



WebSense®

## Hosted Email Security

Dagens trusselbilde kjennetegnes ved sammenfallende angrep mot e-post og Internett, og over 85 prosent av uønskede e-poster inneholder nå URL-addresser. Virksomheter står også overfor en økende risiko forbundet med tap av informasjon og brudd på akseptabel bruk av e-post. Mens trusselbildet knyttet til bruken av e-post blir stadig mer omfattende og avansert, trenger ikke håndteringen av e-postsikkerhet å være det.

WebSense® software-as-a-service (SaaS) e-postsikkerhet integrerer markedets beste løsninger innen Internett-sikkerhet og Informasjonssikkerhet med e-postsikkerhet for å oppnå best mulig beskyttelse mot nye trusler knyttet til e-post. Denne enkle tjenesten tilbyr svært nøyaktig deteksjon av søppelpost, virus, spionware, phishing og sammenfallende trusler mot e-post og Internett. Forhåndsdefinerte innholdsordbøker er med på å gjøre det enklere å hindre datatap, imøtekomme krav og håndheve regler rundt akseptabel bruk av e-post.

“At e-posten kontrolleres i skyen [med WebSense Hosted Email Security] tar bort mye jobb for våre egne servere og fjerner behovet for daglig administrasjon.”

**Terry Kemp**

Infrastructure Manager  
Nelson Marlborough  
District Health Board

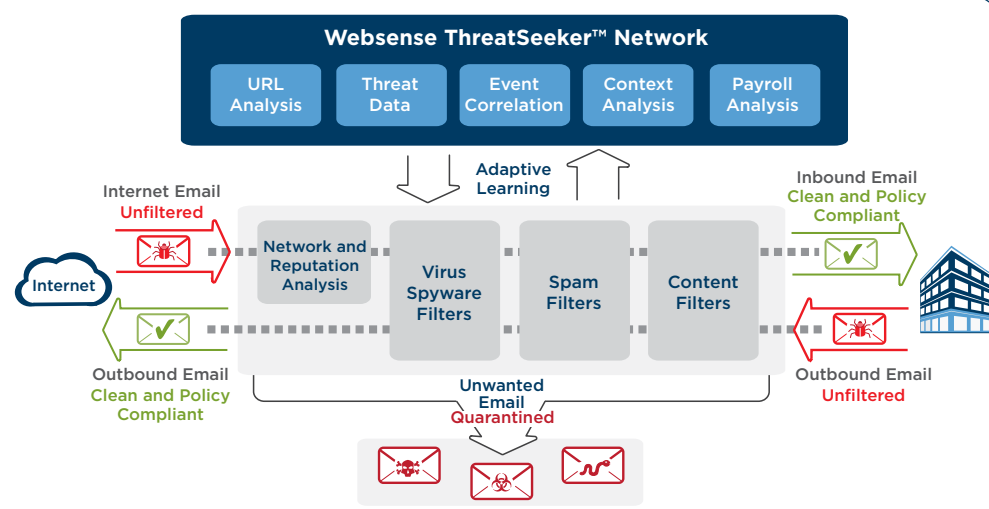
### Slik fungerer det:

Det er enkelt å beskytte e-post med WebSense SaaS e-postsikkerhet. Bare send MX-registre til WebSense, så filtreres alle e-poster før de når nettverket, noe som gir store innsparinger i bredbånd og lagringsplass. WebSense sine datasentre er lastsbalanserte, redundante, distribuerte

clusterer som befinner seg på 10 ulike steder verden over. Tjenesten tilbyr en SLA knyttet til tilgjengelighet på 99,999 prosent og den er også sertifisert i henhold til ISO27001-standarden for å dokumentere nivået for sikkerhet, personvern og konfidensialitet.

WebSense SaaS e-postsikkerhet gjør at kundene kan:

- **Redusere kostnader og kompleksitet** uten utstyr i lokalene som må installeres eller vedlikeholdes, innsparinger i bredbånd og lagringsplass, forutsigbare kostnader og reduserte administrasjonskostnader.
- **Øke sikkerheten** med en markedsledende sikkerhetsløsning som vil fungere mot sammensatte trusselbildet mot e-post og Internett. Løsningen støttes av bransjeledende SLAer og all intelligens knyttet til WebSense ThreatSeeker™ Network.
- **Sikre kontroll** med tilgang døgnet rundt og fleksibel tilpasning av regler, konfigureringsinnstillinger, karantenebehandling og rapportering.



“Når vi tok i bruk  
Websense Hosted  
Email Security forsvant  
søppelposten på et  
blunk.”

**Lee Smith**  
IT Operations Manager  
Harvey Nichols

## Hosted Email Security Capabilities

Hosted Email Security Packages	Antispam	Antivirus	Innholdsfilter	Kryptering
Hosted Antispam	●			
Hosted Email Security	●	●		
Hosted Email Security and Content Control	●	●	●	●

### Antispam

Websense tilbyr svært presis blokkering av søppelpost med svært få falske positive. Tjenesten støttes av en SLA som sier at 99 prosent av søppelpost skal sperres. En kombinasjon av ulike teknologier brukes til å identifisere søppelpost, inkludert avsenderens reputation, tilpasset læring, URL-analyse, heuristikk, digitale fingeravtrykk og optisk gjenkjenning av bildesøppelpost. Viktigst av alt er at dette er den eneste løsningen som integrerer Websense sin markedsledende teknologi innen Internett-sikkerhet, for å beskytte mot phishing og sammenfallende trusler mot e-post og Internett. Hver e-post tildeles en samlet poengsum som sammenlignes med en kundefinert terskel for å avgjøre hva som skal gjøres.

### Antivirus

Innkommende og utgående e-poster skannes for virus, spionvare og andre former for skadeprogrammer med en tilnærming i flere lag med tre separate kommersielle antivirus-løsninger og Websense ThreatSeeker Network som beskytter mot både kjente og ukjente trusler. ThreatSeeker Network tilbyr øyeblikkelig beskyttelse ved å kontinuerlig analysere e-post og nettsider for å oppdage trusler og mønstre som identifiserer gryende trusler og minimerer tiden det går fra et utbrudd til trusselen er fjernet. Tjenesten støttes av 100 prosent SLA på gjenkjenning av kjente virus.

### Innholdsfilter

Integrert teknologi fra Websense sine markedsledende informasjonssikkerhetsløsninger gjør det enkelt å hindre informasjonlekkasjer, imøtekomme krav og håndheve regler for akseptabel e-postbruk. Forhåndsdefinerte ordbøker dekker 20 emner på 12 språk samt innebygd PCI-DSS og personvernmaler som hjelper virksomheter med raskt å identifisere og stoppe brudd gjeldende regler for akseptabel bruk av e-post. Brudd identifiseres gjennom dyptgående inspeksjon av både e-postmeldingen og innholdet i vedlegg. Meldinger kan også settes i karantene basert på vedlegg gjennom filtype og utsettes til senere levering basert på størrelse.

### Kryptering

Websense encryption sikrer e-postkommunikasjon uten å ofre muligheten til å inspisere krypterte e-poster for skadeprogrammer og innhold. Websense støtter server-til-server-kryptering ved hjelp av bransjestandarden TLS (transport layer security) og ad hoc-kryptering for kommunisering til enkeltpersoner. Regler for kryptering kan konfigureres for å kryptere kommunikasjon basert på avsender, mottaker, innstillinger for ulike grenseverdier eller et nøkkelord i emnet. Kryptering kan brukes i kombinasjon med innholdsfiltrering for å kryptere e-poster som inneholder spesifikt innhold, som sensitiv eller konfidensiell informasjon.

Websense SaaS email security fungerer også hånd i hånd med Websense SaaS Web security for å tilby integrert beskyttelse av e-poster og Internett, noe som gjør at virksomheter kan konsolidere administrasjon og rapporteringen for både e-post- og Internett-sikkerhet.

Funksjoner	Fordeler
Beskyttelse mot spam og virus	Svært nøyaktig SLA-støttet beskyttelse mot søppelpost, virus, spionvare, phishing og sammenfallende trusler mot e-post og Internett.
Øyeblikkelig oppdagelse av trusler	Sikkerhetsinformasjon fra ThreatSeeker Network identifiserer og stopper gryende trusler ved å lukke utsettelsesvinduet.
Data loss prevention	Integrert teknologi fra Websense sine markedsledende datasikkerhetsløsninger hindrer tap av informasjon og er med på å imøtekomme regulatoriske krav.
Innholdsfiltrering	Forhåndsdefinerte innholdsordbøker dekker 20 emner på 12 språk og gjør det enkelt å raskt identifisere brudd på regler for bruk av e-post.
Kryptering	Beskytt sensitive og regulert informasjon med sikker e-postkommunikasjon til forretningspartnere og enkeltpersoner
Levering av programvare som en tjeneste	Spar tid og penger uten behov for å installere eller vedlikeholde utstyr, innebygd redundans, forutsigbare kostnader og reduserte administrasjonskostnader.
Global datasenterinfrastruktur i toppklassen	Ti globale datasentre med fullstendig redundans, kjøling og Internett-forbindelse gir høy tilgjengelighet med 99,999 prosent SLA på oppetid.
Sikkerhetssertifiseringer	Uavhengig gjennomgang og sertifisering av sikkerhetspraksis for ISO27001 sørger for høyeste nivå av sikkerhet, personvern og konfidensialitet
Tilgang og kundestøtte døgnet rundt	Aksesser og administrer tjenesten gjennom en nettbasert portal som er tilgjengelig når som helst fra hvor som helst på Internett med døgnåpen kundestøtte for ekstra hjelp når du trenger det.
E-postspoling for nødgenoppretting	Innebygd redundans og e-postspoling sørger for at e-post aldri går tapt når en kunde opplever driftsstans på nettverk eller e-postserver.
Karantenebehandling	Kraftige søkemotorer for meldinger gir komplett synlighet og tilgang til meldinger og logger som er satt i karantene.
Selvbetjening for sluttbruker	Planlagt og forespurt brukertilgang for å se og frigjøre meldinger som er satt i karantene og hvitelistede/svartelistede avsendere reduserer administrasjonskostnader.
Integrering av katalogtjeneste	Automatisk synkronisering av e-postadresser og grupper med Active Directory og LDAP forenkler administrasjon av regelsett.
Rollebasert administrasjon	Separate tilgangskontroller for karantenebehandling, visning av rapporter, tilgang til revisjon og andre nøkkelfunksjoner gir delegert administrasjon.
Forebygging av Directory Harvest Attacks (DHA)	Innebygd beskyttelse hindrer spammere i å få tak i gyldige e-postadresser.
Rapportering	Over 40 forskjellige rapporttyper med oppsummering og detaljert teknisk informasjon gir 360 graders synlighet i trusseltyper og volumer, meldinger som er behandlet, regelbrudd og mer.

## Websense ThreatSeeker™ Network

Websense ThreatSeeker Network sin tilpasningsdyktige sikkerhetsteknologi bruker mer enn 50 millioner datainnsamlingsystemer i sanntid som kontinuerlig overvåker Internett-innhold, inkludert nytt og dynamisk innhold, for øyeblikkelig beskyttelse mot gryende trusler. Denne forskningen og informasjonen kommuniseres i sanntid til Websense sine produkter. Som et resultat kan Websense tilpasse seg til det raskt voksende Internett på en dynamisk og fleksibel måte, noe som ikke er mulige med tradisjonelle sikkerhetsløsninger.

**Websense, Inc.**  
San Diego, CA USA  
tel 800.723.1166  
tel 858.320.8000  
www.websense.com

**Websense UK, Ltd.**  
Reading, Berkshire UK  
tel 0118.938.8600  
fax 0118.938.8697  
www.websense.co.uk

**Australia**  
websense.com.au

**Israel**  
websense.com

**Kina**  
prc.websense.com

**Italia**  
websense.it

**Frankrike**  
websense.fr

**Japan**  
websense.jp

**Tyskland**  
websense.de

**Nederland**  
websense.com

**Hongkong**  
websense.cn

**Singapore**  
websense.com

**India**  
websense.com

**Spania**  
websense.com/latam

**Irland**  
websense.co.uk

**De forente arabiske emirater**  
websense.com

### Innkommende trusler



- Søppelpost
- Virus
- Skadelige URL-adresser



### Innebygd Internett- og datasikkerhetsinformasjon

- ✓ Threatseeker
- ✓ Øyeblikkelig informasjon
- ✓ URL-analyse
- ✓ Forhåndsdefinerte ordbøker
- ✓ Dyp innholdsinspeksjon
- ✓ Avansert mønstermatching

### Utgående risikoer



- Informasjon på avveie
- Akseptabel bruk
- Regulatoriske krav

Intelligent Email Security

## E-postpersonvern

### ISO 27001

Websense SaaS e-postsikkerhet er gjennomgått og sertifisert i henhold til ISO 27001-standarden for å sikre høyeste nivå av sikkerhet, personvern og konfidensialitet. ISO 27001 er en systemstandard for behandling av informasjonssikkerhet. Den ble publisert i oktober 2005 av den internasjonale organisasjonen for standardisering. Denne sertifiseringen er anerkjent bevis på kvaliteten til en veikslomhets sikkerhetsprogram og den strengeste sikkerhetsstandarden i bransjen, og overgår SAS 70-kravene som mange konkurrenter har som sin sertifiseringsreferanse.

### Datasentersikkerhet

Av alle stedene e-posten din rutes via er Websense sine datasentre blant de tryggeste stedene den kan dirigeres til. Websense har strenge mekanismer for sikkerhet og personvern i selve datasenterets leveringsnettverk. Rene e-poster beholdes ikke av tjenesten, og andre e-poster er bare synlige for dem som har administrative rettigheter til systemet, spesifikt nettverks-administratorer og andre som du har gitt tilgang til din konto. Websense-datasentre overholder strenge fysiske sikkerhetskrav i tillegg, inkludert:

- Ansatte på jobb døgnet rundt hele året
- Registreringssystemer for fysisk inntrenging
- Videoovervåking
- Lister over begrenset adgang
- Bilde- og biometriverifisering 24 x 7 x 365 staffing

## Oppsummering av tjenestenivåavtale

Websense tilbyr bransjeledende SLAer som sørger for at tjenesten fungerer på høyeste nivå.

- **Tilgjengelighet** — 99,999 prosent
- **Søppelpost** — 99 prosent eller høyere registreringsgrad
- **Virus** — 100 prosent gjenkjennelse av kjente virus
- **Behandlingsventetid** — 60 sekunder eller mindre for e-post uten søppelpost på under to megabyte
- **E-postlogger og karantene** — Tilgjengelig fem minutter eller mindre etter e-postmottak

Alle SLAer er underlagt de samme betingelser og vilkår som beskrevet i kundeserviceavtalen.