Googles meddelandesäkerhet

OM SÄKERHET OCH ARKIVERING MED GOOGLE

Googles tjänster för säkerhet och arkivering, som drivs av Postini, gör ditt befintliga e-postsystem säkrare och upprätthåller regelefterlevnaden. De här produkterna är byggda på en värdbaserad tjänstplattform och de blockerar skräppost, lösenordsfiske, skadliga program och andra intrång innan de når ditt nätverk samt ger dig innehållshantering och arkivering som hjälper dig att hantera juridiska processer. Googles modell med värdbaserad hantering erbjuder flera tydliga fördelar. Tack vare ”nätverkseffekten” som tiotusentals e-postnätverk innebär, kan Googles teknik upptäcka nya hot i realtid och blockera dem över Googles hela säkerhetsnätverk – utan att uppdateringar behöver göras lokalt. På samma sätt sparar stordriftslagring, enkel distribution och underhållsfri tjänst pengar och ger en låg total ägandekostnad.

Mer information finns på
www.google.com/postini

Googles meddelandesäkerhet, som drivs av Postini, ger mycket effektiv säkerhet för inkommande och utgående e-post för företag i alla storleker. Tjänsten innebär att hanteringen av säkerheten och efterlevnaden för e-postmeddelanden förenklas och att värdefulla IT-resurser kan frigöras. Googles meddelandesäkerhet är alltid aktiv och ständigt uppdaterad för att företag ska vara säkra på att de får ett effektivt, tillförlitligt och oavbrutet e-postskydd.

Tack vare en patenterad arkitektur på begäran kan Googles meddelandesäkerhet blockera skräppost, lösenordsfiske, virus och andra e-posthot innan de når ditt företag. Detta minskar belastningen på e-postservrarna, bevarar bandbredd och förbättrar prestanda för befintlig meddelandeinfrastruktur. Googles meddelandesäkerhet tillhandahålls i en modell där programvaran fungerar som en tjänst (SaaS), vilket sparar pengar och IT-resurser eftersom det inte kräver någon maskin- eller programvara att installera och underhålla.

Googles meddelandesäkerhet frigör IT-resurser genom att de ständiga korrigeringarna och uppdateringarna som andra verktyg och programvarulösningar kräver inte längre behövs. Tjänsten kan även minska belastningen på IT-supporten genom att ge slutanvändarna möjlighet att hantera sina egna meddelandekarantäner och inställningar med ett lättanvänt, webbaserat gränssnitt. I stället för att ringa supporten kan slutanvändare kontrollera sina meddelandekarantäner och leverera önskade meddelanden. Användare får regelbundet ett e-postmeddelande med en karantänsammanfattning med all karantäninformation. De kan även justera sina inställningar för skräppostskydd till önskade nivåer. Alla dessa slutanvändarkontroller kan konfigureras helt på policynivå, vilket ger dig fullständig kontroll över vilka slutanvändare som har behörighet att göra det.

Googles meddelandesäkerhet kan automatiskt utföra dina sekretesspolicyer för e-post. Utförandet av policyerna hjälper dig att efterleva rättsliga krav och bestämmelser för både inkommande och utgående e-post i hela företaget. TLS-stöd (Transport Layer

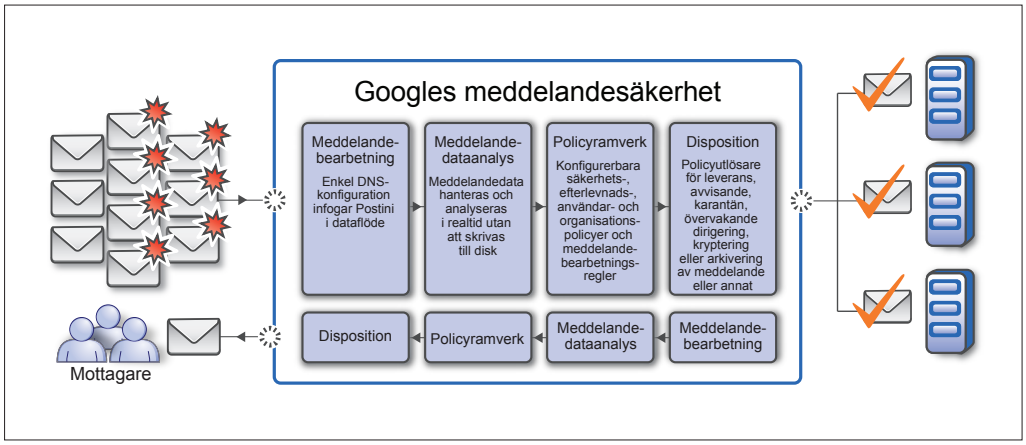

Bild 1: Googles meddelandesäkerhet ger mycket effektiv säkerhet för inkommande och utgående e-post för företag i alla storleker.

Security) ingår för att kryptera känslig e-postkommunikation och kan automatiskt utföras för all kommunikation mellan konfigurerade e-postdomäner. Detta säkerställer att känslig eller reglerad kommunikation alltid levereras med vederbörlig säkerhetsnivå.

Googles meddelandesäkerhet kan även erbjuda en praktisk webbkonsol för administration. Den här konsolen möjliggör konfiguration och policyändringar i realtid, övervakning och varningar, samt omfattande rapportering för administratörer. Användare kan definieras i konsolen eller så kan Googles meddelandesäkerhet integreras med organisationens katalogstruktur för användarsynkronisering.

Googles meddelandesäkerhet innehåller flera olika komponenter som kombineras för att tillhandahålla ett effektivt skydd mot e-posthot. Exempel på specifika funktioner:

- Identifiering av hot i realtid, som baseras på bearbetning av mer än två miljarder e-postmeddelanden per dag, vilket hjälper till att upptäcka globala framtida hot. Den här ”nätverkseffekten” identifierar automatiskt och spårar IP-adresser som skickar ut attacker, till exempel skräppost, virus och blockeringsangrepp (denial of service, DoS). När ett hot identifieras, blockeras det för alla av Googles meddelandesäkerhetskunder. Hotidentifieringen korrigerar även sig själv. När identifierade IP-adresser slutar att attackera kan de återigen upprätta SMTP-anslutningar för att skicka vanliga e-postmeddelanden.
- Patenterad teknik mot skräppost i realtid undersöker tusentals delar i ett e-postmeddelande för att avgöra om det rör sig om skräppost. Det ger en mycket effektiv skräppostfiltrering och exceptionellt låg andel falska positiva värden.
- Antivirusskydd bygger på skräppostidentifiering och innehåller heuristik och signaturbaserade utforskningsmetoder i realtid, samt flera kommersiella antivirusmotorer.
- Med innehållshantering kan du definiera policyer för både inkommande och utgående e-post, genom att ge ytterligare lager av skydd mot externa hot. Den ger även skydd mot oavsiktligt och avsiktligt läckage av konfidentiella data i utgående e-postmeddelanden och bifogade filer.
- Med tekniken för hantering av bifogade filer kan du definiera särskilda policyer beträffande bifogade filer och meddelande kan blockeras eller sättas i karantän baserat på typ och storlek på filer som har bifogats i e-postmeddelanden. Hanteringen av bifogade filer kontrollerar även arkivfiler, till exempel .zip-filer och .rar-filer, för att utvärdera innehållet i filerna. Detta innebär att du kan definiera särskilda policyer för hantering av krypterade arkivfiler.

Funktion	Fördelar
Patenterad genomgående arkitektur	Ger mycket effektiv skräppostfiltrering och låg andel falska positiva värden
Virusblockering i flera lager, heuristik och signaturbaserad utforskning	Ger skydd i realtid mot snabbt muterande virus, 100 % virusfri enligt servicenivåavtal
Mycket skalbar och tillgänglig SaaS-plattform, 99,999 % filtreringsdrifttid enligt servicenivåavtal	Ger alltid aktivt, alltid uppdaterat skydd med lägre total ägandekostnad
Webbaserad administrationskonsol	Möjliggör användar- och policyuppdateringar, konfigurationsändringar och rapportering i realtid
Skydd mot automatisk datainsamling/blockeringsangrepp (denial of service)	Förhindrar attacker med patenterad beteendeanalys
Policystyrd TLS-kryptering	Säkerställer överföringen av e-post
Filtrering av bifogade filer	Verkställer policyer för bifogade filer i e-post
Hantering av innehållspolicyer	Utför godkända användarpolicyer och efterlevnad av innehåll
E-postbuffring	Fortsätt att ta emot e-postmeddelanden även om det blir avbrott i e-postservern

Google™