Kiteworks

SOLUTION BRIEF

Uw Data, Uw Soevereine Controle

Bescherm gegevens tegen ongewenste toegang door cloudproviders met een Private Data Network (PDN)

Organisaties willen in toenemende mate het risico beperken dat cloudproviders en buitenlandse overheden toegang krijgen tot hun gevoelige gegevens. Zeker in Europa, waar datasoevereiniteit cruciaal is onder de AVG en NIS 2, stellen standaard clouddiensten organisaties bloot aan aanzienlijke juridische en compliance-risico's, zoals door de Amerikaanse CLOUD Act en vergelijkbare extraterritoriale wetgeving.

Het Private Data Network (PDN) van Zivver en Kiteworks helpt deze risico's effectief te beheersen door volledige datasoevereiniteit te waarborgen. Uw gevoelige gegevens blijven altijd onder uw controle, ongeacht de opslag- of verwerkingslocatie. Hiermee voorkomt u ongewenste toegang door derden, waaronder cloudproviders en overheden en behoudt u volledige soevereine controle over uw data.

Gebouwd voor veiligheid en datasoevereiniteit

Single-tenant cloud: maximale veiligheid in publieke cloud

Kiteworks minimaliseert risico's met een unieke single-tenant architectuur:

1. Volledige isolatie van data en verkeer van andere klanten
2. Eigen infrastructuur, exclusief gebruikt door uw organisatie
3. Specifieke beveiligingsmaatregelen uitsluitend voor uw omgeving
4. Aanpasbare beveiligingsinstellingen afgestemd op uw organisatiebehoeften

Gehost door u of uw partner: totale regie over dataresidentie

Voor organisaties met strikte eisen voor dataresidentie of zorgen over Amerikaanse wetgeving biedt Kiteworks geharde virtuele appliances die eenvoudig te implementeren zijn in eigen datacenters, cloudomgevingen of via een Managed Service Provider (MSP). Zo kunt u:

1. Data volledig binnen specifieke regio's bewaren
2. Bescherming bieden tegen buitenlandse toegangseisen
3. Volledige controle houden over fysieke beveiligingsmaatregelen

Datasoevereiniteit voor internationaal opererende operaties

Europese organisaties worden geconfronteerd met complexe datasoevereiniteitsvereisten per land. Kiteworks biedt oplossingen via:

1. Configureerbare geofencing met IP-adrescontrole
2. Regionale dataopslag om aan lokale regelgeving te voldoen
3. Blokkeren van ongeoorloofde grensoverschrijdende gegevensoverdracht
4. Uitgebreide auditlogs van alle gegevensactiviteiten en -toegang

Solution Highlights

Kies uit Single-tenant, on-premises of private cloud

Mogelijkheid tot air-gapped implementatie

Ontworpen voor data-soevereiniteit

Ingebouwde hardening en beleidscontrols

Air-gapped implementatie voor hoogst mogelijke beveiliging

Organisaties met vertrouwelijke data of kritieke infrastructuur hebben specifieke uitdagingen bij het opzetten van air-gapped omgevingen. Kiteworks maakt dit eenvoudig met:

1. Zelfstandige implementatie met minimale externe afhankelijkheden
2. Offline updatemechanismen voor veilige updates zonder internetverbinding
3. Intern certificaatbeheer
4. Robuuste offline authenticatiemethoden

Geïntegreerd platform: beveiliging voor alle uitwisselingskanalen

Kiteworks biedt, in tegenstelling tot oplossingen die zich beperken tot SFTP of bestandsoverdracht, een geïntegreerd beveiligingsframework voor:

1. Veilige bestandsdeling met gedetailleerde toegangscontrole
2. Veilige SFTP voor geautomatiseerde systeemoverdracht
3. Managed file transfer (MFT) met uitgebreide beveiligings- en auditmogelijkheden
4. Beveiligde e-mailuitwisseling met encryptie en integratie van DLP-servers

Deze geïntegreerde aanpak garandeert uniform beveiligingsbeleid, eenvoudig beheer en heldere auditlogs en rapportages.

Compliancevoordelen voor Europese regelgeving

De flexibele implementatie-opties van Kiteworks bieden specifieke voordelen voor naleving van Europese regelgeving, waaronder:

AVG (GDPR)

De datasoevereiniteitsfuncties van het platform zorgen ervoor dat persoonsgegevens binnen de juiste jurisdicties blijven en ondersteunen het beheer van betrokkenenrechten en meldplicht bij datalekken.

NIS 2

De geharde virtuele appliances van Kiteworks voldoen aan het security-by-design-principe uit de NIS 2-richtlijn, inclusief uitgebreide auditlogs voor verplichte incidentrapportages.

SOC2 Type II, ISO 27001/27017/27018

Kiteworks beschikt over een SOC 2 Type II-certificering voor beveiliging, beschikbaarheid, vertrouwelijkheid, integriteit en privacy, evenals ISO 27001, 27017 en 27018-certificeringen voor informatie- en cloudbeveiliging en bescherming van persoonsgegevens.

Security by Design bij alle vormen van implementatie

Ongeacht het gekozen implementatiemodel garandeert PDN optimale beveiliging door:

1. Encryptiesleutels volledig onder controle van de klant, zonder toegang door de leverancier
2. Een geharde virtuele appliance-architectuur met meerdere geïntegreerde beveiligingslagen
3. Zero-trust principes zijn toegepast op alle diensten en gegevensuitwisselingen
4. Uitgebreide auditlogs van alle activiteiten rondom data-toegang en gegevensuitwisseling
5. Role-based en attribute-based access controls in lijn met NIST CSF, ISO 27001 en andere relevante normen

Organisaties in zorg, financiële sector, juridische dienstverlening en overheid vertrouwen op de flexibele implementatie van Kiteworks voor veilige uitwisseling van gevoelige gegevens en naleving van regelgeving, ongeacht hun specifieke eisen.