



“Genom att få kontroll på vår e-post med en värd-baserad lösning avlastas våra servrar inom kontoret och behovet av daglig administration eliminerar.”

Terry Kemp

Infrastructure Manager
Nelson Marlborough
District Health Board

Websense® Hosted Email Security

Det som främst hotar dagens e-postmiljö är kombinerade e-post- och webbattacker med mer än 85 % oönskad e-post innehållande en bifogad URL. Organisationer ställs också inför ökande risker associerade med dataförluster. Samtidigt som e-posthoten blir alltmer komplexa, behöver inte säkerhetslösningarna genomgå samma utveckling.

Websense® software-as-a-service (SaaS) integrerar den bästa webbsäkerhets- och datasäkerhetsteknologin med en säkerhetslösning för e-post. Det ger en oslagbar insyn i e-posthoten och ett marknadsledande skydd mot säkerhetsrisker för in- och utgående e-post. Den här lätthanterliga tjänsten erbjuder effektivt skydd mot spam, virus, spionprogram, nätfiske och kombinerade e-post- och webbattacker. Fördefinierade innehållslistor gör det enkelt att förhindra dataförlust, uppfylla regelmässiga krav och använda tvingande policys för acceptabel e-postanvändning.

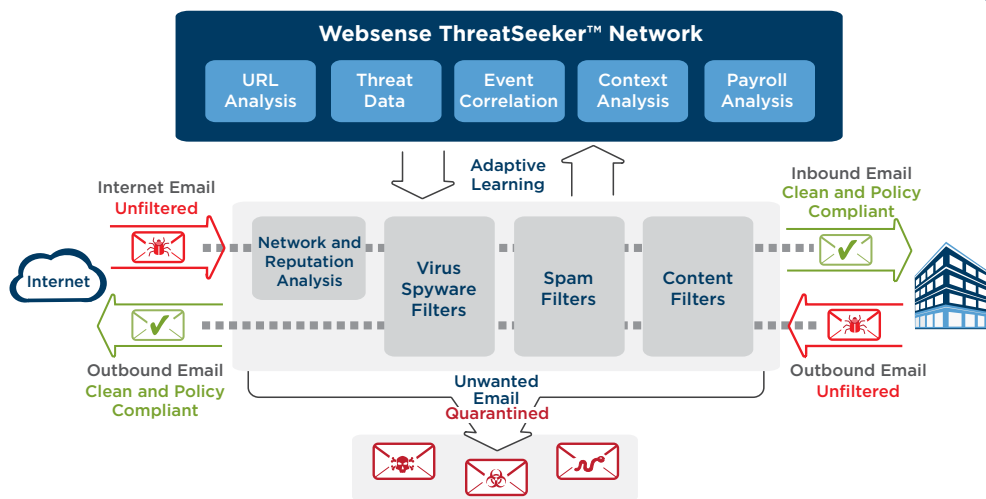
Så här fungerar det:

Det är enkelt att skydda e-post med Websense® SaaS email security och samtidigt få ökade besparingar kring tex, lagring. Websense alla datacenters består av belastningsbalanserade och redundanta kluster med hög tillgänglighet. De är utplacerade på tio olika platser runt om i

världen. Tjänsten erbjuder en SLA-uppbackad tillgång på 99,999 % och är certifierad enligt ISO27001-standarden för att erbjuda den högsta graden av global och anpassad säkerhet, sekretess och tillförlitlighet.

Websense SaaS email security gör det möjligt för kunder att:

- **Minskad kostnad och komplexitet** eftersom det inte finns någon utrustning på plats som ska installeras eller underhållas. Dessutom ges bättre bandbreddsprestanda och lagringskapacitet, minskade administrativa omkostnader och inga oväntade utgifter.
- **Ökat skydd** tack vare marknadsledande säkerhetsteknik mot kombinerade e-post- och webbattacker. Allt uppbackat av ett branschledande serviceavtal och styrkan i Websense ThreatSeeker™ Network.
- **Behåll kontrollen** med åtkomst dygnet runt och få flexibla samt anpassade policys och konfigurationsinställningar, karantänshantering och rapportering.



“Så fort vi hade implementerat Websense Hosted Email Security, försvann nästan alla spam helt.”

Lee Smith
IT Operations Manager
Harvey Nichols

Funktioner i Hosted Email Security

Hosted Email Security lösningar	Antispam	Antivirus	Content Filter	Kryptering
Hosted Antispam	●			
Hosted Email Security	●	●		
Hosted Email Security and Content Control	●	●	●	●

Antispam

Websense erbjuder effektiv blockering av spam med mycket låg andel felbedömningar, vilket backas upp av 99 procent tjänstenivåavtal för spamdetektering. En kombination av teknologier används för att identifiera spam, inklusive avsändarrykte, anpassad inlärning, URL-analys, heuristik, digitala fingeravtryck och optisk identifiering av bildspam. Varje e-post tilldelas ett sammanlagt protokoll, som jämförs mot en kunddefinierad tröskel för att avgöra vilken åtgärd som ska vidtas.

Antivirus

Ingående och utgående e-post genomsöks efter virus, spionprogram och andra former av skadlig programvara, med en inställning i flera lager med tre separata, kommersiella antivirusmotorer och Websense ThreatSeeker Network för att skydda mot både kända och okända hot. ThreatSeeker erbjuder ständigt skydd genom att kontinuerligt undersöka e-post- och webbplatser för att identifiera trender och mönster som detekterar framträdande hot – stänger fönstret vid risk för exponering inför ett hot från ett nytt skadligt program och förekomst av detekteringssignatur. Tjänsten backas upp genom ett serviceavtal för 100 procent virusdetektering.

Content Filter

Integrerad teknologi från Websense marknadsledande datasäkerhetslösningar gör det enkelt att förhindra dataförlust, uppfylla regelkrav och ålägga policier för acceptabel e-postanvändning. Fördefinierade ordböcker som täcker 20 ämnen på 12 språk, samt inbyggd PCI-DSS och datasekretessmallar hjälper organisationer att snabbt identifiera och stoppa e-postangrepp. Unika undersökningskrav kan enkelt uppfyllas med avancerade regelmässiga uttryck och flexibla regler. Angrepp identifieras genom djupgående undersökning av både e-postmeddelanden och innehåll inom bilagan. Meddelanden kan även placeras i karantän baserat på filtyp i bilagan och levereras senare baserat på storlek.

Kryptering

Websense-kryptering säkrar e-postkommunikation utan att göra avkall på förmågan att undersöka krypterad e-post när det gäller skadliga program och innehållsangrepp. Websense stöder server-till-server-kryptering genom användning av branschstandardens transport layer security (TLS) och ad hoc park-and-pull-kryptering för kommunikation med individer. Krypteringspolicier kan upprättas för att kryptera kommunikationer baserat på avsändare, mottagare, känslighetsinställningar för Outlook eller ämnesnyckelord. Kryptering kan användas kombinerat med innehållsfiltrering för att kryptera e-post med specifikt innehåll, såsom känslig eller konfidentiell information.

Websense SaaS email security samverkar även med Websense SaaS Web security för att erbjuda integrerat e-post- och webbskydd för att göra det möjligt för organisationer att konsolidera hantering och rapportering för både webb- och e-postsäkerhet.

Egenskaper	Fördelar
Spam- och virussydd	SLA-uppbackat skydd med hög precision mot spam, virus, spionprogram, nätfiske och kombinerade e-post- och webbattacker.
Konstant hotdetektering	Skyddsprogram från ThreatSeeker Network identifierar och stoppar hot som uppkommer genom att stänga exponeringsfönstret.
Förhindrande av dataförlust	Integrerad teknik från Websense marknadsledande datasäkerhetslösningar förhindrar dataförlust och bidrar till att uppfylla regelkrav.
Innehållsfiltrering	Fördefinierade innehållsordlistor som täcker 20 ämnen på 12 språk gör det enkelt att snabbt identifiera e-postangrepp.
Kryptering	Skydda känsliga och regelbundna data med säker e-postkommunikation för affärspartners och personer
Software-as-a-Service-leverans	Spara tid och pengar genom att slippa installera och underhålla utrustning, inbyggd återhämtning, förutsägbara kostnader och minskade administrativa omkostnader.
Övergripande infrastruktur för datacenter	Tio globala datacentra med fullt redundant effekt, kylning och Internet-anslutning erbjuder hög tillgänglighet med en drifttid på 99,999 procent enligt serviceavtal.
Säkerhetscertifieringar	Oberoende granskning och certifiering av säkerhetsåtgärder för ISO27001 säkerställer högsta nivån av säkerhet, sekretess och integritet
Service och support dygnet runt	Öppna och hantera tjänsten genom en webbaserad portal som är tillgänglig dygnet runt på Internet, med ständig support för extra hjälp vid behov.
E-mail spooling för katastrofåterställning	Inbyggd redundans och e-mail spooling garanterar att e-post aldrig försvinner när en kund får problem med ett nätverk eller en e-postserver.
Karantänshantering	Kraftfull meddelandesökmotor erbjuder full insyn och åtkomst till meddelanden och loggar i karantän.
Självbetjäning för användare	Schemalagd åtkomst och åtkomst på begäran för att visa och publicera meddelanden i karantän och godkända/svartlistade avsändare minskar de administrativa omkostnaderna.
Katalogtjänstintegrering	Automatisk synkronisering av e-posttjänster och grupper med Active Directory och LDAP förenklar policyhanteringen.
Rollbaserad administration	Separat åtkomstkontroll för karantänshantering, visning av rapporter, åtkomst till revisionsökningar och andra nyckelfunktioner för delegerad administration.
Kataloginsamlingsskydd	Inbyggt skydd hindrar avsändare av spam att samla in giltiga e-postadresser.
Rapportering	Över 40 olika rapporttyper med sammanfattning och detaljerad forensik som erbjuder fullständig insyn i olika hottyper och -volym, bearbetade meddelande, angrepp på policier och mycket mer.

Websense ThreatSeeker™ Network

Den anpassade säkerhetstekniken för Websense ThreatSeeker Network använder mer än 50 miljoner insamlingssystem för data i realtid, vilka ständigt övervakar Internet-innehåll, inklusive nytt och dynamiskt innehåll för konstant skydd från hot som uppstår. Den här forskningen och intelligensen matas i realtid in i Websense-portföljen med olika lösningar. Resultatet av detta är att Websense kan anpassa sig till ett Internet i snabb förändring, med en hastighet som traditionella säkerhetslösningar inte klarar av att hålla.

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

Australien
websense.com.au

Israel
websense.com

Kina
prc.websense.com

Italien
websense.it

Frankrike
websense.fr

Japan
websense.jp

Tyskland
websense.de

Nederländerna
websense.com

Hongkong
websense.cn

Singapore
websense.com

Indien
websense.com

Spanien
websense.com/latam

Irland
websense.co.uk

Förenade arabemiraten
websense.com

Ingående hot



- Spam
- Virus
- Farliga adresser

Integrerad intelligens för webb- och datasäkerhet

- ✓ Threatseeker
- ✓ Zero-Hour Intelligence
- ✓ URL-analys
- ✓ Fördefinierade ordböcker
- ✓ Djupgående innehållsgranskning
- ✓ Avancerad mönstermatchning

Utgående risker



- Dataläckage
- Godkänd användning
- Efterlevnad

Intelligent Email Security

Email Privacy

ISO 27001

Websense SaaS email security är oberoende reviderad och certifierad enligt ISO 27001 standard för att säkerställa högsta säkerhetsnivå, sekretess och tillförlitlighet. ISO 27001 är ett system för informationssäkerhet som har publicerats i oktober 2005 enligt den internationella organisationen för standardisering. Den här certifieringen är allmänt godkänd som bevis på kvaliteten för en organisations säkerhetssystem och den mest betydande säkerhetsstandard i branschen med mer än 70 SAS-krav och många konkurrenter använder certifieringen som ett riktmärke.

Datacentre Security

Bland alla de platser din e-post besöker är Websense datacentra bland de säkraste den kan dirigeras till. Websense har skapat omfattande säkerhets- och sekretesssystem och skyddar därmed själva öveförningen inom datacentranätverket. Rena e-postmeddelanden hålls inte kvar av tjänsten och andra e-postmeddelanden är bara synliga för de som har administratörsbehörighet för systemet - det vill säga nätverksadministratörer och andra som du kan ha gett tillgång till ditt konto. Websense datacentra innehåller omfattande säkerhetssystem, inklusive:

- 24 x 7 x 365 bemanning
- System för fysisk intrångsdetektering
- Videoövervakning
- Listor över begränsad åtkomst
- Bild- och biometriverifiering

Sammanfattning över tjänstenivåavtal

Websense erbjuder branschledande tjänstenivåavtal för att säkerställa att tjänsten utförs med högsta kvalitetsnivå.

- **Tillgänglighet** – 99,999 procent
- **Spam** – 99 procent eller högre detekteringsfrekvens
- **Virus** – 100 procent detektering av kända virus
- **Bearbetningslatens** – 60 sekunder eller mindre för e-post som inte är spam och understiger två megabyte
- **E-postloggar och karantän** – tillgängliga fem minuter eller mindre efter e-postmottagande

Alla tjänstenivåavtal omfattas av de regler och villkor som beskrivs i kundens tjänsteavtal.

Om du vill ha mer information, få en gratis testversion av Websense email solutions, eller se en demonstration online, besöker du sidan www.websense.com/evaluations.