

ANVÄNDARVÄNLIG E-POSTKRYPTERING

E-postkryptering är en specialiserad säkerhetsteknik för att skydda sekretess och integritet för e-postmeddelanden och bilagor under överföring, användning eller lagring. I det ständigt föränderliga IT-landskapet, behöver organisationer ett integrerat e-postkrypteringsverktyg som fungerar sömlöst med deras befintliga molnsäkerhetstjänster.

Vår egen e-postkryptering

VIPRE Email Security Encryption gör det möjligt för organisationer av alla storlekar att låta sina användare kryptera e-postmeddelanden som innehåller känsliga uppgifter. Den använder den befintliga Advanced Policies-funktionen i Encryption och kopplar den med VIPREs krypteringstjänst för att tillhandahålla en sömlös användarupplevelse.

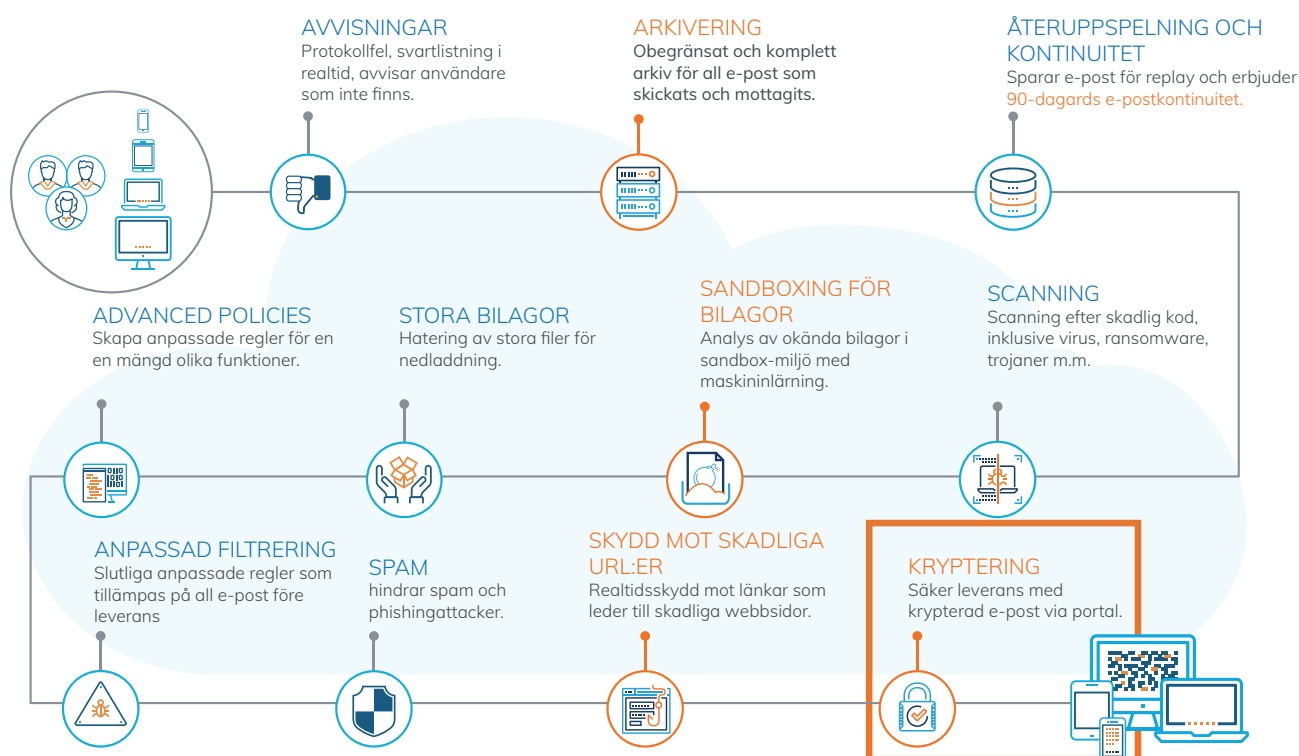
IT-administratörer kan upprätta egna policies för kryptering eller använda redan fördefinierade policies i VIPRE Email Security Encryption. Detta gör det möjligt för en administratör att skydda känsliga uppgifter som delas med användare utanför organisationen, på ett effektivt och säkert sätt.

SNABBFAKTA

- Skyddar privata eller konfidentiella uppgifter i e-postmeddelanden
- Ser till att kunduppgifter överförs på ett säkert sätt
- Medverkar till efterlevnad av lagstiftning och föreskrifter
- Varken avsändaren, mottagaren eller administratören behöver installera någon mjuk- eller hårdvara
- Använd färdiga policies eller upprätta egna som är specifika för din organisation
- Krypterar hela e-postmeddelandet
- Hanteras via VIPRE-portalen

FLER SKYDDSLAGER

Processen för e-posthantering



IT-administratörer

VIPRE Email Security Encryption gör det möjligt för IT-administratörer att spara värdefull tid och resurser. Det finns inte längre något behov av att manuellt spåra och kryptera e-postmeddelanden som innehåller känsliga företagsuppgifter. Ställ bara in önskade policies i VIPRE-portalerna så tillämpar Encryption dessa regler på de e-postmeddelanden som utlöser dem. Enkelt!

E-postavsändrare

Avsändaren behöver inte vidta några åtgärder. Genom att använda Encryption, är e-postsystemet redan inställt för att kryptera e-postmeddelanden som innehåller känsliga uppgifter. IT administratörer behöver bara välja vilken typ av e-postmeddelanden som ska krypteras och Encryption sköter allt i bakgrunden, avsändarens arbetsprocess störs inte.

E-postmottagare

Tidigare var mottagare av krypterad e-post tvungna att ladda ned en programvara till sin dator för att dekryptera ett meddelande. Med Encryption behövs inte det längre. Dekrypterade e-postmeddelanden kan enkelt nås via en säker webbportal.

VIPRE EMAIL SECURITY

Baspaket och tillägsprodukter

	Advanced Threat Protection	Cloud	Essential
Continuity	X	X	Add-on
Sandboxing	X	Add-on	Add-on
Phishing Protection	X	Add-on	Add-on
Archiving	Add-on	Add-on	Add-on
Encryption	Add-on	Add-on	Add-on

Ökad säkerhet

Encryption använder ett antal olika metoder för att säkerställa att din e-post överförs på ett säkert sätt.

EncryptSMART krypterar texten i meddelandet och även alla bilagor med OpenSSL med AES-256-CBCL.

Meddelandena överförs med det säkra TLS-protokollet.

Meddelandena kan endast nås via en unik länk som är kopplad till mottagarens e-postadress och som skickas till dennes e-postkonto.

Dessutom måste mottagaren ange ett lösenord för att få tillgång till e-postmeddelandet och dess innehåll i den säkra portalen. Sökresultaten kan presenteras i olika flikar i browsern för att underlätta.

Färdiga policies

En IT-administratör kan använda fyra fördefinierade policies som utlöser kryptering för organisationens e-postmeddelanden. Krypteringen utlöses om ett eller flera av följande kriterier är uppfyllda:

- Texten i ett e-postmeddelande innehåller känsliga uppgifter som personnummer eller kreditkortsuppgifter
- E-postmeddelandets känslighetsnivå är satt till "Konfidentiellt" i MS Outlook
- E-postavsändaren inleder ämnesraden i ett meddelande med ordet [Encrypt], [ENCRYPT], eller [encrypt]