

ADVANCED THREAT PROTECTION (ATP)

Flerlagssikkerhet med Sandboxing og phishing-beskyttelse

Datakriminalitet er en økende trussel som utvikles kontinuerlig, i takt med at cyberkriminelle tar i bruk avansert teknologi som zero-hour exploits og tilpasset skadelig programvare for å ligge et steg foran. Tradisjonell e-postbeskyttelse er nødvendig, men mangler ofte den moderne teknologien som trengs for å analysere og stoppe slike angrep. Det kreves en sikkerhetsløsning i flere lag som skanner og oppdager ulike typer skadelig kode, også i vedlegg og nettlenger.

Skadelige e-postvedlegg blir stadig mer vanlig

Små og mellomstore bedrifter blir ofte utsatt for ulike typer angrep, der kriminelle blant annet forsøker å trenge gjennom e-postbeskyttelsen. Disse bedriftene har ikke de samme ressursene som store selskaper, men trenger samme beskyttelse, og de har dessuten stort behov for kostnadseffektivitet og enkel administrasjon. VIPRE ATP er en løsning som passer perfekt for denne gruppen.

- "Gjennomsnittsbedriften fikk over 94 % av den oppdagede skadelige programvaren via e-post, og over 45 % av den skadelige programvaren ble levert via e-postvedlegg som inneholdt vanlige Microsoft Office-dokumenter."
- Verizon 2019

VIPRE Email Security Advanced Threat Protection (ATP) tilbyr kraftfull e-postbeskyttelse som er enkel å bruke og administrere. VIPRE ATP forsvarer sluttbrukeren mot de nyeste og mest sofistikerte typene av skadelig programvare, skadelige vedlegg og phishing, som ofte ikke oppdages eller stoppes av tradisjonelle løsninger for e-postbeskyttelse.

En plattform med lokal støtte

VIPRE leverer en komplett sikkerhetsplattform som også inkluderer profesjonell støtte på det lokale språket.

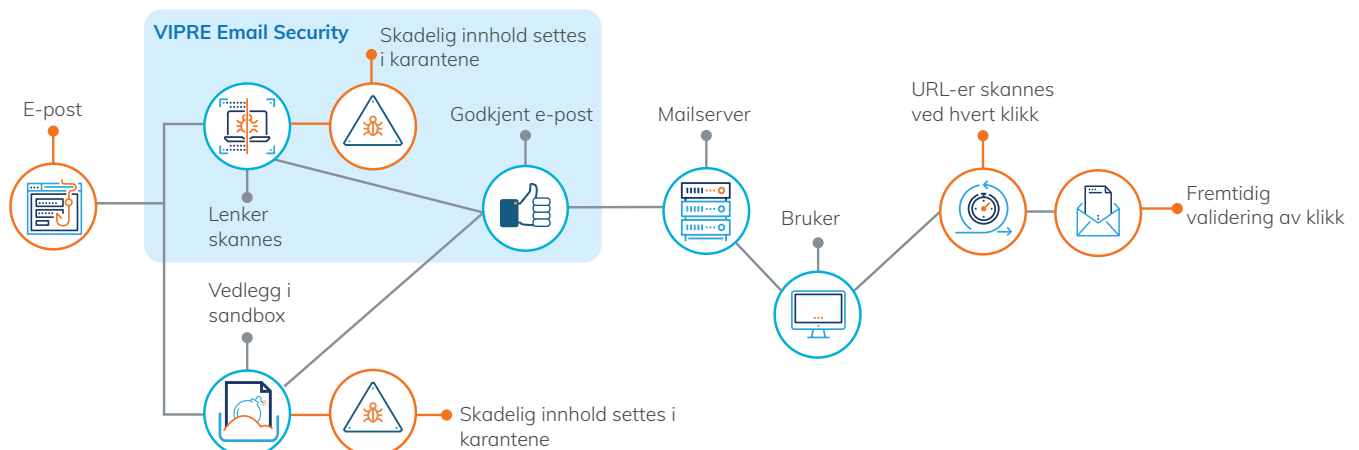
En løsning som stopper ulike typer angrep

Beskytter mot skadelige e-postvedlegg og skadelige nettlenger.

Beskyttelse mot zero-hour-angrep

Signaturbasert deteksjon kombinert med sandboxing og maskinlæring med atferdsanalyse gir deg kraftfull beskyttelse mot zero-hour-angrep.

VIPRE Email Security Cloud: E-posthåndtering med ATP



Kraftfull beskyttelse i flere lag

Kjernen i VIPRE ATP består av VIPRE Email Security Cloud, en plattform for e-postsikkerhet som muliggjør sikker håndtering av e-posten din. Plattformen beskytter mot spam, virus og phishing, og omfatter dessuten e-postkontinuitet og mange muligheter for egen tilpasning av filtrering og regler.

- Kraftfull beskyttelse mot spam, virus og phishing
- Avansert funksjon for å opprette egne regler/retningslinjer tilpasset dine behov
- 90 dagers e-postkontinuitet som sikrer at e-posten alltid fungerer, også når e-postserveren er nede
- Pålitelig og kraftfull tjeneste med lokal støtte

Attachment Sandboxing utvider sikkerheten ved å teste e-postvedlegg i et sandbox-miljø. Ved hjelp av maskinlæringsteknologi observeres vedlegg ved utførelse, og sammenlignes deretter med tidligere kjent skadelig kode for å vurdere om de utgjør en sikkerhetsrisiko.

- Kraftfull sandboxing-teknologi
- Beskytter mot skadelig kode som normalt består tester i sandbox
- Dynamisk isolert skyløsning med virtuelt miljø som enkelt kan oppskaleres
- Detaljert atferdsanalyse som beskriver hva skadelig kode i vedlegg forsøker å oppnå ved utførelse

Phishing Protection beskytter mot skadelige nettlenger ved å redusere tiden som utnyttes av kriminelle, fra skanning ved mottak av e-post (via basisplattformen) til brukeren klikker på en nettlengde. Ofte venter de kriminelle med å sette opp det skadelige domenet til en stund etter at e-postmeldingen er sendt, noe som kan lure mottakeren til å gå inn på en nettside med phishing. VIPRE Phishing Protection beskytter brukeren ved å skanne lenkene hver gang han/hun klikker på dem, uansett når det skjer.

- Skanner nettlenger og blokkerer lenker som fører til nettsider med skadelig innhold
- Omskriver URL-er i e-postmeldinger for å gi beskyttelse ved hvert klikk
- Rapporter og statistikk, samt mulighet for å tilpasse meldinger for advarsel og blokkering

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

