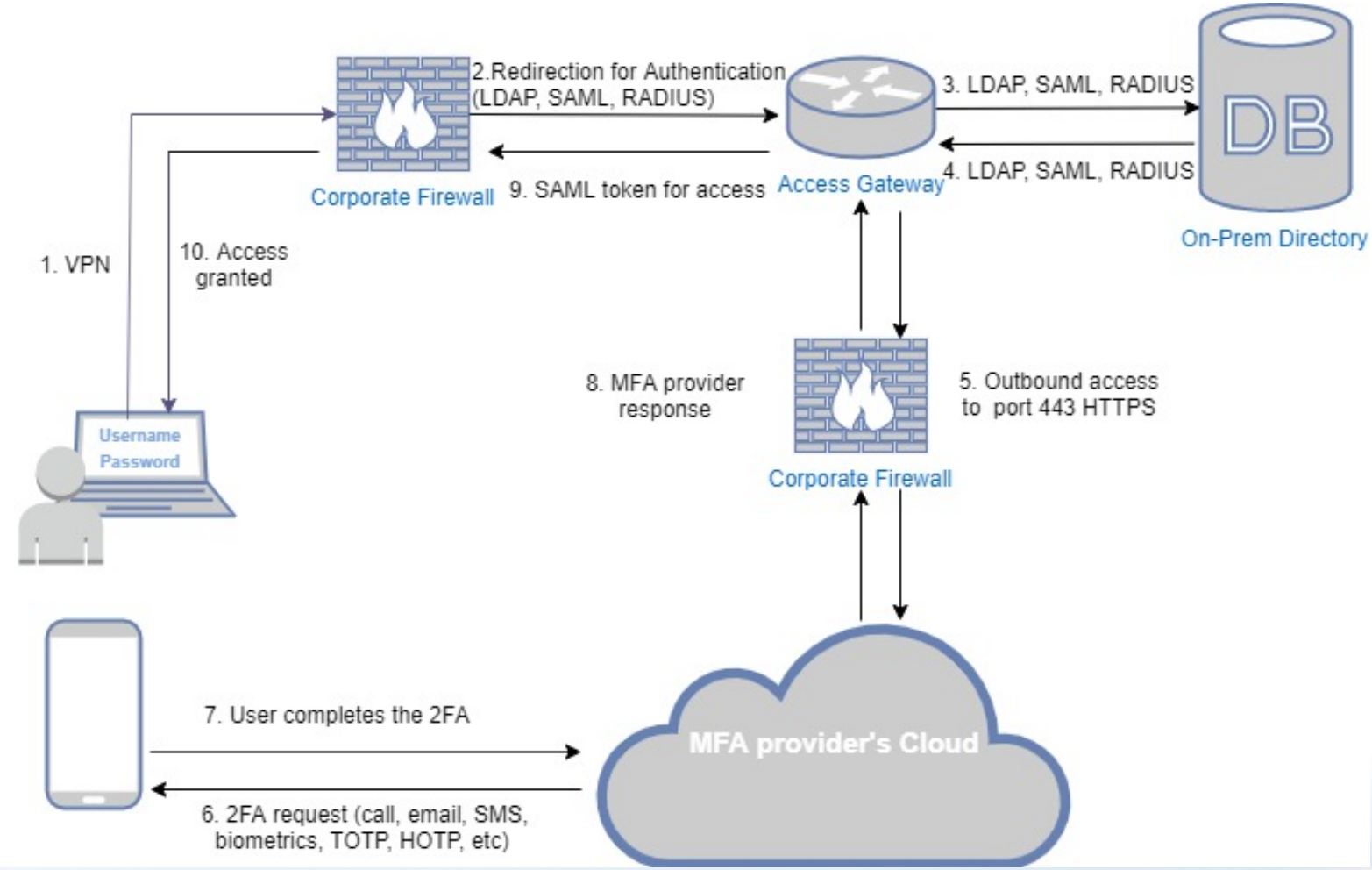
COMPUGEN
Simplifying the business of technology . . . together

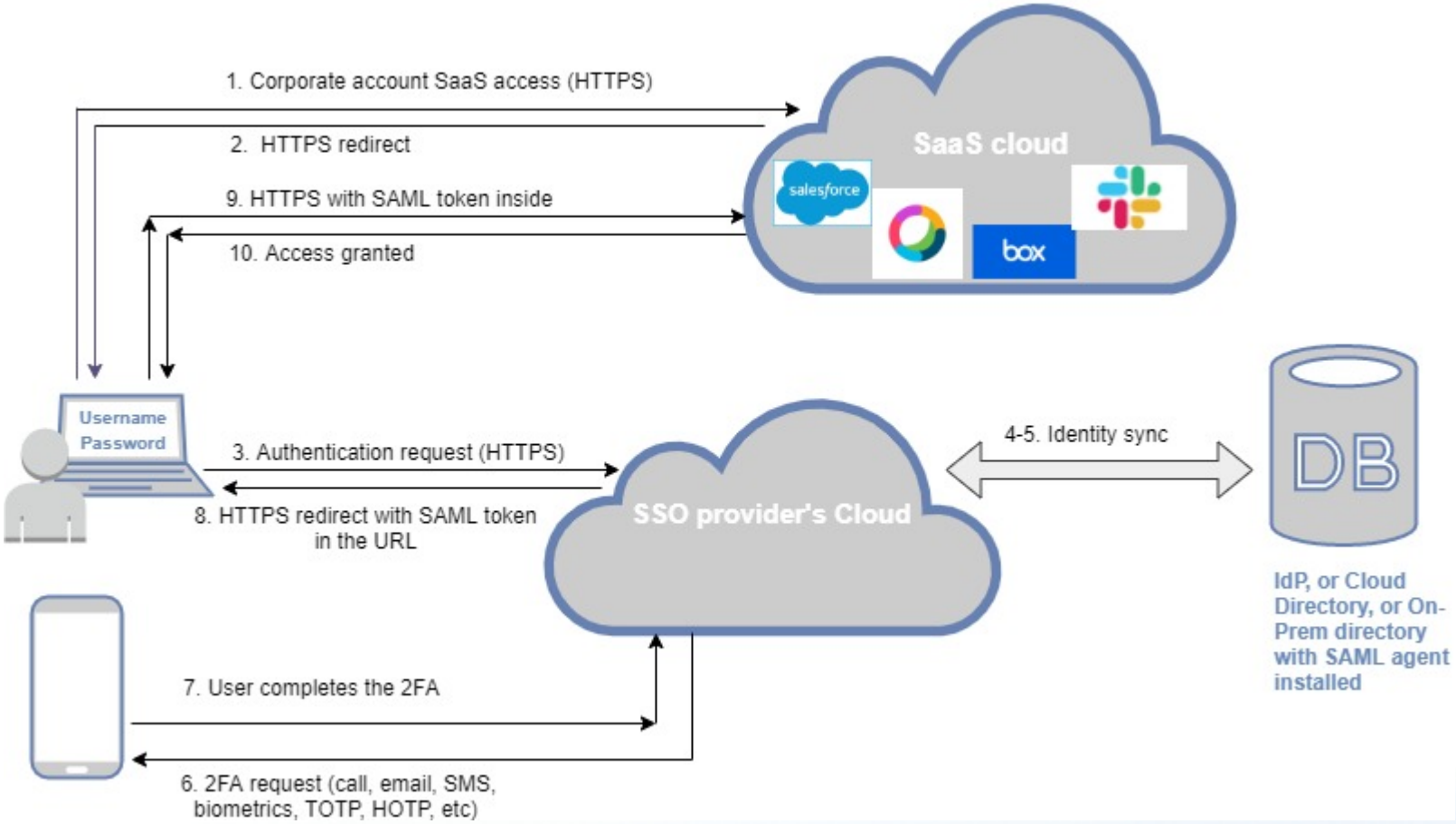
Single Sign-On and Multi-Factor Authentication

Daria Alavidze, Principal Consultant
2019

On-prem applications example



SaaS application example



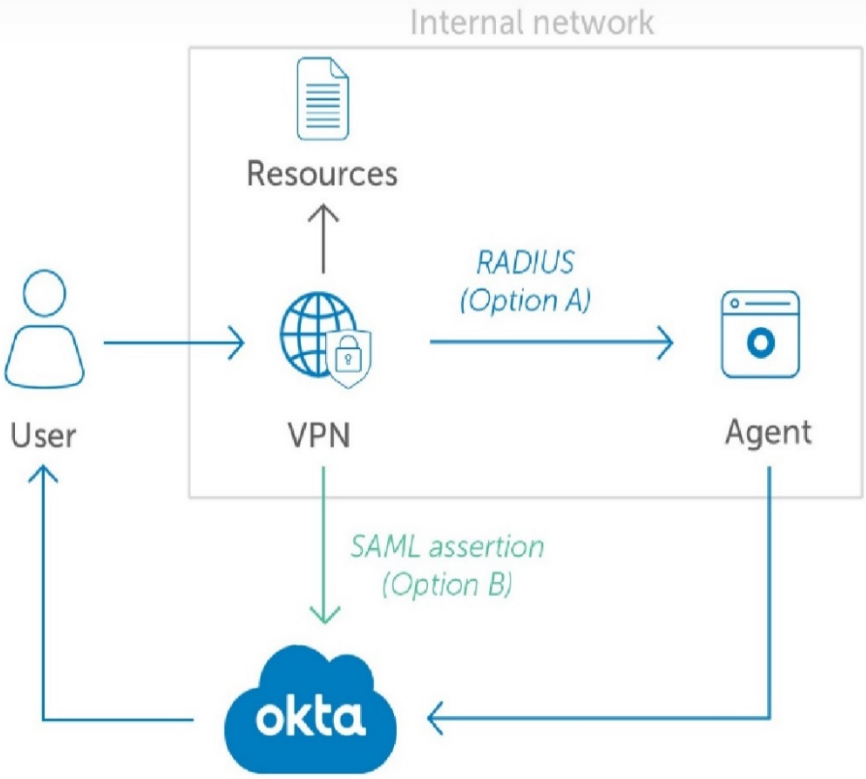
SSO + MFA vendors (Okta)

Vendor	Overview	Pros	Cons
okta	Superior identity product, better suited to support cloud app heavy as well as adaptive use cases. Well-respected in the IDaaS arena. Features list includes security policies that support MDM and geolocation, the ability to integrate multiple sources of identity data, and all packaged in a solution that is relatively easy to use	Ease of deployment and administration. Intelligent access policies, contextual access management, robust platform for directory services, OKTA integration Network, okta SSO, okta lifecycle management. **Does not require an on-prem gateway for SSO to cloud apps.** **6000+ pre-built integrations**	Limited reporting and monitoring functionality. **Limited out-of-the-box on-prem integrations.** Requires additional components for on-prem integrations (Okta Radius agent). Integration costs for 3rd party apps, on-prem.

Products:

- Okta Universal Directory is a cloud-based directory service that can serve as a single source of truth for IT organizations, and it serves as an integration point to multiple Ads and other on-premises directory services
- Okta SSO - makes managing and securing the extended enterprise simpler for IT and eliminates the password proliferation that plagues user
- Okta Access Gateway-Secure access to on-prem apps and protect your hybrid cloud – without changing how your apps work today
- Okta Advanced Server -IT can extend the same access control to the server layer, bringing secure access management to the full breadth of on-premises and cloud resources IT needs to manage.
- Okta Adaptive MFA
- Okta LifeCycle Management -Automate all lifecycles with any business process for external and internal users

Okta MFA for VPN



Okta MFA for VPNs typically supports integrations through RADIUS (Option A) or SAML (Option B).

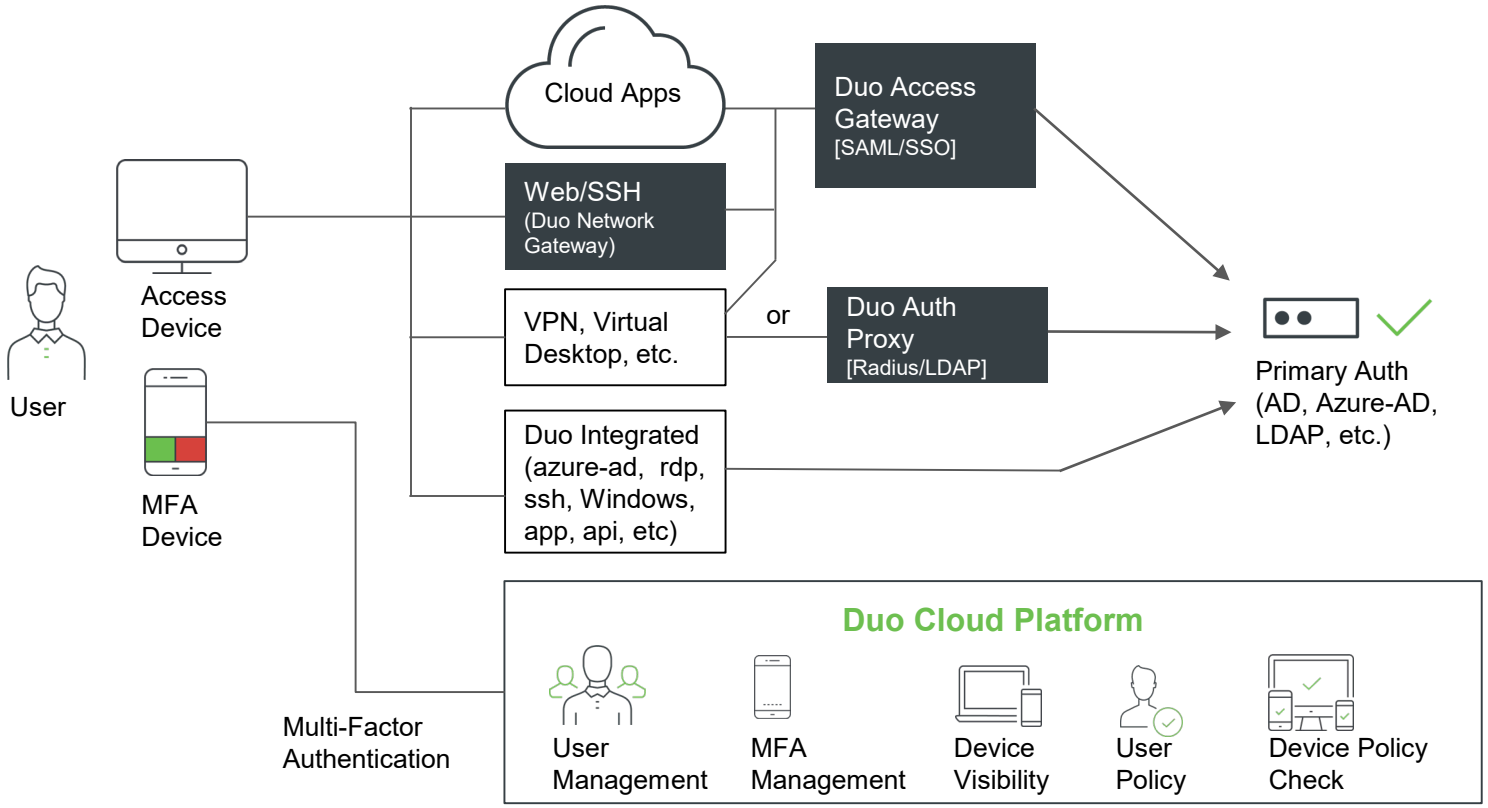
SSO+MFO vendors (Duo)

Vendor	Overview	Pros	Cons
	Duo positions itself as a very strong MFA vendor, not an IDaaS provider. Duo is a feature-rich MFA solution that competes directly to Okta's Adaptive MFA.	Duo leads in some advanced features and **on-prem integrations**, it supports out of the box integrations to many on-prem apps like OWA and VPNs**, has native solutions for MFA into Linux and Windows servers and SSH session**s. Easy self-enrollment process. Coverage for all types of devices, continuous monitoring of all trusted endpoints. User-based policies (geolocation, ip range, etc.), device-based policies, group-based policies. Integrates with external IdPs (Including OKTA, Shibboleth and Azure). Because Duo can put MFA on anything you'll be more likely to be compliant against NIST, GDPR.	**Duo requires an on-prem components for SSO to cloud apps.** **Duo is not an IdP or IdaaS**. Almost all integrations require manual configurations.

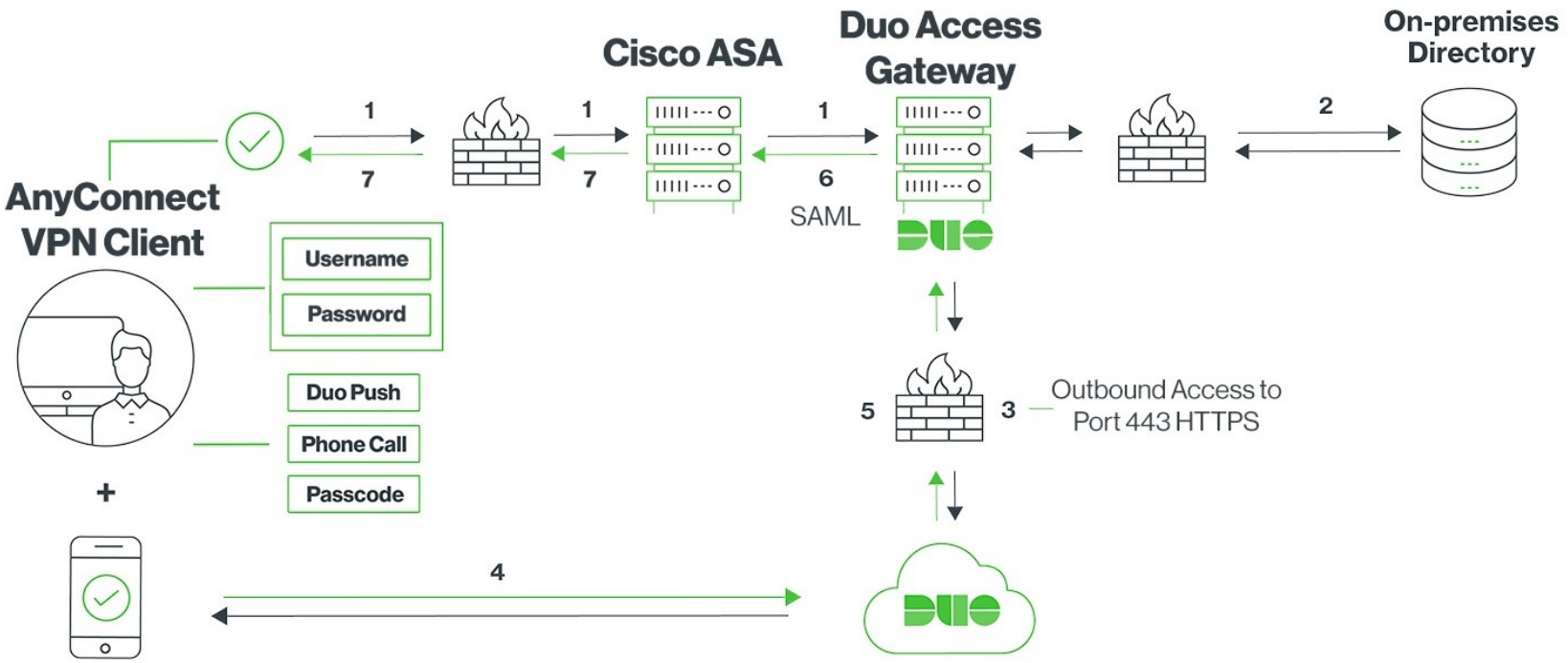
Products:

- Duo Access Gateway (SAML/SSO) - an IdP that verifies authentication requests against an on-premises or cloud identity database (MS AD, OpenLDAP, SAML IdP, OpenID connect)
- Duo Auth Proxy (Radius/LDAP) - Allows application integration with Duo cloud to enable 2FA for apps that support RADIUS or LDAP
- Duo Network Gateway (Web/SSH) -Detect user & device context for internal HTTP/S and SSH apps

Duo Product Architecture



Duo MFA for VPN



SSO+MFO vendors (Microsoft Azure)

Vendor	Overview	Pros	Cons
Microsoft	Microsoft's Azure AD tight integration with Windows Server Active Directory and Office 365. Azure AD also offers the lowest entry-level pricing for handling multi-factor authentication, and offers advanced toolsets for managing identities and the cloud apps used by your organization.	Best-in class integration with Windows Server Active Directory. Tight integration with Microsoft's array of cloud services. Identity Protection allows for security policies based on Big Data and machine learning. Conditional Access.	Limited security policies compared to SSO specific products. Some competitors have better integration with third-party directories and SaaS platforms. Advanced reporting capabilities only available in Premium pricing tiers. Limited second factor choices and does not provide its own soft token

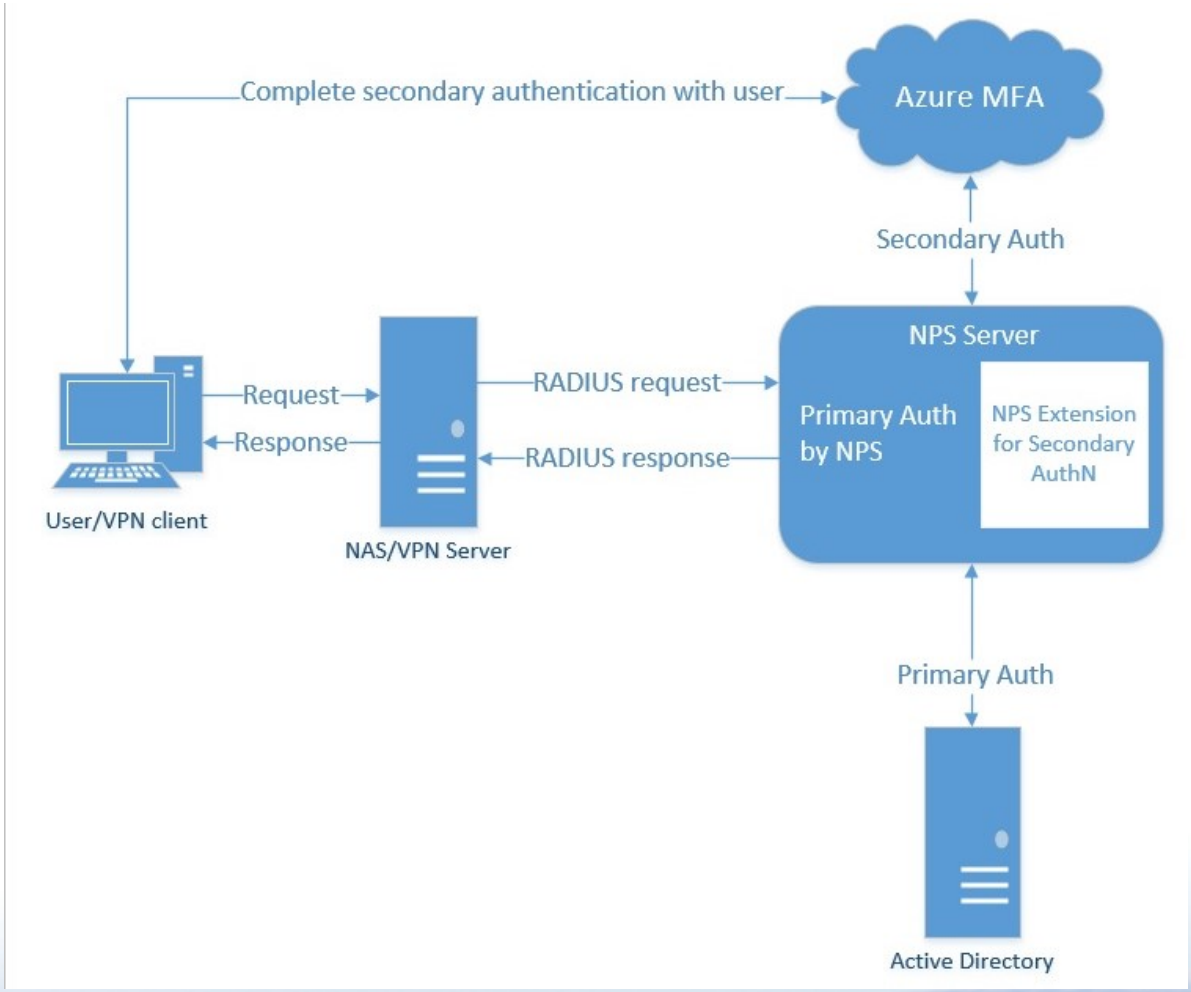
Multi-Factor Authentication comes as part of the following offerings:

Azure Active Directory Premium or **Microsoft 365 Business** - Full featured use of Azure Multi-Factor Authentication using Conditional Access policies to require multi-factor authentication.

Azure AD Free or standalone **Office 365** licenses - Use pre-created Conditional Access baseline protection policies to require multi-factor authentication for your users and administrators.

Azure Active Directory Global Administrators - A subset of Azure Multi-Factor Authentication capabilities are available as a means to protect global administrator accounts.

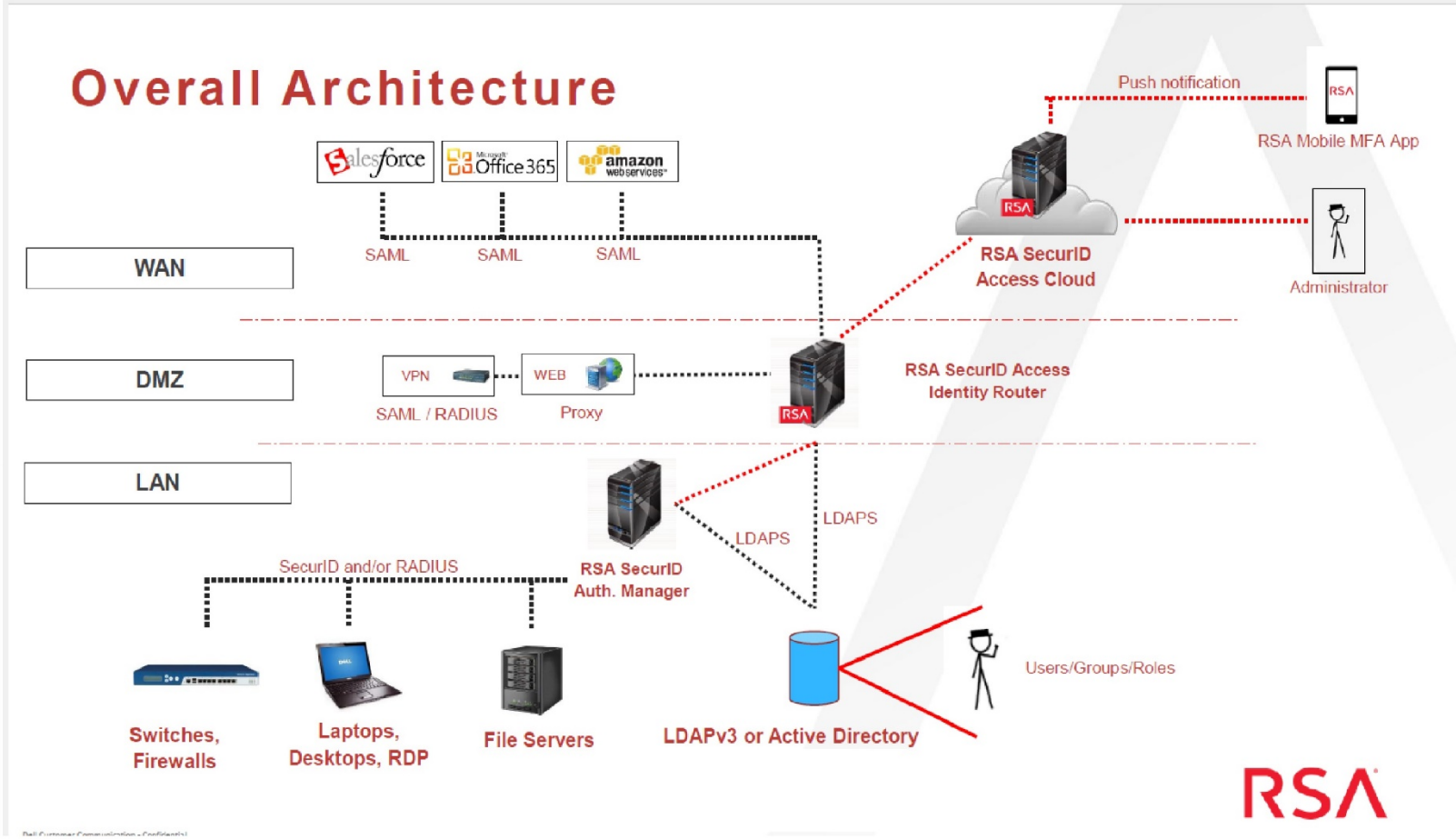
Azure MFA for VPN



SSO+MFO vendors (RSA SecurID)

Vendor	Overview	Pros	Cons
RSA	Strong MFA solution. Very strong on-prem story.	Supports the widest variety of factors. Full self-service portal. Hybrid architecture, risk-based authentication Assurance Levels, Policies, and Applications. . Levels of authentication (Low, Medium and high). machine learning algorithms, combining several contextual factors, to assess user risk based on anomaly detection 400+ integrations documented	**RSA requires an on-prem components for SSO to cloud apps.** **RSA is not an IdP or IdaaS**. Almost all integrations require manual configurations.

RSA architecture



Factors supported

	okta	DUO	RSA	Microsoft
What authentication methods are supported?	-OKTA Verify -Voice Call Authentication -U2F Security Key (FIDO) -Windows Hello -Duo -On-Prem MFA -Email authentication -Custom TOTP authentication -SMS Authentication -Google Authenticator -WebAuthn (FIDO2) -YubiKey -Symantec VIP -Security question -IdP authentication https://help.okta.com/en/prod/Content/Topics/Security/MFA.htm	-U2F tokens -Phone Callback -Mobile passcodes (HOTP, TOTP) -Duo Push -Biometrics -SMS passcodes -Bypass codes -Hardware tokens	-Mobile OTP -Phone Callback -RSA Push -Wearables (smartwatch) -Biometrics -Face ID -Proximity -SMS -FIDO keys -Hardware token -Software token	-Password -Security questions -Email address -Microsoft Authenticator app -OATH Hardware token -SMS -Voice call -App passwords

Mobile applications

	okta	DUO	RSA	Microsoft
Does the product support authentication apps for iOS/Android devices? (Google Authenticator? Proprietary app?) Are other devices supported? (Apple Watch, Android Wear)	**Okta Mobility Management (OMM)** For the proprietary app: -iOS 7.1 or higher -Android 4.0 or higher -Apple Watch is supported -Google Authenticator is supported https://support.okta.com/help/s/article/Okta-Mobility-Management-OMM-Knowledge-Hub	**DUO Mobile:** Duo Mobile works on every device - including smartwatches. Use your Apple Watch to receive login requests on your wrist, and authenticate on your iPhone, iPad or Apple Watch. Duo Mobile for iOS also supports Touch ID, an additional layer of security to verify your users' identities. Duo Mobile works with Apple iOS, Google Android, Palm, Windows Phone 7, Windows Mobile 8.1 and 10, and J2ME/Symbian. Download Duo Mobile for iPhone or Duo Mobile for Android - they both support Duo Push, passcodes and third-party TOTP accounts.	**RSA SecurID:** The RSA SecurID Authenticate App can serve as the one authenticator for all of your authentication needs. It supports push notification, mobile OTP and biometrics, and provides secure access to both cloud-based and on-premises applications from all major mobile platforms, including iOS, Android and Windows Phone.	**Microsoft Authenticator:** The Microsoft Authenticator app provides an additional level of security to your Azure AD work or school account or your Microsoft account. The Microsoft Authenticator app is available for Android, iOS, and Windows Phone.

Contextual access management

	okta	DUO	RSA	Microsoft
Can different authentication methods be applied based on criteria such as role, application, location, other criteria? If so, does this functionality cost extra? If it does, how much extra?	**Identity Provider Routing Rules:** Identity Provider (IdP) routing rules enable you to direct end users to identity providers based on the user's location, device, email domain, attributes, or the app they are attempting to access. (This feature is also known as IdP Discovery, because these routing rules allow Okta to discover which identity provider to use based on this context.) **!!! There are limitations and pre-requisites** https://help.okta.com/en/prod/Content/Topics/Security/Identity_Provider_Discovery.htm	**Adaptive Authentication & Policy Enforcement** Set policies to grant or block access attempts by identity or device and based on contextual factors such as user location, network address ranges, biometrics, device security and more. **Requires Duo Access License.** https://duo.com/product/adaptive-authentication-and-policy-enforcement	**Seamless Identity Assurance** Uses machine learning algorithms, combining several contextual factors, to assess user risk based on anomaly detection. Risk Level is calculated based on Context (Network, Location, Behavior, Country, Agent, Browser), User (Admin, Executive, Employee), Resource (Classified, Public, I.P.Data)	Yes, Microsoft highly recommends Administrators enable users to select more than the minimum required number of authentication methods in case they do not have access to one. Profiles can be created based on user groups and job roles.

Supported applications

	okta	duo	RSA	Microsoft
Institution-hosted VPNs	YES (Using an agent)	YES	YES	YES
RDP	YES (Using an agent)	YES	YES	YES
VDI (VMWare, Citrix)	YES	YES	YES	YES
SSH	YES	YES	YES	YES
Banner SSO	YES			
Linux PAM	NO	YES	YES	YES
Privilleged access management systems (Cyberark, Thycotic Secret Server)	Cyberark and Thycotic are supported: https://www.okta.com/partners/cyberark https://www.okta.com/resources/find-your-apps/?keywords=thycotic&page=204	Cyberark https://duo.com/docs/cyberark Thycotic https://duo.com/docs/thycotic	Cyberark https://community.rsa.com/community/products/securid/blog/2018/11/08/privileged-access-the-poster-child-for-modern-mfa Thycotic https://community.rsa.com/docs/DOC-104894	YES https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/cyberark-saml-authentication-tutorial