PineApp

Common email security headaches and how to avoid them

Contents

The problem 3

The solution 4

Common security challenges and solutions 5

- Scenario one 5
  - How it works now
  - How it should work
- Scenario two 7
  - How it works now
  - How it should work
- Scenario three 8
  - How it works now
  - How it should work

Get the Best Email Security Solution Around 11

Common email security headaches and how to avoid them

Email is still the fastest, most effective, and widely used method of business communication today. Businesses continue to use it to communicate across the globe in a matter of seconds and connect with professionals in virtually any location, opening up a world of opportunity and possibility. But along with this opportunity comes risk. As an organization's geographic distribution expands and they begin to rely on an ever increasing spectrum of business applications, the greater the security threat becomes.

As a professional in charge of the security of your corporation's communications, your job is to protect your company from email security threats by choosing an effective defense. When it comes to email security solutions today, the options appear to be limitless. There are a staggering number of products on the market that promise to solve just about every corporate email security concern through features like anti-spam protection, anti-virus capability, zero-hour detection, and in some cases, advanced threat remediation options.

A close inspection of all the product options reveals that many are virtually identical, and it is difficult to determine what sets one solution apart from all the others. In addition to the standard features and services each solution offers, some companies promote features that do not seem to directly relate to email security issues. It is challenging to know which details and features are necessary and which are just extras.

Before choosing an email security solution that will be the most appropriate and effective option, you must be aware of all the challenges facing your company with regard to securing email. The problem is that the security risks you face are growing and changing just as fast as your company. New threats are developing every day, and you need a solution that can adapt and defend effectively.

This white paper will present several common email security threat scenarios businesses face today. It will also discuss why the most effective solution should be flexible enough to adapt to your company's evolving needs. Finally, it will present PineApp Mail Secure as an ideal solution for both enterprises and small and medium-sized businesses.

How can you choose among a staggering number of similar email security products?

The problem

Every business needs email security. Just about every product out there offers, at the very least, functional anti-spam and anti-virus solutions, but this is not enough. Many modern businesses are increasing their reach geographically and opening communication in every direction. There are employees working from home, business being conducted remotely, and national and global partners thousands of miles away. In between these long distance communicators are countless cybercriminals, government spying programs, and security threats using more than just spam and viruses to exploit vulnerabilities and steal your data.

Companies are conducting business using a variety of technology and applications, not all of which are easily compatible with each other. When you open up communication with other companies your strategies may not always sync up in a way that promotes secure email. Each business chooses email solutions, such as Office 365, according to its unique needs. Even if you think you have a secure plan in place, you cannot say the same for those on the other side of your communication. Data leakage has become an ever-present threat.

Within your own company there are probably numerous applications working side by side with your email, and these can also create incompatibilities and cause potential vulnerabilities in your security. One of the biggest changes sweeping the business world today is cloud technology. More and more companies are shifting their IT infrastructure and business applications to the cloud, which creates a whole new set of security concerns to address. You may be working solely with local hardware, entirely in the cloud, or using a combination of hardware and virtual platforms according to your business needs.

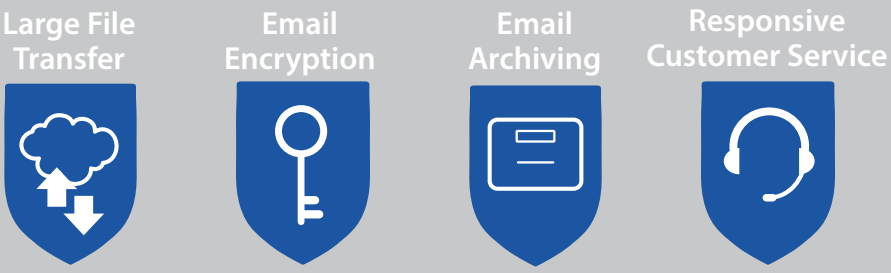
What you need is an email security solution that can adapt quickly to your changing business environment and grow with your needs to keep you protected no matter what direction your business moves in next. Your email security solution should be able to protect on- and off-site resources and manage compliance and regulatory requirements should they be necessary. You need something much more than just a run-of-the-mill email security solution.

The solution

Email programs like Office 365 protect against basic threats that come along with email, but security is not their focus. You need to put supplemental security and services in place which will keep your information safe in the face of more severe threats. This is where those seemingly extraneous features offered by some of the more capable email security solutions come in handy.

At first it may seem like large file transfer, email encryption, email archiving, and responsive customer service are outside the realm of necessary email protection. When you explore the problem more closely you will see that these features are actually vital components to a comprehensive messaging solution for your business. What they do is expand the capabilities of your business itself, providing effective and secure Web portals for collaboration, protecting your outgoing messages, preventing you from exposing your business to the dangers of third-party archiving storage, and make troubleshooting in the event of a problem a simpler and less stressful process for your IT department.

These additional features give an email security solution the flexibility it needs to adapt as your company grows and changes. With these security precautions working in sync your professional communication will be guarded from every side possible, on premises and in the cloud, and your business processes will be streamlined to promote growth.



Extraneous? No. Vital to a comprehensive solution for your business

Common security challenges and solutions

The business world is filled with many different kinds of companies, but when it comes to email security they all face similar challenges. Furthermore, most companies suffer from the same inadequate solutions that cause frustration, complication, and extra cost. The following scenarios are examples of a few common communication security problems that plague professionals today, along with the solutions generally offered by a commonplace security solution. Each is followed up with details of all that a comprehensive security strategy can offer in safety and service.

1 Scenario one

It is common for businesses to work out of a number of locations across the country and around the world. For example, a business may have one office location in San Francisco and another one in New York. Collaboration between the offices is imperative to successful operations, and a large number of emails are sent back and forth on a regular basis. In these emails, employees often share files to get pertinent information, forms and other business data in the hands of those who need it. Sometimes, however, those files are too large to be attached in an email.

That is the problem facing a San Francisco executive in this scenario. She wants to send a large file to a colleague in the New York office, but internal company policy restricts the size of files that can be attached to emails. She needs a way to send her oversized file to New York that is at least as fast as email, while still being secure and compliant with company policy.

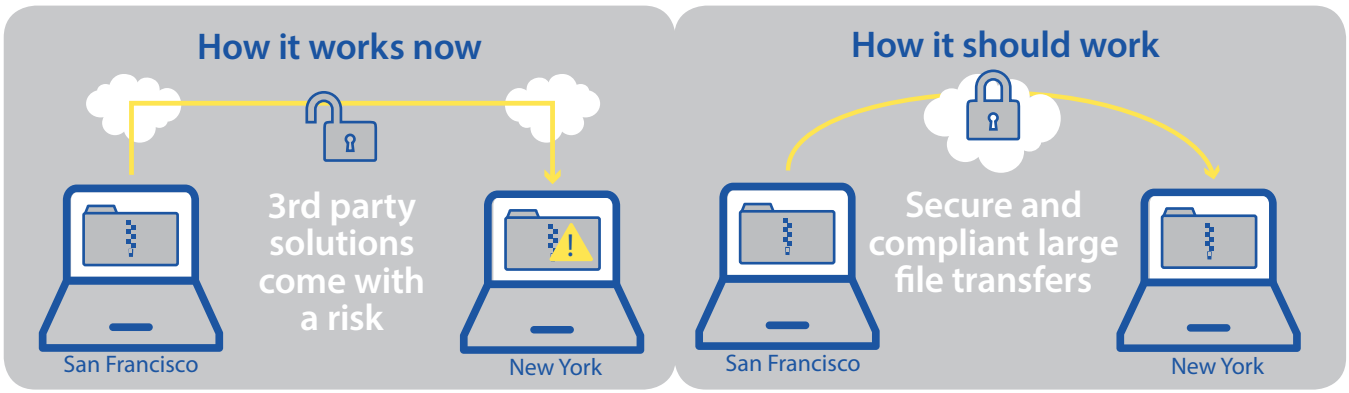
How it works now: If her company is like many today and does not have an effective, comprehensive communication solution, then she will have to rely on a third party option. The standard today is to have separate services for email, security, file sharing, and more, which means the executive has to take extra steps in order to complete her communication. She will have to open a different program outside of her email portal, upload the file, and then rely on someone else to send it where it needs to go.

A separate file transfer application has to be deployed across the whole company, and that means installing it and teaching everyone to use it. In addition, third party services can be a major security risk, as well as a problem in terms of compliance requirements. She is trusting the safety and privacy of her corporate information to people, equipment, and security outside of her control. Basically, the third party solution strategy comes with extra cost, extra risk, and extra complications that she does not need.

How it should work: If our San Francisco executive's company employed a comprehensive security solution, the whole problem would cease to exist. Effective email security should include large file transfer features that allow users to use the same Web portal they already use for other email management tasks, like white lists, black lists, and releasing email. The San Francisco executive could simply upload the file and send it directly and securely to her New York colleague. No need to run multiple applications and have a stack of windows open on her computer. She can keep things simple and efficient.

Her large files will have the same security protections as her email system even though they are not being sent via email. This type of solution should be entirely customizable, allowing for unique configuration to comply with applicable company policies as well as industry regulatory requirements. This will reduce her compliance concerns and provide more uniformity for her business processes. Additionally, she will not have to create yet another account and password for another service, and she will not be adding to her operations costs.

Mail Secure includes the Big Email Data Module, which lets users get around file size limits on email attachments. Large files can be sent and received securely — and will be available for as long as the sender indicates.



Scenario two

Regulatory compliance often requires companies to keep old data for a certain period of time. Email is a part of this data, and it can take up quite a bit of storage space. In an effort to reduce storage costs and hassle, an increasing number of companies are moving their email servers into the cloud. While this certainly does expand the storage capabilities and relieve stress on company hardware, it opens businesses up to increased risk of data leakage and theft. The business in this scenario needs to keep years of email data in order to meet company regulations. Not only must the archiving solution be compliant, but it must also be searchable and make it easy to respond to any litigation requests.

How it works now: Cloud-based email services like Office 365 are common email options used by businesses, and most email security solutions complement them to a certain extent. But when it comes to the extras like archiving, companies have to look outside of their existing solution to a third party provider in order to prevent journaling issues and complications. In fact, many businesses have a collection of third party vendors for each different service they need, cluttering up their processes and opening them up to incompatibility and security risks.

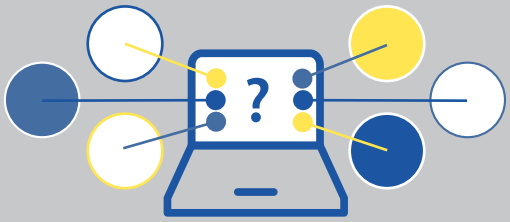
Working with numerous vendors to get the combination of services necessary can be expensive and frustrating. There can be little uniformity and consistency with professional processes because everything requires a different program and different steps. The business in this scenario needs archiving capability, but it does not need the added cost, frustration, and complication. Plus, the more separate parties there are with access to sensitive information, the higher the risk is of data leaks and threat exposure. This company does need increased archiving space and capabilities, but it does not need to rely on someone else to keep the archived mail and attachments secure.

How it should work: What the company in this scenario needs is a security solution that not only includes archiving, but can also integrate seamlessly with a cloud email solution like Office 365. A security solution that can work compatibly with cloud email prevents problems with user experience, so everyone can manage all of their email features like journaling in a single, central program. Even better, now the business does not have to rely on yet another outside party to store and protect archived emails and attachments.

Keeping that archived data secure is now a greatly simplified process, because the archive functionality is tied to the existing security solution. The data will be stored within company databases, and protected by company security measures. There will be no need to worry about compliance issues, as everything can be tailored to suit the unique requirements of any business.

Mail Secure's Archiving Module lets employees easily store, search and retrieve emails. It reduces the stress of complying with regulatory requirements while completely integrating with cloud-based email systems like Office 365.

How it works now



Multiple vendors and confusion

How it should work

Archiving made easy and secure

Scenario three

No matter how great an email security solution is, it is bound to have issues sooner or later. Cybercriminals come up with devious new methods for stealing information every day, and keeping up is a true challenge. Suppose a spear phishing attack occurs, and an internal IT technician is on the case. She has tracked in the solution reports, but has encountered an issue that requires additional information. The IT technician needs to call customer service for the security system, and she needs feedback and advice quickly in order to remediate.

How it works now: If our IT technician's company is like many today, then this phone call for assistance is not going to go well or be very helpful. The customer service attached to many email security solutions today is less than satisfactory. Our technician makes the phone call and is immediately put on hold. Not just for a minute or two, but an obscene amount of waiting time. This is definitely not conducive to solving the spear phishing problem as quickly as possible.

When the technician finally reaches a person, he is a "tier 1" or entry level call service representative. This person has limited, if any, experience in the industry. His ability to engage on challenging technical questions is low. As a result, our technician's call will have to be escalated to someone with more knowledge and experience. So our technician is put on hold yet again to wait for another frustrating amount of time until the next person can be reached. This person hopefully has the answers she needs, but more than likely not. She will be stuck in the escalation chain on hold for quite some time, and she may never get the answers she is looking for.

This is unacceptable customer service, but it is pretty standard for the industry of email security solutions. Every interaction is an arduous climb upward through layer upon layer of customer service in hopes of getting a helpful response. It adds more work to the already difficult job of keeping corporate email safe and secure, and that does not help anyone in the end.

How it should work: If this IT technician worked for a company employing an effective and comprehensive email security solution, her job would be much simpler and more pleasant. Her phone call would have been taken by someone sitting at the help desk of the corporate headquarters. The first person she spoke to would be a qualified support engineer with deep customer service experience and a commitment to remediation and excellent service that is shared by all of his colleagues company-wide. He would be able to answer all of her questions in a timely fashion and help her get everything back on track.

Her needs would be a central force of the organization's technical priorities. This call center would not be an afterthought type of service, but rather one of the most important services offered. The mark of a quality email security solution is its ability to offer an excellent customer experience at every level. Any company working with a lesser solution is only making its employees jobs more difficult, and jeopardizing the security of its information.

PineApp's help desk is in the same hall as the CEO's office and the R&D department. The CEO established the help desk and managed it personally for several years to guarantee the highest quality service and standards. Mail Secure users can be assured that they are in good hands with PineApp's customer service.

Get the Best Email Security Solution Around

As you can see, email security is more involved than simply preventing spam and phishing attacks. It is about centrally managing your professional communication in a way that protects your interests and improves your business processes. You need a shield that can stretch and grow with your company to cover new vulnerabilities as they arise. Your email security should not only protect your business, but help it grow and develop. That is where PineApp stands head and shoulders above every solution out there.

PineApp is built upon a deep understanding of secure communication, and our platform addresses a broad spectrum of the needs that so often arise in the modern environment of business. From compliance concerns to encrypting information, both incoming and outgoing, we have the experience and tools that you need to guard your business against security threats from the inside out. Even better, we are 100 percent dedicated to your satisfaction. You will not deal with unskilled help desk jockeys and agonizing customer service wait times. When you need answers, we will give them to you as quickly and effectively as possible.

An email security solution capable of defense on multiple fronts must offer centralized management and protection of all email-related activity, from message contents and attachments, storage and retrieval of archived messages, and additional functionalities like email branding, through to online collaboration and large-file transfer activities. The solution that can cover all those requirements is the one that differentiates itself most clearly from the rest.

That solution is called Mail Secure and it is changing the face of email security for small and medium-sized businesses (SMBs)and larger organizations. To find out more, talk to the team at PineApp today.

info@pineapp.com
+972 (4) 8212-321

PineApp