Microsoft

Verwalten und Absichern des Zugriffs auf Ihre Anwendungen mit Azure Active Directory

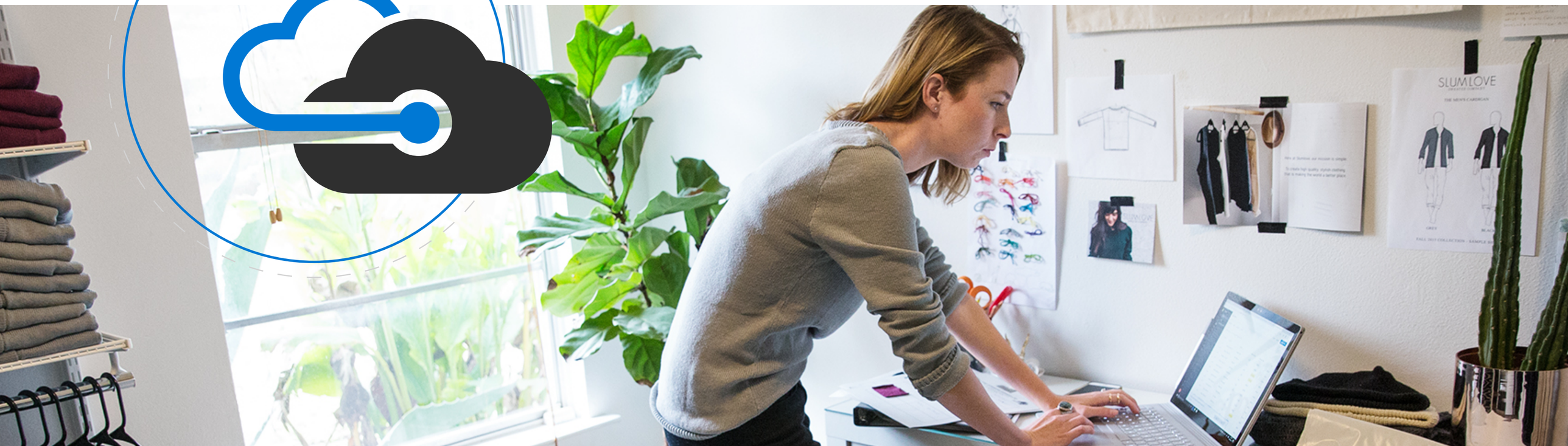
Abschnitt 1

Was ist Identitäts- und Zugriffsverwaltung?

Was ist Identitäts- und Zugriffsverwaltung?

Digitale Transformation

Cloud Computing und mobile Geräte haben den modernen Arbeitsplatz verändert. Eine zunehmend globale Arbeitskultur bietet die Flexibilität, von jedem Ort aus mit kostenlosen und kostengünstigen SaaS-Anwendungen (Software as a Service) zu arbeiten, um die Herausforderungen der Produktivität und Zusammenarbeit zu meistern. Große Unternehmen migrieren Anwendungen und Computing in die Cloud, um ihre Architektur zu modernisieren, und ganze Branchen nutzen die Vorteile neuer Clouddienste, um maßgeschneiderte Apps für ihre spezifischen Anforderungen zu entwickeln. Unternehmen profitieren vom Aufschwung der neuen Technologien mit größerer Produktivität, aber die digitale Transformation bringt auch drei neue Herausforderungen mit sich.



Was ist Identitäts- und Zugriffsverwaltung?

Neue Herausforderungen

Sicherheitsrisiko: Vor der Cloudrevolution diente die IT als Technologie-Gatekeeper. Ihre verwalteten und abgesicherten Anwendungen und Plattformen befanden sich innerhalb des Netzwerkumkreises, und jeder, der sich bei Ihren Unternehmensressourcen anmeldete, wurde zunächst von der Firewall validiert. Diese Zeiten sind vorbei. Ihre Mitarbeiter haben mehr Kontrolle über die von verwendeten Technologien, auf die zu einem großen Teil über das Internet zugegriffen wird. Cyberangreifer haben gelernt, diese Schwachstellen auszunutzen. Selbst wenn ein Benutzer das richtige Kennwort für ein Konto kennt, können Sie nicht immer sicher sein, dass er derjenige ist, für den er sich ausgibt.

Verwaltungsaufwand: Die explosionsartige Vermehrung der Endpunkte bietet den Benutzern mehr Möglichkeiten, sich zu verbinden, schafft aber auch einen administrativen Alptraum. Viele Unternehmen kennen nicht alle Werkzeuge, die ihre Mitarbeiter verwenden, und selbst wenn sie über einen guten Bestand verfügen, bedeutet die schiere Anzahl von Cloud-Apps, dass mehrere Identitätssysteme verwaltet werden müssen, wodurch die Kosten steigen und sich die bestehenden Sicherheitsrisiken verschärfen.

Schlechte Benutzerfreundlichkeit: Auch die Benutzer bekommen die Nachteile zu spüren. Benutzer lieben die Flexibilität, sind aber frustriert wegen der Vielzahl an Zugangsdaten, die sie sich merken müssen.

Herausforderungen durch die digitale Transformation

Sicherheitsrisiko

Verwaltungsaufwand

Schlechte Benutzerfreundlichkeit

Was ist Identitäts- und Zugriffsverwaltung?

Identitäts- und Zugriffsverwaltung als zentrale Steuerungsebene

Der gemeinsame Nenner in dieser Situation sind ineffiziente Systeme zur Überprüfung der Identität. "Identität" hat den Netzwerkumkreis als neue Steuerungsebene ersetzt. Sie benötigen Lösungen, die unterschiedliche Werkzeuge, Architekturen, Geräte und Dienste im gesamten Unternehmen miteinander verbinden, um die Organisation besser zu schützen und den Zugriff sowohl für Mitarbeiter als auch für externe Partner zu verwalten. Identitäts- und Zugriffsverwaltungssysteme (IAM) vereinen den Zugriff unter einem System und geben Ihnen mehr Kontrolle. Sie ermöglichen eine nahtlose Zusammenarbeit über die Grenzen Ihrer Organisation hinweg und verbessern gleichzeitig die Sicherheit Ihrer Unternehmensressourcen. Eine gute IAM-Lösung ermöglicht Ihren Benutzern, sich mit einem einzigen Satz von Anmeldeinformationen mit all ihren Arbeitsanwendungen verbinden, ganz gleich, ob diese in der Cloud oder lokal gehostet werden. IAM-Lösungen sind so konzipiert, dass Benutzer nur auf die Ressourcen zugreifen können, die sie benötigen, und nicht autorisierte Benutzer daran gehindert werden, auf Daten zuzugreifen, für die sie keine Berechtigungen besitzen. Sie verwalten Benutzerzugriffsrechte und -berechtigungen von einem zentralen Portal aus und reduzieren so einen Großteil der manuellen Prozesse, die mit der Bereitstellung und Entziehung von Benutzerkonten verbunden sind. IAM-Lösungen bieten auch Werkzeuge zur Verwaltung von Sicherheitsrichtlinien für Ihre Identitäten und Apps. Die besten IAM-Lösungen bieten mehr Schutz für Identitäten, verbessern die Benutzererfahrung und steigern die administrative Effizienz.

IAM-Lösungen bewältigen diese Herausforderungen

Besserer Schutz für Identitäten

Verbesserte Benutzererfahrung

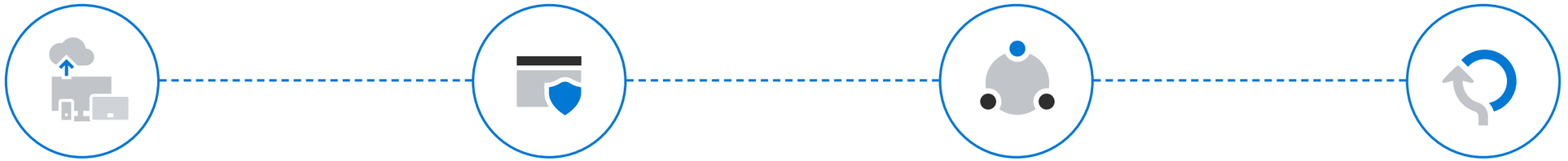
Höhere administrative Effizienz

Abschnitt 2

Übersicht über Azure AD

Eine umfassende Lösung

Microsoft Azure Active Directory (Azure AD) ist eine umfassende IAM-Lösung in der Cloud und marktführend für Verzeichnisverwaltung, Anwendungszugriff und erweiterten Identitätsschutz. Azure AD ermöglicht Organisationen, Identitäten für Mitarbeiter, Partner und Kunden zu verwalten und abzusichern, damit diese auf die benötigten Apps und Dienste zugreifen können. Azure AD hilft Millionen von Organisationen bei der Verwaltung und Absicherung von über einer Milliarde Identitäten.



Modernisierter Zugriff

Verwalten und schützen Sie den Zugriff auf die lokalen und die in der Cloud gehosteten Daten und Ressourcen Ihres Unternehmens. Verbinden Sie alle Ihre Benutzer, Anwendungen und Geräte mit der Cloud, um einen nahtlosen und sicheren Zugriff sowie eine größere Transparenz und Kontrolle zu gewährleisten. Durch die Automatisierung von Workflows und die Aktivierung von Self-Service-Optionen können Sie die Kosten niedrig halten und die Produktivität Ihrer Benutzer verbessern.

Sicherheit und Kontrolle

Angesichts der jeden Tag stattfindenden hohen Anzahl von Angriffen auf Anmeldeinformationen von Benutzern besteht die Möglichkeit zur Verhinderung von Manipulationen darin, normales und anormales Verhalten über eine möglichst breite Palette von Signalen kontinuierlich zu verfolgen, künstliche Intelligenz anzuwenden und die Reaktionen zu automatisieren. Ein ausgewogenes Verhältnis zwischen Produktivität und Sicherheit wird durch die rechtzeitige Bereitstellung der richtigen Ressourcen sowie durch regelmäßige Zugriffsüberprüfungen und die Durchsetzung von Richtlinien erreicht.

Verbindung und Zusammenarbeit

Erweitern Sie Ihr Unternehmen mit einem zuverlässigen Clouddienst, der sich mit branchenführender Sicherheit und Flexibilität auf Millionen von Benutzer skalieren lässt. Stellen Sie eine Verbindung zu Ihren externen Benutzern her, und ermöglichen Sie deren Produktivität durch benutzerfreundliche Self-Service-Umgebungen und integrierte Sicherheitskontrollen.

Entwicklung und Integration

Erstellen Sie Anwendungen, bei denen sich Benutzer auf einfache Weise mit ihrem persönlichen Microsoft-Konto, Geschäfts-, Schul oder Unikonto bzw. Social Media-Konto anmelden können. Stellen Sie eine Verbindung zu Microsoft Graph her, dem Tor zu Daten und Intelligenz in Microsoft 365, und erstellen Sie vielseitige Anwendungen. Aktivieren Sie einmaliges Anmelden (Single Sign-On, SSO), automatisieren Sie die Benutzerbereitstellung und erreichen Sie die größten Organisationen der Welt.

Abschnitt 3

Azure AD für Ihre Anwendungen

Azure AD für Ihre Anwendungen

Eine universelle Plattform

Mit Azure AD können Sie eine gemeinsame Identität für jeden Benutzer in Ihrer hybriden Infrastruktur verwalten, um auf alle benötigten Anwendungen zuzugreifen, einschließlich Cloudanwendungen und lokale Branchenanwendungen. Verwalten Sie alle Ihre Identitäten über eine universelle Plattform, wodurch sich die administrative Effizienz erhöht und Sie mehr Kontrolle erhalten. Wenden Sie differenzierte Sicherheitsrichtlinien auf alle in Ihrer Organisation verwendeten Anwendungen an.

Azure AD für Ihre Anwendungen

Zeit und Geld sparen

Azure AD ist in Tausenden von Anwendungen vorintegriert, darunter beliebte Anwendungen wie Workday, ServiceNow, SuccessFactors, Adobe und Concur, wodurch Sie Ihren Benutzern diese Apps noch einfacher zur Verfügung stellen können. Stellen Sie in einer Konsole konsistente Richtlinien bereit, und überwachen Sie die Zugriffsrechte. Sie können die Workflows für Benutzerbereitstellung und Lebenszyklusverwaltung automatisieren und mit der Self-Service-Kontenverwaltung Zeit und Ressourcen einsparen. Sie können auch eingehende Benutzerinformationen aus HR-Werkzeuge als zuverlässige Wissensquelle verwenden, wodurch die Notwendigkeit von benutzerdefinierten Skripts oder manuellen Prozessen zur Verwaltung von Benutzerattributen entfällt.

Über Azure AD konfigurierte Apps ermöglichen Einmaliges Anmelden (Single Sign-on, SSO) für einen nahtlosen Zugriff, d. h. Benutzer brauchen sich nicht für jedes App-Konto eigene Anmeldedaten zu merken oder schwache Kennwörter wiederzuverwenden und so eine Datenverletzung zu riskieren. Konten, die für die automatische Bereitstellung konfiguriert wurden, geben Benutzern so schnell wie möglich Zugriff auf neue Ressourcen. Azure AD stellt sicher, dass Neueinstellungen ab dem ersten Tag Zugriff auf alle relevanten Ressourcen haben.

Einsparungen von Zeit und Geld

SaaS-Integration

Single Sign-On

Benutzerzugriff vom ersten Tag

Azure AD für Ihre Anwendungen

Bereitstellen von sichererem Zugriff auf alle Apps

Azure AD bietet Ihnen umfassenden Identitätsschutz für alle Ihre Apps – sowohl für SaaS-Apps als für auch Ihre lokalen Branchen-Apps. Unabhängig davon, ob der Benutzer Zugriff auf Microsoft Word oder Box anfordert, stellt Azure AD sicher, dass seine Identität bestätigt wird, bevor der Zugriff gewährt wird. Sie können auch Richtlinien für die Zugriffskontrolle einrichten, um sicherzustellen, dass Benutzer nur Zugriff auf erforderliche Daten erhalten, und zwar nur genau dann, wenn sie diese benötigen. Sie können von Benutzern verlangen, eine Berechtigung für den Zugriff zu beantragen, Sie können eine zeitliche Begrenzung für ihren Zugriff auf die Anwendung festlegen, und Sie können regelmäßige Konformitätsüberprüfungen für den Zugriff durchführen.

Azure AD nutzt zudem die Leistungsfähigkeit von Microsoft Intelligent Security Graph und Machine Learning, um Billionen von Signalen über alle unsere Produkte und Dienste hinweg zu analysieren, um atypisches Verhalten aufzudecken und jeder Sitzung ein relatives Risiko zuzuweisen. Azure AD betrachtet Gerät, Standort und andere Kontextinformationen, um das Risiko der Anmeldung zu bewerten. Sie können Azure AD-Richtlinien für den bedingten Zugriff festlegen, wodurch automatisch Sicherheitsmaßnahmen angewendet werden, wie z. B. das Blockieren einer Zugriffsanforderung oder das Anfordern einer Kennwortzurücksetzung, wenn eine Anmeldung als riskant eingestuft wird oder bestimmte Richtlinienbedingungen erfüllt sind.

Anwendungssicherheitsmaßnahmen

Identitätsschutz

Zugriffskontrolle

Richtlinien für den bedingten Zugriff

Abschnitt 4

Verwalten und Absichern von Apps mit Azure AD

Azure AD macht es durch Automatisierung, Self-Service und Durchsetzung von Richtlinien einfach, die Kontrolle zu behalten und die Kosten zu reduzieren.

Verwalten und Absichern von Apps mit Azure AD

Azure AD-App-Integrationen

Der Azure AD-Anwendungskatalog erleichtert das Konfigurieren und Verbinden von Tausenden vorintegrierter Apps mit Ihrem Mandanten. Diese Apps unterstützen alle eine SSO-Erfahrung, und es ist einfach, die Apps mit anwendungsbasierten oder unternehmensweiten Richtlinien für den bedingten Zugriff in Azure AD zu konfigurieren. Sobald Sie die App hinzugefügt und Ihren Anforderungen entsprechend konfiguriert haben, können Benutzer mit autorisiertem Zugriff diese leicht unter "Meine Apps" im Azure AD-Portal finden, einem zentralen Portal zum Erkunden und Starten von Endbenutzer-Apps.

Wenn Sie eine App erstellt haben oder eine App in Ihre Organisation integrieren müssen, können Sie auch ihre Aufnahme in den Azure AD-Anwendungskatalog anfordern.

Entdecken Sie Tausende von vorintegrierten Apps >

Sicherer Hybridzugriff

Verwenden Sie den Azure AD-Anwendungsproxy, um einen sicheren Fernzugriff auf anspruchsbasierte lokale Webanwendungen ohne die Notwendigkeit eines VPN zu ermöglichen. Der Anwendungsproxy erfordert eine schlanke Connectorinstallation und bietet die gleiche IT- und Endbenutzererfahrung wie SaaS-Anwendungen, die über den Azure AD-Anwendungskatalog verbunden sind.

Wenn Sie bestehende Investitionen in die Infrastruktur, z. B. bei Partnern wie F5 ZScaler, SAP, Oracle oder Ping Identity, weiterhin nutzen möchten, um andere Arten von Apps einzubinden, beispielweise Apps, die headerbasierte oder Kerberos-Authentifizierungsprotokolle verwenden, können Sie dies ebenfalls tun und trotzdem von den Zentralisierungs- und Sicherheitsvorteilen von Azure AD profitieren.

Lesen Sie, wie Sie eine lokale Anwendung über einen Anwendungsproxy hinzufügen können >

Stellen Sie eine Verbindung mit anderen Partner-App-Netzwerken und -Clouds her >

Verwalten und Absichern von Apps mit Azure AD

Automatisierte Bereitstellung

Mit Azure AD können Sie die Erstellung, Verwaltung und Entfernung von Benutzeridentitäten in beliebten SaaS-Anwendungen automatisieren. Sie können für Personen, die Ihrem Team oder Ihrer Organisation beitreten, automatisch neue Konten in den richtigen Systemen erstellen. Sie können Richtlinien festlegen, mit denen die Konten von Mitarbeitern, die ein Team oder eine Organisation verlassen, automatisch in den richtigen Systemen deaktiviert werden. Durch die Automatisierung dieser Aufgaben können Sie sicherstellen, dass die Identitäten in Ihren Apps und Systemen bei Änderungen im Verzeichnis oder in Ihrem Personalsystem auf dem neuesten Stand gehalten werden, wodurch Fehler und Aufwand reduziert werden.

Erfahren Sie mehr über das Einrichten automatisierter Bereitstellung und das automatische Entfernen von Bereitstellungen für SaaS-Anwendungen >

Gruppenverwaltung

Azure AD hilft Ihnen dabei, Zugriff auf die Ressourcen Ihrer Organisation über Zugriffsrechte zu gewähren, die Sie einzelnen Benutzern oder einer ganzen Azure AD-Gruppe erteilen. Durch die Verwendung von Gruppen kann der Ressourcenbesitzer Zugriffsberechtigungen für alle Mitglieder der Gruppe festlegen, anstatt die Rechte einzeln vergeben zu müssen. Dies ist eine sicherere Methode, da es weniger wahrscheinlich ist, dass Sie einer Person versehentlich unangemessenen Zugriff gewähren, und die Methode kann Ihnen Zeit sparen. Sie können Ihre Gruppenverwaltung auch dynamisch skalieren, indem Sie die Registrierung durch auf Identitätsattributen basierende Richtlinien automatisieren lassen.

Erfahren Sie, wie Sie eine Gruppe im Azure-Portal erstellen >

Verwalten und Absichern von Apps mit Azure AD

Benutzer-Self-Service

Für einige Aufgaben ist kein IT-Fachmann erforderlich, und mit Azure AD können Sie diese Aufgaben an andere Personen in der Organisation delegieren. Sie können Benutzern ermöglichen, ihre eigenen Sicherheitsgruppen in Azure AD zu erstellen und zu verwalten. Gruppenbesitzer können Mitgliedschaftsanfragen genehmigen oder ablehnen oder die Kontrolle über die Gruppenmitgliedschaft delegieren.

Einrichten selbstverwalteter Gruppen >

Self-Service erstreckt sich auch auf Benutzer. Benutzer können sich über das Self-Service-Portal für ein Konto registrieren, wenn sie über eine verifizierte E-Mail verfügen, und das Portal nutzen, um eigene Kennwörter zurückzusetzen. Dies kann Ihrem Helpdesk erheblich Zeit und Kosten ersparen.

Konfigurieren der Self-Service-Kennwortzurücksetzung >

Modernisieren der Authentifizierung

Wenn Sie derzeit lokale Authentifizierung wie Active Directory-Verbunddienste (AD FS) verwenden, können Sie die Migration Ihrer Apps zu Azure AD in Betracht ziehen. Die Benutzervorteile von SSO bleiben erhalten, Sie können jedoch von Skalierbarkeit und Sicherheitsvorteilen aus der Cloud profitieren, wie z. B. der Anwendung differenzierter Zugriffskontrollen pro Anwendung mit bedingtem Zugriff in Azure AD oder der Gewährung des Zugriffs auf Ressourcen für Partner mit B2B-Zusammenarbeit in Azure AD. Alle Apps, die die Standards SAML 2.0, WS-Federation, OAuth oder OpenID Connect für die Verbundanmeldung verwenden, können migriert werden.

Erstellen Sie Richtlinien für den bedingten Zugriff in Azure AD zur Absicherung des Zugriffs auf Ihre Apps >

Verwenden Sie Azure AD B2B für die nahtlose Zusammenarbeit mit Ihren externen Partnern >

Sichere Verbindung beliebiger Apps in jeder beliebigen Cloud oder auf jedem beliebigen Server mit Azure AD.

1 Million aktive, einzigartige Apps verfügbar.

Microsoft

Steigen Sie heute um.

Starten Sie ein kostenloses einmonatiges Testabonnement von Azure AD, und finden Sie heraus, wie einfach es ist, den Benutzerzugriff auf alle Ihre Apps zu verwalten und Ihr Unternehmen abzusichern.