Hewlett Packard Enterprise

Data sheet

HPE SecureMail Application Edition

Data-centric security for applications, portals, and websites that use email

New possibilities for email protection: application email

HPE SecureMail provides data-centric security for email and unstructured data in files. HPE SecureMail Application Edition extends these security capabilities to protect email messages and attachments that are sent and received by business applications, portals, and websites that contain information intended only for recipients.

Businesses are using HPE SecureMail Application Edition to benefit from broader reaching, more comprehensive data protection and compliance for their application driven business processes. Until now internal application email could not be systematically secured, end-to-end.

Business email is not always sent from person-to-person, for example, by an employee using an email client to an external recipient reading it from an email client. Email is also used extensively by applications. Applications typically generate, store, and use emails in the context of a business workflow or process. Just like email sent between people, email that is sent and read from applications also contains sensitive information that needs to be protected.

Organizations trying to comply with data protection and privacy regulations (HIPAA, HITECH, PCI, and SOX) should not only encrypt email sent between people, they should also be concerned with email sent to and from applications.

Highlights

- **Protects application email** like invoices, statements, approvals, workflows, CRM, collaboration systems, credentials, and more.
- **Data-centric approach** that persistently protects email data wherever it goes, making it available under tight policy control only when needed.
- **Simplest user experience**, using any client on the desktop, mobile, and the Web. Compatible with all current browsers, both desktop and mobile.
- **Cuts complexity and costs** by integrating encryption without changing email architectures, rerouting email flows, or integrating with SDKs.
- **Proven infrastructure** that's secure, scalable, and manageable, with low operational costs.

There are many applications that send and receive email with sensitive information intended only for recipients which should not be disclosed to outsiders. Examples include:

- **Internal approval workflows:** multi-step workflows involving requests, approvals, and denials (ensures authenticity).
- **Inbound Web form submissions:** information submitted by customers, patients, or partners via online forms (e.g., claim forms).
- **Scheduled reports:** reports emailed to business users that contain confidential metrics and key performance indicators (KPIs) about business performance.
- **Credential provisioning:** account information created and emailed to users by a provisioning system (e.g., temporary authorization codes, PINs, passwords).
- **Password management:** password reset messages that contain temporary passwords emailed to users by a website or application.
- **Fax to email:** faxes containing sensitive information such as social security numbers or credit card numbers sent to inboxes as email attachments (e.g., PDF files).
- **Enterprise collaboration tools:** email communications between members of collaboration websites and communities.

A unique solution

Past approaches of not encrypting internal application email or using a TLS gateway or outbound SMTP gateway to encrypt and decrypt application emails at the network edge are insufficient. These approaches do not address the security gaps where data is vulnerable as it travels internally or from applications to outgoing TLS or SMTP gateways. These approaches also leave data vulnerable while at rest in applications, mail servers, and desktops. Data is at risk before the email is encrypted and after it is decrypted—even within your network.

Applications may also require data protection for emails exchanged outside the organization, for example, with customers or suppliers. It is often impractical to leverage the email backbone infrastructure to get end-to-end email protection. HPE SecureMail Application Edition can protect the data in the email as it leaves the application, before it transits the email backbone, and keeps it protected until the recipient opens the message.

Larger enterprises have hundreds of business applications that send and receive emails containing private and sensitive data. They are subject to compliance and privacy regulations such as HIPAA, HITECH, PCI, and SOX, and they must be kept safe from potential breaches which could result in fines and reputation damage. HPE SecureMail Application Edition provides the end-to-end protection and regulation compliance to these emails.

Integrating HPE SecureMail with applications

HPE SecureMail Application Edition gives email-enabled applications two ways to exchange protected information, via a REST-style Web service or over SMTP.

HPE SecureMail Application Edition provides a simple yet powerful REST-style Web service. This API allows applications to interact with HPE Identity-Based Encryption (IBE) over HTTPS. When this interface is invoked, encryption and decryption services will be performed for the application. Integrating via Web services enables a data-centric approach to protecting application emails at rest and in motion—without changes to email architectures or email routing.

In addition, HPE SecureMail Application Edition includes an optional gateway interface. Applications can send emails over SMTP into the HPE SecureMail gateway, and the gateway will take care of encryption and decryption. In this case the application will not require modification. In fact, the application will not be aware that the email is being encrypted, but the email is not encrypted end-to-end as it is with the Web service.

HPE SecureMail Application Edition is designed to minimize the complexity and cost associated with integrating encryption and security into applications. Both interfaces are designed with simplicity in mind. The Web services API can be called from any modern application programming language today, since almost all (application programming languages) support calls to Web services. For those applications that cannot be modified or the application is already sending emails over SMTP, the HPE SecureMail gateway provides a security layer around emails into and out of an application.

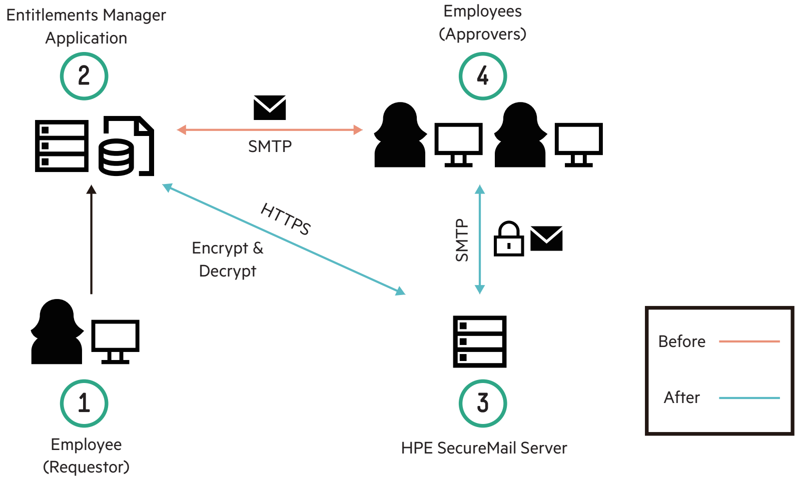


Figure 1: An email-based approval workflow that uses HPE SecureMail Application Edition Web service for encrypting email.

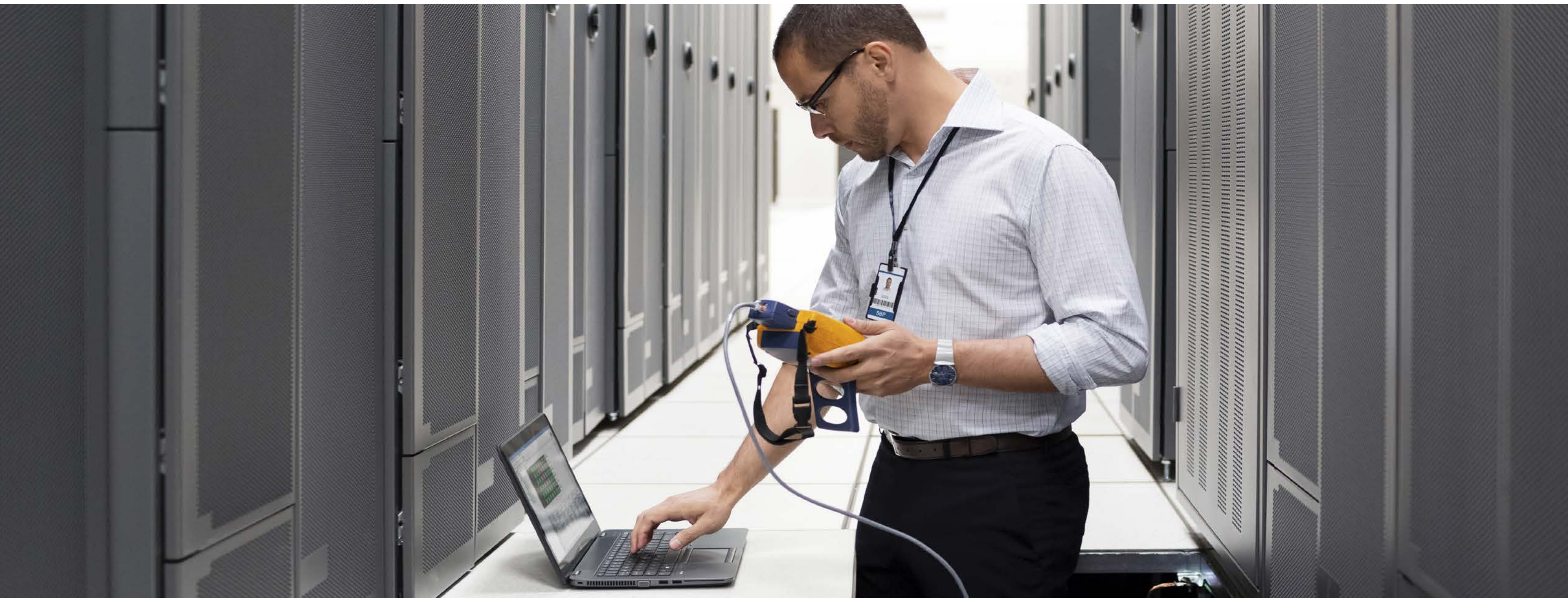
HPE SecureMail architecture

HPE SecureMail Application Edition leverages the established HPE SecureMail infrastructure. It employs the HPE Security Voltage proven encryption technologies and innovations that enable global scale deployments that are simple to manage and administer. Senders and receivers benefit from a simple user interface that makes secure messaging as easy and familiar as standard email communication.

HPE SecureMail is designed to provide end-to-end security for email, while helping to achieve and maintain regulatory compliance. It integrates with existing infrastructure without disrupting existing email services or business processes, and it can be rapidly deployed and scaled up for even the largest organizations. Server components can be deployed on a single hardened appliance, or distributed to meet scale and availability requirements. HPE SecureMail can be employed without any client software, or with software on the user's desktop and mobile devices.

HPE Identity-Based Encryption (IBE) offers an elegant architecture that is lowest cost to manage. Stateless key management and on-demand key generation offers lower on-going operational costs compared to competing solutions that force enterprises to manage keys or messages. Because keys can be generated on-demand, HPE IBE also eliminates the risk of losing access to data, and simplifies disaster recovery and e-discovery.

HPE SecureMail has broad and flexible administration features. It provides robust centralized management, logging, and reporting. It integrates with existing systems for authentication, journaling, and archiving. Operational management is simplified through stateless key management, which eliminates stored encryption keys.



About HPE Security—Data Security

HPE Security—Data Security is a leader in data-centric security safeguarding data throughout its entire lifecycle—at rest, in motion, in use—across the cloud, on-premise and mobile environments with continuous protection.

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

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise

4AA6-0214ENW, April 2016, Rev. 1