VIPRE EMAIL SECURITY CLOUD
Tilleggsmoduler

SIKKERHET OG SAMSVAR

For nesten alle bedrifter, små eller store, er e-post det viktigste kommunikasjons-verktøyet både internt og eksternt. Problemet er at cyberkriminelle og ondsinnede aktører vet dette, og angriper bedrifter hver dag i form av phishing, vedlegg og lenker med skadelig programvare. De fleste bedrifter bruker en grunnleggende form for e-postskanning, støttet av en sikkerhetsløsning for endepunkt. Med dagens komplekse sikkerhetssituasjon gir dessverre ikke passiv skanning tilstrekkelig beskyttelse. VIPRE tilbyr multilagsløsninger for e-postsikkerhet som bekjemper de verste malware-truslene i dag.

VIPRE Email Security har samlet inn ondsinnede og godartede prøver i over 20 år, og tilbyr moderne maskinlæringsteknologi med nøyaktig og effektiv levering. Med VIPRE Email Securitys unike modulbaserte arkitektur kan du velge nøyaktig de komponentene du trenger for å oppnå maksimal e-postsikkerhet i ethvert spesifikt miljø, og bekjempe både dagens og fremtidens trusler.

Omfattende serie

Alt fra samme leverandør VIPRE er din eneste kilde, fra bestilling og levering til støtte. Få mer for mindre med én pålitelig leverandør.

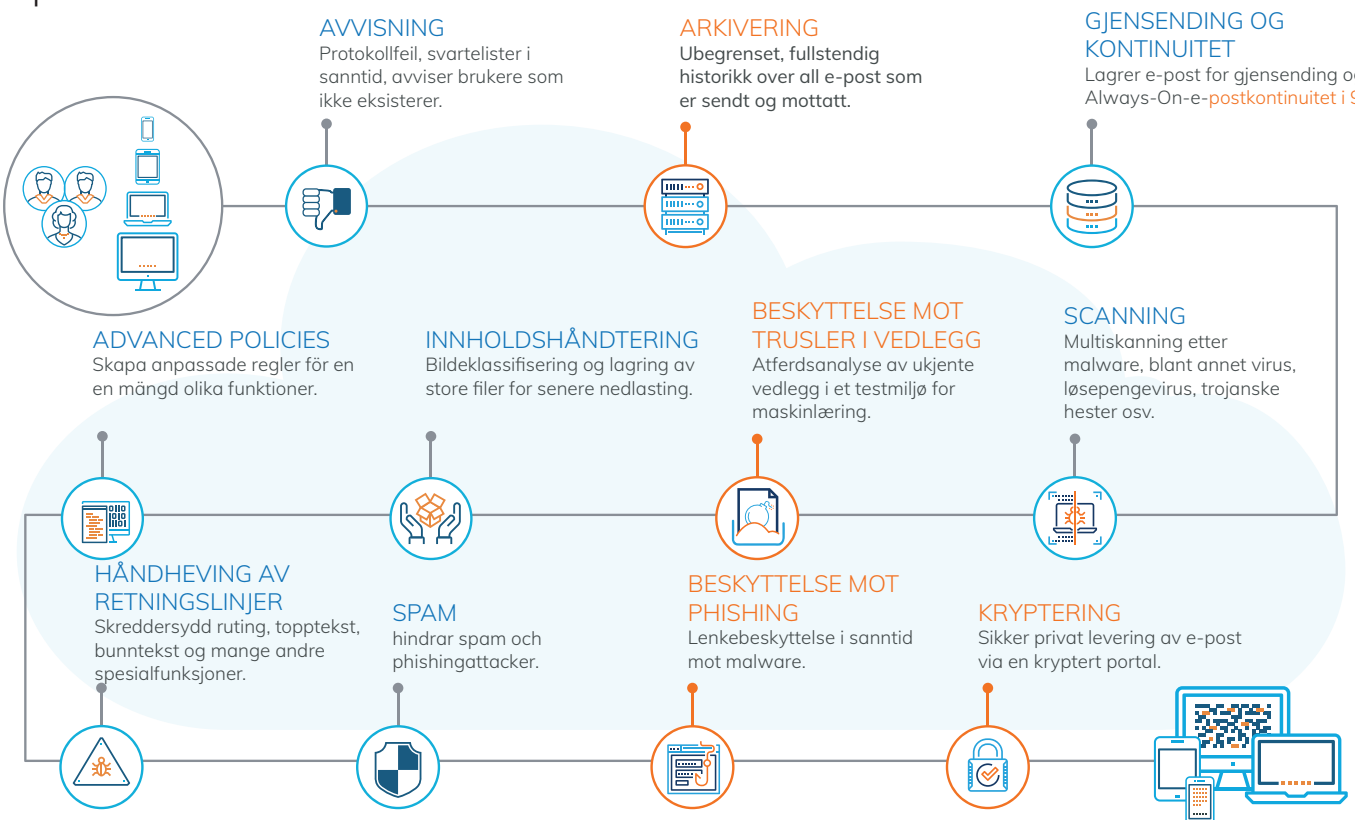
Skreddersydd e-postsikkerhet

Med VIPREs modulbaserte design får du full kontroll og kan skreddersy nøyaktig den e-postpakken som passer for din bedrift.

Enkel å bruke og konfigurere

Spar tid, penger og ressurser med bare én styringskonsoll fra VIPRE, som gir deg fleksibel og strømlinjeformet administrasjon. Enkelt oppsett og levering holder virksomheten i gang uten avbrudd.

BESKYTTELSESLAG:
E-postreisen



Supplement til grunnleggende e-postbeskyttelse

Dagens zero-day-angrep, ulike former for malware og trusler i vedlegg krever en sofistikert multilagsløsning for å sikre bedriften. VIPRE Email Security med tilleggsmoduler, som leveres i form av en fleksibel, skybasert arkitektur, er et trygt valg for å håndtere moderne e-posttrusler.

Email Security Attachment Threat Protection: VIPREs Behavioural Determination Engine er en kunstig intelligens-motor som bruker maskinlæring for å vurdere om det er potensielt ondsinnet atferd i ukjente vedlegg, og brukes mot zero-day-trusler uten tidligere deteksjonshistorikk.

- Maskinlæringsmodell basert på atferd i millioner av observerte malware-prøver.
- Vedlegg testes i et beskyttet miljø for å fange opp eventuell ondsinnet aktivitet, eller forsøk på å laste ned ytterligere komponenter som også utfører ondsinnet aktivitet.
- Dynamisk og isolert skybasert virtuelt maskinmiljø som enkelt skaleres for å håndtere belastningen fra alle klienter.
- Detaljert atferdsanalyse som forklarer nøyaktig hva vedlegget forsøkte å gjøre ved iverksettelse.
- Alternativ for tidlig frigivelse som gjør det mulig for brukeren å frigi sine egne vedlegg, avhengig av sluttbrukernes og organisasjonens risikoprofil.

Email Security Phishing Protection: Automatisk deteksjon og blokkering av ondsinnede lenker beskytter mot lenker som kan bli skadelige etter at de har passert spam- og virusfiltre.

- Skanner og blokkerer lenker som kan føre til infisering med malware.
- Reduserer angrep fra ondsinnede lenker.
- Omskriver alle nettlenker i e-post.
- Skreddersydde meldinger og fleksibel rapportering.
- Velg relevante meldinger for advarsler og blokker sider.
- Enkel tidsplanlegging av statistiske rapporter.

Email Security Archiving: Rask og enkel arkivering med skreddersydde styringsregler.

- Arkiverer all intern og ekstern inngående og utgående e-post.
- Alt e-postinnhold er fullt ut indeksert og søkbart.
- Sluttbrukertilgang til arkivet kan enkelt aktiveres og deaktiveres.
- Avansert søk støtter komplekse forespørsler i alle e-postattributter.

Email Security Encryption: Enkelt å opprettholde taushetsplikt og sikkerhet i e-post.

- Du kan lage skreddersydde retningslinjer eller bruke praktiske, forhåndskonfigurerte retningslinjer.
- Det kreves ingen ytterligere fremgangsmåte eller prosedyre fra avsenderens side.
- Dekryptert e-post er lett tilgjengelig via en sikker nettportal.
- Krypterer ved hjelp av OpenSSL med AES-256-CBCL, meldinger flyttes via TLS-protokoll.

Email Security Continuity: E-postkontinuitet og gjensending av e-post i 90 dager fra sikkerhetsportalen for e-post.

- Always-On-e-postkontinuitet.
- Gjensending av e-post i 90 dager.
- Brukeren kan logge inn fra en hvilken som helst enhet med internettforbindelse for å sende og motta e-post.

VIPRE Attachment Threat Protection, Phishing Protection, Archiving, Encryption og Continuity er tilleggstjenester som krever VIPRE Email Security Essentials eller VIPRE Email Security Cloud.

MER INFORMASJON: Gå inn på global.VIPRE.com
ring +47 6779 2324 eller send en e-post til sales@VIPRE.com