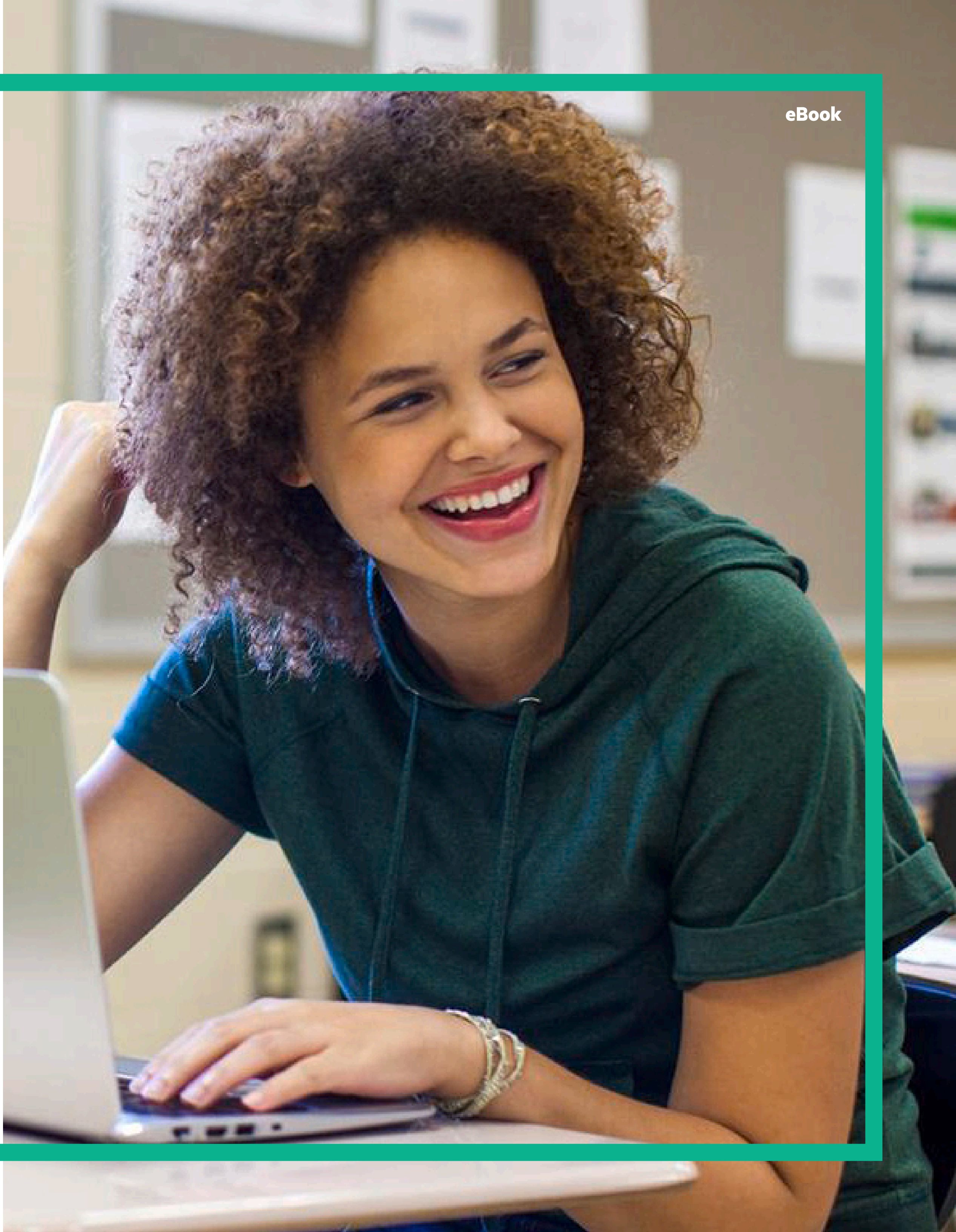
eBook

Peace of Mind in the Cloud

HPE SecureMail and Office 365



Hewlett Packard
Enterprise

Email remains the dominant collaboration platform for corporations

Despite the growth of file sharing and instant messaging platforms, email remains the leading form of communication in the enterprise.

The average user sends a median of 30 emails and receives a median of 100 and spends more than 150 minutes per day doing work in email. That adds up to an average of 2.5 hours a day working in email. In addition, 98% of the bits that flow through a typical corporate email system are attachments.[1]

Clearly, email is the environment in which much of our business takes place and is still the collaboration platform of choice.

30emails

The average user sends a median of 30 emails

150minutes

The average user spends minutes per day doing work in email

98%

of the bits that flow through a typical corporate email system are attachments.

[1] Osterman Research survey data

But email remains one of the most vulnerable systems in IT

Cyber attackers are well aware of email's continued prevalence. From Oct. 2013 through Feb. 2016, law enforcement received reports from more than 17,000 victims of business email scams, exposing companies to losses estimated in $2.3 billion. And since 2015, the FBI has seen a 270% increase in victims and losses.

From an IT perspective, this means that email infrastructure is in constant need of protection. Failure can put companies at risk for losses measured in the millions of dollars.

"Email is the preferred channel to launch advanced targeted attacks.[2]"

- Gartner

From Oct. 2013 through Feb. 2016[3]

17,000victims

Law enforcement received reports from more than 17,000 victims

$2.3billion

Losses being exposed

Since 2015

270%

Increase in victims and losses

[2] Gartner, Inc., "Magic Quadrant for Secure Email Gateways," by Peter Firstbrook and Bryan Lowans, 2 July 2013
[3] Federal Bureau of Investigations press release: "FBI Warns of Dramatic Increase in Business E-Mail Scams", April 04, 2016

Enter Microsoft Office 365

Microsoft® Office 365 is a highly capable bundle of email, calendaring, scheduling, task management, desktop productivity, telephony, real-time communications, and collaboration tools. All based on Microsoft servers “in the cloud.”

Users can tailor it to their specific requirements, including customizations for specific user groups within the organization. All of this can mitigate the upfront costs of deploying new or upgraded messaging systems, reduce ongoing costs by minimizing IT labor requirements, and cut out future upgrade and migration challenges.

☑ Performance

☑ Low cost

☑ Easy migration

☑ Upgrades

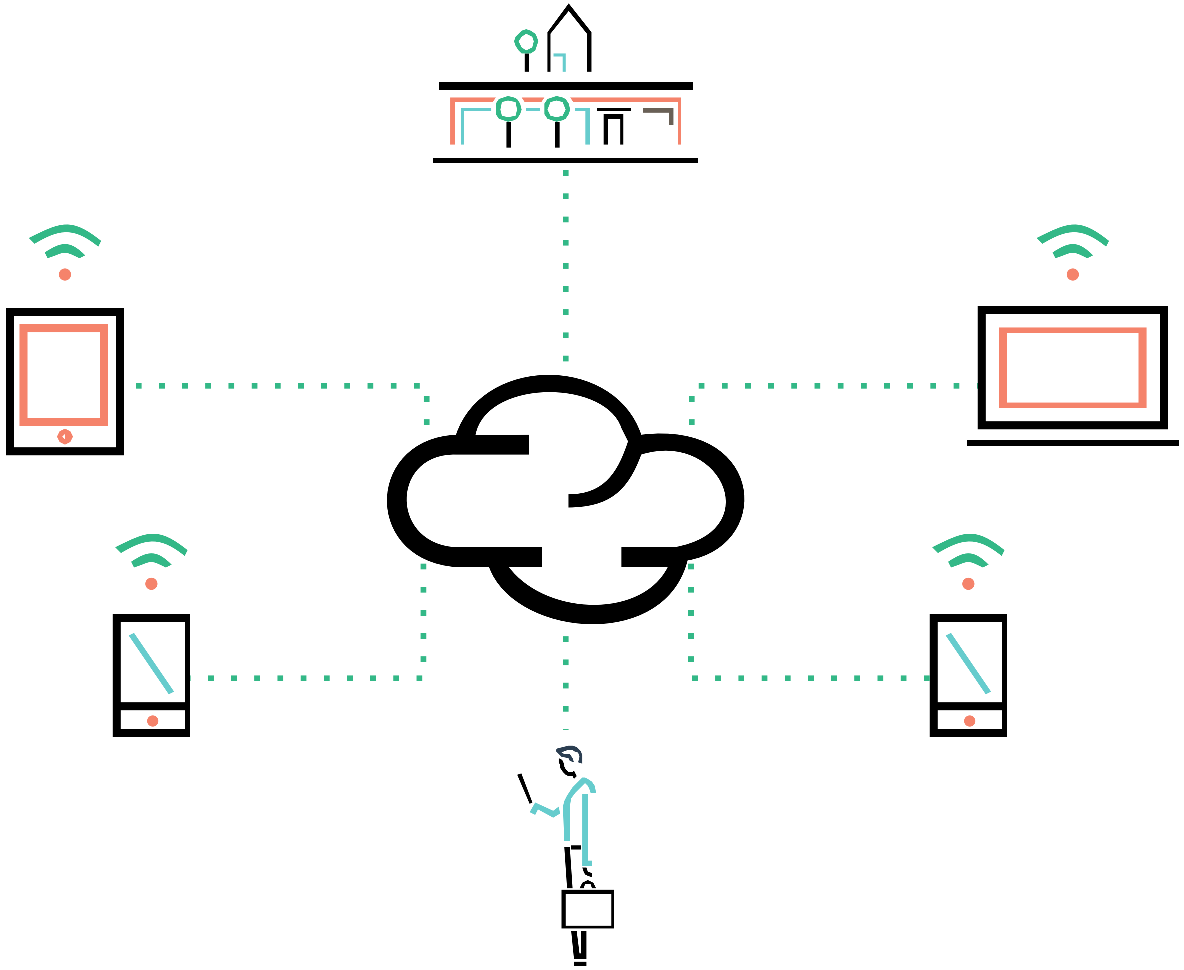
But with increased convenience come increased concerns about combining vulnerable email systems with cloud-based platforms, however secure they may be.

The cloud adds a new set of security concerns about email and sensitive data

Cloud-based systems provide a wealth of resources to organizations large and small, but they come with important challenges, especially in terms of security and handling sensitive data.

IT security professionals should ask several questions of any Office 365 deployment:

- Are built-in security and encryption capabilities enough?
- Should all emails and files be encrypted before they reach the cloud?
- Is there a need for better usability?
- Is there a need for more flexible implementation options?
- Do companies need to own their encryption keys?



Forrester Research weighs in

1 Encrypt emails before reaching Office 365.

"While Office 365 provides many financial and operating benefits, it raises several security challenges…"

"…encryption solutions can encrypt emails before they're stored in the Microsoft cloud and give S&R pros control of the encryption keys."

FORRESTER®

Kelley Mak
Analyst - Security & Risk
Brief: Five Key Capabilities for
Microsoft Office 365
Email Security,
July 29, 2016

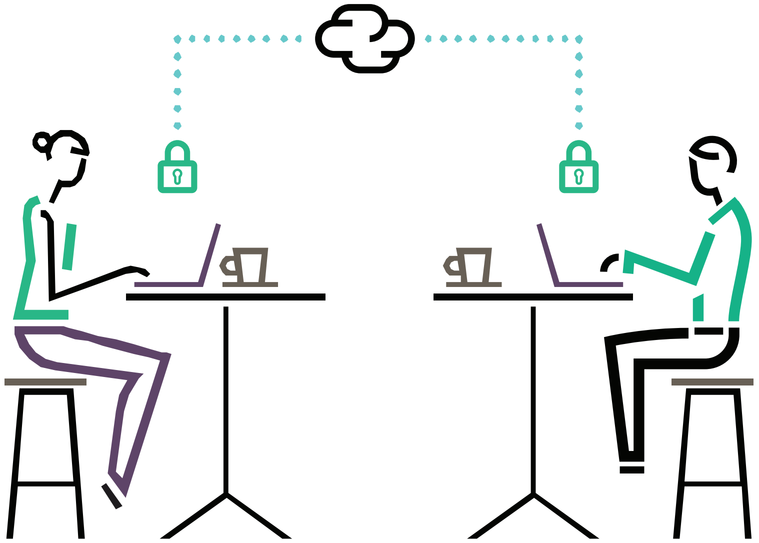
2 End-to-end encryption is a must.

"Data, while in transit or at rest, needs to stay protected. Select an encryption solution that provides full lifecycle data protection, regardless if accessed internally, externally, or through a mobile device."

HPE SecureMail and Office 365: Peace of Mind in the Cloud

HPE SecureMail is a natural fit for Office 365, enhancing its security, privacy, and usability capabilities.

- HPE SecureMail enables end-to-end data protection, full privacy, and confidentiality on Office 365. Only your organization has access to the decrypted data—not Microsoft or even Hewlett Packard Enterprise.
- HPE SecureMail adds multiple usability features that make encryption easy to use. In addition, it provides a full-featured solution to protect collaboration in the cloud.
- HPE SecureMail offers flexible deployment options—in the cloud, on-premise, or on a hybrid model that allows organizations to migrate to the cloud at their own speed and convenience.



By encrypting emails when generated on desktop, mobile or web, HPE SecureMail eliminates privacy and security concerns, because all content is encrypted end-to-end before reaching the Office 365 cloud.

HPE SecureMail: End-to-end encryption and full privacy in the cloud

HPE SecureMail provides corporations with end-to-end encryption of all emails and files. This means encryption of individual emails and files from their point of origin—no matter what device type they originate from—all the way along their lifecycle, without any air gaps. That means all internal and external emails can be protected even from internal admins.

And that offers complete privacy control (even from Microsoft) by encrypting emails before they get to Office 365 servers.

HPE SecureMail: Just click “Send Secure”

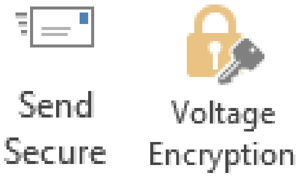
HPE SecureMail client software adds a simple “Send secure” button to send encrypted email from most devices. The HPE SecureMail mobile app is compatible with most mobile operating systems. The desktop plug-in adds an encryption button to outlook and all office apps. And the web interface enables customers and recipients to view secure email on any device.

Mobile

Native user experience for smartphones and tablets

Desktop

Easy-to-use “Secure” buttons within apps

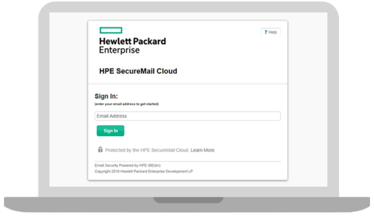


HPE SecureMail

HPE SecureFile

Web

Simple HTML message, easy sign-on, full Mac support



HPE SecureMail Cloud

Sign In:

(enter your email address to get started)

Email Address

Protected by the HPE SecureMail Cloud. Learn More

Email Security Powered by HPE IBE(tm)

Copyright 2016 Hewlett Packard Enterprise Development LP

HPE SecureMail: A complete set of compliance, collaboration, and productivity features.

All features needed to transition from paper to electronic communication

Secure file collaboration

The HPE SecureFile feature encrypts files for cloud collaboration, independent if they are sent via email or not. Users define who can open or edit any sensitive file for full security on cloud collaboration

Large attachments

The HPE SecureFile feature encrypts files for cloud collaboration, independent if they are sent via email or not. Users define who can open or edit any sensitive file for full security on cloud collaboration.

eDiscovery compliance tool

HPE SecureMail eDiscovery decrypts all secure email to facilitate easy indexing and full text searches of pst files and archived emails.

Integration APIs

HPE SecureMail Application Edition uses RESTful API to protect email from different applications and websites that generate, store, and use email.

Secure statements

The HPE SecureMail Statements Edition securely delivers automatically-generated invoices, account information, and other electronic statements automatically generated.

Good dynamics add-on

HPE SecureMail for Good Dynamics simplify regulation compliance, user experience, and management for enterprises leveraging the Good Dynamics MDM platform.

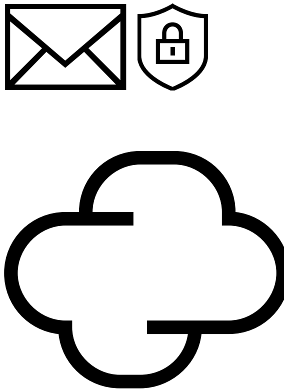
HPE SecureMail: Flexible deployment options

HPE SecureMail comes in several versions to accommodate the varied needs of customers.

HPE SecureMail On-Premises

- **HPE SecureMail On-Premises** is usually deployed by major corporations and companies that want to retain the management of their keys and encryption solution.

HPE SecureMail Cloud



- **HPE SecureMail cloud version** is usually preferred by smaller corporations or those that do not want to manage keys themselves.

Hybrid deployments

- **Hybrid deployments** have been preferred by some customers to enable some aspects of the solution to be on-premises (for example, the key server) and others to be based in the cloud. Customers can also migrate from one case to another.

Customer use case: Top global credit card company

Encrypt all email before it reaches Microsoft Office 365

Description:

This customer, one of the top global credit card companies with operations spread in several continents was very excited about the possibilities collaboration in the cloud could offer their geographically dispersed employees. But, they were also concerned about the privacy and security of their internal and external e-mails and files transiting or stored in the cloud.

Challenge:

- They wanted to have no sensitive data unencrypted in the cloud.
- They wanted end to end security for all internal and external e-mails.
- They wanted an easy to use "send-secure" button.

Solution: HPE SecureMail

We gave them "peace of mind in the cloud" by deploying HPE SecureMail to encrypt all sensitive e-mails and files before they reached the cloud. We replaced legacy e-mails encryption solutions which were hard to use and to manage and added a simple "send secure" button to their e-mail clients. This solution is now used by tens of thousands of employees and millions of external recipients.

Customer use case: Regional Law Firm

Secure collaboration in the cloud

Description:

A large regional law office wanted to collaborate in the cloud using Office 365, but they were concerned about having sensitive data and files in the cloud. They were also not happy with their built-in encryption solution and the fact that Office 365 would own and manage the keys.

Challenge:

- Collaborate securely in the cloud
- Own and manage the keys for complete security
- Define rules for who could open and edit files

Solution: HPE SecureMail with SecureFile

This customer added HPE Securemail with the SecureFile feature to encrypt files when generated on the desktop by simply clicking an “encrypt” button on office applications. Using SecureFile, the users are able to define who can view or edit the file so that only those people can open or edit the file on Office 365, dropbox and other cloud tools. With HPE SecureMail, the customer owns and manages the keys for complete security in cloud collaboration.

Who trusts HPE SecureMail?

Thousands of enterprise and midsize businesses including...

2 of the top 3

US Banks

2 of the top 4

European Banks

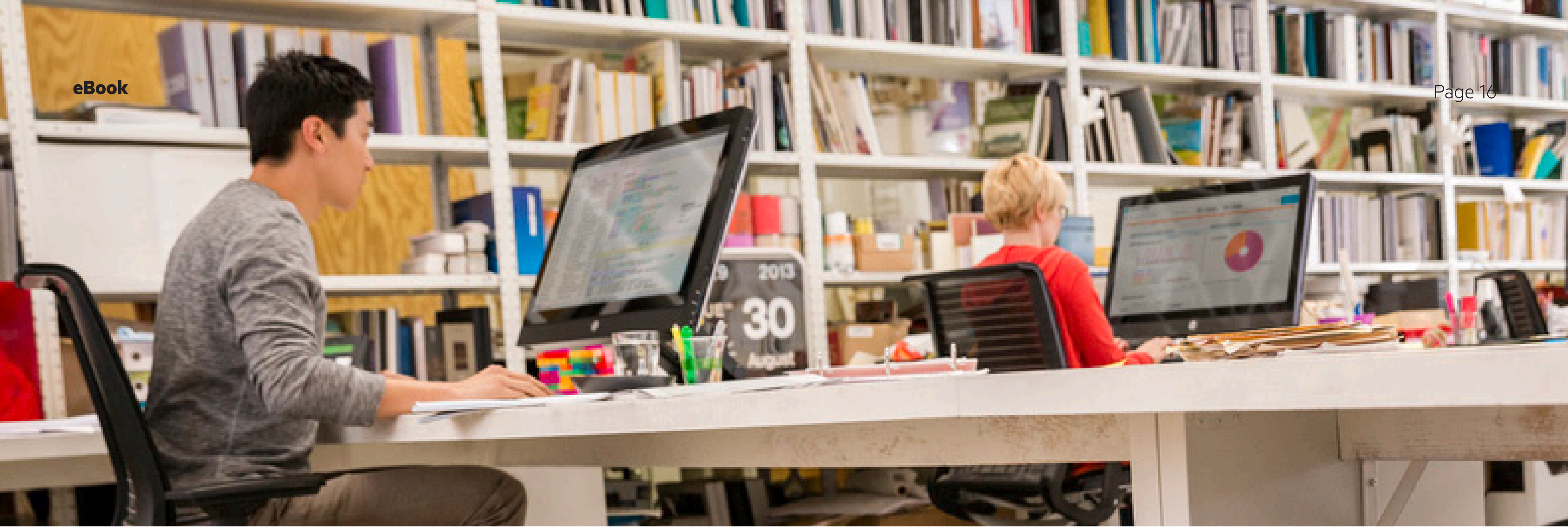
2 of the top 4

Health Insurers

Plus top insurance companies, airlines, telecoms and many others

HPE SecureMail: the most widely deployed email encryption solution

HPE SecureMail is the most widely deployed email encryption solution in the world. We have more than 75 million users worldwide across thousands of enterprise and midsize businesses. These customers cover financial, health care, insurance, and other highly regulated industries.



HPE SecureMail: a natural fit for the Office 365 transition

HPE SecureMail is a natural fit for companies transitioning to Office 365, enabling a wide variety of use cases and functionality:

- **End-to-end protection for internal and external email**
- **Protection for files used in cloud collaboration**
- **Simple user experience: desktop, mobile, and web**
- **Flexible cloud, on-premises, and hybrid deployment**
- **Robust compliance, productivity, and collaboration features**

Contact us today to learn more about how HPE SecureMail can enable your Office 365 use case.

Learn more:

- HPE SecureMail for Office 365
- HPE SecureMail add-ons
- HPE SecureMail Cloud
- Sign-up for a free trial of HPE SecureMail

Sign up for updates

★ Rate this document

Hewlett Packard
Enterprise

2017, Rev. 1