

# HOSTED EMAIL POLICY BASED ENCRYPTION

## UTMERKELSER

“Denne tjenesten gir bedrifter mulighet til å ta ansvar for sikkerheten til alle personlige og sensitive data de sender i e-postmeldinger. Samtidig styrker det tilliten til meldingsmottakere, både enkeltpersoner og organisasjoner, ettersom dataene deres er beskyttet uten at de må investere i eller forstå sikkerhetsteknologi av høy kvalitet.”

Dommer Louise Bennett, styreleder for British Computer Society Security Forum MessageLabs' krypteringstjeneste med utgangspunkt i retningslinjer  
Vinner: kategorien “Information Security & Data Management”  
BCS IT Industry Awards 2008

## MESSAGELABS-FORSKJELLEN

- Detaljert søk i e-postinnhold og -vedlegg for å identifisere sensitivt innhold.
- Automatisk kryptering av sensitive data med tilpassede retningslinjer du oppretter med MessageLabs' gjennomprøvde innholdskontrollmotor.
- Omfattende sikkerhet og beskyttelse for krypterte e-postmeldinger.
- Rask konfigurasjon, fullstendig vertsbasert og brukervennlig tjeneste. Ikke behov for intern programvare eller maskinvare.
- Støtte for flere språk for sikker global kommunikasjon.
- Støtte døgnet rundt fra MessageLabs' eksperter.

## KAN EN E-POST SOM INNEHOLDER SENSITIVE DATA, UTSETTE BEDRIFTEN FOR RISIKO?

E-post er en akseptert metode for å dele informasjon med partnere og kunder over hele verden. Imidlertid kan en enkelt e-post som inneholder sensitiv eller konfidensiell bedriftsinformasjon, utsette hele organisasjonen for risiko. Manglende beskyttelse av denne informasjonen kan bli kostbart: etterforskning av brudd, fastsettelse av juridiske problemer og å måtte betale bøter fra bransjemyndigheter kan skade bedriften alvorlig.

MessageLabs' kryptering med utgangspunkt i retningslinjer er en vertsbasert tjeneste som hjelper deg med automatisk å verne sikkerheten og personvernet rundt sensitive data du utveksler med kunder og forretningspartnere via e-post. Tjenesten lar deg opprette og håndheve fleksible regler i henhold til bedriftens retningslinjer. Ved å velge en vertsbasert krypteringsløsning kan du beskytte sensitiv informasjon i løpet av noen dager – ikke måneder – og avlaste den krevende oppgaven med å administrere digitale sertifikater og krypteringsnøkler.

MessageLabs' kryptering med utgangspunkt i retningslinjer hjelper deg med å:

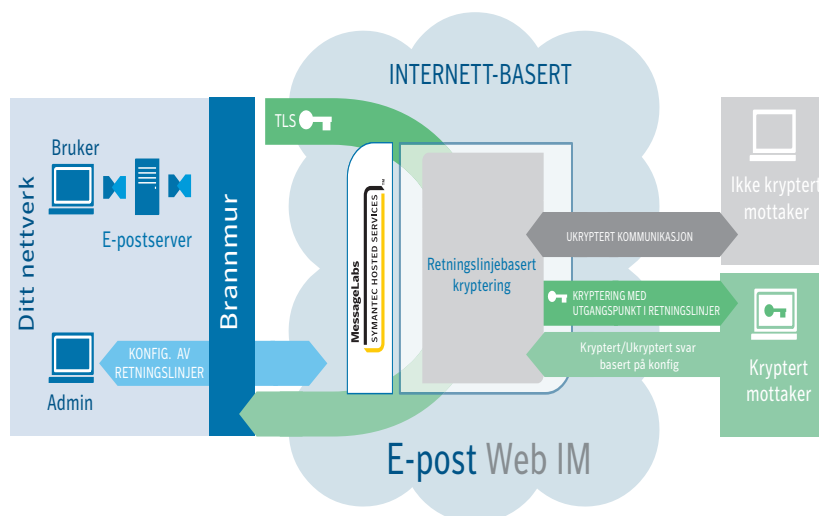
**implementere tiltak for samsvar med regler** mer effektivt ved å iverksette kryptering automatisk basert på tilpassede regler og retningslinjer.

**styrke forhold** med viktige forretningspartnere ved å tilby sikker, umiddelbar levering av konfidensielle data.

**administrere kostnader** ved å eliminere manuelle løsninger for å sende sikre data, og raskt ta i bruk og redusere løsningskostnader.

**beskytte mot e-postvirus** ved å legge til søkemuligheter i MessageLabs' e-postsikkerhetstjenester.

## KRYPTERING MED UTGANGSPUNKT I RETNINGSLINJER – MESSAGELABS-METODEN



## HOLD SENSITIVE DATA SIKRE

- MessageLabs-løsningen lar deg sende og motta sikker, kryptert e-post.
- Utgående e-postmeldinger sendes mellom bedriftens e-postserver og vår infrastruktur via en TLS-kryptert (Transport Layer Security) tunnel.
- Når den brukes sammen med våre e-postsikkerhetstjenester, får du fordelen av et ekstra sikkerhetslag når bedriftens e-postsikkerhet og beskyttelsesretningslinjer blir brukt for å kryptere e-post.
- Hver melding har en unik AES-krypteringsnøkkel for å gi et høyere sikkerhetsnivå.
- MessageLabs' sikre portal lar eksterne brukere skrive og svare på sikre meldinger.

## MESSAGELABS OPPLEVELSEN

- E-postavsendere: Tjenesten er enkel å bruke, og individuelle avsendere trenger ikke bestemme seg for hva som er eller ikke er sensitive data. Det er ingen ekstra trinn for å kryptere meldinger.
- E-postmottakere: Innhenting av krypterte meldinger er raskt og enkelt, samtidig som krypterte svar gir toveis e-postsikkerhet.
- Tjenesteadministratore: Enkelt oppsett, konfigurasjon og rapportgenerasjon minimerer belastningen på administratorene og behovet for opplæring av sluttbrukere.

## NESTE TRINN

Kontakt en produktspesialist:  
Norge: +47 2257 7780  
info@messagelabs.com

Du finner informasjon om kontorer i andre land og kontaktnumre på:  
www.messagelabs.no/contact

Når du konfigurerer tjenesten, har du maksimal fleksibilitet til å fastslå hvordan krypterte meldinger blir håndtert av mottakeren. Du kan velge at utgående meldinger blir levert rett i mottakerens innboks, eller du kan sende mottakeren et varsel med en kobling slik at vedkommende kan hente den krypterte meldingen fra en sikker webportal. Du kan eventuelt la det være opp til mottakerne å håndtere krypterte meldinger på den måten som passer dem best.

Tjenesten er fullstendig vertsbasert og krever ikke installasjon av programmer eller maskinvare hos avsendere eller mottakere – uavhengig av om organisasjonene eller enkeltpersonene som utveksler e-postmeldinger med bedriften, er MessageLabs-kunder eller har sine egne krypteringsmuligheter.



| FUNKSJONER   | FORDELER  |
|--|---|
| Automatisk kryptering av sensitive e-postmeldinger   | Bruker bedriftens krypteringsretningslinjer automatisk og på en sikker måte, og legger til rette for å overholde tiltak for samsvar med regler  |
| Stort utvalg av leveringsmekanismer for e-post   | Gir enkel tilgang til krypterte e-postmeldinger   |
| Sikre muligheter til å svare på og skrive e-post   | Tillater sikker, toveis e-postsending for alle mottakere  |
| Lesekvitteringer blir automatisk videresendt til e-postavsender  | Gir tillit til at meldingene blir "plukket opp" av mottakeren   |
| Kompatibilitet med forskjellige plattformer, inkludert BlackBerry og Windows Mobile                      | Sikre meldinger kan leses uavhengig av hvilken teknologi mottakeren bruker. Og det er ikke behov for at mottakerne må ha krypteringsmuligheter. |
| Fullstendig vertsbasert tjeneste, inkludert administrasjon av digitale sertifikater og krypteringsnøkler | Reduserer IT-administrering og kostnader uten behov for programvare, programmer eller oppgraderinger  |
| Raskt og enkelt å sette opp, konfigurere og bruke  | TLS-aktiverte selskaper kan komme i gang i løpet av noen dager. Minimerer belastningen på administratorene og brukere.                          |



Confidence in a connected world.