Hewlett Packard Enterprise

Business white paper

Rethinking email encryption:

Eight best practices for success

Table of contents

Executive summary

Email continues to play a fundamental role in an organization's communications and day to day business—and represents a critical vulnerability in its defenses. Too often, the sensitive data being transmitted via email is susceptible to attack and inadvertent disclosure. Email encryption represents a vital defense in addressing these vulnerabilities, but to date, many email encryption solutions have failed to meet all of an organization's security and business requirements. This paper reveals the best practices IT organizations should adopt in order to realize a successful email encryption implementation, one that addresses IT's security needs and aligns to the business.

Introduction: Growing email usage and continued exposure

In an era of ubiquitous texting, social networking and cloud-based file sharing, one may assume that the relevance of email would be on the wane. However, usage trends show that's not the case; in fact, according to a recent survey, more than half of employees rely on email more today than they did one year ago.[1] Further, email continues to be the primary means with which files get transmitted, with files accounting for 98 percent of the bits being transmitted through email channels.[2]

The reality is that email remains a vital communications channel for enterprises and it also represents a security vulnerability. Intellectual property, customers' personal information, regulated data like healthcare information and payment card information, and other sensitive data continue to be transmitted via email. However, this channel remains susceptible to a host of risks, including inadvertent distribution to unauthorized parties, access by malicious insiders, and attacks from outside criminal organizations.

Further, as employees increasingly bring their own technologies whether devices, applications or cloud services to their jobs, the task of managing security grows more difficult. Either IT teams have to abdicate more control and visibility, or they have to significantly expand the number of technologies and use cases they support.

To address their security and compliance mandates, it will be increasingly incumbent upon organizations to employ email encryption. However, according to a recent study, more than 60 percent of employees don't have access to email encryption, and most of those that do are reliant on manual, sender-initiated approaches.[3] This often means encryption is being inconsistently applied and susceptible to the sender's discretion.

To combat these types of incidents, and safeguard sensitive assets in an increasingly mobile, cloud-connected world, many organizations will have to leverage email encryption more broadly. In fact, the use of email encryption is poised to grow substantially in the coming years. While both user-initiated and policy-initiated approaches are expected to grow more common, policy-based encryption is set to grow most rapidly, from 28 percent in 2014 to 45 percent in 2016.[4]

Written for those business leaders who are looking to introduce email encryption into their businesses, or seeking to expand or replace their current encryption capabilities, this white paper offers a look at critically important best practices for implementing email encryption successfully.

[1] Osterman Research, March 2014

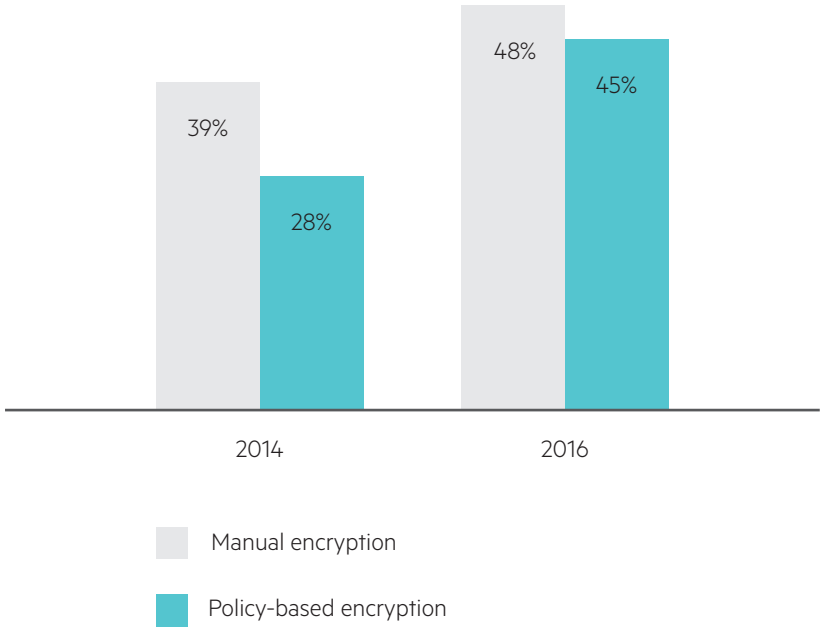
[2] Osterman Research, March 2014

[3] Osterman Research, April 2014

[4] Osterman Research, April 2014

Best practice #1. Take a data-centric approach

Enterprises should take a data-centric approach, meaning encryption of the data itself so that it is protected persistently wherever it goes, whether inside or outside the enterprise. Find a solution that protects email end-to-end, from the point it is sent to the point it is read, and throughout its lifecycle.



Avoid solutions that have large security gaps in the mail flow, such as solutions that support only gateway encryption for outbound mail. Or, solutions that use multiple different encryption technologies, each with their own limitations, so they can address both internal and external use cases. For example, some solutions rely on PGP or S/MIME for email encrypted internally within the enterprise, but they use webmail encryption for email that is delivered to external recipients. Those solutions also create security gaps because inbound replies are decrypted so they can be read by internal users who do not have the same encryption technology as external users. This means sensitive data is distributed throughout the enterprise in clear text on inbound replies.

If you are using cloud-based email, or considering using it, find a solution that supports separation of duties, where the cloud provider does not have both the email content (messages and attachments) and keys. Additionally, look for a solution that can encrypt email at the moment it is sent, before it travels over the Internet or through your cloud provider's infrastructure. Data-centric protection and separation of duties ensure that email will be protected from cloud email operators/administrators, and from breaches of cloud services.

To avoid security gaps, organizations need to take a more strategic approach, focusing on data and ensuring it is secure throughout the email lifecycle, ideally using a single encryption technology that works across all use cases and devices. Today, encryption technology exists that can encrypt email internally and externally, and across all endpoints, including desktop, mobile, applications, and cloud. Using a single technology that can address all uses cases ensures that the sensitive data is protected end to end—with no security gaps.

Best practice #2. Work with your compliance infrastructure

Implementing email encryption historically meant organizations have had to battle with competing demands, protecting data to comply with regulations and mandates on the one hand, while still being able to conduct compliance (i.e., filter, archive, and discover) investigations, and audits on the other hand. This often meant a tradeoff, either complicating or breaking compliance processes or settling for less data protection. No longer do enterprises need to make these severe tradeoffs.

Encryption does not have to break, modify, or require extensive additional infrastructure to maintain existing compliance functions, such as data leak prevention (DLP), archiving, and eDiscovery. Your solution should be able to enforce data protection policies, with little to no impact on existing compliance business processes. Additionally, organizations should ensure that the email encryption solution preserves all aspects of the message in relation to forensic tools and for use in electronic discovery requests, where integrity and consistency are required.

Modern email encryption technologies, such as Identity-Based Encryption, can easily work with existing compliance infrastructure via a combination of policy rules and mail routes over standard SMTP, or simple plug-ins or tools that can also perform policy-based decryption as needed.

HPE Security—Data Security has customers all over the world today that are using HPE SecureMail with DLP, mail hygiene, and archiving and eDiscovery solutions from a variety of vendors, including Cisco, Symantec, Websense, Microsoft®, McAfee®, and many others. These organizations are able to leverage the full benefits of data-centric email encryption, while still retaining critical compliance functions such as content filtering, data classification, and keyword searching of their email content for regulatory purposes. A proper email encryption solution enhances, rather than hinders, compliance capabilities.

Best practice #3. Implement a stateless architecture

Traditional encryption technologies, such as S/MIME, PGP, OpenPGP, and symmetric key, generally require heavy-duty key management and complex infrastructure for storage, replication, backup, and archival. Proprietary webmail solutions were later bolted on to make these encryption technologies easier for external recipients, but with additional burden to IT because they now had to manage separate message databases for encrypted email, making these solutions even more complex and costly. Finally, traditional solutions are "one size fits all", meaning a separate, duplicate infrastructure needs to be deployed for each region and line of business.

All of this infrastructure increases the complexity of the system, prolongs deployment timeframes, adds recurring operational costs, and results in scalability and growth challenges when an organization needs to support additional lines of business or geographies.

To avoid cost and complexity, organizations should deploy stateless email encryption architectures, such as those enabled by HPE Identity-Based Encryption (IBE). Stateless key management enables simplified operations, easy disaster recovery across global data centers, effortless scaling to millions of users without corresponding cost increases, and simplified infrastructure with the least "moving parts"—no key databases, message stores, key escrows, certificates, etc. The cost benefits are typically measured as 60–80 percent reduction over legacy encryption technologies, both in infrastructure and operational costs. To summarize, choose a solution that is not bound by the storage of cryptographic key or message data, so that it scales in a linear fashion, at a much lower cost.

TRADITIONAL ARCHITECTURES	STATELESS ARCHITECTURES
Keys stored and managed on the server	Keys generated on the fly when needed
Ongoing backups required	One-time backup of master secret only
Key replication required among servers	All servers can derive the same keys (no replication required)
In disaster scenarios a lost key can result in lost data	Keys and data can never be lost
Webmail creates an additional database for secure messages	Messages reside in the recipient's existing inbox

Best practice #4. Leverage one technology for all use cases

In years past, IT teams looking to leverage email encryption have been stuck with limited point tools and legacy products. As a result, it has been common for IT organizations to be running a patchwork of technologies to meet all their demands. Quite simply, there hasn't been a single technology that could address all of their requirements. For example, a lot of organizations started using PGP, but since that technology is not practical for emails with external recipients, they've had to use additional technologies, such as webmail.

Legacy email encryption solutions support multiple incompatible encryption technologies, message formats, and/or delivery models because none are capable of addressing all use cases and client endpoints. Vendors know this is a major weakness, so they attempt to position it as a feature (e.g., "best method of delivery"). The reality is that bolting together multiple incompatible legacy and proprietary encryption technologies translates into complexity for users, high total cost of ownership to manage and support the infrastructure and end users, and security gaps where data is vulnerable.

Additionally, a given encryption platform may only support a subset of the endpoints required, for example, not offering support for common mobile device platforms or Gmail. Given the inherent security gaps, complexity, and cost associated with managing multiple encryption technologies, it is critical to leverage a single solution that can support internal and external use cases, commonly used email clients and services, all major client endpoints, and encrypt email generated by applications and websites. Reference customers should be able to point to success in addressing a wide variety of use cases, including employee to employee, employee to external party (e.g., customer, client, partner), application and website-based use cases, mobile use cases, and more.

Not only is it clearly more elegant to use a single method, doing so also directly reduces cost and increases usability by focusing on a simple to manage solution that is universally easy to use.

Organizations should insist on a single technology that supports internal and external users, as well as gateway, client-based, browser-based, and mobile delivery—all with Identity-Based Encryption, true push delivery, and a single message format.

Additionally, using a single message format and delivery method makes it easier for the vendor to create clients, apps, and plug-ins for endpoints because it only needs to design those for one technology, not a combination of multiple different technologies. In the end, this means better endpoint coverage for users.

As a final note, avoid solutions that use a proprietary message format that contains active JavaScript content. Many organizations block or quarantine messages with JavaScript. Or, recipient email systems and browsers may remove, modify, or disable it. In most cases customers don't even know that they haven't received a message. Message formats containing JavaScript introduce security concerns (it can be used as an attack vector) and increase help desk costs and frustrate users.

Best practice #5. Provide ease of use for senders and recipients

An organization can implement the most robust encryption mechanisms possible, but in the end, they won't do any good if they're not used consistently. That's why, beyond any security or technology consideration, ease of use is a make-or-break factor for an email encryption deployment. If procedures are too complex, cumbersome or time consuming, users will find ways to avoid or circumvent them, leaving the organization exposed to breaches and lack of compliance.

For email encryption, there are a number of considerations that impact the user experience. For example, is the enrollment process simple? Are the major endpoints covered? Does it drastically change the native user experience? Do messages expire? Can users send ad-hoc encrypted email? Can implementations federate with one another? Does it support single sign-on? Do users have access to the contacts on their mobile devices? Can users send to distribution lists? Does the solution support shared mailboxes? And many others.

This is why it's so critical that organizations implement a solution that is similar to using regular email, without adding too many additional steps or hurdles, and that integrates with the users' existing email workflows and endpoints. Systems that require users to manage keys or certificates, that pull the user to a separate webmail inbox for encrypted email, or that do not work on common mobile devices have all been rejected by users.

Encrypted messages should be push delivered to the recipient's existing inbox (e.g., Gmail, Yahoo Mail, Outlook, iOS Mail, Android Mail), the same place they receive plain text email. If push is offered, it should not require an external recipient to download any software—it should work with any standard browser, particularly on the desktop. Be careful of the many vendors that claim to support a push delivery model, but their technology does not work for recipients on common mobile devices such as iPhone®, iPad®, and Android. Look for a solution that offers plugins or apps that work with the native email client on the desktop, Web, and mobile devices, without drastically changing the user experience. The solution should support ad-hoc usage, meaning any user should be able to send an encrypted email to anyone without having to worry about whether they have a certificate, account, or shared password.

For external recipients, enrollment should not require a lot of steps, and enrollment should be handled in the flow of reading the message, not a separate flow that leaves the user wondering what they do next to read their message. Users should not be forced to create a parallel ID before they can enroll. The enrollment form should not require too much information from users, particularly PII. Enrollment should be as simple as creating a password and setting up a recover method—that's it.

Best practice #6. Choose a Multi-Tenant Ready Solution

Pre-Internet email encryption technologies were not designed to address the complex requirements of today's business environments. Most email encryption solutions do not support multi-tenancy, which can constrain and limit your business.

For example, they cannot accommodate multiple lines of business, departments, or use cases where each require different policies, workflows, or branding requirements. Or they cannot accommodate multi-national enterprises that have mail infrastructure and messaging teams in several countries.

Legacy solutions are often "one size fits all", meaning separate duplicate infrastructure needs to be deployed for different regions, lines of business, or departments, often with very limited capabilities and policy controls relative to modern systems.

With modern systems, such as HPE SecureMail, an organization can have multiple virtual deployments within a single, global infrastructure. For example, one tenant can be setup for general corporate email, a second tenant can be setup for a particular line-of-business (LOB), and a third tenant can be used to send monthly statements. Each of these tenants can have its own policies, workflows, authentication, branding, and cryptographics.

Many of HPE Security—Data security's customers, for example, will use a dedicated tenant for specific use cases. Some use different tenants for different geographic regions that manage their own mail infrastructure. Others use a unique tenant for different lines of business or departments. For global firms that have country offices or lines of business with separate privacy and regulatory requirements, multi-tenancy allows them to easily segregate their email encryption to meet their specific privacy and regulatory concerns but all within a single, centrally managed infrastructure.

Multi-tenancy ensures that the solution remains completely flexible to meet the changing needs of the business. Even if you don't have a need for multi-tenancy initially, it is smart to invest now in a platform that can grow and adapt with you.

Best practice #7. Invest in architectural flexibility

Continued innovations in platforms, including cloud, mobile, and others, present significant opportunities for organizations. When evaluating email encryption alternatives, it is important to look for platforms that provide maximum architectural flexibility, which is vital for addressing today's business demands and those that will emerge in the years to come.

While many organizations' initial implementations of email encryption platforms were done on premises, it is growing increasingly common to migrate these platforms to external managed service providers or cloud services. Even if migrating to the cloud isn't a part of an organization's near-term plans, it is important to invest in platforms from vendors that support cloud-based hosting, if and when the need should arise.

Look for a solution that can be deployed on-premises, in the cloud, or with a hybrid architecture (enabling a mix of integrated email infrastructure running both on premises and in the cloud). Ensure that you can easily migrate from on-premises to the cloud and vice versa—without a service outage. If your organization is a large enterprise, do not get locked into shared tenant environment, where your cryptographics are held hostage, and that does not allow you to migrate if your needs change. Starting all over again is costly, and painful for users. Find a solution that allows you to easily move, or even migrate to a different solution.

Some other important considerations include: Can the solution easily integrate with business applications and websites? Can it easily integrate with Microsoft Active Directory, LDAP, or other platforms for authentication, such as Web Access Managers or Web Portals? Will the solution work across mobile devices and MDM platforms?

Best practice #8. Implement a modern and proven standard

Most vendors refer to their use of standard encryption technologies, such as OpenPGP, S/MIME, or AES. Vendors will talk about these standards, but ultimately guide customers towards non-standard, proprietary solutions such as webmail, Secure PDF, or push methods that use proprietary message formats that incorporate non-standard, non-published ciphers that can be poorly implemented.

These legacy standards and proprietary delivery models do not hold up to real world use cases, so the adoption rate has been extremely low and limited to small pockets of users. Over time it has been proven that these pre-Internet technologies do not scale and offer a poor user experience. In effect, these technologies have failed in real-world commercial markets. There is a real and growing trend where Identity-Based Encryption (IBE) is replacing these legacy technologies.

When evaluating email encryption alternatives, it is important to look for a solution that has been peer reviewed, is standards-based, and proven in real-world deployments. Effective platforms employ encryption technologies that have been vetted by the cryptography community and international standardization bodies such as Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO), and The Internet Engineering Task Force (IETF).

Companies should look for modern technologies, such as HPE Identity-Based Encryption (IBE). HPE SecureMail, for example, uses AES CBC for message encryption, HPE IBE for key wrapping and public key exchange, a standard elliptic curve-based algorithm for public key operations, and an S/MIME based message structure. HPE IBE has been standardized in IEEE 1363.3.

Finally, companies should work with vendors that can point to successful deployments across entire organizations and large external user populations. Over the past 10 years, HPE IBE has become one of the fastest deployed encryption technologies as measured by the commercial adoption of HPE SecureMail and the use of IBE as a general purpose key management solution globally. Since its commercial launch in 2004, HPE SecureMail has become one of the most widely adopted secure email products in the world—with more than 68 million users worldwide (based on a survey conducted in 2013).

Conclusion

Email encryption was not broadly deployed and used in the past for a number of reasons: legacy products lacked the ease of deployment, ease of use, and low cost of operations that are required by IT and business. Today, however, there are modern, advanced email encryption platforms that address these shortcomings. By finding solutions that deliver or enable the best practices outlined above, organizations can address their critical security requirements enterprise-wide, without impacting compliance, and align to the business now and in the future.

About HPE SecureMail

HPE SecureMail is an end-to-end email encryption solution that can scale to millions of users, while keeping sensitive assets secure and private. HPE SecureMail offers these capabilities:

- **Comprehensive coverage**—HPE SecureMail enables both internal and external users to decrypt emails, whether they're on a desktop, the Web or a mobile device. The solution also supports scanning and filtering for all inbound and outbound email.
- **Data-centric protection**—HPE SecureMail encrypts data and attachments so that if a security breach does occur, the encrypted content is of no value to the attacker.
- **Stateless key management**—Using HPE Identity-Based Encryption (IBE), there are no keys to manage or store. HPE SecureMail requires minimal administrative or infrastructure support and has been proven to scale across global enterprises.
- **Standards support**—HPE SecureMail is built on proven, standards-based encryption technologies, and seamlessly integrates with essential email infrastructure, such as antivirus, antispam, content filtering and mail archives.
- **eDiscovery support**—HPE SecureMail provides multiple options for internal supervisory control and policy-based archiving of secure mail. Providing the ability to index, search, view and discover data inside secure email, the solution simplifies responses to requests during audits, investigations and litigation.
- **Flexible deployment options**—HPE SecureMail can be deployed on premise, in the cloud, or across hybrid deployments, and it supports cloud email services such as Office 365. The solution also works seamlessly with Outlook, Exchange and BlackBerry Enterprise Server (BES); mobile device management (MDM) products; and business applications and websites.

Learn more at
voltage.com
hpe.com/software/datasecurity

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0085ENW, April 2016, Rev. 1