p≡p

p≡p Secure Email

Takes away all big email attack vectors

For cloud and on-premises

For every device and platform

All messages fully end-to-end encrypted with no central element

Full protection, oversight, and control of all your data

Zero Trust Architecture by design as defined by NIST

Product Overview

p≡p Secure Email

p≡p Secure Email adds the strongest security for any existing email system while simultaneously allowing full oversight and control of the message flow via the cloud.

The p≡p Secure Email **encrypts all email messages peer-to-peer** and end-to-end and allows for full central oversight and control of all messages through special read-only keys.

The p≡p Secure Email can be deployed **on any end point** that needs to be protected, whether it is an outlook client, an Android or IOS phone, whether **in the cloud, on-premises, or in mixed environments**.

All p≡p solutions achieve **Zero Trust Architecture** as defined by the National Institute of Standards and Technology (cf. NIST SP 800 – 207). p≡p does not replace existing email solutions whether they are cloud based or on premises implementations. Instead, p≡p adds NIST SP 800-207 compliant communication security to heterogenous email setups.

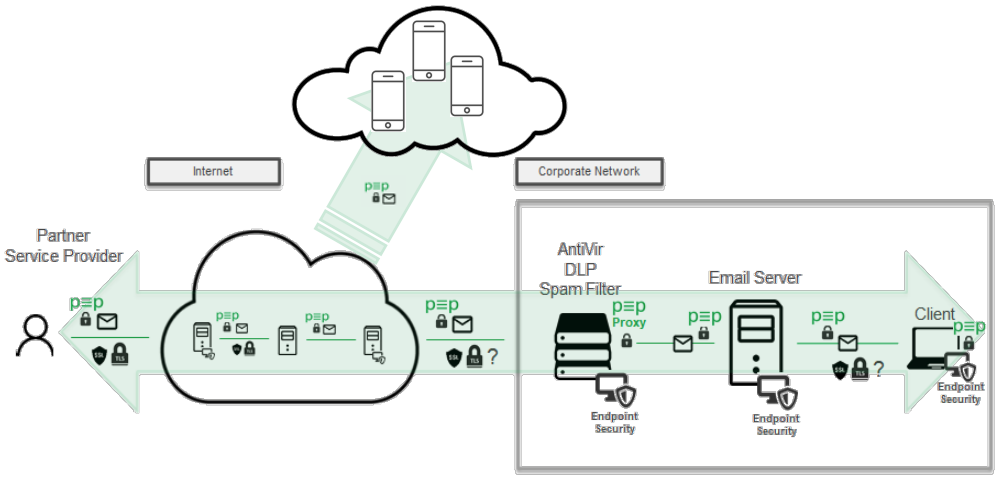
The p≡p Secure Email is designed to **eliminate all major e-mail attack vectors** that are currently still omnipresent in almost any email implementation in the field despite spam filtering and related technologies, thus leaving enterprises and government bodies vulnerable. pEp Secure Email protects against:

- Eavesdropping (Man-in-the-Middle (MITM)) attacks resulting in spying/data theft
- PGP/S/MIME decryption (EFAIL) attacks resulting in spying/data theft
- Identity spoofing (Mailsploit) - Phishing/spear-phishing/social engineering attacks delivering malware/ransomware and data theft
- Data Theft - Mailbox attacks /MITM resulting in spying/data theft

p≡p brings unparalleled advantages to the world of email, including:

1. True end-to-end email security through asymmetric encryption
2. Zero Trust Architecture enabling a peer-to-peer, on-demand, easy to enhance, trusted security community.
3. Ensuring encrypted transport and storage of email
4. Complete email ecosystem protection from desktop to smartphones using desktop client plugins and mobile apps for both iOS and Android.
5. Automatic key-, identity- and trust management eliminating the need for a centrally managed PKI and admin and eliminating key attack vector.
6. Documented front door (read key) to allow for compliance with regulatory content inspection
7. Ease of use through plug & play, set and forget implementation
8. (Encrypted) spam reduction because public keys are not centrally stored on key server
9. Email security classification: trusted & secure, secure and un-secure
10. Ensures GDPR compliance

p≡p can be **rolled out incrementally, step-by-step**. It is not required to implement the "big switch," which otherwise would interrupt existing services. There is no need of the laborious and failure prone task to configure Individual Policies after deciding for General Policies. Instead, p≡p can be rolled out user-by-user, network-by-network, organization-by-organization. p≡p immediately delivers all security properties for all protected users, because it is based on machine learning in the initial set-up phase.



End-to-End Protection
