SECURE YOUR EVERYTHING™

The Importance of a Complete Data Loss Protection Service

Executive Summary

- Data breaches are becoming ever more expensive both in terms of the number of lost records and loss of customer trust.
- In order to fully protect against data leakage, enterprises need to implement comprehensive phishing protection and customizable data leakage protection options.
- Complete data leakage protection will include full suite protection, with DLP policies also applying to collaboration and file sharing apps.

In today's business environment, data is a form of currency. Data is used to build better products, to improve processes, to serve customers better. The more data you can obtain and properly deploy, the better off your business will be.

Hackers know that where there is access to data, money will follow. In fact, according to a report from IBM, the average total cost of a data breach has increased by nearly 10%, rising from $3.86 million in 2020 to $4.24 million in 2021.

As companies harness more and more data in the course of their daily operations, the cost of a data breach—both in reputation and in finances—becomes even more damaging.

This report will discuss the importance of data loss protection; why hackers find data so valuable; and how to best secure your most important asset.

Why Data is an Ideal Target for Hackers

Data is everywhere. Healthcare organizations hold reams of patient data, whether it's basic information like addresses and social security numbers, to more private forms of data like sensitive medical information. Schools hold student data, from test scores and allergies, behavioral reports and family histories. Many companies, at the least, hold names, email addresses and credit card information.

When users hand over this data, there's an expectation that it will be safe, that it will be only for the intended audience, that it will not get into the hands of hackers.

Unfortunately, that's not what happens. Data breaches are happening at a frightening velocity. Recently, the financial trading app Robinhood had five million email records exposed in a breach; a breach at the California State Controller's office meant hackers had access to 9,000 social security numbers of state employees; a breach of a VPN provider resulted in 300 million records being available.

Whenever a company holds data, there is a chance for a breach. And since companies continue to hold valuable data of all kinds, it is becoming more costly. Data breaches cost, on average, $4.24 million in 2021, a 10% increase over 2020, according to IBM. In 2017, the average cost was $3.62 million. The most common record lost was personally identifiable information (PII), included in 44% of breaches.

Hackers want this information because it pays. For example, according to a report from Comparitech, a stolen credit card number can go for $17.36 on the dark web. A stolen PayPal account can go up to $197.

The real jackpot, though, is medical records. According to Experian, a stolen medical record can go for up to $1,000.

In 2020, some 29 million healthcare records were breached. Plus, the average cost of a healthcare-related data breach was $9.23 million, the highest of any industry, and up from $8.13 million in 2020.

According to a study from Ping Identity, 81% of consumers would actually stop engaging with a brand after a breach.

Regardless of where the attack occurs, whether it's a LinkedIn hack that exposed up to 700 million user emails, or a 2018 attack on Marriott exposing sensitive information, the biggest victim is the end-user. In the first half of 2020 alone, over 160 million individuals were impacted by just 540 data breaches.

Because 96% of social engineering attacks are delivered via email, according to the Verizon DBIR, and because 20% of breaches start with compromised credentials, according to the IBM report, it's incredibly important to ensure that your email is fully protected. That includes stopping malicious emails before they reach the inbox so that users can't mistakenly click on them. It includes understanding and stopping credential harvesting attempts, and knowing when someone is trying to get access to the most personal data.

It also means understanding where data flows. This may be different for different industries. For example, some organizations may only share sensitive information via email; others may only share it via Microsoft Teams. Some may share it on a variety of platforms. Knowing where data is shared, and protecting those applications accordingly, is essential to keeping your users and your business safe.

Why Other Solutions Fall Short

Though not all breaches start via email, many do. In fact, some of the most costly forms of breaches have their origins in an email-borne attack.

The IBM report breaks down which types of attack methods lead to expensive breaches. The average cost of the following attack methods are:

- Compromised credentials ($4.37 million)
- Social engineering ($4.47 million)
- Malicious insider ($4.61 million)
- Ransomware ($4.62 million)
- Phishing ($4.65 million)
- Business Email Compromise ($5.01 million)

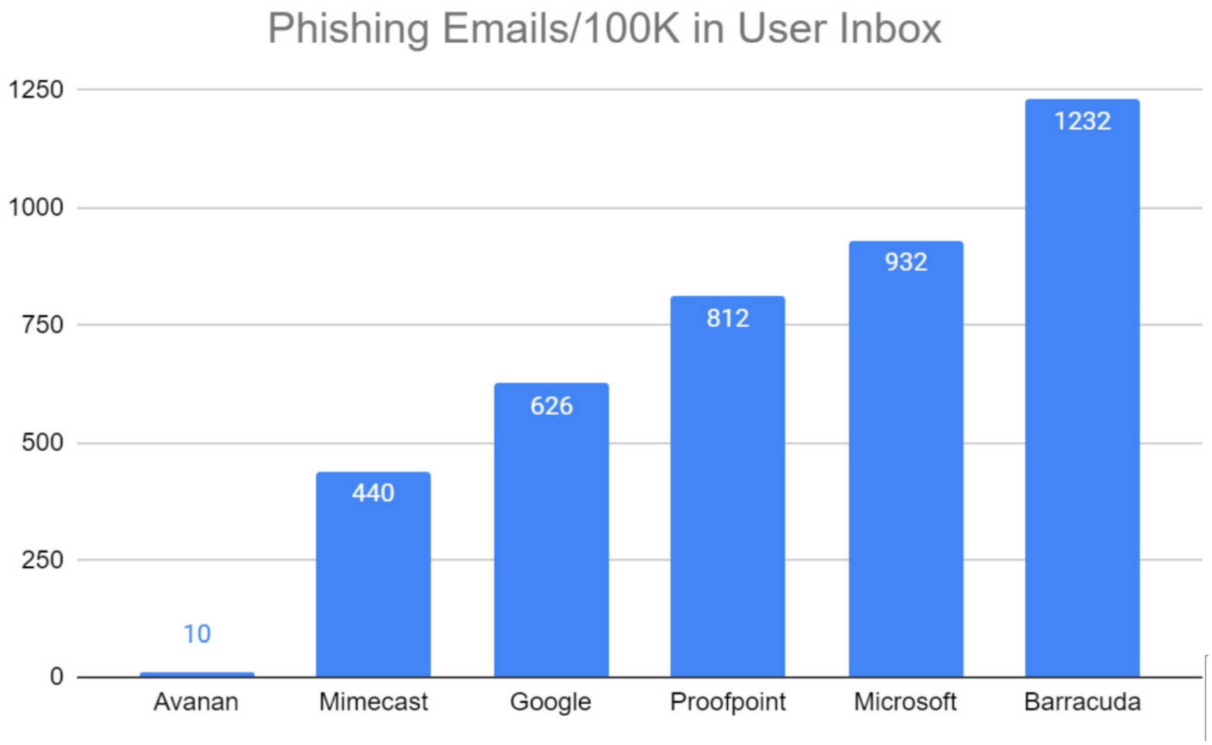
There are, of course, other forms of breaches. But these tend to cost (relatively) less. Consider::

- System error ($3.34 million)
- Physical security compromise ($3.54 million)

These are still damaging, but not quite as damaging as those that start via email. Plus, the most common forms of breaches resulting in data loss are compromised credentials (20%) and phishing (17%), according to the IBM report.

That means that in order to secure your enterprise from data loss, organizations have to secure email.

However, other solutions let far more phishing emails into the inbox. In a recent study, Avanan analyzed over 300 million emails to calculate the miss rates, or the number of phishing emails delivered into the inbox, of numerous email solutions:



That doesn't take into account other API-based solutions, which let all malicious emails into the inbox before remediating. On average, these solutions take three minutes and three seconds to remediate a malicious email yet the average user clicks in just 82 seconds. Given that the average phishing click rate is, according to some studies, as high as 25%, that means that when there are phishing emails in the inbox, someone will click.

To best protect against data breaches, an organization needs to install phishing protection that prevents the message from ever reaching the inbox.

How the Avanan Solution Works

Avanan's DLP solution is called SmartDLP. It is a powerful AI-driven engine that combines several DLP classification tools with both Avanan's machine learning and third-party pattern classifiers. It detects data patterns over email, files, attachments and text messages on collaboration. Any SmartDLP findings are processed by the standard Avanan DLP policies that generate security events and determine what actions to apply, such as adding to vault, encryption or blocking. Further, SmartDLP provides actionable insights on the security events that can be used during the investigation process.

SmartDLP comes with powerful default settings that are already tuned to your geography – United States, European Union, Canada, Australia, etc, and then allows you to configure your customer-specific policy with the set of DLP rules relevant to you, out of +100 available rule. Avanan uses cloud-native controls to enforce granular share policies for individual files or folders based upon their contents and context. Files can be deleted, quarantined, or encrypted before they become security incidents.

Organizations have the flexibility to choose which types of activity to monitor, such as PII or PHI. They can decide which action to take, whether it's blocking the email entirely or encrypting it for an authorized user. All matches and activities are easily accessible on the Avanan dashboard, including the ability to aggregate all detections of a specific rule into a single entry, for quick and easy analysis of potential threats.

Additionally, there's seamless integrations with other security engines offered on the Avanan Platform, including SmartPhish, providing organizations with a centralized, single-pane-of-glass view to all their security events.

Consider the story of the City and County of San Francisco. With a wide range of departments, all holding sensitive information, from social security numbers to health data, they needed a way to better improve their use of data protection and encryption. Within days of deploying Avanan, the city saw a 30% increase in the use of data encryption.

To do so, San Francisco and Avanan worked together to implement a custom policy and workflow. When users are properly encrypting and protecting data, they are rewarded for following proper security practices. If, however, a busy employee attempts to send sensitive data outside the city, they are stopped and given notice. An alert will say, "Did you mean to send this medical file unencrypted?" In order to take a risky action, users must make an active decision. This both prevents unintended data loss and offers a valuable reminder at the right time.

Consider also the story of one of the largest hospitals in the United States. They are frequent users of Microsoft Teams. The most common security event in this environment for this hospital is DLP.

We found that doctors tend to share patient medical information with no limits on the Teams platform. Medical personnel tend to know the security risks and rules of sharing information via email. On Teams, however, they tend to ignore those rules.

In one extreme case, we identified a Teams channel with roughly 250 end-users many of them using email addresses outside the hospital's domain. On this channel, sensitive information is continuously shared. In one case, medical information, procedure status and the family circumstances of a minor were shared, along with name and social security number.

Conclusion

When considering an email security solution, it is important to consider its capabilities regarding data loss protection. That means evaluating its ability to create custom workflows and policies, and that leverages AI to learn an organization's system. It also means ensuring that the solution has DLP at all. Not all API-based email solutions offer a DLP program. That means that organizations either have to integrate a separate DLP product or go without one. Instead, organizations should choose a comprehensive solution that integrates with all of your existing security; a solution that is customizable and easy-to-use; a solution that keeps data flowing without it ending up in the wrong hands. It means protecting all places where data lives. If you are protecting data in email but not in collaboration or file sharing, your data is not truly protected.

Data loss can come from anywhere. It can be the result of a rogue employee taking data. It can come in the form of an accidental share or somebody mistakenly including sensitive data attached to an email or other message. It can also be in the form of a hack, whether it's ransomware or a simple credential harvesting attack. When a company loses data, that company loses consumer trust. Further, end-users are getting the short end of the stick by having valuable personal data exposed and sold on the dark web. That has lasting consequences, including credit card, medical or tax fraud.

As the price of data breaches increase for companies, it's essential to implement a data loss protection solution that not only secures all avenues of communication but does so with flexible and customizable workflows, one that's driven by artificial intelligence and machine learning and can work to ensure that the sensitive data that drives your business stays within your business.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com