Single Sign-On op de juiste manier

Zes manieren waarop Citrix Workspace naadloze toegang tot alle apps mogelijk maakt en tegelijk de security en gebruikerservaring verbetert

Single Sign-On (SSO) is bedoeld om het leven van medewerkers en IT-afdelingen gemakkelijker te maken.

SSO-oplossingen moeten de beheerkosten verlagen en security en gebruikerservaring verbeteren. Maar veel oplossingen schieten tekort omdat ze slechts gelden voor een bepaald soort applicaties. Dit betekent dat u meerdere toegangsoplossingen nodig hebt, van verschillende makers, wat weer ten koste gaat van de productiviteit en gebruikerservaring. De complexiteit van een dergelijke implementatie doet de ‘zero trust’-initiatieven die veel organisaties nu ondernemen, weer teniet.

Met Citrix Workspace brengt u alle apps en data in uw hele gedistribueerde IT-architectuur bij elkaar en krijgen medewerkers door middel van SSO toegang tot alle applicaties en data die ze voor hun werk nodig hebben.

Citrix Secure Workspace Access werkt met uw bestaande infrastructuur samen om verschillende remote access solutions te consolideren (zoals traditionele VPN’s of SSO-oplossingen), wat het beheer voor de IT-afdeling vereenvoudigt en uniforme toegang voor medewerkers mogelijk maakt.

Zes voordelen van Citrix Workspace SSO

1 VPN-loze en veilige toegang tot de resources van de organisatie

2 Fijnmazige controle voor SaaS-apps en internet

3 Controle over uw gebruikersidentiteit

4 Meer security dan alleen gebruikersnaam en wachtwoord

5 Naadloze integratie met bestaande omgevingen

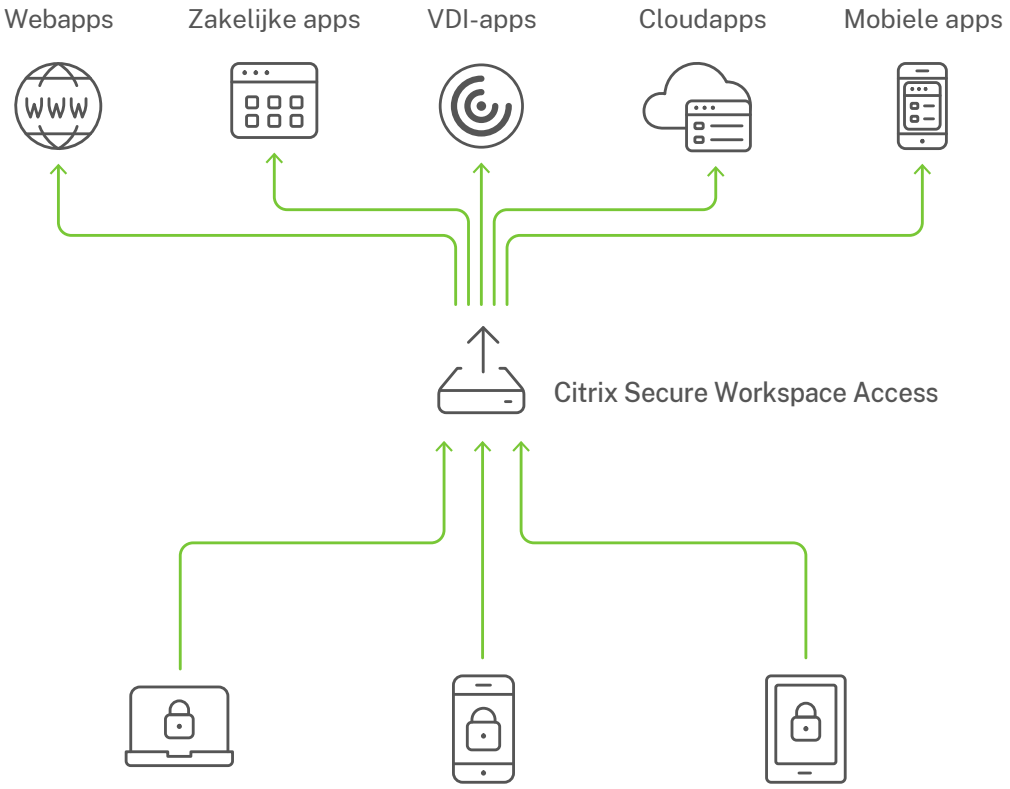
6 Snellere probleemoplossing met end-to-end zichtbaarheid

Lees op de volgende pagina's meer over elk voordeel.

1 VPN-loze en veilige toegang tot de resources van de organisatie

Veel oplossingen dekken vaak niet het hele applicatielandschap. Als u een oplossing hebt die alleen geschikt is voor bijvoorbeeld uw virtuele en zakelijke apps, dan hebt u een aparte SSO-oplossing nodig om toegang mogelijk te maken tot uw web- en SaaS-applicaties.

Citrix Workspace vereenvoudigt de toegang – met SSO – tot virtuele, SaaS- en webapps, maar ook tot bestandsopslag in de cloud en in uw datacenter. De IT-afdeling lost hiermee de complexiteit van het hebben van meerdere toegangsoplossingen zoals VPN's en SSO op, en maakt het mogelijk om zowel de 'zero trust'-strategie als de gebruikerservaring te verbeteren.



Citrix Workspace met Citrix Secure Workspace Access biedt toegang tot al uw apps en data

2 Fijnmazige controle voor SaaS-apps en internet

Uw SSO-oplossing moet meer bieden dan simpele toegang. Wat u zeker ook moet hebben, is fijnmazige contextafhankelijke controle over uw SaaS- en webapps.

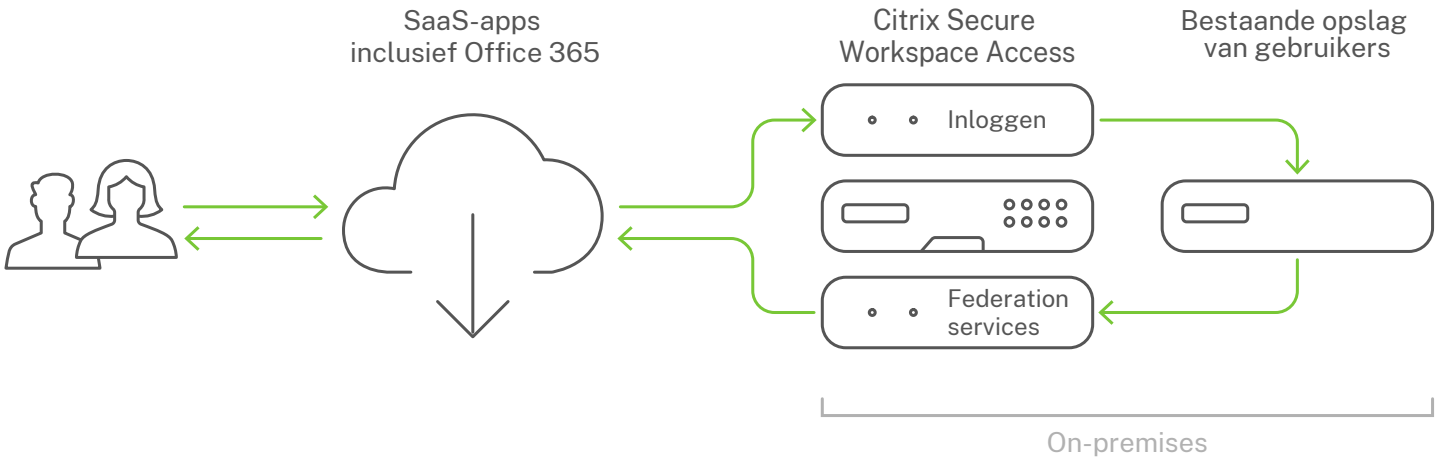
Bovendien houdt ook onbewaakt internetten grote risico's in voor uw organisatie. Sommige organisaties maken internet (deels) ontoegankelijk, maar dit is niet altijd goed voor de productiviteit.

Gegevensbescherming is iets wat veel organisaties proberen te bereiken met hun 'zero trust'-strategie. Met de securitypolicy's voor SaaS- en webapps van Citrix Secure Workspace Access zorgt u voor maximale bescherming van uw data. Met deze policy's is het bijvoorbeeld mogelijk om kopiëren/plakken, printen of downloaden onmogelijk te maken. Of u bepaalt wat er mogelijk is met de navigatiebalk of de knoppen om vooruit en terug te gaan, of mobiele toegang mogelijk is en of u met watermerken wilt werken.

Met black- en whitelisting van URL-categorieën bepaalt de systeembeheerder welke websites wel en niet toegankelijk zijn. Verder kunt u het onmogelijk maken dat URL's worden geopend vanuit SaaS-apps. Of ervoor zorgen dat onbekende SaaS-apps of weblinks worden geopend in een veilige browser, waardoor ze volledig gescheiden blijven van het bedrijfsnetwerk of systemen van de organisatie. Malware die via schadelijke sites binnenkomt, kan op deze manier nooit iets veranderen aan de infrastructuur van de organisatie, waardoor u maximale bescherming hebt.

Citrix Secure Workspace Access ondersteunt standaard de populairste SaaS-apps zoals SalesForce, G Suite, Office 365, Zoom, Workday en Expensify. Voorgeconfigureerde applicatiesjablonen maken het gemakkelijk om apps te publiceren en om SSO-regels te configureren.

3 Controle over uw gebruikersidentiteit



SaaS-applicaties zoals Microsoft Office 365, Salesforce, Workday en ADP zijn onmisbaar aan het worden. Het is zelfs zo dat de gemiddelde grote organisatie tegenwoordig gebruikmaakt van 1427 aparte cloudservices.[1]

Om SSO mogelijk te maken voor deze apps, die worden aangeboden vanuit de cloud en geen deel van het eigen datacenter en netwerk uitmaken, zijn organisaties bij de meeste oplossingen verplicht om hun user directory ook in de cloud te plaatsen en daardoor hun bestaande infrastructuur voor identiteitsbeheer ook op de schop te nemen. Citrix Secure Workspace Access maakt het mogelijk om te kiezen en om uw eigen identiteitssysteem te gebruiken met Citrix Workspace.

Wij ondersteunen hiervoor diverse platforms, zoals Microsoft, Google en Okta. Dit is mogelijk door middel van identity federation en interne SAML of ADFS federation services. Daarmee wordt de cloudservice een token aangeboden met daarin een aantal claims met betrekking tot de geauthenticeerde gebruiker, zoals zijn of haar identiteit. De cloudservice controleert deze claims daarna op basis van zijn eigen federation services.

Deze keuzemogelijkheid zorgt ervoor dat u uw eerdere investeringen in identiteitssystemen niet overboord hoeft te gooien en toch veilige toegang tot de systemen van uw organisatie mogelijk maakt.

4 Meer security dan alleen gebruikersnaam en wachtwoord

Gebruikersauthenticatie wordt steeds belangrijker, zeker nu organisaties hun continuïteit willen versterken en met grote aantallen thuiswerkers zitten. Deze medewerkers, maar ook partners of tijdelijke krachten die niet per se op de personeelslijst van de organisatie staan, werken buiten het bedrijfsnetwerk en op eigen devices. Dit maakt het cruciaal om snel de identiteit van de gebruiker te controleren en toegang tot de organisatie toe te staan (of niet).

Dit is de reden waarom Citrix Secure Workspace Access niet uitgaat van alleen gebruikersnaam en wachtwoord.

Ook meervoudige authenticatie wordt ondersteund. Daarmee heeft de IT-afdeling fijnmazige controle over wie toegang krijgt tot het bedrijfsnetwerk, wat die persoon kan benaderen, wanneer, en met welk device.

Citrix Secure Workspace Access integreert met en ondersteunt alle authenticatiemechanismen en -protocollen, zoals RADIUS, TACACS, NTLM, Diameter, SAML 2.0, OAuth 2.0 en OpenID 2.0. Voor meervoudige authenticatie en aanmelding zonder wachtwoord wordt ook Azure Active Directory ondersteund, evenals on-premise Active Directory voor tweevoudige authenticatie met native OTP.

5 Naadloze integratie met bestaande omgevingen

Een oplossing voor Single Sign-On heeft een groot aantal raakpunten binnen uw organisatie, van user directory tot authenticatiemechanismen en van applicaties tot de devices die worden gebruikt.

Citrix Secure Workspace Access wordt heel eenvoudig geïntegreerd in uw bestaande infrastructuur en ligt dan aan de basis van een geweldige gebruikerservaring en sterk vereenvoudigd IT-beheer.

- Uw eigen huisstijl voor uw applicatieportal
- Ondersteuning voor alle authenticatie-mechanismen zoals RADIUS, Diameter, Kerberos, Microsoft NTLM, TACACS en formulieren
- Ondersteuning voor alle gebruikersdevices van Windows, Mac en Linux tot iOS en Android
- Ondersteuning voor alle SSO-protocollen zoals SAML, OAuth en OpenID

Eenvoudige integratie met bestaande systemen was de belangrijkste factor bij de evaluatie van authenticatieoplossingen.[2]

6 Snellere probleemoplossing met end-to-end zichtbaarheid

Omdat Citrix Secure Workspace Access toegang biedt in uw volledige applicatielandschap, is het nu ook mogelijk om problemen met de application delivery en gebruikerservaring te monitoren en op te lossen.

Citrix Analytics, een aanvullende component van Citrix Workspace, maakt alle TCP en HTTP user sessions end-to-end inzichtelijk. Insight registreert authenticatiefouten, bijvoorbeeld als gevolg van een vervallen wachtwoord, een geblokkeerd account of een probleem met een endpoint. Ook SSO-fouten of fouten bij het opstarten van applicaties worden vastgelegd, wat de troubleshooting eenvoudiger maakt voor u.

Citrix Analytics biedt bovendien continue authenticatie en autorisatie, wat bij veel organisaties hoog op het verlanglijstje staat als het gaat om zero trust. Het systeem houdt rekening met de context, wat het mogelijk maakt om bijvoorbeeld bij een verandering van locatie of device een extra controle toe te passen, bijvoorbeeld een tweede authenticatiefactor, voordat toegang wordt verleend.

Risico-indicatoren en criteria maken het mogelijk om afwijkingen op gebruikersniveau te detecteren. U kunt regels configureren om snel op de hoogte gebracht te worden van ongeoorloofd of riskant gebruikersgedrag, bijvoorbeeld iemand die informatie up- of downloadt naar of van malafide, riskante websites. Automatisering op basis van Citrix Analytics maakt het mogelijk om dingen voor u te laten doen, zoals het opnemen van een sessie, het laten verlopen van links naar gedeelde documenten of het blokkeren van het account van een gebruiker.

Geef mensen de vrijheid om te werken op hun manier. Met Citrix Workspace biedt u echte Single Sign-On voor alle applicaties en hebt u geen traditionele VPN's of SSO-toegangsoplossingen meer nodig. Wat u hiermee krijgt, is eenvoudiger IT-beheer, betere security en een betere gebruikerservaring.

Meer informatie: citrix.nl/workspace.

Bronnen:
1. 12 Must-Know Statistics on Cloud Usage in the Enterprise, Skyhigh Networks.
2. 2017 State of Authentication Report, Javelin.

RES13 11/20