

Google Message Discovery

Komplet e-mail-sikkerhed og -arkivering i én pakke



OM GOOGLE-SIKKERHED OG -ARKIVERING FRA POSTINI

Googles sikkerheds- og arkiveringsprodukter, som er leveret af Postini, gør e-mail-systemer mere sikre effektive og i stand til at overholde de påkrævede standarder ved at blokere for spam og andre trusler, før de når frem til dit netværk, og ved at sørge for kryptering og arkivering, så du lever op til kravene om overholdelse af standarderne. Googles hostede model udnytter "netværkseffekten" af milliarder daglige e-mail-forbindelser til at opdage og blokere trusler i realtid uden at det kræver lokale opdateringer. Stordriftsfordele ved lagring giver sammen med enkel implementering og vedligeholdelsesfri service lave samlede omkostninger.

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

Gør dine e-mail-servere mere sikre og effektive, og sørg for, at de overholder de påkrævede standarder. Bloker e-mail trusler, før de når frem til din organisation. Opret et sikkert og søgbart e-mail-arkiv uden at foretage store investeringer i infrastruktur takket være cloud-lagring. Find relevante meddelelser hurtigt og udførligt, selv mens e-mail-mængden og kravene til overholdelse af standarder bliver stadig større. Udnyt cloud-tjenester til at reducere vedligeholdelsen, beskytte båndbredden og frigøre ressourcer til arbejde på strategiske forretningstiltag.

Produktoversigt

Google Message Discovery fra Postini er en sikker, hosted tjeneste, der leverer spam- og virusbeskyttelse på erhvervsniveau samt omfattende e-mail-arkivering til virksomheder, der er på udkig efter omkostningseffektiv e-mail-administration og store fordele i forhold til arkivering på lokal server eller mediebaseret arkivering. Med Google Message Discovery kan du:

- oprette en centraliseret og søgbar e-mail-database til din organisation
- foretage hurtige søgninger i arkivet for at finde e-mail og gemme resultatsæt
- sikre dine e-mail mod spam, virus, phishing og andre trusler, der overføres via e-mail
- fastlægge e-mail-politikker fra centralt hold til administration af krav til indhold og overholdelse af standarder

Google Message Discovery er cloud-hosted og bygger på en SaaS-model (Software as a Service), så det er ikke nødvendigt at opstille prognoser eller planlægge fremtidig lagerkapacitet. Googles sikre og redundante datacentre yder komplet backup og beskyttelse af meddelelserne, hvilket eliminerer risikoen for tab af data ved servernedbrud. Din organisation bevarer ejerskabet af dataene og dermed kontrollen over oplysningerne.

Du kan arkivere e-mail uden at bekymre dig om diskplads og slipper for at bekymre dig om lagerkvoter ved at give brugerne adgang til arkiverede e-mail. Desuden kan du ved at fjerne gamle e-mail fra dine servere gøre både backup-perioderne og gendannelsesperioderne kortere.

Google Message Discovery omfatter også et komplet sæt af sikkerhedsfunktioner, så du kan sørge for det højeste mulige sikkerhedsniveau i dine e-mail-systemer – uden at installere dyr hardware eller software. Derved kan du blokere for spam, virus og andre eksterne trusler, før de når frem til din organisation, og sørge for, at virksomhedens oplysninger, som skal forblive fortrolige, ikke kommer uden for din organisation.

Hovedfunktioner

- **Sikker og redundant** Sikrer adgang og redundans ved at udnytte Googles netværk af sikre, energibesparende datacentre. Minimerer dyr lokal infrastruktur og reducerer it-vedligeholdelse
- **Skalerbar** Ubegrænset kapacitet uden ekstra administration og kontrakter
- **Nem adgang og søgning** Find hurtigt specifikke e-mail uden at skulle søge i flere datakilder
- **Eksporterer resultatsæt** Eksporter hurtigt meddelelser eller meddelelsessæt i PST- og MBOX-format
- **Håndterer politikker om bevarelse af e-mail** Reducer risici, og spar tid ved at implementere pålidelige og auditerbare politikker for bevarelse af e-mail, og gem meddelelsessæt i længere tid end den periode, der er fastlagt i politikkerne

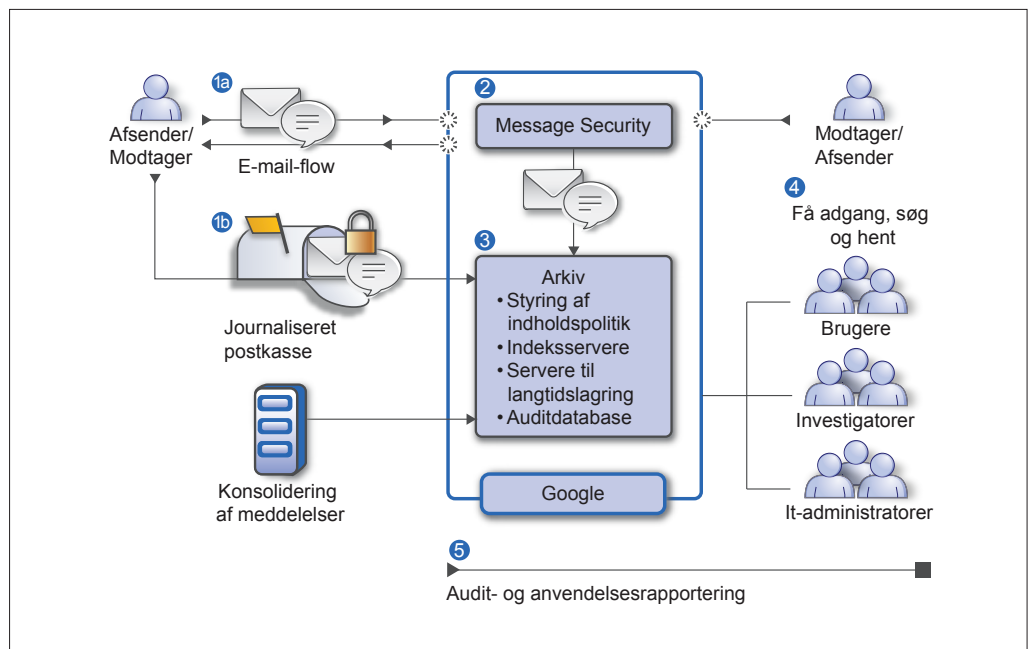
SYSTEMKRAV

Google Message Discovery understøtter følgende e-mail-servere:

- Microsoft Exchange Server 2000 Standard eller Enterprise Edition
- Microsoft Exchange Server 2003 Standard eller Enterprise Edition
- Microsoft Small Business Server med Exchange Server 2000 eller 2003 Standard Edition
- Microsoft Exchange Server 2007
- Lotus Domino 6.5-7x

For at anvende journaliseringsmuligheden i Microsoft Exchange Server Standard Edition kræver det, at du har mindst to af disse servere i dit netværk, som kun bruges til modtagelse af journaliserede meddelelser. Serveren må ikke indeholde andre brugerpostkasser.

- **Adgang til arkiv for slutbrugere** Giver slutbrugerne adgang til deres eget personlige arkiv via en webbaseret grænseflade eller en MS Outlook-værktøjslinje uden at skulle tilkalde hjælp fra it-afdelingen
- **Arkiverer aktivitetsrapporter** Få vist lograpporter over alle arkivaktivitet, herunder søgninger og eksporter fra arkivet, af hensyn til behovet for at overholde de påkrævede standarder
- **Spam- og virusbeskyttelse** Få markedets førende e-mail-sikkerhed, herunder spam- og virusbeskyttelse i realtid samt indholdsfiltrering af indgående og udgående e-mail
- **Kryptering fra domæne til domæne** Overfør sikre meddelelser med politikbaserede TLS-protokoller (Transport Layer Security)
- **Intelligent routing** Omdirigerer nemt e-mail-trafik til decentraliserede datacentre



Figur 1: Message Discovery-flow

Google Message Discovery giver dig mulighed for at styre, beskytte og få adgang til de nødvendige arkiverede meddelelser på følgende måde:

1. **Effektiv indsamling af meddelelser:** Meddelelser sendes i realtid til Googles sikre datacentre via det fælles journaliseringssystem på din e-mail-server. Ind- og udgående e-mail kan også i stedet arkiveres som en del af den overordnede behandling, Google udfører under trusselsanalysen i realtid.
2. **"Altid aktiv, altid opdateret" Message Security:** Ved at føre meddelelser gennem Googles Message Security-system, der er markedets førende, får du beskyttelse mod trusler i realtid, virusbeskyttelse, filtrering af indhold og politikbaseret TLS-kryptering.
3. **Sikker hosted arkivering:** Meddelelser og deres vedhæftede filer bliver lagret og indekseret på et centralt lager. Styring af politikker for opbevaring gør det muligt for de it-ansvarlige at fastlægge politikker på bruger- eller organisationsniveau, så man kan overholde interne og eksterne krav om opbevaring.
4. **Søgning og hentning:** Adgang baseret på tilladelser giver autoriserede brugere avancerede værktøjer, der gør det muligt hurtigt og nemt at søge efter og hente relevante e-mail samt sørge for, at de ikke bliver slettet.
5. **Omfattende rapportering:** Anvendelses- og auditrapportering leverer de oplysninger, der kræves for at holde styr på alle aktiviteterne inden for virksomhedens arkiver.

