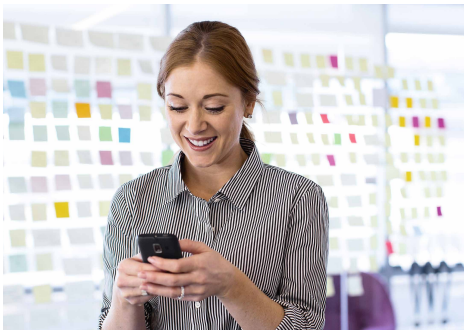
Hewlett Packard Enterprise

HPE SecureMail

Achieving End-to-End Email Security without Impacting the User Experience



In regulated industries such as healthcare and financial services, consumer privacy and data security have become a top priority for most IT departments. The regulations and penalties for non-compliance seem onerous but pale in comparison to the loss of trust from customers when a security breach does occur. Email is the de facto way for how organizations communicate especially outside their firewalls. If not properly protected, email can be one of the most vulnerable systems in a company's infrastructure. The challenge is to implement a secure email system that complies with all regulations and is easy to integrate with existing business systems.

Flaws of traditional email encryption

Most traditional email encryption approaches must rely on multiple delivery methods resulting in security gaps from messages being split. Legacy S/MIME and PGP PKI are complex for IT and incompatible with Gmail, Yahoo, and Android. Proprietary Symmetric Key requires complex key database management, and can also lead to data loss if a key is corrupted. Proprietary Webmail surfers from end-user confusion with multiple inboxes, blocked or expired links, and no access to contacts.

HPE SecureMail Solution

HPE SecureMail is the best of breed end-to-end encrypted email solution available for desktop, cloud, and mobile that is scalable to millions of users, while keeping Personally Identifiable Information (PII) and Personal Health Information (PHI) secure and private. This level of secure email communication gives organizations the confidence to transition from paper to electronic communication.

- **Single solution for desktop, cloud, and mobile—**HPE SecureMail enables decryption on desktop, Web, and mobile, by both internal and external users and supports scanning and filtering for all inbound and outbound email.
- **Data-centric protection for email and attachments—**HPE SecureMail encrypts data and attachments so that if a security breach does occur, the encrypted content is of no value to the attacker. Attachments are stored on internal servers, not external third-party servers.
- **Stateless key management—**The underlying key management system is arguably the most important factor governing the performance and quality of experience of a secure email system. Using standards-based HPE Identify-Based Encryption (IBE), secure messages can be sent to any recipient, without first requiring the recipient to take special action. Since there are no keys to manage or store, HPE SecureMail requires minimal administrative or infrastructure support and allows for scale across global enterprises.

- **Tight integration with existing enterprise infrastructure and investment—**HPE SecureMail seamlessly integrates with essential email infrastructure such as anti-virus, anti-spam, content filtering, and mail archives. With HPE IBE, there is no need for complicated Alternate Decryption Keys (ADKs) required by legacy PKI and OpenPGP systems.
- **eDiscovery—**HPE SecureMail provides multiple options for internal supervisory control and policy-based archiving of secure mail. Messages are stored and managed like regular mail. With the ability to index, search, view, and discover data inside secure email, HPE SecureMail simplifies responses to requests during audits, investigations, and litigation.
- **Flexible deployment options—**HPE SecureMail supports on-premise, in the cloud, or hybrid deployments, as well as cloud email services such as Office 365. The solution also works seamlessly with Outlook, Exchange, Blackberry Enterprise Server (BES), mobile device management (MDM), and business applications and websites. HPE IBE offers a clean separation between encryption and authentication, meaning it can support a variety of authentication methods, including Active Directory, LDAP, portals, and Web access managers to name a few.

Integrated with your existing email workflows for a simple user experience

In highly regulated environments such as healthcare and financial services, compliance is mandatory but difficult for companies to enforce. This is especially true with email because end-users strongly resist any changes to their standard email workflow. HPE SecureMail delivers a simple user experience across all platforms including computers, tablets, and native mobile platform support with full capability to send secure, originate, read, and share messages. Within Outlook, iOS, Android, and BlackBerry, for example, senders can access their existing contacts and simply click a "Send Secure" button to send an encrypted email. The recipient receives secure messages in their existing inbox, just as they would with clear text email. See Figure 1.

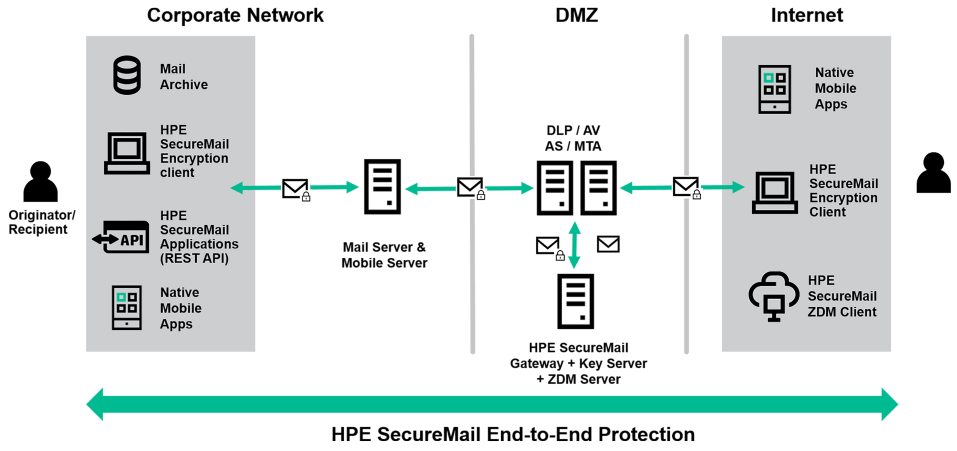


Figure 1: How HPE SecureMail works

HPE Security - Data Security
U.S. Tel: +1 (408) 886-3200
EUR Tel: +44 (0) 203 468 0559

Sign up for updates

★ Rate this document

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

4AA6-0206ENW, May 2016, Rev. 3

Hewlett Packard Enterprise