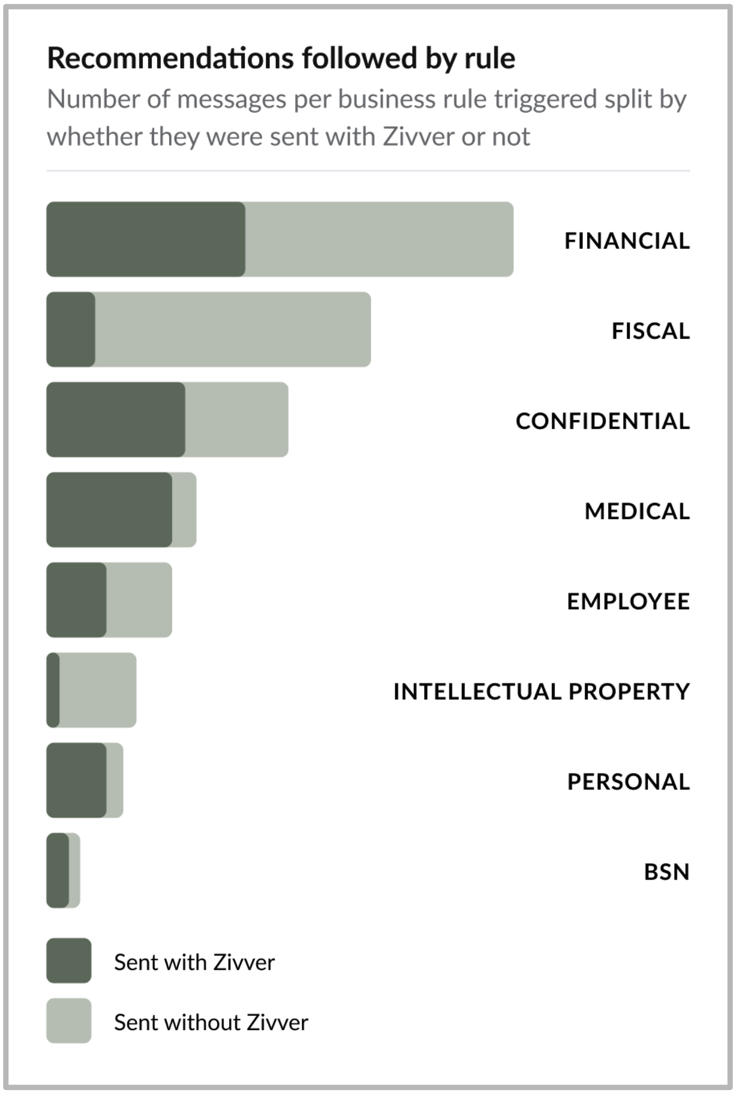


Figure 9: Recommendations followed based on business rules triggered

Figure 9 shows the split of the types of messages triggering a business rule. It also shows us the portion of messages sent normally or with Zivver. By comparing this graph with our organization's digital security priorities, we can assess whether we are adequately protecting our sensitive information.

For example, if we have a requirement to protect medical data but are less concerned about protecting intellectual property, then we don't need to worry as this report clearly shows that a larger proportion of medical data is being sent securely with Zivver. However, if we were interested in protecting intellectual property then further investigation would be necessary. We may want to fine-tune the business rules or provide additional security awareness training to our end users.

Receiver Verification

Emails sent using a Zivver account are always secured using 2 factor authentication (2FA) to ensure that only authorized persons access the information.

When users send emails to guests without a Zivver account, additional verification is required. The sender sets up verification using an SMS with the recipient's mobile number, an access code that is agreed ahead of time or an email that they send to the same email address as the notification. Figure 10 shows a breakdown of the different verification methods used to send messages to guest recipients.

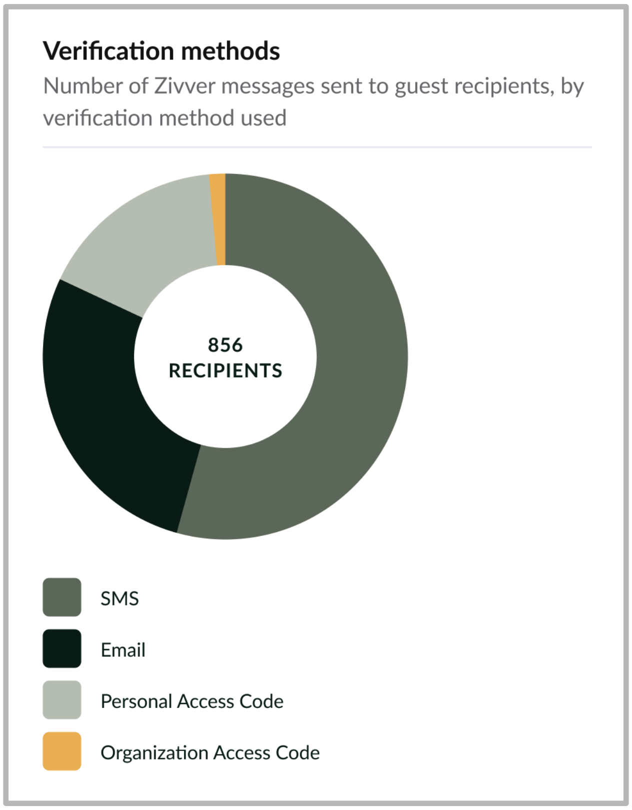
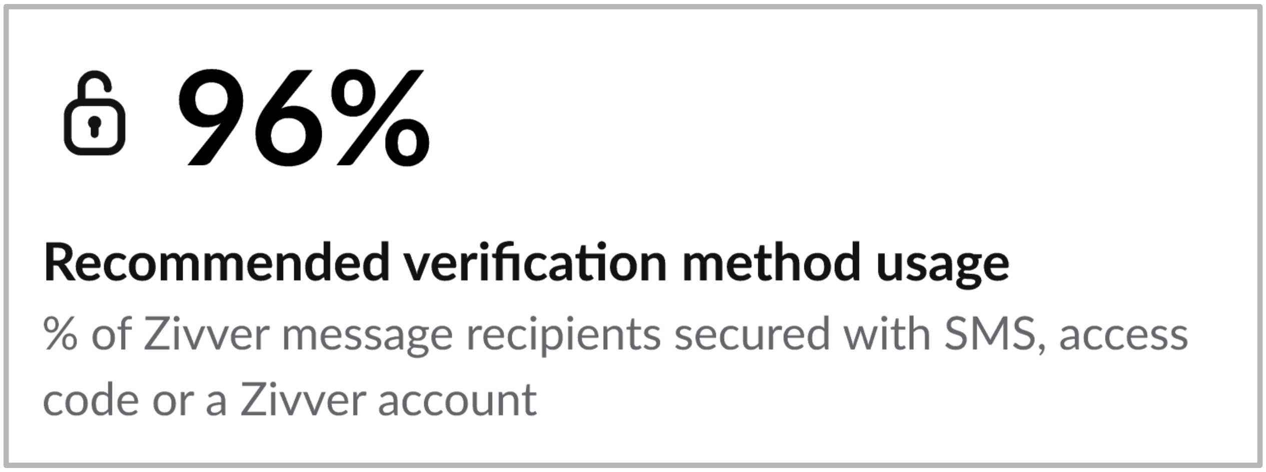


Figure 10: Breakdown of different verification methods used to send to guests recipients

Zivver recommends using either SMS or access codes as using email is a two-step rather than two-factor verification method. It is, therefore, less secure and considered less user-friendly by recipients resulting in them opening fewer emails.



96%

Recommended verification method usage

% of Zivver message recipients secured with SMS, access code or a Zivver account

Figure 11: Percentage of recipients verified using recommended verification methods

The dashboard in Figure 11 shows us the percentage of Zivver message recipients secured using our preferred secure verification methods of SMS and access code. Figure 12 shows this statistic over time so we can monitor any significant changes in the trend of recommended verification methods being used.

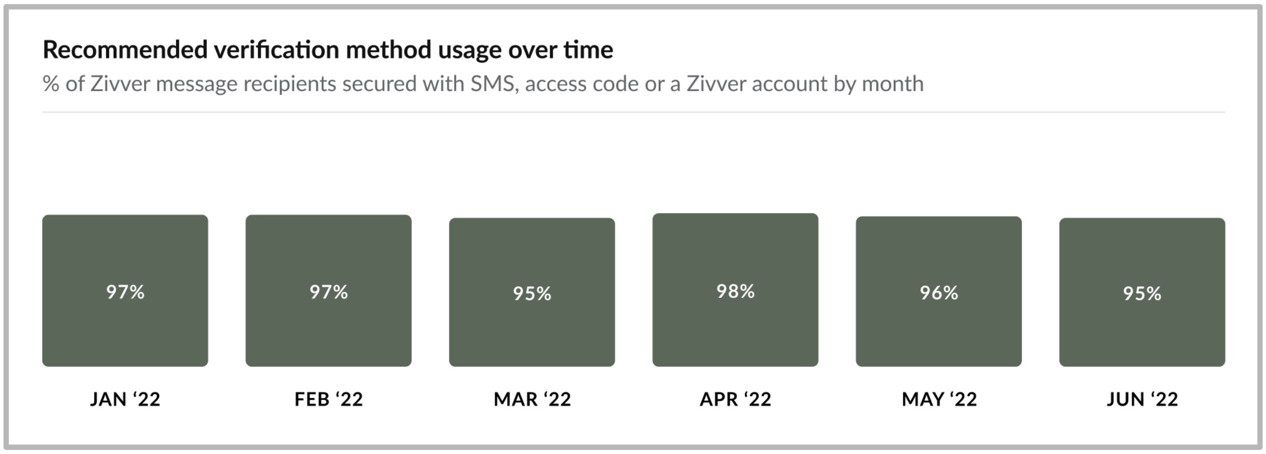


Figure 12: Recipients verified using recommended verification methods over time

To improve on this metric and thus reduce the risk of an email data leak, we can examine the Statistics by Sender (Figure 2) and Top Recipient Domains (Figure 14) dashboards.

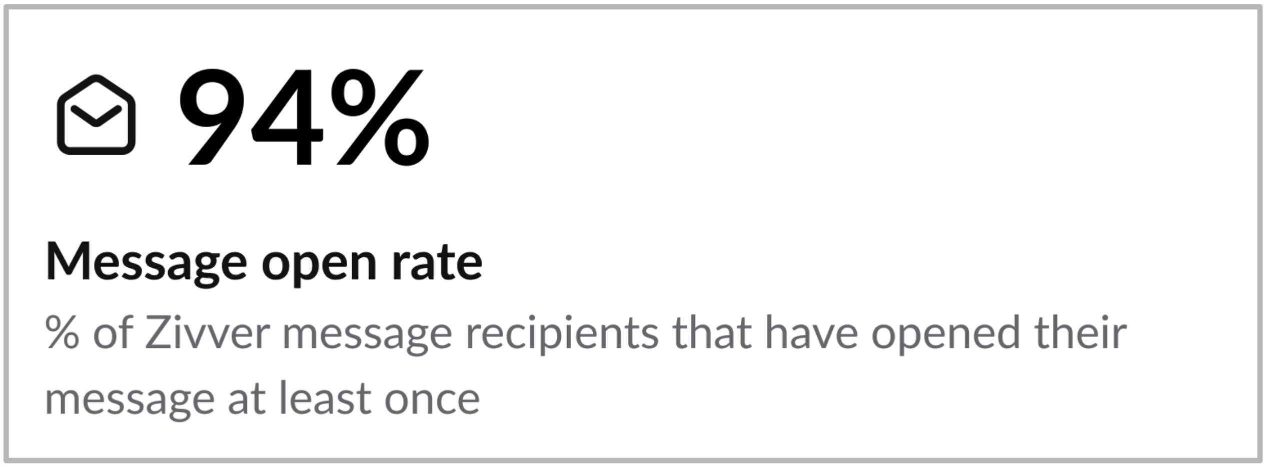
By examining the percentage of emails sent using the recommended 2FA methods broken down by sender (Figure 2), we can quickly identify the users that don't use the preferred method to investigate why not. Using this information, we can work with individual employees to increase their security awareness so they understand the importance of using 2FA to ensure that only authorized users can access sensitive emails.

Similarly, the breakdown by recipient domains (Figure 14) highlights which organizations we send to without using the preferred 2FA methods. For domains with a low percentage, this could be because there are no adequate processes in place to either obtain mobile phone numbers for individual recipients or to communicate access codes. In these cases, we need to work with the receiving organizations to implement these measures to prevent unnecessary email data leaks.

If we decided that email verification was adequate to verify recipients based on the sensitive information we want to protect, we could use exported data to report on how well individuals or teams are protecting their email communications.

Message Open Rate

It is important to ensure that sending secure emails using Zivver does not deter recipients from opening them. Insights tracks the message open rate so that we can verify that they are not negatively impacted.



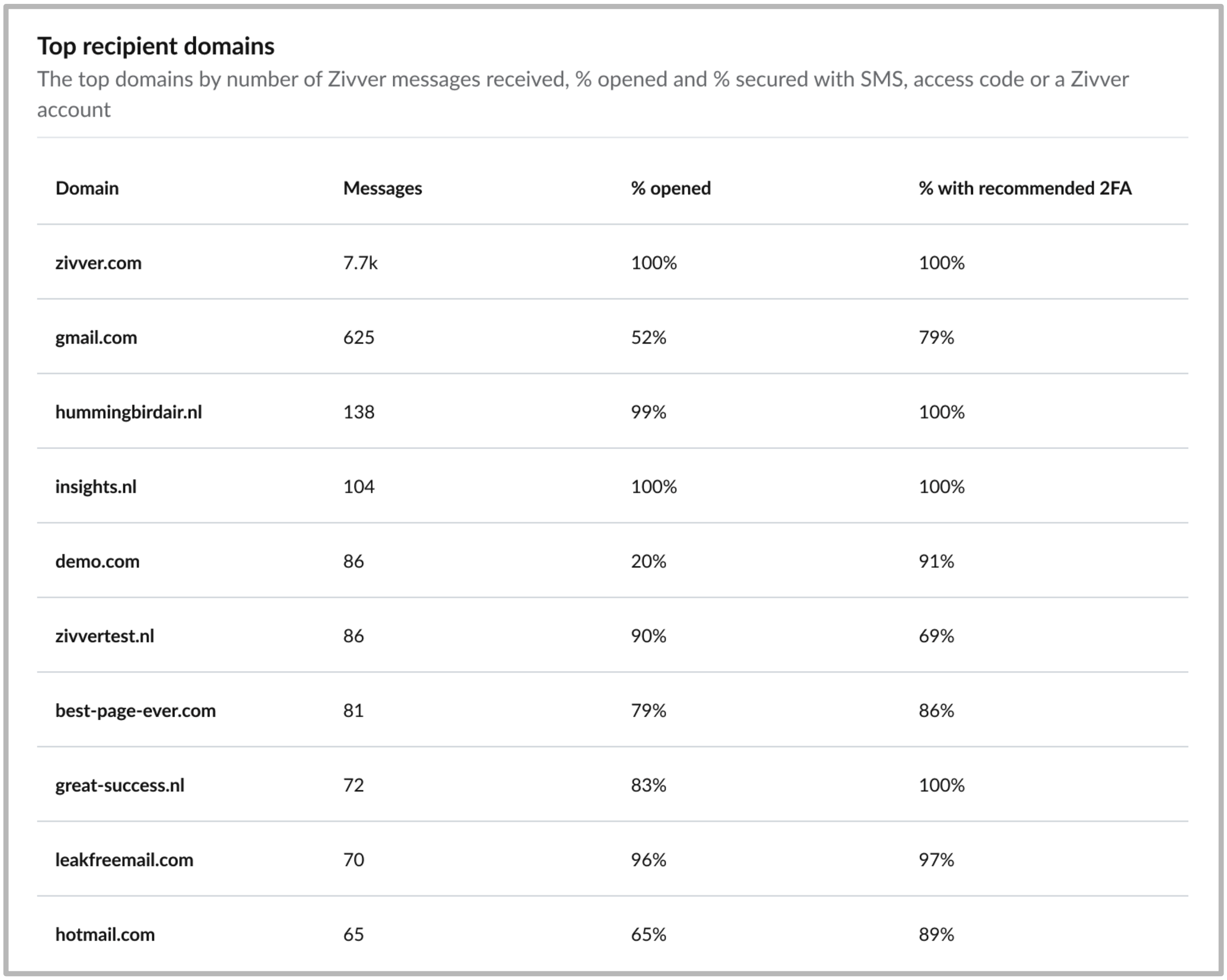
94%

Message open rate

% of Zivver message recipients that have opened their message at least once

Figure 13: Percentage of recipients opening secure emails

Figure 13 shows that recipients have opened 94% of messages at least once. This number is high compared to the best practices average of 75%, so it should not concern us. However, this percentage might differ for your organization depending on your recipients. If it is significantly lower, we will need to use other dashboards to determine if particular users are not reading the emails - for example, users from specific domains or companies (Figure 14). Using this information, we can determine how to address the issue.



Top recipient domains

The top domains by number of Zivver messages received, % opened and % secured with SMS, access code or a Zivver account

Domain	Messages	% opened	% with recommended 2FA
zivver.com	7.7k	100%	100%
gmail.com	625	52%	79%
hummingbirdair.nl	138	99%	100%
insights.nl	104	100%	100%
demo.com	86	20%	91%
zivvertest.nl	86	90%	69%
best-page-ever.com	81	79%	86%
great-success.nl	72	83%	100%
leakfreemail.com	70	96%	97%
hotmail.com	65	65%	89%

Figure 14: Report showing the percentage of opened emails by recipient domain

File Transfer Usage

Zivver enables users to address the file size limitation imposed by traditional email systems, which is often as low as 25 MB. Zivver allows senders to securely send up to 5 TB directly from their email client without using a third-party file transfer website.

Using the dashboard in Figure 15, we can see how many attachments of a particular size Zivver has sent securely. If we expected the number of emails containing attachments to be higher due to the nature of our business, we would need to investigate further by examining individual senders (as shown in Figure 2). We may find that, for example, employees are using third-party file transfer websites instead. These alternatives may not be secure enough to protect our sensitive data and are more difficult to control and audit.

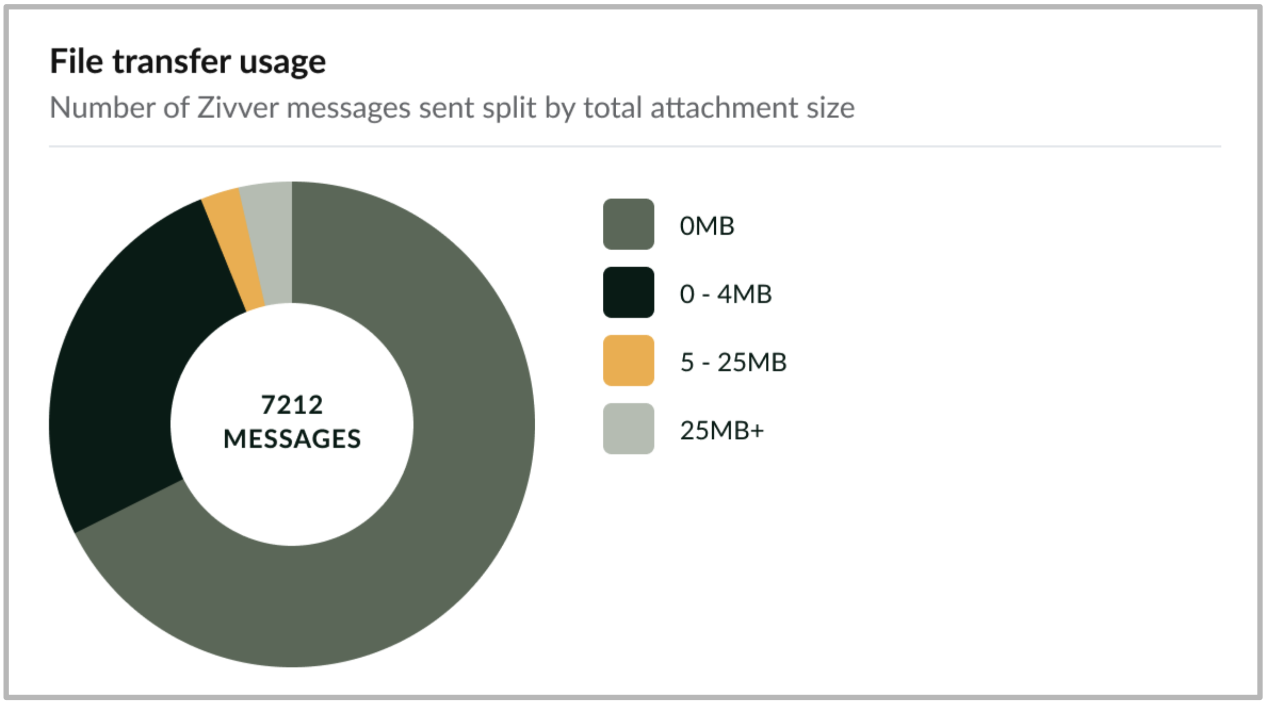


Figure 15: Number of emails sent by attachment size

Answering Questions with Flexible Reporting

As well as out-of-the-box reports, Insights allows us to answer questions from senior management and auditors specific to our organization.

For example, rather than just analyzing the sending patterns of individuals as in Figure 2, we may be asked to assess the level of adoption or security awareness of a department, such as accounts, as they have access to specific sensitive information that we want to ensure is handled securely.

Insights provides a high degree of flexibility by allowing us to export the data for further manipulation and analysis. By combining Insights data with our employee records, we can produce granular, team-level reports to answer questions unique to our situation. In addition, we can share this information with relevant internal groups using access controls via our preferred business intelligence solution, such as PowerBI.

Summary

Implementing Zivver Secure Email enables us to protect sensitive data such as financial information, customer records, patient details and intellectual property, by preventing such information from being shared incorrectly via email causing unnecessary data leaks. Insights provides us with visibility to continually monitor the effectiveness of secure email and fine-tune our implementation to ensure ongoing protection.

It also allows us to answer questions from senior management and external auditors about the effectiveness of our email data leak prevention strategy.

In this ebook, we discovered the best practices we should adopt to monitor and fine-tune our data leak prevention implementation to ensure that we remain protected.

By using Insights with the best practice recommendations, we will remain in a strong position to ensure that we not only protect our organization but also can prove that we have implemented a strong email data leak prevention strategy.