

Google Message Security



OM GOOGLE-SIKKERHED OG -ARKIVERING

Googles sikkerheds- og arkiveringssystemer, som er leveret af Postini, gør dit eksisterende e-mail-system mere sikkert og kompatibelt. Disse produkter, som bygger på en hostet serviceplatform, blokerer for spam, phishing, malware og andre trusler, før de når frem til dit netværk, og giver dig mulighed for at styre indhold og arkivering, så du kan undgå juridiske problemer. Googles hostede system giver dig mange fordele. Ved at udnytte "netværkseffekten" af titusindvis af e-mailnetværk kan Googles teknologi registrere nye trusler i realtid og blokere for dem over hele Googles sikkerhedsnetværk – uden at det kræver lokale opdateringer. På samme måde fører stordriftsfordele inden for lagring, enkel anvendelse og vedligeholdelsesfri service til lave samlede omkostninger.

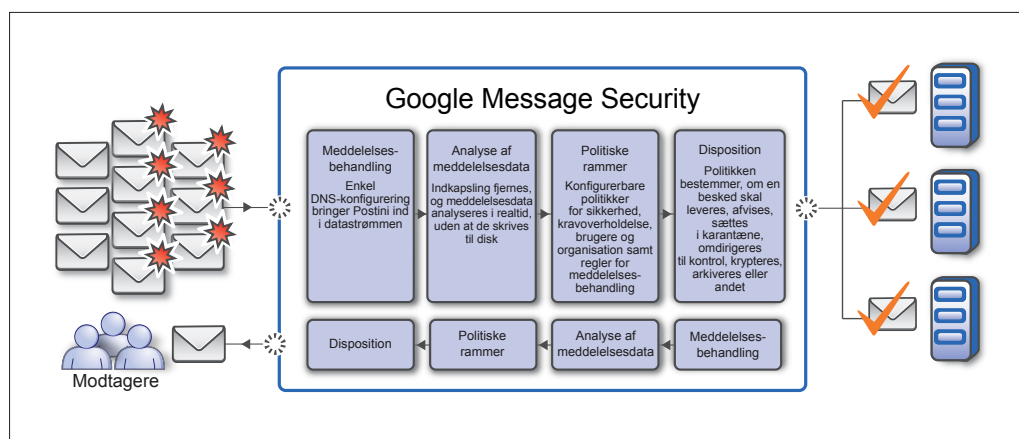
Du kan finde flere oplysninger på www.google.com/postini

Google Message Security, som er leveret af Postini, giver yderst effektiv sikkerhed omkring ind- og udgående e-mail til organisationer i alle størrelser. Den gør det nemmere at håndtere sikkerhed og kravoverholdelse for e-mail og frigør dermed værdifulde it-ressourcer. Google Message Security er altid slået til og altid opdateret, så organisationer kan være sikre på at have effektiv og pålidelig beskyttelse af deres e-mail til hver en tid.

Ved at anvende en patenteret, on-demand arkitektur blokerer Google Message Security for spam, phishing, virus og andre e-mail-trusler, før de når frem til din organisation, og den reducerer dermed belastningen på dine e-mail-servere, bevarer din båndbredde og forbedrer ydeevnen i din eksisterende e-mail-infrastruktur. Google Message Security leveres som en SaaS-løsning (Software-as-a-Service), hvilket sparer penge og it-ressourcer, fordi der ikke skal installeres eller vedligeholdes hardware eller software.

Google Message Security betyder besparelser af it-ressourcer ved at eliminere behovet for konstante rettelser og opdateringer, som andet udstyr og software kræver. Den mindsker også belastningen på din helpdesk ved at gøre dine slutbrugere i stand til selv at styre deres e-mail-karantæneområde og opsætninger med en brugervenlig, webbaseret grænseflade. I stedet for at ringe til din helpdesk kan slutbrugerne selv gennemgå deres e-mail-karantæneområde og levere eventuelle ønskede e-mail. Brugerne modtager jævnligt en detaljeret oversigt over karantæneområdet via e-mail. De kan også tilpasse deres spambeskyttelse til deres egne ønskede niveauer. Alle disse slutbrugermuligheder kan fuldstændigt konfigureres på politikniveau, så du har fuld kontrol over, hvad slutbrugerne har tilladelse til at gøre.

Google Message Security kan automatisk håndhæve dine politikker om e-mail-sikkerhed. Denne håndhævelse af politikker hjælper med til at sikre overholdelse af lovgivning og myndighedskrav i forbindelse med både indgående og udgående e-mail på tværs af din organisation. TLS-understøttelse (Transport Layer Security) er inkluderet, så følsomme e-mail krypteres, og den kan automatisk indføres for al kommunikation



Figur 1: Google Message Security giver yderst effektiv sikkerhed omkring ind- og udgående e-mails for organisationer i alle størrelser

mellem udpegede e-mail-domæner. Dette sikrer, at kommunikation, som er følsom eller underlagt regulering, altid leveres med det relevante sikkerhedsniveau.

Google Message Security har også en praktisk webbaseret administrationskonsol. Denne konsol gør det muligt at foretage konfiguration i realtid samt ændring af politikker, overvågning og underretninger foruden omfattende rapportering til administratorer. Brugere kan defineres i konsollen, eller Google Message Security kan integreres i din organisations mappestruktur med henblik på brugersynkronisering.

Google Message Security indeholder mange komponenter, som tilsammen giver effektiv beskyttelse mod e-mail-trusler. Af specifikke funktioner kan nævnes:

- Identificering af trusler i realtid, baseret på behandlingen af mere end to milliarder e-mail hver dag, giver global synlighed af nye trusler. Denne "netværkseffekt" identificerer og sporer automatisk IP-adresser (Internet Protocol), som udsender angreb såsom spam, virus, DoS (Denial of Service) osv. Så snart en trussel identificeres, blokeres den for alle Google Message Security-kunder. Identificeringen af trusler er også selvkorrigerende. Efterhånden som de identificerede IP-adresser ophører med at angribe, får de igen lov til at etablere SMTP-forbindelser (Simple Mail Transfer Protocol), så de kan sende legitime e-mail.
- Patenteret antispamteknologi i realtid undersøger tusindvis af elementer i en e-mail for at afgøre, om det er spam. Det giver et ekstremt effektivt spamfilter og ualmindeligt få falske positive resultater.
- Antivirusbeskyttelse bygger på antispamregistrering og omfatter nultidsheuristik og signaturbaserede registreringsmetoder foruden flere forskellige kommercielle antivirussystemer.
- Indholdsstyringssystemer giver dig mulighed for at definere politikker for både ind- og udgående e-mail, så du får et ekstra lags beskyttelse mod eksterne trusler. Det kan også beskytte mod, at nogen utilsigtet eller ondsindet lækker fortrolige data i udgående e-mail og vedhæftede filer.
- Teknologi til styring af vedhæftede filer giver dig mulighed for at definere specifikke politikker for vedhæftede filer samt mulighed for at blokere meddelelser eller anbringe dem i karantæne ud fra typen eller størrelsen af deres vedhæftede filer. Teknologien til styring af vedhæftede filer undersøger også arkivfiler såsom .zip- og .rar-filer for at vurdere filernes indhold og giver dig mulighed for at definere specifikke politikker for håndtering af krypterede arkivfiler.

Funktion	Fordele
Patenteret "pass-through" arkitektur	Giver et ekstremt effektivt spamfilter og meget få falske positive resultater
Flere lag af virusblokering, heuristik og signaturbaseret beskyttelse	Giver "nultids"-beskyttelse mod virus, der hurtigt breder sig, 100 % antivirus-SLA
Meget skalerbar og tilgængelig SaaS-plattform samt SLA med 99,999 % filtreringsopetid	Sørger for altid tilgængelig, altid opdateret beskyttelse med lavere samlede omkostninger
Webbaseret administrationskonsol	Giver mulighed for bruger- og politikopdateringer i realtid, ændringer i konfigurationen og rapportering
Blokerer for directory harvest attack/DoS (denial of service)	Forhindrer angreb med patenteret funktionsanalyse
Politikbaseret TLS-kryptering	Sikrer transmissionen af e-mail
Filtrering af vedhæftede filer	Håndhæver politikker for filer, der er vedhæftet e-mail
Styring af indholdspolitik	Håndhæver politikker for acceptabel anvendelse og tilladeligt indhold
E-mail-spooling	Fortsæt med at modtage e-mail, også selv om din e-mail server er gået ned

