



DATASHEET

Simple Security

PGP for Email and Files

The Internet is an open, flexible playground and there are many pitfalls for both experienced and inexperienced users alike. Many threats exist from viruses, phishing and other scams to the illegal interception of email by governments and individuals. Against this background the average user finds it difficult to make an educated decision on how best to protect themselves. What's more, many people are simply overwhelmed by the sheer number of security solutions to choose from – and ultimately take no action at all!

OX Guard is designed to work within the Open-Xchange environment and also when communicating outside that OX environment.

Within the OX environment

OX Guard delivers user-friendly security with complete transparency – for hosting partners and end-users alike. Users who have subscribed to the service simply create an email as usual. They then hit the 'Send Secure' button. The message is then encrypted before it is sent to the recipient. At the other end, it is automatically decrypted and displayed as normal.

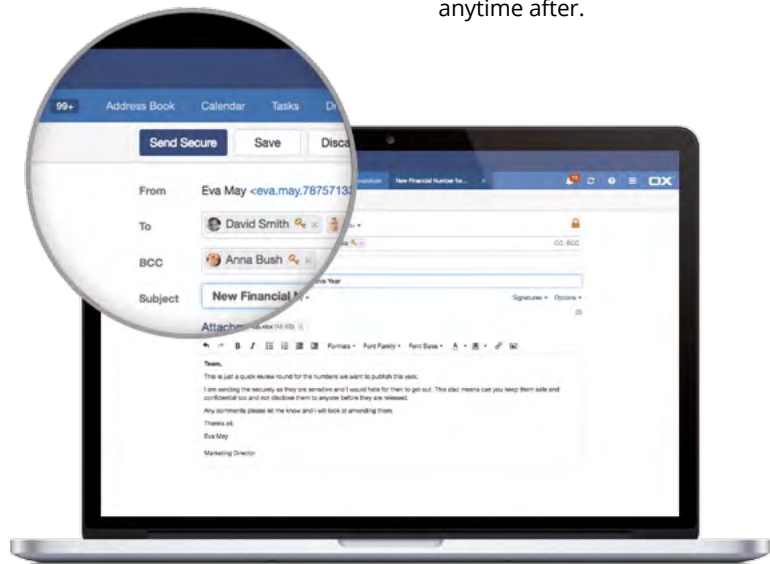
Outside the OX environment

So what happens if the recipient uses a different email service? Instead of receiving the sent email, they receive a special notification email that contains a URL to a secured message reader. By following the link and entering a password, the recipient gains access to the encrypted content.

The web application also provides the opportunity to address new customers through additional marketing, messaging and advertising.

Taking security to a new level

OX Guard not only secures email traffic, but also protects files sent as attachments and stored in OX Drive. Any file stored in OX Drive can be encrypted on upload or anytime after.



Secure because it's simple

PGP Enriched

OX Guard 2.0 adds full PGP compliance to its existing PGP encryption technology. This allows users with regular web clients, as well as mobile devices, to communicate securely using PGP.

Users also have the option to export their personal encryption keys giving them compatibility with other PGP clients such as GPG for Apple Mail and Thunderbird, enabling offline capabilities and integration into existing encryption environments.

OX Guard supports the verification and sending of PGP signed emails. This enhances security and creates another level of compliance with PGP environments.

OX Guard users can manually import and manage PGP public keys from other email recipients. For external recipients without a PGP key, OX Guard provides automated key creation. This makes sending and receiving secure messages and storing secure files completely transparent. More experienced users can share, upload and manage public keys manually. This also lets them fully migrate to OX App Suite from any existing PGP product.

OX Guard for Everyone

OX Guard can be used to encrypt and send emails to recipients that are both inside and outside the OX App Suite ecosystem. This means that recipients using any email client can receive encrypted emails sent from OX Guard without any special security setup upfront.

OX Guard at a glance:

Guest Mode

Public key management available for non-OX Guard users via web interface.

Proven PGP Security

OX Guard uses PGP, one of the world's most secure encryption technologies, to send and receive secure emails and encrypt files.

Simple Email Security

Single click email security: Just press 'Send Secure' to send an encrypted email.

External Secure Email Delivery

Send secure emails outside the OX App Suite environment. Recipients use a secure guest mode client.

PGP Key Management

OX Guard seamlessly integrates into existing PGP environments by allowing users to import, export and share their PGP keys.

Offline Support

OX Guard lets users import and export their personal encryption keys. This enables the use of offline PGP clients such as GPG Mac Mail, Thunderbird, etc.

Signing and Verification

OX Guard supports PGP signing and verification of emails and files.

Encrypted File Storage

Secure files when uploading to OX Drive (Drag and Drop) or manually after uploading.

