

Eenvoudige beveiliging van digitale communicatie in Gmail



Stel je mensen in staat om veilig aan de slag te gaan binnen Gmail dankzij ongeëvenaarde encryptie, contextuele, door machine learning (ML) aangestuurde bedrijfsregels en veilige bestandsoverdracht. Zivver voorkomt gegevensverlies en ondersteunt de naleving van onder andere de AVG, NTA 7516, CCPA en LGPD.

Naadloze integratie met de Google-omgeving

Gmail alleen is niet voldoende om je gevoelige gegevens te beveiligen. Zivver integreert met Gmail om robuuste communicatiebeveiliging eenvoudig te maken – zonder bestaande workflows of processen te veranderen.

Hoe Zivver digitale communicatie met Gmail beveiligt

01. Contextuele, door ML aangedreven foutcorrectie

Door ML aangedreven bedrijfsregels classificeren inhoud en waarschuwen gebruikers voor potentiële fouten in Gmail voordat e-mails worden verzonden. Dit kan gaan om onjuiste ontvangers die zijn toegevoegd door de functie ‘automatisch invullen’, verkeerde bijlages voor een specifieke ontvanger, de aanwezigheid van gevoelige gegevens en meer. Dit gebeurt allemaal tijdens het opstellen van een e-mail.

02. Ongeëvenaarde versleuteling

Gmail ondersteunt beveiligde verzending van e-mail via STARTTLS, een zeer elementaire beveiligingsmaatregel die vertrouwt op de serverinstellingen van je ontvanger om een bericht veilig af te leveren. Om een beveiligde verbinding tot stand te brengen, moeten zowel de verzender als de ontvanger gebruikmaken van TLS. Wanneer er geen beveiligde verbinding tot stand kan worden gebracht, levert Gmail berichten af via niet-beveiligde verbindingen – of zelfs helemaal niet.

Zivver past de hoogste industriestandaarden toe om de verbinding tussen verzender en ontvanger te beveiligen en onderschepping van berichten te voorkomen. Onze semantisch-bewuste, op maat gemaakte encryptie analyseert de gevoeligheid van inhoud van e-mails en detecteert de beveiligingsniveaus van de ontvanger. Waar deze onvoldoende zijn voor het vereiste beveiligingsniveau, leidt Zivver de e-mail via onze eigen server om, om zo veilige verzending te garanderen.

03. Meervoudige verificatie

Zorg ervoor dat alleen geverifieerde ontvangers toegang hebben tot gevoelige gegevens dankzij technologie voor meervoudige verificatie, ingebouwd in Gmail. Zivver past het vereiste verificatieniveau aan op basis van het type ontvanger en hun beveiligingsinstellingen, en slaat deze op in het adresboek van je organisatie zodat de gegevens van de ontvanger slechts één keer hoeven worden ingevoerd.

04. Geen sleutels, geen toegang

In tegenstelling tot Gmail werkt Zivver op basis van een strikt “zero-knowledge”-beleid. Berichten worden asymmetrisch versleuteld, en we slaan geen klantensleutels of afgeleiden op om ze te kunnen decoderen. Er worden alleen versleutelde gegevens op schijf opgeslagen, waardoor het onmogelijk is voor Zivver om de inhoud van berichten te bekijken die met onze dienst zijn verzonden. Dit betekent dat alleen de verzender en de ontvanger toegang hebben tot de inhoud van het bericht en deze kunnen decoderen en lezen.

05. Betrouwbaar intrekken van berichten

Trek berichten in en stel vervalperiodes in om de toegang voor ontvangers te beheren, zelfs na verzending. Als het bericht wordt ingetrokken voordat de ontvanger het heeft geopend, kan Zivver garanderen dat een eventueel gegevenslek is ingedamd.



Verstuur elk type bestand tot 5 TB vanuit Gmail

Verstuur elk type bestand tot 5 TB vanuit Gmail. Je hoeft niet langer aan de slag met onhandige sites voor bestandsoverdracht en kunt bestanden nu gewoon eenvoudig verzenden.

Intelligente, eenvoudige compliance

Ons dashboard en onze auditlogs bieden een handig overzicht van e-mailactiviteiten, zodat je snel kunt handelen als er zich een incident voordoet.

Eenvoudig voor zowel de verzender als de ontvanger

Met een eenmalige aanmelding zijn werknemers onmiddellijk ingelogd in Zivver wanneer ze inloggen op hun werkstation, waardoor de vertrouwtheid met Gmail behouden blijft op het werk, thuis of onderweg. Bovendien hoeven ontvangers geen account aan te maken of software te downloaden om een beveiligde e-mail van Zivver te openen - we houden het voor iedereen eenvoudig.

Eenvoudig voor beheerders

Onze nauwkeurig afgestemde out-of-the-box bedrijfsregels vereenvoudigen gegevensclassificatie onmiddellijk, en de oplossing kan met minimaal onderhoud worden ingezet. De proactieve meldingen van Zivver maken het tot een oplossing die werknemers ook daadwerkelijk willen gebruiken, waardoor er sprake is van een organisatiebrede beveiligingsstijl.

Veilig Mailen

Veilig mailen staat aan

Aan

Onderwerp

Beste Gea,

Kom je er niet uit of heb je vragen over veilig mailen? Zoek dan contact met de helpdesk van jouw organisatie. Zij kennen Zivver en helpen je graag.

Veel succes met veilig mailen!

Verzenden



Zivver

Kon. Wilhelminaplein 30
1062 KR Amsterdam

085 016 0555
contact@zivver.com

www.zivver.nl