5 Features That Set an Email Security Solution Apart

CYBONET
formerly PineApp

Cybercrime is on the rise, with email traffic presenting an attractive target for data theft attempts.

$3.5 million - the average cost of a company data breach

5 Features That Set an Email Security Solution Apart

An increasingly connected commercial world presents fresh challenges, with email security standing out as a prime example. Cybercrime is on the rise, with email traffic presenting an attractive target for data theft attempts. With the average cost of a company data breach standing at $3.5 million (according to research by The Ponemon Institute), companies can ill afford to ignore the dangers of inadequate email security.

With this in mind, email security has become a primary concern for organizations worldwide. Interestingly, email security solutions have not evolved a great deal in the last few years. They all seem to offer the same anti-spam functionality.

This makes ancillary features that appear to have little relevance to the security of email communication vitally important. These ancillary features simplify email security. When a company does not have to use multiple vendors offering disparate supplemental solutions, it reduces its risk and cost when moving to cloud-based email services like Office 365.

The five features described in this eBook are those which distinguish future-ready email security products and position them as the obvious choice for organizations seeking a full service messaging solution for on premise security needs or integration with cloud based applications such as Microsoft's Office 365.

1) Email archiving

Many companies are either living with the limitations of on-premise email-archiving or maybe using a public cloud archiving solution. Small businesses as well as enterprises wind up using a third party application to increase archiving space and improve on the search features built into commercial email systems. Apart from any potential increase in risk, using the public cloud for email archiving potentially creates compliance issues. In any event, it entrusts potentially proprietary information to a third party.

Archiving: the solution

When integrated with your productivity software suite (Office 365 for example), an email security solution with its own archiving functionality solves the problems associated with putting email and attachments into the care of a third party. Because your archiving facility is integral to the security solution, you're unlikely to find a more robust way to protect your archived files. If your company is under regulatory obligations to keep data secure, integrating your archiving into a strongly secured environment is the best possible way to ensure compliance.

Using a public cloud archiving solution is risky and may create compliance issues.

An email security solution with its own archiving functionality solves the problem.

Sending confidential information over unencrypted email puts companies at risk of fines, lawsuits and lost revenue — to say nothing of the bad PR.

2) Encryption

Organizations all over the world are dealing with highly public security breaches on top of regulatory pressure and an increase in identity theft. Sending confidential information over unencrypted email puts companies at risk of fines, lawsuits and lost revenue — to say nothing of the bad PR. Conventional email security solutions may be great for filtering spam, alerting you of phishing emails, and stopping other threats, but what about the sensitive and business-critical data contained in outgoing messages? Of course you can choose to use on-premise, hardware encryption solution, but that's typically useful only for intra-company communication, since in most cases, client software is necessary to enable encryption of outgoing mail and decryption of messages at the recipient's end.

Outgoing email protection: the solution

Email data is frequently subject to regulations imposed by PCI and other agencies. If you use email to transfer information subject to these standards precaution in the form of encryption is necessary to keep your data safe.

An email security solution should activate based on pre-set, automatic policies and be clientless encryption so that any specified recipient can receive the message. This significantly improves the effectiveness of inbound-only protection. The best security applications provide policy-driven encryption that allows administrators to configure encryption policies to automatically detect the presence of personally identifiable information such as social security numbers. When such "trigger" information is detected in the body of an email message, messages are automatically encrypted reducing the chance of user error. Recipients only need to register in order to obtain a decryption key, so the need for specialized software is eliminated.

The best security applications can be configured to automatically detect the presence information that should be encrypted. Recipients only need to register in order to obtain a decryption key.

3) Large file transfers

You have probably been frustrated more than once by the difficulties in attaching large files to emails that exceed company restrictions on message size. But you could be forgiven for wondering what that has to do with security and why an email security provider would get involved in file transfer solutions.

To see the connection, it's necessary to descend a little from the 20,000-foot viewpoint and think about how large-file sharing and collaboration is typically managed. Many email systems limit the size of attachments, meaning large files have to be sent via some other channel. Like the archiving issue, transferring large files puts you in the position of exposing data files to cloud-based storage — making that data more vulnerable to potential attacks.

Sharing large files: the solution

Imagine if your company had its own Web portal, allowing files of any size to be uploaded for retrieval by an authorized recipient — and only by that recipient. That is exactly what you get when your enterprise invests in an email security solution with a large file transfer module. Your files do not clog the traffic in the email system and do not carry the risks associated with consumer solutions. Large file transfer should include encryption, customizable expiration dates and access keys for additional security.

Files too large to attach to emails are often sent via some other channel, making the data more vulnerable to potential attacks
Instead, use an email security solution with a large file transfer module, encryption and expiration dates.

Using a third party to brand your email spawns a potential security vulnerability.

Keep your email branding in-house and enjoy greater security and affordability.

4) Email branding

Making your corporate emails over with branding, such as logos, banner ads, links to landing pages, and other lead-generating elements is a great way to deliver marketing messages. After all, informational emails almost always get opened and read. However, branding your own emails can be technically complex and expensive, which is why many organizations entrust their email branding to specialist service providers. The problem with using a third party to brand your email is that in providing the service, the vendor gains access to proprietary information (such as your customers' email addresses), spawning a potential security vulnerability.

Email branding: the solution

A new breed of email security application is finally emerging in a market that has spent some years in the doldrums. The developers of these on-premise and cloud-based solutions are approaching security from a non-traditional perspective. Email branding, including easy to use templates and policies that are centrally managed, are some functionality that you can expect and keep in-house, enjoying greater security, along with affordability and a simpler process for branding corporate emails.

An integrated solution keeps your IT team in total control of email security.

5) Integration

Productivity and communication platforms come with some degree of built-in security. However the level of protection is really just enough to guard against basic threats. For advanced threat detection and prevention, your company needs additional assurances, especially if you are in an industry where regulatory compliance demands a no-compromise approach to online security. It is critical, however, that these services are compatible with Office 365 and similar platforms.

Integrated email security: the solution

To supplement the basic security features of Office 365, organizations need a third-party partner. An email security solution that integrates seamlessly with your exchange systems can simplify the monitoring and protection of inbound and outbound mail. An integrated solution keeps your IT team in total control of email security, combining advanced policy-based capabilities with easy-to-use features and reporting for end-users.

Archived

Encrypted

Large Files Transferred

Branded

Integrated

Email security will never be the same again

Protecting your company's email from spam and phishing attacks is only one facet of today's continual battle against sophisticated cybercrime rings and data leakage.

There are multiple ways business email traffic can generate vulnerabilities in digital communication security. To ensure these potential security gaps stay closed you need a multi-faceted solution that can guard your email effectively and keep you from compliance issues, data loss or the theft of intellectual property.

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 functionality like email branding, through to online collaboration and large-file transfer activities. The solution which can cover all those requirements is the one that differentiates itself most clearly from the rest.

That solution is called PineApp Mail Secure and it's changing the face of email security for SMBs and larger organizations. To find out more, talk to the team at Cybonet today.

info@cybonet.com
+972 (4) 8212-321
North America +1 64 68 83 34 55
UK +44 20 37 69 51 20

CYBONET
formerly PineApp