Solution Brief

Zero Trust Network Access met Citrix Secure Private Access

Digitale transformatie, de cloud, hybride medewerkers... de dynamiek van het security- en connectiviteitslandschap is fundamenteel veranderd. Organisaties en medewerkers maken meer gebruik van internet en (beheerde en onbeheerde) devices dan ooit om applicaties te benaderen.

Onder invloed van deze veranderingen stellen cybersecurity-professionals alles in het werk om de security te handhaven en op te schalen, met behoud van continuïteit en de allerbeste werknemerservaring. Tegelijkertijd worden meer applicaties naar de cloud verplaatst en worden er meer workloads verspreid over public clouds en SaaS. Deze transformatie van het applicatielandschap verhoogt de complexiteit.

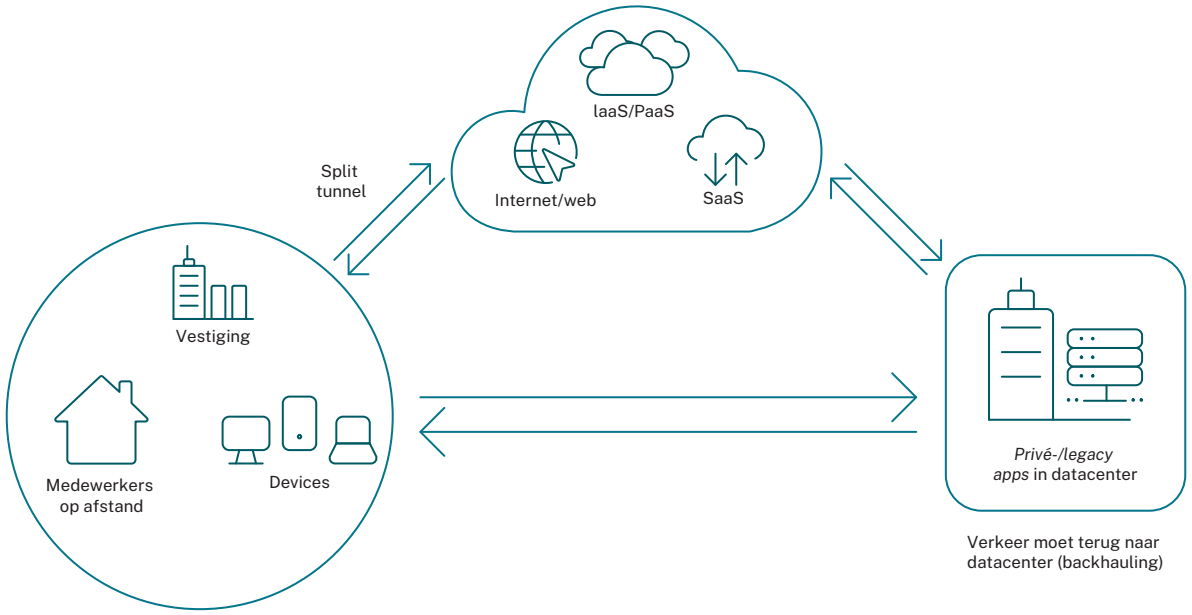
Toenemend risico

Traditionele architecturen van organisaties, met gescheiden systemen, zijn voornamelijk gebaseerd op datacentersecurity, aparte producten en redundante firewalls in het bedrijfsnetwerk. Helaas is deze aanpak niet afdoende voor de dynamische vereisten van vandaag als het gaat om applicatieconnectiviteit, compliance en security.

SaaS leidt ertoe dat gevoelige data en bedrijfskritische applicaties zich nu vaker in de cloud bevinden dan in een datacenter of private cloud. Het nadeel is dat deze complexe omgevingen moeilijker te beveiligen en te beheren zijn, en specifieke expertise vereisen om complexiteit te bestrijden.

De toename van het hybride werken en het toegenomen gebruik van verschillende soorten devices hebben het risico voor organisaties vergroot. Devices die door de organisatie zelf worden beheerd, zijn vaak de veiligste manier om toegang op afstand te bieden (de eigen IT-afdeling heeft immers de meeste controle). Maar er zijn ook medewerkers of externe partners die liever hun eigen devices gebruiken, en dat verhoogt de kans op securityincidenten.

Deze complexiteit en het verhoogde risico creëren kansen voor aanvallers. Organisaties moeten hun securityaanpak anders invullen en zo naadloos mogelijk laten werken, zodat medewerkers altijd en overal op een veilige manier toegang hebben tot applicaties, vanaf elk device.



Figuur 1: traditionele netwerk- en securitybenaderingen

Het nieuwe hybride werken en de uitdagingen van een traditionele benadering

Organisaties die het nieuwe hybride werken willen invoeren, moeten op een allesomvattende manier zicht krijgen op (en controle over) gebruikers, data en applicaties. Pas dan kan de verdere beveiliging worden aangepakt. Het traject naar de cloud ziet er voor elke organisatie anders uit. De specifieke uitdagingen zijn afhankelijk van de applicaties die de organisatie gebruikt, welke security- en netwerktechnologie er aanwezig is, wat de gewenste connectiviteit is, en welke tekortkomingen nog moeten worden opgelost.

Als het gaat om security en netwerken, hebben aparte producten en traditionele benaderingen vaak dezelfde uitdagingen:

- **Onvoldoende en inconsistente securitypolicy's:** Veel verschillende aanmeldingen en overlappende policy's kunnen leiden tot onveilige praktijken en een verhoogd securityrisico
- **Hogere IT-kosten en complexiteit:** Het beheer van meerdere vendors is duur, inefficiënt en complex
- **Mindere gebruikerservaring:** Matige gebruikerservaring, matige acceptatie en het ontstaan van 'schaduw-IT'

Wat is Citrix Secure Private Access?

Secure Private Access maakt deel uit van de bredere Secure Access oplossing van Citrix die helpt bij het aanpakken van de uitdagingen en het verminderen van de complexiteit in moderne gedistribueerde zakelijke omgevingen.

Citrix Secure Private Access

Citrix Secure Private Access is een ZTNA-oplossing in de cloud die altijd beschikbare security biedt vanuit het principe van zero trust, ongeacht de identiteit, locatie of het device van de gebruiker. De oplossing staat garant voor een veilige en snelle verbinding met alle door de IT-afdeling goedgekeurde applicaties en voorkomt backhauling van het verkeer (zoals dat bij traditionele VPN-benaderingen het geval is). Verder is de mogelijkheid aanwezig om regels af te dwingen en gebruikers en infrastructuur te beschermen tegen onbevoegde toegang of gevaren die verband houden met onbeheerde devices en BYO-devices.

Als cloudservice is deze oplossing beschikbaar op elke locatie. Neemt het aantal gebruikers of het gebruik toe, dan schaalt de service automatisch mee. Dit creëert vervolgens de flexibiliteit en beschikbaarheid die nodig zijn om de allerbeste gebruikerservaring en security mogelijk te maken. Aangezien de service volledig voor de klant wordt verzorgd, kan de eigen IT-afdeling van de organisatie zich richten op meer strategische initiatieven, in plaats van veel tijd te besteden aan het beheer van appliances in datacenters.

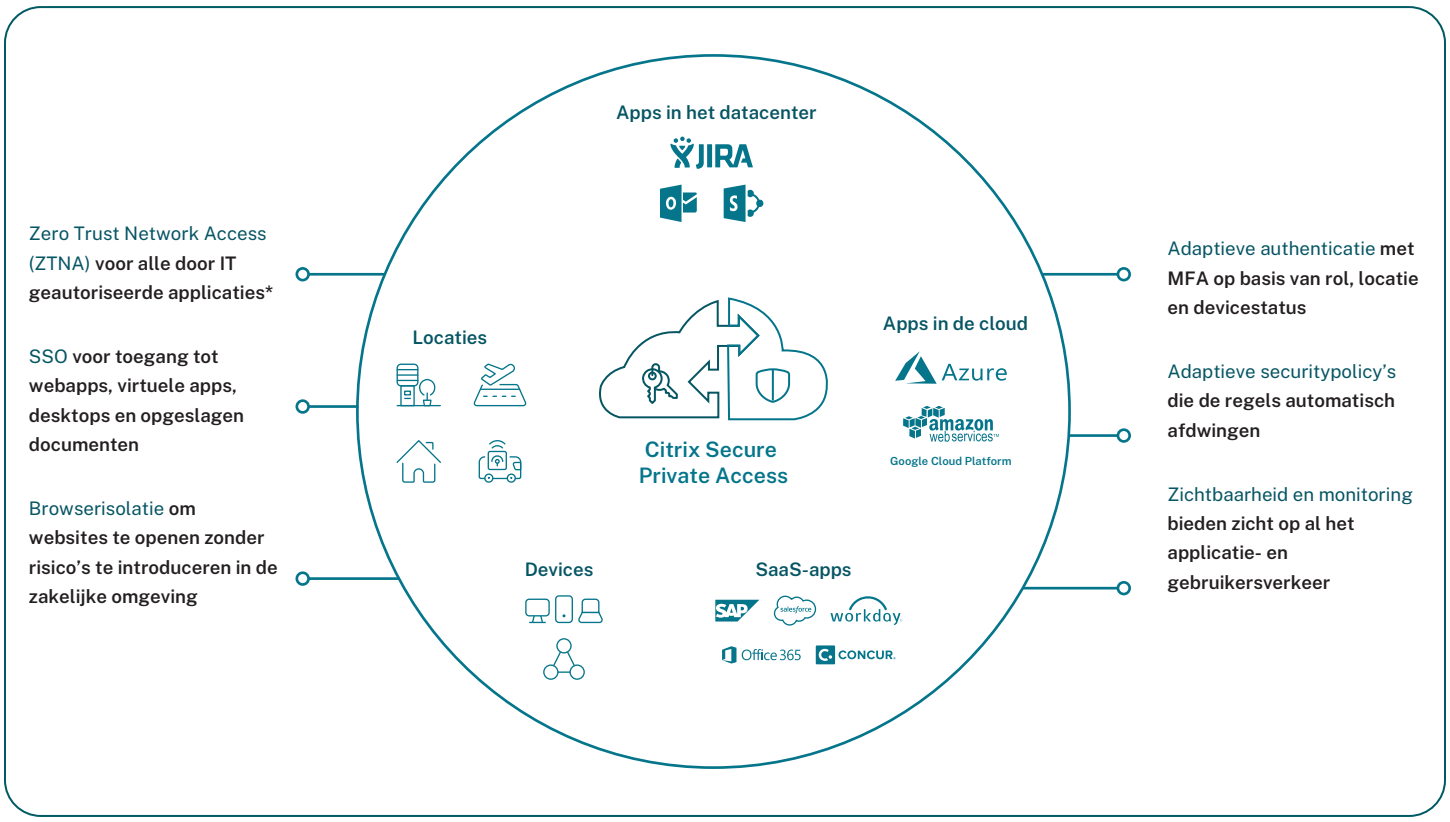
Met Citrix Secure Private Access biedt de IT-afdeling medewerkers, contractors en partners toegang tot de applicaties die zij nodig hebben. Het staat medewerkers op afstand vrij om hiervoor een BYO-device te gebruiken, de veiligheid is gegarandeerd.

Adaptieve toegangsregels leiden gebruikerssessies op een BYO-device automatisch om naar een externe sessie in een geïsoleerde browser. Schadelijke content kan op deze manier nooit worden overgedragen van een BYO-device naar applicaties of netwerken. Ook is het nu niet meer mogelijk om data van de organisatie te downloaden op een persoonlijk device. Verder ondersteunt Secure Private Access allerlei policy's om apps, gebruikerssessies en gevoelige informatie in Workspace te beschermen tegen keyloggers en screencapture-malware.

Zero Trust Network Access (ZTNA)

Zero trust gaat in tegen het vertrouwensprincipe van vroeger. Zero trust gaat uit van het idee dat niemand te vertrouwen is en dat iedereen blijvend moet worden gecontroleerd. Traditionele oplossingen op basis van het 'castle-and-moat' model richten zich alleen op het authenticeren en autoriseren van gebruikers op het moment van aanmelden. Is de authenticatie eenmaal goed verlopen, dan geniet zo'n gebruiker alle vertrouwen. Met gestolen devices of gebruikersgegevens kon dit model echter gemakkelijk om de tuin worden geleid, met onbevoegde toegang tot gevolg.

Met zero trust worden alle gebruikersactiviteiten tijdens de sessie blijvend bewaakt en beoordeeld. Wordt iets afwijkends geconstateerd, dan komen automatische securitymechanismen in actie.



Allesomvattende, geconsolideerde zero trust-securitystrategie	Stelt IT in staat om een allesomvattende zero trust-securitystrategie te implementeren voor alle gebruikers, applicaties, bestanden en endpoints.
Zero Trust Network Access (ZTNA) voor alle door IT geautoriseerde applicaties	VPN's zijn moeilijk schaalbaar, geven aanleiding tot zorgen met betrekking tot privacy en voldoen niet aan de securitynormen van vandaag. Citrix Secure Private Access biedt echter Zero Trust Network Access (ZTNA) voor alle door de IT-afdeling geautoriseerde IT-applicaties, van web-, SaaS- en client-serverapplicaties (TCP) tot virtuele applicaties, on-premise geïmplementeerd of in een public cloud, en benaderd binnen Citrix Workspace of daarbuiten. Het resultaat is precies wat u mag verwachten van zero trust.
Adaptieve authenticatie, SSO en verbeterde security	Citrix Secure Private Access biedt de mogelijkheid om devices van gebruikers te scannen voor en na het opzetten van een gebruikerssessie. Daarbij wordt gekeken naar de gebruikerslocatie en status van het device, en op basis daarvan kan dan worden bepaald hoe de toegang tot applicaties moet worden geauthenticeerd en geautoriseerd. Met deze policy's hebben systeembeheerders controle over de dingen die gebruikers kunnen doen binnen deze applicatie. Deze policy's kunnen worden geïmplementeerd voor alle applicaties, ook voor Citrix Virtual Apps and Desktops service.
Veilige toegang tot door IT goedgekeurde apps met BYO- en unmanaged devices dankzij geïntegreerde Remote Browser Isolation	Citrix Secure Private Access geeft gebruikers vanaf hun eigen BYO-devices toegang tot apps die de IT-afdeling heeft goedgekeurd, zonder dat er een endpoint agent op het device van de gebruiker hoeft te worden geïnstalleerd. In plaats daarvan wordt de sessie omgeleid van een lokale browser naar een gehoste Secure Browser Service. Gebruikers krijgen nu in een sandbox-omgeving toegang tot hun apps en kunnen daardoor toch productief blijven. Browserisolatie beschermt endpoints en netwerken tegen schadelijke content die van internet kan komen, waardoor er een echte 'air-gapped' omgeving ontstaat.
Bescherming tegen keyloggers en malware die screenshots maakt	Devices die de organisatie zelf beheert, kunnen exact worden gemonitord. De status van onbeheerde devices is echter een groot vraagteken. Dit brengt grote risico's met zich mee. Devices kunnen malware bevatten zoals keyloggers of malware die screenshots maakt en waarmee gevoelige data van de organisatie kan worden gestolen. Citrix Secure Private Access maakt het onmogelijk dat een keylogger met gebruikersgegevens aan de haal gaat of dat malware screenshots maakt van applicaties die in de Workspace app zijn geopend.

End-to-end zicht op alle applicaties en gebruikers	Citrix Secure Private Access biedt complete end-to-end monitoring en zichtbaarheid van al het gebruikersverkeer naar alle door de IT-afdeling geautoriseerde applicaties. Klanten die werken met meerdere toegangsoplossingen en meerdere dashboards voor het monitoren van al het gebruikersverkeer, profiteren voortaan van één dashboard dat de monitoring vereenvoudigt en aparte omgevingen bij elkaar brengt.
Detectie van en bescherming tegen potentiële risico's	Citrix Analytics for Security biedt inzicht in applicaties, devices en netwerken, waardoor de security kan worden geautomatiseerd op basis van gebruikersgedrag en gedetecteerde afwijkingen. Dit resulteert in minder handmatig werk voor de IT-afdeling. Regels worden hiermee altijd op het juiste moment afgedwongen en de kans op een inbreuk wordt tot een minimum beperkt.

Kort samengevat

Veilige toegang tot applicaties en data houdt meer in dan bescherming tegen dreigingen en kwetsbaarheden. Om medewerkers productief en betrokken te houden, is het belangrijk dat de toegang tot systemen probleemloos verloopt, zonder dat gebruikers zich steeds opnieuw hoeven aan te melden en zonder gedoe met wachtwoorden.

Citrix Secure Access oplossingen zijn daarom ontwikkeld om het beste te bieden van twee werelden: een ongeëvenaarde applicatie-ervaring op elke werklocatie en geavanceerde adaptieve, in de cloud aangeboden security.

In tegenstelling tot traditionele on-premise VPN's maakt end-to-end zero-trust security het mogelijk dat gebruikers alle applicaties die de IT-afdeling heeft goedgekeurd, benaderen zonder toegang tot het volledige netwerk te krijgen. Zero trust maakt het voor u mogelijk om toegang te verlenen op basis van context (afhankelijk van identiteit, tijdstip en devicestatus bijvoorbeeld) en waar en hoe applicaties worden gebruikt.

Naarmate steeds meer medewerkers thuis aan de slag gaan, wordt een volledig in de cloud aangeboden securitysysteem steeds belangrijker. Bij gebruik van wereldwijde cloudservices die zijn ontwikkeld voor complete dekking en resiliency, worden uw policy's en bescherming steeds automatisch afgestemd op de risico's van dat moment.

Meer informatie over Citrix Secure Private Access:
https://www.citrix.nl/products/citrix-secure-private-access/

Enterprise Sales
Noord-Amerika | 800-424-8749
Internationaal | +1 408-790-8000

Locaties
Hoofdkantoor | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, Verenigde Staten
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, Verenigde Staten