okta

Vorteile der Migration von ADFS auf Okta

Okta Deutschland
Oskar-von-Miller-Ring 20
80333 München

info_germany@okta.com
+49 (89) 26203329

Herausforderungen bei der Bereitstellung von Single Sign-On

Die Akzeptanz von Cloud-Anwendungen hat sich in den letzten Jahren stark erhöht. Cloud-Anwendungen wie Salesforce.com, Box und Office 365 werden im gesamten Unternehmen eingesetzt. Infolgedessen haben viele Unternehmen entweder Richtlinien für Cloud-Anwendungen entwickelt oder wollen dies in naher Zukunft tun.

Viele Unternehmen erwägen heute die Einführung von Single Sign-On (SSO), damit ihre Benutzer problemlos auf Cloud- und Webanwendungen zugreifen können, ohne sich bei jeder Anwendung erneut zu authentifizieren. Sie wollen alle Cloud-Anwendungen an eine zentrale, verbindliche Informationsquelle anbinden, wofür in vielen Fällen Microsoft Active Directory dient. Dabei kommen viele Unternehmen zu dem Schluss, dass Active Directory-Föderationsdienste (ADFS) die Lösung für Single Sign-On in Verbindung mit Active Directory sind – ganz einfach, weil beide von Microsoft angeboten werden.

Aber nicht alle Active Directory-Integrationslösungen sind gleich. IT-Abteilungen, die ADFS in Betracht ziehen, sollten alle Aspekte der Implementierung für SSO prüfen. Während die Lizenz für ADFS kostenlos ist, gibt es mehrere versteckte, mit ADFS verbundene Kosten, wie z. B. Einrichtung, laufender Support und Hardware. Sie sollten sich auch Gedanken darüber machen, was eine vollständige Identitätsmanagementlösung ausmacht. Berücksichtigen Sie dabei die Bereitstellung, kontextbezogenes Zugriffsmanagement für mobile Geräte, zentralisierte Berichterstellung und vorintegrierte Unterstützung für die Vielzahl von Anwendungen, die Unternehmen heute einsetzen.

In diesem Whitepaper werden die Merkmale einer erfolgreichen Active Directory-Integration und SSO-Bereitstellung besprochen. Wir zeigen darin insbesondere die Vorteile der Migration von lokalen ADFS auf den umfassenden, 100 % Cloud-basierten Okta-Dienst.

Schlüsselelemente einer erfolgreichen SSO-Lösung

Wenn Sie eine Single Sign-On-Implementierung erwägen, sind mehrere Dinge zu beachten. Am besten konzentrieren Sie sich auf einige Schlüsselelemente, um den Erfolg zu sichern. Viele Elemente mögen zunächst unbedeutend erscheinen, können aber später große Probleme verursachen, wenn Unternehmen wachsen und mehr Anwendungen einsetzen.

- **Active Directory-Integration**
  Wenn Ihr Unternehmen Active Directory verwendet, muss Ihre SSO-Lösung Ihnen die Möglichkeit verschaffen, diese Investition zu nutzen und Cloud-Anwendungen, die SSO unterstützen, mit Active Directory zu synchronisieren.

- **Anwendungsintegration und Support**
  Die Zukunftssicherheit, also die Fähigkeit, alle Ihre Anwendungen nicht nur heute, sondern auch in Zukunft zu unterstützen, sollte bei der Betrachtung einer unternehmensweiten Lösung immer berücksichtigt werden. Heute müssen Sie vielleicht nur eine oder zwei Cloud-Anwendungen integrieren. Aber wie sieht die längerfristige Strategie Ihres Unternehmens aus? Da Ihre Anwendungen skalierbar sind, können unterschiedliche Konfigurationsanforderungen vorliegen, die sich im Laufe der Zeit ändern, sodass ein IT-Administrator die Kontrolle über die einzelnen Anwendungen behalten muss. Der mit jeder Anwendung verbundene Arbeitsaufwand und die Einrichtung können sowohl für die Mitarbeiter als auch für die IT-Budgets zu einer Belastung werden.

- **Hohe Verfügbarkeit**
  Jeder mit der SSO-Bereitstellung verbundene Ausfall bedeutet eine Arbeitsunterbrechung für Ihre Benutzer. Diese Arbeitsunterbrechung kann geplant, aber auch unerwartet sein. Ein SSO-Dienst und der dazugehörige Support müssen agil genug sein, um auch bei Änderungen der Anwendungskonfigurationen durch den Provider funktionsfähig zu bleiben. Jede Ausfallzeit – gleichgültig ob sie durch Ihre Server oder durch Änderungen an der Anwendung bewirkt wird – führt zu einer geringeren Produktivität für Endbenutzer und das gesamte Unternehmen.

- **Bereitstellung von Benutzern und Cloud Apps**
  Die Bereitstellung umfasst das Erstellen, Aktualisieren und Entfernen des Zugriffs auf eine Anwendung oder andere Ressourcen. Im Durchschnitt benötigt ein IT-Administrator 30 Minuten, um die Erteilung oder den Entzug von Berechtigungen zu bearbeiten. Dabei sind die Helpdesk-Aufrufe für die Passwort-Rücksetzung und die Konfiguration von Mitarbeitern auf allen Geräten noch nicht eingerechnet. Durch die Automatisierung der Bereitstellung und des User Lifecycle Managements kann das Management der IT und anderen Abteilungen wertvolle Zeit und unnötige Frustration ersparen.

- **Kontextabhängiges Zugriffsmanagement mit mobilen Endgeräten**
  Mobile Endgeräte sind vielleicht die nächste Stufe der Produktivitätsverbesserung Ihrer Teams. Aber Sie zögern aufgrund der Lösung der Sicherheitsfrage. Ihre SSO-Lösung sollte sich in jede beliebige MDM-Lösung (Mobile Device Management) integrieren lassen, die Sie bereits verwenden. Sie sollte mit Richtlinien konfigurierbar sein, um zu verhindern, dass nicht verwaltete Geräte auf Ihre Anwendungen und Daten zugreifen. Und sie sollte auch die mehrstufige Authentifizierung mit mobilen Geräten und anderen Faktoren unterstützen, um die Sicherheit zu erhöhen.

- **Effiziente Domänenkonsolidierung**
  Wenn Fusionen und Übernahmen verschiedene Unternehmen und ihre Ressourcen zusammenbringen, kann die Konsolidierung von Bereichen, Tools und Sicherheitsansätzen eine Herausforderung darstellen. Ein moderner, Cloud-basierter Ansatz für SSO kann diesen Prozess beschleunigen und vereinfachen.

- **Protokollierung und Berichterstattung**
  Einige Regulierungsbehörden erfordern Audit-Trails für Benutzer, einschließlich der transparenten Darstellung, auf welche Anwendungen und Systeme Mitarbeiter Zugriff haben (oder hatten). IT-Abteilungen müssen Details zum Sperren von Anwendungen für ausscheidende Mitarbeiter bereitstellen. Die ideale SSO-Lösung sollte in der Lage sein, Nutzungsinformationen für IT-Administratoren zu sammeln, um die notwendigen Anforderungen an die Berichterstattung von Unternehmen und Branchen schnell zu erfüllen.

Verwendung von Active Directory-Verbunddiensten als SSO-Lösung

Kunden vertrauen auf Active Directory-Verbunddienste (ADFS), um die Identitätsverwaltung von Active Directory auf Cloud-Anwendungen außerhalb der Firewall zu erweitern. ADFS ist eine „kostenlose“ Lösung, erfordert jedoch mehrere Hardwarekomponenten, zusätzliche Microsoft-Software sowie umfangreiche Konfiguration und Wartung. Unternehmen, die ADFS für SSO einsetzen, sind mit komplexen Konfigurationsanforderungen und der Abhängigkeit von anderen Ressourcen konfrontiert, um die Mindestanforderungen für eine SSO-Lösung zu erfüllen.

ADFS-Komponenten

Wenn Sie ADFS für SSO-Anforderungen in Betracht ziehen, ist es wichtig, alle zugrunde liegenden Komponenten zu verstehen. ADFS besteht aus drei Komponenten: dem ADFS-Server, dem Verbunddienstproxy, der zwischen der ADFS-Serverfarm und externen Anwendungen installiert wird, und der ADFS-Konfigurationsdatenbank.[1]

ADFS wurde als Toolkit – eine Funktion von Windows Server – entwickelt und ist keine End-to-End-Lösung für Single Sign-On-Anforderungen. Toolkits können flexibel sein, erfordern aber eine erhebliche zusätzliche Unterstützung bei der Entwicklung einer Komplettlösung. Und diese Arbeit muss Ihr IT-Team leisten.

Jede ADFS-Komponente benötigt eine maßgeschneiderte Entwicklung und Administrationszeit, um die SSO-Verbindungen zu den Ziel-Cloud-Anwendungen zu ermitteln, zu konfigurieren und zu pflegen. Dadurch wird die Skalierung auf eine größere Anzahl von Anwendungen erschwert.

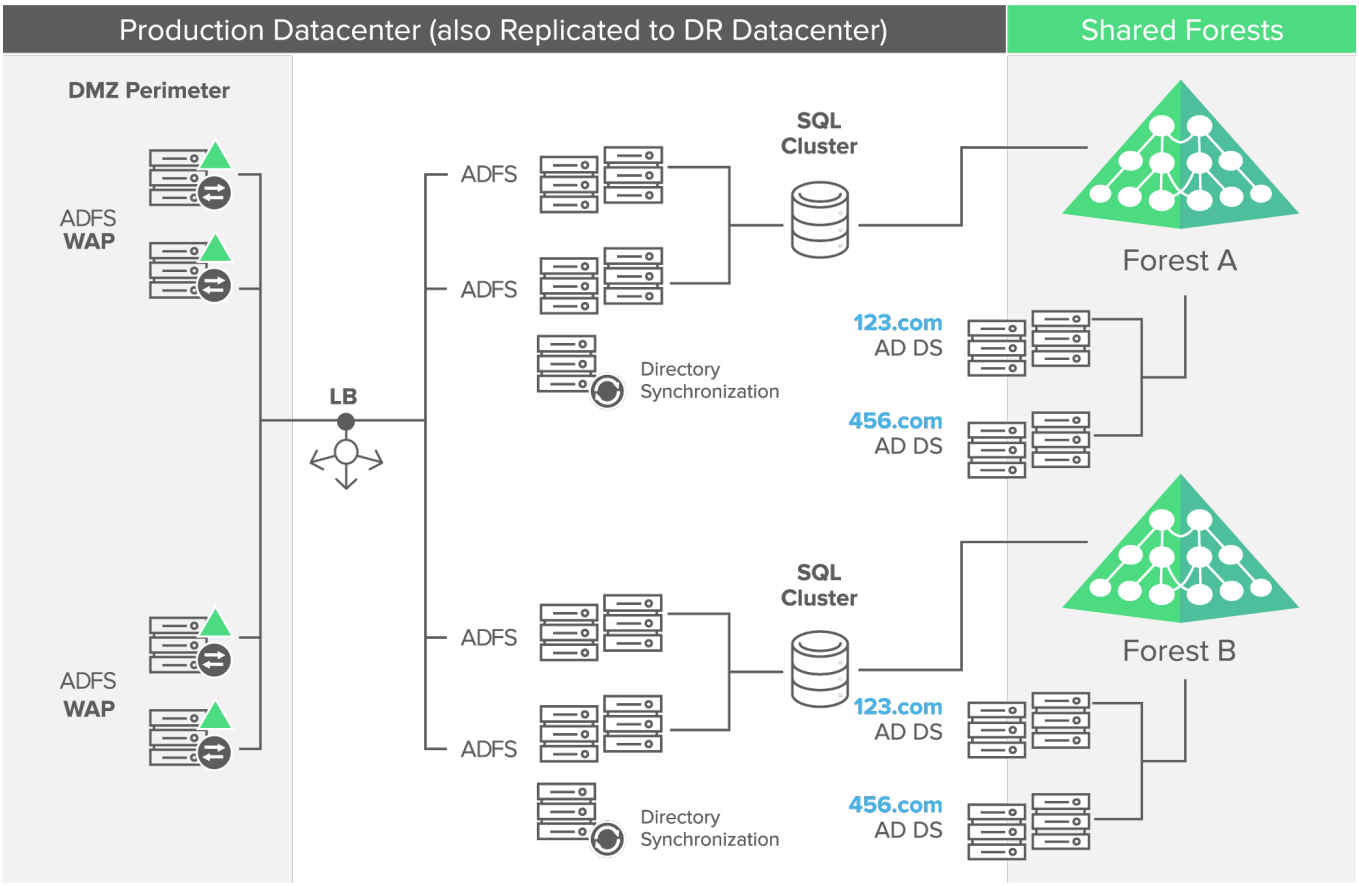

Abbildung 1: ADFS erfordert eine komplexe lokale Infrastruktur zur Integration mit Active Directory

[1] SQL oder interne Windows-Datenbank (WID)

ADFS-Anpassung

Um ADFS für SSO zu konfigurieren, müssen Sie Richtlinien zur Authentifizierung von Benutzern, zur Autorisierung des Zugriffs und zur Generierung von Anforderungsregeln einrichten, um die Authentifizierung mit jeder Cloud-Anwendung zu ermöglichen. Dies erfordert den Aufbau von Vertrauen zwischen ADFS und den Zielanwendungen unter Verwendung eines gültigen SSL-Zertifikats, das sich an den ADFS-Dienst bindet. Für die Prüfung genügt ein selbstsigniertes Zertifikat, für die Produktion ist jedoch ein von einem Drittanbieter signiertes Zertifikat erforderlich. Sobald Vertrauen aufgebaut ist, müssen Anforderungsregeln für die Authentifizierung mit der Ziel-Cloud-Anwendung generiert werden. Das Entwickeln der Anforderungsregeln für jede Anwendung war früher ein manueller Prozess für ADFS-Administratoren, hat sich aber mit den neuen Vorlagen für Zugriffskontrollrichtlinien in ADFS 2016 etwas verbessert.

Die Regeln für jede Anwendung können sich im Laufe der Zeit ändern und Ihre SSO-Integration außer Kraft setzen. Sie müssen diese Anwendungsänderungen im Auge behalten und die Zugriffskontrollrichtlinien entsprechend aktualisieren.

Nachdem Sie die ADFS-Infrastruktur aufgebaut und die entsprechenden Schadensfallregeln für jede Ziel-Cloud-Anwendung entwickelt haben, müssen Sie noch festlegen, wie Benutzer tatsächlich SSO für den Zugriff auf diese Anwendungen verwenden. Am häufigsten erfolgt dies über Azure Active Directory.

Single Sign-On und Provisionierung

Wenn Ihr Unternehmen plant, ADFS von einer Anwendung heute auf fünf oder sechs in den nächsten drei Jahren zu erweitern, muss jede neue Anwendung manuell konfiguriert werden. Seien Sie darauf vorbereitet, regelmäßige Wartungsarbeiten durchzuführen, um sicherzustellen, dass jede Anwendung mit den Unternehmensnetzwerken und der Infrastruktur verbunden bleibt. Dies sieht zwar vielleicht nicht nach hohen Vorlaufkosten aus, aber die Anzahl der für jede neue Anwendung erforderlichen Arbeitsstunden wird bei einer Skalierung nicht abnehmen.

Um Anwendungen für SSO aus Active Directory über ADFS zu integrieren, muss eine Kopie jedes Benutzers in Azure Active Directory eingetragen werden. Dies erfordert Lizenzen für die Cloud-basierte Identitäts- und Zugriffsmanagementlösung von Microsoft für Microsoft Enterprise Mobility + Security (EMS) auf Azure Active Directory.

Die Bereitstellung und das Lifecycle-Management mit ADFS erfordern den Kauf und die Konfiguration eines weiteren Tools – Microsoft Identity Manager (MIM), früher Forefront Identity Manager.

Vorteile der Migration von ADFS auf Okta

Wenn Ihr Unternehmen bereits ADFS eingesetzt hat, aber die Abdeckung erweitern möchte, um mehr Cloud-Anwendungen und einen größeren Funktionsumfang zu unterstützen, bietet das Hinzufügen von Okta mehrere Vorteile:

Einfachheit

Die Gründer von Okta untersuchten den Funktionsumfang von ADFS und bauten die besten Aspekte davon in eine skalierbare Cloud-Plattform ein. Okta verwaltet die vollständige Bereitstellung und Serviceverfügbarkeit und bietet eine Zuverlässigkeit, die die große und komplexe Identitätsföderationsinfrastruktur vor Ort übertrifft.

Okta ist ein integrierter Identitätsmanagement-Dienst, der entwickelt wurde, um Personen von jedem Gerät, überall und zu jeder Zeit sicher mit ihren Anwendungen zu verbinden.

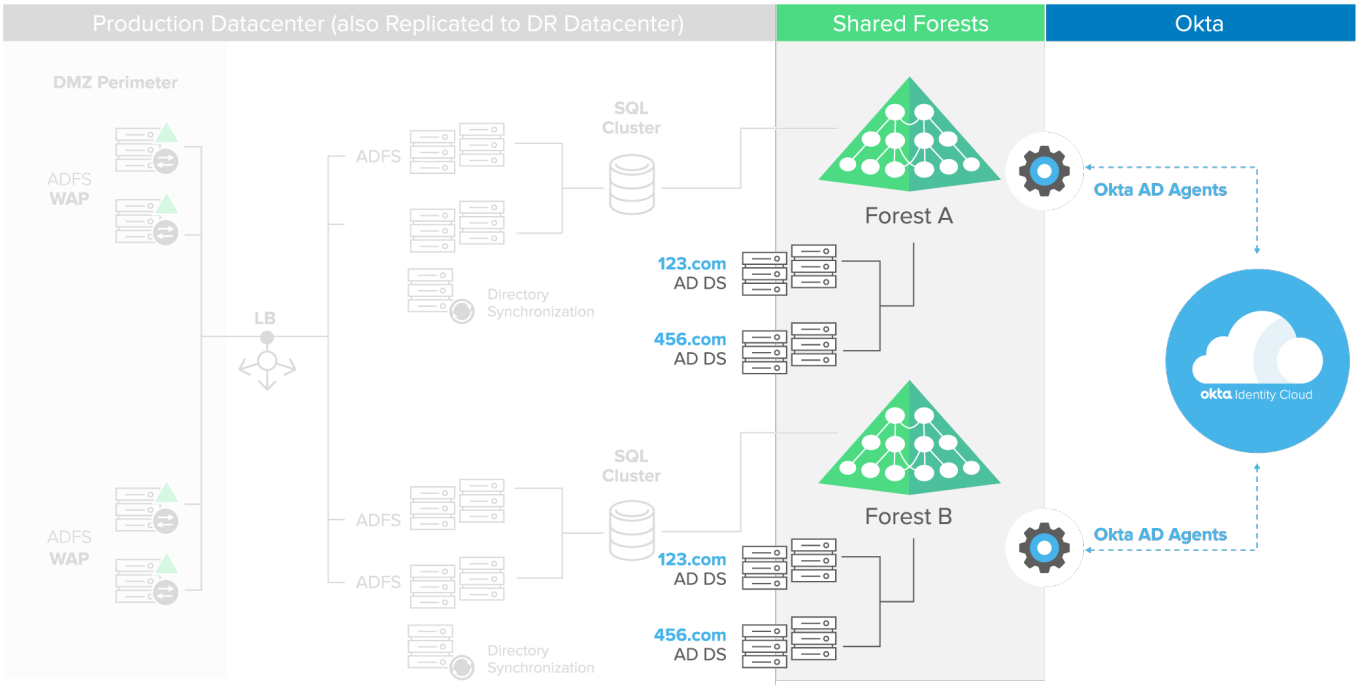

Abbildung 2: Oktas unkomplizierte AD-Agenten und Cloud-Plattform bieten eine sichere Integration in Ihre bestehende Active-Directory-Infrastruktur.

Active Directory-Integration

Die Cloud-Plattform von Okta ist ein 100-prozentiges On-Demand-Angebot, das eine sichere Integration in Ihre bestehende Active Directory-Infrastruktur ermöglicht.

Der Kernservice von Okta ist eine mandantenfähige Lösung mit einem Active Directory-Agenten, die lokal installiert wird, aber keine Geräte oder Server zum Kauf oder zur Wartung benötigt. Oktas Agent stellt eine sichere, reine Outbound-Verbindung über HTTPS her – es sind keine Änderungen an der Firewall-Konfiguration erforderlich. Sobald Okta einen Benutzer mit der Cloud-Anwendung authentifiziert hat, gibt es die Verbindung frei. Der gesamte laufende Datenverkehr findet zwischen dem Benutzer und der Anwendung statt.

Okta unterstützt delegierte Authentifizierung, Bereitstellung und Aufhebung der Bereitstellung (Provisioning und Deprovisioning), Verzeichnisabgleich und AD-Passwortverwaltung. Wann immer eine Änderung in eine der beiden Richtungen zwischen Active Directory oder Okta erfolgt, werden diese Änderungen schrittweise synchronisiert. Ein Administrator kann einen Benutzer im Okta Universal Directory deaktivieren, und der Eintrag des Benutzers im Active Directory wird ebenfalls sofort deaktiviert.

Single Sign-On mit einfacher Anwendungsintegration

Das Okta Integration Network ist ein großer Katalog aus vorintegrierten geschäftlichen und persönlichen Anwendungen, Infrastrukturen und Geräten. Endbenutzer sehen ein zentrales Anwendungsportal, das ihnen einen einfachen Zugriff auf die ihnen bereitgestellten Anwendungen ermöglicht. Wie in Abbildung 3 dargestellt, können Single Sign-On-Funktionen von Active Directory-, Federated SSO- und Deep Application-Integrationen dank der integrierten Cloud-Plattform mit Okta in viel kürzerer Zeit bereitgestellt werden.

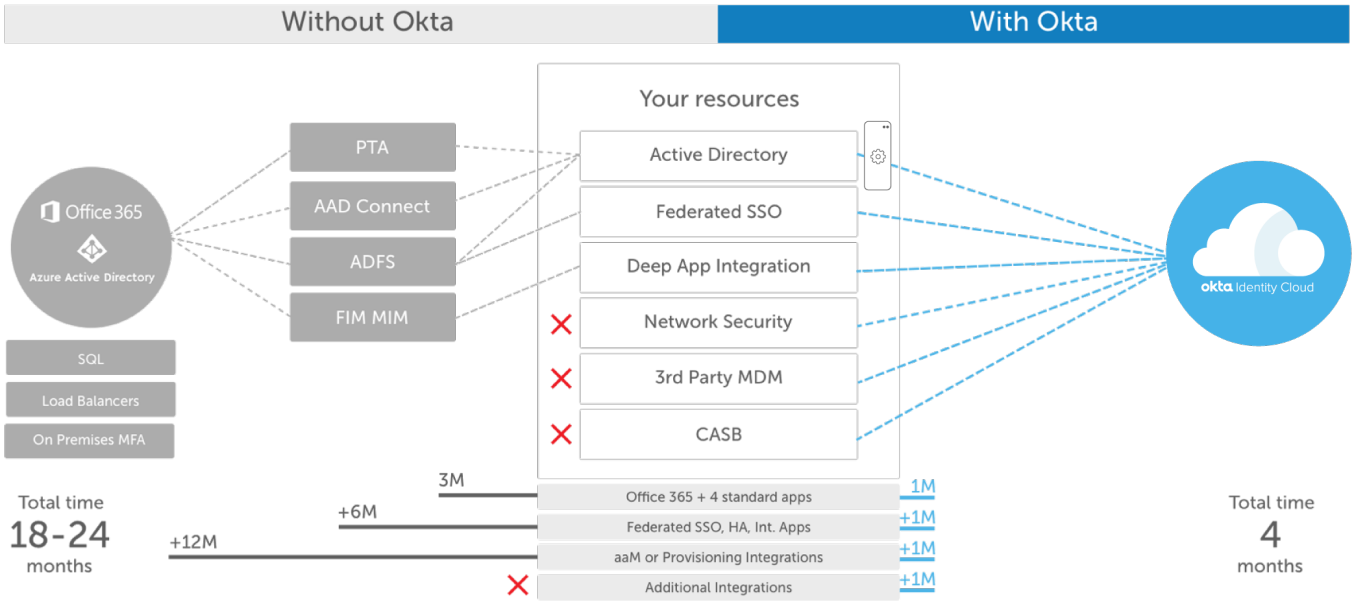

Abbildung 3: Okta vereinfacht und beschleunigt SSO, Bereitstellung und Integration in andere Anwendungen und Dienste

Hohe Verfügbarkeit

Ein Ausfall Ihrer SSO-Lösung kommt nie zur rechten Zeit, ebenso wie geplante Wartungsarbeiten. Oktas Cloud-Plattform ist für eine garantierte Verfügbarkeit von 99,9 % und null geplante Ausfallzeiten ausgelegt.[2] Oktas Cloud-Architektur ist 100 % mandantenfähig, staatenlos und extrem redundant über mehrere Verfügbarkeitszonen und -regionen hinweg. Sie brauchen sich nicht um Änderungen an den zugrunde liegenden Anwendungen zu kümmern, da Okta kontinuierlich Cloud-Anwendungsintegrationen verwaltet und überwacht. Mitarbeiter, Partner und Kunden erhalten ununterbrochenen Zugriff auf geschäftskritische Anwendungen.

Bereitstellung (Provisioning) von Benutzern und Anwendungen

Okta unterstützt ein gruppenbasiertes Managementsystem, das Benutzer für eine Reihe von Anwendungen bereitstellen kann, die auf der in Active Directory definierten Jobrolle basieren. Wenn ein Mitarbeiter innerhalb eines Unternehmens die Rolle wechselt, aktualisiert Okta automatisch die Anwendungen, auf die der Benutzer Zugriff hat, basierend auf Änderungen am Mitarbeiterdatensatz im Active Directory. Wenn Mitarbeiter ausscheiden, erkennt Okta die Änderung ihres Status im Active Directory und entfernt automatisch alle Zugriffe.

Okta bietet vorintegrierte Bereitstellung für über 80 der führenden SaaS-Anwendungen und ermöglicht Identity Mastering und Provisioning von Benutzern unter Verwendung von Identitätsattributen aus HR-Systemen wie Workday, SuccessFactors und mehr.

Kontextbezogenes Zugriffsmanagement mit Geräteerkennung

Das kontextbezogene Zugriffsmanagement von Okta reduziert das Risiko, indem es verwaltet, wie Benutzer und Geräte Zugriff auf Unternehmensressourcen erhalten. Durch eine Kombination aus adaptiver Multi-Faktor-Authentifizierung und Device Trust-Registrierungsrichtlinien stellt Okta sicher, dass nur autorisierte Benutzer und Geräte auf unternehmenseigene Anwendungen und Daten zugreifen können. Mit Okta können Unternehmen eine granulare Zugriffskontrolle für Tausende von Anwendungen und für die am häufigsten verwendeten Geräte durchsetzen. Mithilfe der adaptiven Multi-Faktor-Authentifizierung von Okta entscheidet ein Administrator, ob er den Zugriff erlaubt, eine Step-up-Authentifizierung anfordert, den Zugriff verweigert oder den Umfang des Zugriffs eines Benutzers auf bestimmte Anwendungen einschränkt. Diese Entscheidungen basieren nicht nur auf Passwörtern, Sicherheitsfragen und Token, sondern auch darauf, wer der Benutzer ist, aus welchem Netzwerk oder Land er sich verbindet und welche Geräte er verwendet.

Multi-Faktor-Authentifizierung für ADFS

Für Kunden, die ADFS weiterhin als ihren Identity Provider (IdP) für bestimmte Anwendungen verwenden möchten, können sie weiterhin Okta Multi-Factor Authentication verwenden, um eine starke Authentifizierungsmethode bereitzustellen, ohne zusätzliche lokale MFA-Infrastruktur aufbauen zu müssen.[3]

[2] https://www.okta.com/a-secure-reliable-service-you-can-trust/
[3] https://help.okta.com/en/prod/Content/Topics/integrations/adfs-okta-int.htm

Effiziente Domänenkonsolidierung

Oktas Universal Directory ermöglicht es Unternehmen, eine unbegrenzte Anzahl von Verzeichnissen zu verbinden und Legacy-Daten ins Web zu bringen, ohne dass AD Forest Trusts benötigt werden oder das Öffnen von Firewall-Ports erforderlich ist. Beispielsweise können Sie eine Umgebung mit mehreren AD-Domänen haben – einige vertrauenswürdig, andere nicht vertrauenswürdig. Mit Okta installieren Sie einen AD-Agenten hinter der Firewall (zwei für eingebaute Hochverfügbarkeit) und Okta verwaltet diese Verzeichnisse von einer zentralen Verwaltungskonsole aus.

Protokollierung und Berichterstattung

Das einheitliche Dashboard von Okta erleichtert es der IT-Abteilung, den Status von Benutzern, Zugängen und Anwendungen anzuzeigen und Berichte für die Einhaltung von Vorschriften zu erstellen.

Immer verfügbar, immer auf dem neuesten Stand

Okta wurde im Hinblick auf unsere Kunden entwickelt und stellt regelmäßig neue Updates für das Produkt zur Verfügung, ohne Ausfallzeiten. Endbenutzer können über ein zentrales Anwendungsportal auf die ihnen bereitgestellten Anwendungen zugreifen. Eine ähnliche Lösung über ADFS müsste entweder manuell erstellt oder an ein anderes Unternehmen ausgelagert werden, was die Unternehmenskosten weiter erhöht.

Okta ist eine Software as a Service-Plattform (SaaS), die alle Vorteile von ADFS und den anderen Microsoft-Tools, die für eine komplette SSO-Lösung benötigt werden, auf einer einzigen Cloud-basierten Plattform bietet.

Kostenvorteile

Wie in Abbildung 4 dargestellt, verursacht ADFS mehrere Kosten: Hardware- und Softwareinstallation, Wartung, kundenspezifische Integrationen, Lizenzierung für virtuelle Maschinen, Enterprise Mobility + Security (EMS) und Microsoft Identity Manager (MIM) Software. Es gibt auch die Opportunitätskosten für den Verlust von Monaten der Produktivität aufgrund der Zeit, die benötigt wird, um alles einzurichten.

Installation, Wartung und kundenspezifische Integrationen verursachen weitere Kosten, selbst wenn EMS kostenlos im Paket enthalten ist. Für Unternehmen, die bereits ADFS einsetzen, müssen sie möglicherweise die Installations- und Lizenzkosten für MIM und EMS für erweiterte Funktionen hinzurechnen.

Oktas minimale Anpassungsanforderungen und Lizenzmanagementfunktionen können bei Unternehmen bis zu 60 Prozent der Gesamtbetriebskosten einsparen. Wenn neue Anwendungen eingeführt werden, steigen die Kosten für Okta nicht. Daher erzielen Unternehmen größere Einsparungen, wenn sie weiterhin Cloud-Anwendungen in ihre Infrastruktur integrieren.

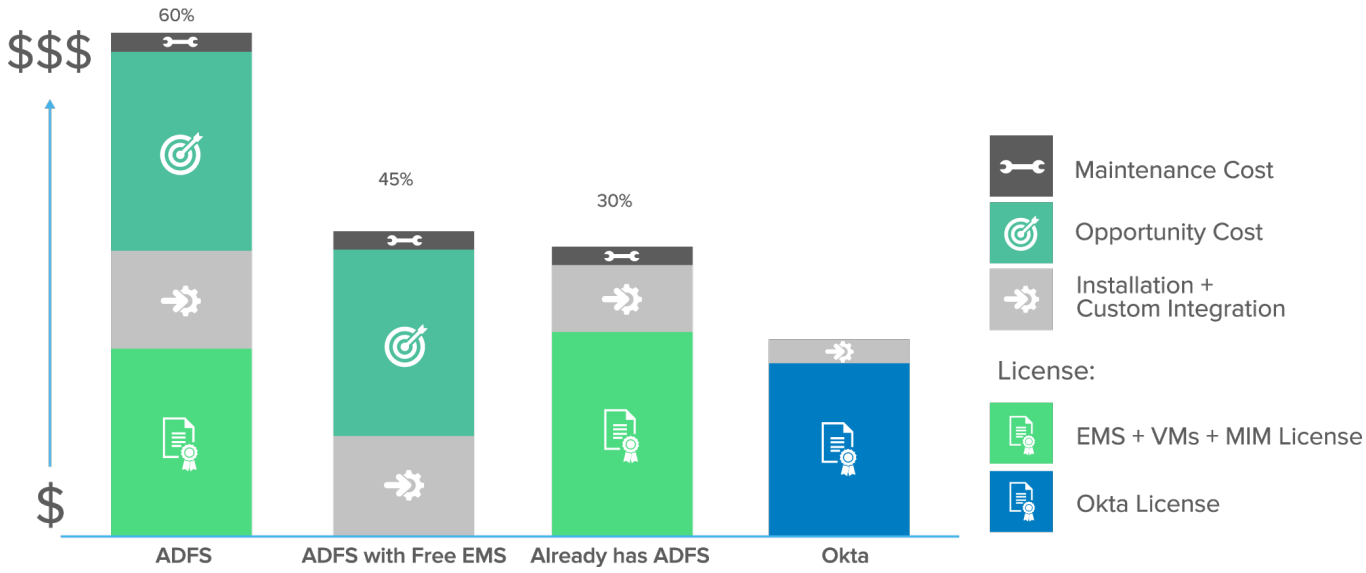

Abbildung 4: Relative ADFS-Kosten für eine Anwendungsintegration

Schnellvergleich von Okta und ADFS

Metrik	Okta-Ansatz	ADFS-Ansatz
Anwendungsintegrationen	Tausende von vorintegrierten Anwendungen Keine Konfiguration und Wartung von Anwendungsintegrationen erforderlich	IT-Administratoren erstellen und pflegen jede Integration
Verfügbarkeit	100 % mandantenfähige Lösung Immer einsatzbereit und ohne Ausfallzeiten Keine Änderungen an der AD-Infrastruktur erforderlich	Muss konfiguriert, installiert und verwaltet werden Wartungsbedarf bei der Weiterentwicklung von Anwendungen Verfügbarkeitsredundanz Erfordert mehrere Server (Installation und Ausfallsicherung)
Zugriffs- und Benutzerverwaltung	Kontrollieren Sie den Zugriff auf alle Ihre Anwendungen Einfache Zuordnung verschiedener Benutzernamenformate Einfaches Hinzufügen, Ändern oder Entfernen von Benutzern und Zugriffsrechten Direkter Import aus AD, Sicherheitsgruppen Automatische Konfiguration für alle integrierten Anwendungen	Muss benutzerdefinierte AD-Attribute erstellen und verwalten Jede Anwendung kann Änderungen erfordern Kein Konzept des Benutzerimports, des Abgleichs und der Anpassung
Berichterstattung	Dashboard mit Metriken, um den allgemeinen Zustand von Benutzern und Anwendungen zu sehen Einfacher Zugriff auf Benutzerberichte für Compliance-Zwecke	K. A.

Erste Schritte mit der kostenlosen Testversion

Um herauszufinden, wie einfach es ist, Okta einzusetzen und mit der sicheren Skalierung Ihrer Cloud-basierten Anwendungen zu beginnen, besuchen Sie www.okta.com/freetrial, um noch heute damit zu beginnen.

Über Okta

Okta ist der führende unabhängige Anbieter von Identitätslösungen für Unternehmen. Die Okta Identity Cloud verbindet und schützt Mitarbeiter vieler der weltweit größten Unternehmen. Zudem verbindet sie Unternehmen auf sichere Weise mit ihren Partnern, Lieferanten und Kunden. Durch nahtlose Einbindung in über 5.000 Anwendungen ermöglicht die Okta Identity Cloud den einfachen und sicheren Zugriff von jedem Gerät aus.

Tausende von Kunden, darunter 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn und News Corp, verlassen sich auf Okta, um schneller zu arbeiten, ihren Umsatz zu steigern und ihre Sicherheit zu wahren. Mit Okta kommen Kunden schneller ans Ziel, denn Okta macht den Zugang zu Technologien, die Kunden für ihre Arbeit unbedingt benötigen, sicher und benutzerfreundlich.

Weitere Informationen dazu finden Sie unter www.okta.com