

# Einführung

1 Minute

100 XP

In diesem Modul werden Sie in die Dienste und Tools zur Azure-Identität, dem -Zugriff und der -Sicherheit eingeführt. Sie erfahren mehr über Verzeichnisdienste in Azure, Authentifizierungsmethoden und die Zugriffssteuerung. Sie werden auch Zero Trust und Defense-in-Depth kennenlernen und erfahren, wie diese Features Ihre Cloud sicherer machen. Den Abschluss bildet eine Einführung in Microsoft Defender für Cloud.

## Lernziele

Nach Abschluss dieses Moduls können Sie folgende Aufgaben durchführen:

- Beschreiben der Verzeichnisdienste in Azure, einschließlich Microsoft Entra ID und Microsoft Entra Domain Services
- Beschreiben der Authentifizierungsmethoden in Azure, einschließlich des einmaligen Anmeldens (Single Sign-On, SSO), der Multi-Faktor-Authentifizierung (MFA) und der kennwortlosen Authentifizierung
- Beschreiben von externen Identitäten und Gastzugriff in Azure
- Beschreiben Sie den bedingten Zugriffs mit Microsoft Entra.
- Beschreiben der rollenbasierten Zugriffssteuerung in Azure (Role Based Access Control, RBAC)
- Beschreiben des Zero Trust-Konzepts.
- Beschreiben des Zwecks des Defense-in-Depth-Modells
- Beschreiben des Zwecks von Microsoft Defender für Cloud

# Beschreiben von Azure-Verzeichnisdiensten

100 XP

6 Minuten

Microsoft Entra ID ist ein Verzeichnisdienst, mit dem Sie sich anmelden und sowohl auf Microsoft-Cloudanwendungen als auch auf selbst entwickelte Cloudanwendungen zugreifen können. Mit Microsoft Entra ID können Sie auch Ihre lokale Active Directory-Bereitstellung verwalten.

Für lokale Umgebungen bietet Active Directory unter Windows Server einen Dienst für die Identitäts- und Zugriffsverwaltung, der von Ihrer Organisation verwaltet wird. Microsoft Entra ID ist der cloudbasierte Identitäts- und Zugriffsverwaltungsdienst von Microsoft. Mit Microsoft Entra ID steuern Sie die Identitätskonten, aber Microsoft stellt sicher, dass der Dienst global verfügbar ist. Wenn Sie bereits mit Active Directory gearbeitet haben, wird Microsoft Entra ID Ihnen vertraut vorkommen.

Wenn Sie Identitäten lokal mit Active Directory schützen, überwacht Microsoft keine Anmeldeversuche. Wenn Sie Active Directory mit Microsoft Entra ID verknüpfen, kann Microsoft Ihnen helfen, sich zu schützen, indem verdächtige Anmeldeversuche ohne zusätzliche Kosten erkannt werden. Beispielsweise kann Microsoft Entra ID Anmeldeversuche von unerwarteten Standorten oder unbekannten Geräten erkennen.

## Wer verwendet Microsoft Entra ID?

Microsoft Entra ID eignet sich für:

- **IT-Administrator\*innen:** Administrator\*innen können Microsoft Entra ID verwenden, um den Zugriff auf Anwendungen und Ressourcen basierend auf ihren Geschäftsanforderungen zu steuern.
- **App-Entwickler\*innen:** Entwickler\*innen können mit Microsoft Entra ID einen standardbasierten Ansatz für das Hinzufügen von Funktionen zu den von ihnen entwickelten Anwendungen umsetzen. So lässt sich beispielsweise eine App mit SSO-Funktionen ergänzen oder so konfigurieren, dass sie die vorhandenen Anmeldeinformationen eines Benutzers oder einer Benutzerin akzeptiert.
- **Benutzer** Benutzer\*innen können ihre Identitäten verwalten und Wartungsaktionen wie die Self-Service-Kennwortzurücksetzung ausführen.
- **Abonent\*innen von Onlinediensten:** Abonent\*innen von Microsoft 365, Microsoft Office 365, Azure und Microsoft Dynamics CRM Online verwenden bereits Microsoft Entra ID für die Kontoauthentifizierung.

## Was kann Microsoft Entra ID?

Microsoft Entra ID enthält Features wie:

- **Authentifizierung:** Dazu gehört die Überprüfung der Identität für den Zugriff auf Anwendungen und Ressourcen. Dazu gehören auch Funktionen wie Self-Service-Kennwortzurücksetzung, mehrstufige Authentifizierung, eine benutzerdefinierte Liste verbotener Kennwörter und intelligente Sperrdienste.
- **Einmaliges Anmelden:** Beim einmaligen Anmelden (Single Sign-On, SSO) müssen Sie sich nur einen Benutzernamen und ein Kennwort merken, um auf mehrere Anwendungen zuzugreifen. Eine Identität ist jeweils an einen Benutzer gebunden, wodurch das Sicherheitsmodell vereinfacht wird. Wenn Benutzer die Rolle wechseln oder ein Unternehmen

verlassen, sind Zugriffsänderungen an diese Identität gebunden. So wird der Aufwand für das Ändern oder Deaktivieren von Konten erheblich reduziert.

- **Anwendungsverwaltung:** Sie können Ihre Cloud- und lokalen Apps mithilfe von Microsoft Entra ID verwalten. Mit Features wie Anwendungsproxy, SaaS-Apps, dem Portal „Meine Apps“ und dem einmaligen Anmelden wird die Benutzerfreundlichkeit verbessert.
- **Geräteverwaltung:** Microsoft Entra ID unterstützt die Registrierung von Konten für Einzelpersonen als auch von Geräten. Die Registrierung ermöglicht die Verwaltung von Geräten mithilfe von Tools wie Microsoft Intune. Dies ermöglicht es gerätebasierten bedingten Zugriffsrichtlinien auch, Zugriffsversuche unabhängig vom anfordernden Benutzerkonto nur auf solche Versuche zu beschränken, die von bekannten Geräten stammen.

## Kann ich mein lokales AD mit Microsoft Entra ID verknüpfen?

Wenn Sie über eine lokale Umgebung mit Active Directory und eine Cloudbereitstellung mit Microsoft Entra ID verfügen, müssen Sie zwei Identitätssätze verwalten. Sie können jedoch eine Verbindung zwischen Active Directory und Microsoft Entra ID herstellen, um eine einheitliche Identitätsfunktion zwischen Cloud- und lokaler Umgebung zu ermöglichen.

Eine Methode zum Verbinden von Microsoft Entra ID mit Ihrem lokalen AD ist die Verwendung von Microsoft Entra Connect. Microsoft Entra Connect synchronisiert Benutzeridentitäten zwischen lokalem Active Directory und Microsoft Entra ID. Microsoft Entra Connect synchronisiert Änderungen zwischen beiden Identitätssystemen, sodass Sie Features wie SSO, Multi-Faktor-Authentifizierung und Self-Service-Kennwortzurücksetzung unter beiden Systemen verwenden können.

## Was ist Microsoft Entra Domain Services?

Microsoft Entra Domain Services ist ein Dienst, der verwaltete Domänendienste wie Domänenbeitritt, Gruppenrichtlinien, Lightweight Directory Access Protocol (LDAP) und Kerberos-/NTLM-Authentifizierung bereitstellt. Mit Microsoft Entra ID können Sie Verzeichnisdienste ohne Verwaltung der entsprechenden Infrastruktur nutzen. Microsoft Entra Domain Services bietet den Vorteil, Domänendienste verwenden zu können, ohne Domänencontroller (DCs) in der Cloud bereitstellen, verwalten und patchen zu müssen.

Mit einer verwalteten Microsoft Entra Domain Services-Domäne können Sie Legacyanwendungen in der Cloud ausführen, für die keine modernen Authentifizierungsmethoden genutzt werden können oder bei denen Sie nicht möchten, dass Verzeichnislookups immer in einer lokalen AD DS-Umgebung durchgeführt werden. Sie können diese Legacyanwendungen per Lift & Shift-Vorgang aus Ihrer lokalen Umgebung in eine verwaltete Domäne verschieben, ohne dass Sie die AD DS-Umgebung in der Cloud verwalten müssen.

Microsoft Entra Domain Services kann mit Ihrem vorhandenen Microsoft Entra-Mandanten integriert werden. Diese Integration ermöglicht es Benutzer\*innen, sich bei Diensten und Anwendungen, die mit der verwalteten Domäne verbunden sind, mithilfe ihrer vorhandenen Anmeldeinformationen anzumelden. Sie können auch vorhandene Gruppen und Benutzerkonten verwenden, um den Zugriff auf Ressourcen abzusichern. So können Sie für eine reibungslosere Lift & Shift-Migration lokaler Ressourcen zu Azure sorgen.

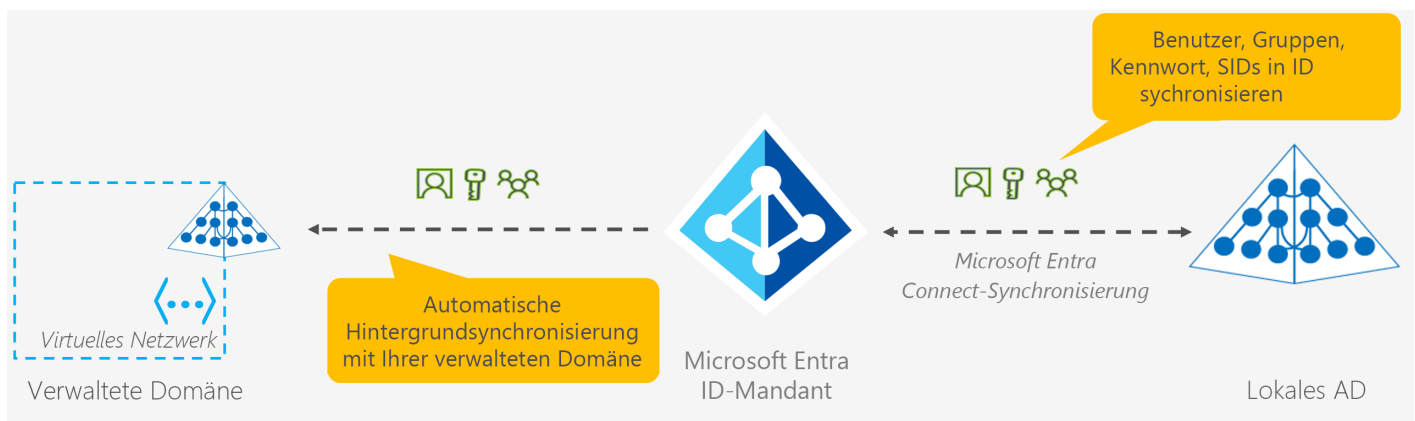
## Wie funktioniert Microsoft Entra Domain Services?

Nachdem Sie eine verwaltete Microsoft Entra Domain Services-Domäne erstellt haben, können Sie einen eindeutigen Namespace festlegen. Dieser Namespace ist der Domänenname. Anschließend werden zwei Windows Server-Domänencontroller in Ihrer ausgewählten Azure-Region bereitgestellt. Diese Bereitstellung von Domänencontrollern wird als Replikatgruppe bezeichnet.

Sie müssen diese Domänencontroller nicht verwalten, konfigurieren oder aktualisieren. Die Azure-Plattform führt die Schritte für die Domänencontroller im Rahmen der verwalteten Domäne aus – einschließlich Sicherung und Verschlüsselung ruhender Daten mit Azure Disk Encryption.

## Werden die Informationen synchronisiert?

Eine verwaltete Domäne ist so konfiguriert, dass eine unidirektionale Synchronisierung von Microsoft Entra ID zu Microsoft Entra Domain Services erfolgt. Sie können Ressourcen direkt in der verwalteten Domäne erstellen, die aber nicht wieder mit Microsoft Entra ID synchronisiert werden. In einer Hybridumgebung mit einer lokalen AD DS-Umgebung synchronisiert Microsoft Entra Connect Identitätsinformationen mit Microsoft Entra ID, die dann wiederum mit der verwalteten Domäne synchronisiert werden.



Anwendungen, Dienste und VMs in Azure, die mit der verwalteten Domäne verknüpft sind, können gängige Microsoft Entra Domain Services-Features wie Domänenbeitritt, Gruppenrichtlinien, LDAP und Kerberos-/NTLM-Authentifizierung nutzen.

# Grundlegendes zu Authentifizierungsmethoden in Azure 100 XP

6 Minuten

Die Authentifizierung ist der Vorgang, bei dem die Identität einer Person, eines Diensts oder eines Geräts festgelegt wird. Personen, Dienste oder Geräte müssen Anmeldeinformationen angeben, um ihre Identität zu bestätigen. Sie können sich die Authentifizierung wie Ihren Reisepass vorstellen. Dieser bestätigt nicht, dass Sie ein Ticket für einen Flug besitzen, er bestätigt nur Ihre Identität. Azure unterstützt mehrere Authentifizierungsmethoden, einschließlich Standardkennwörtern, einmaliges Anmelden (Single Sign-On, SSO), die Multi-Faktor-Authentifizierung (MFA) und kennwortlos.

Für eine lange Zeit schien es so, als können Sicherheit und Komfort nicht nebeneinander existieren. Glücklicherweise bieten neue Authentifizierungslösungen sowohl Sicherheit als auch Komfort.

Das folgende Diagramm zeigt die Sicherheitsebene im Vergleich zum Komfort. Beachten Sie, dass die kennwortlose Authentifizierung hohe Sicherheit und hohen Komfort bietet. Kennwörter alleine zwar hohen Komfort, jedoch weniger Sicherheit.



## Was ist einmaliges Anmelden (Single Sign-On, SSO)?

Einmaliges Anmelden (SSO) ermöglicht es einem Benutzer oder einer Benutzerin, sich einmalig anzumelden und diese Anmeldeinformationen für den Zugriff auf mehrere Ressourcen und Anwendungen von unterschiedlichen Anbietern zu verwenden. Damit SSO funktioniert, müssen die verschiedenen Anwendungen und Anbieter dem ursprünglichen Authentifikator vertrauen.

Mehrere Identitäten implizieren mehrere Kennwörter, die verwaltet und geändert werden müssen. Kennwortrichtlinien können zwischen Anwendungen variieren. Wenn die erforderliche Kennwortkomplexität zunimmt, wird es für Benutzer immer schwieriger, sich diese Kennwörter zu merken. Je mehr Kennwörter ein Benutzer verwalten muss, desto größer ist das Risiko eines Sicherheitsincidents in Zusammenhang mit Anmeldeinformationen.

Denken Sie an den Aufwand für die Verwaltung all dieser Identitäten. Helpdesks werden durch das Bearbeiten von Kontosperrungen und Kennwortzurücksetzungen zusätzlich belastet. Wenn ein\*e Benutzer\*in ein Unternehmen verlässt, kann es zudem schwierig sein, alle seine Identitäten zu finden und zu deaktivieren. Wenn eine Identität übersehen wird, könnte dies den Zugriff ermöglichen, obwohl er eigentlich hätte unterbunden werden müssen.

Bei Verwendung von SSO müssen Sie sich nur eine Identität und ein Kennwort merken. Der anwendungsübergreifende Zugriff wird einer einzigen Identität gewährt, die an den Benutzer gebunden ist, wodurch das Sicherheitsmodell vereinfacht wird. Wenn sich Benutzerrollen ändern oder Benutzer eine Organisation verlassen, ist der Zugriff an eine einzige Identität gebunden. Durch diese Änderung wird der erforderliche Aufwand zum Ändern oder Deaktivieren von Konten erheblich reduziert. Durch die Verwendung von SSO für Konten ist es für Benutzer\*innen einfacher, ihre Identitäten zu verwalten, und für die IT, um Benutzer\*innen zu verwalten.

### **Wichtig**

Das einmalige Anmelden ist nur so sicher wie der anfängliche Authentifikator, da die nachfolgenden Verbindungen alle auf der Sicherheit des anfänglichen Authentifikators basieren.

## **Was ist Multi-Faktor-Authentifizierung?**

Bei der Multi-Faktor-Authentifizierung wird ein\*e Benutzer\*in nach einem zusätzlichen Formular (oder einen Faktor) zur Identifizierung während des Anmeldevorgangs gefragt. Die Multi-Faktor-Authentifizierung hilft beim Schutz vor einer Kennwortkompromittierung in Situationen, in denen zwar das Kennwort kompromittiert wurde, aber der zweite Faktor nicht.

Überlegen Sie, wie Sie sich bei Websites, E-Mail-Clients oder Onlinediensten anmelden. Mussten Sie nach Eingabe Ihres Benutzernamens und Kennworts jemals einen Code eingeben, der an Ihr Smartphone gesendet wurde? Wenn dies der Fall ist, haben Sie mehrstufige Authentifizierung für die Anmeldung verwendet.

Mehrstufige Authentifizierung bietet zusätzliche Sicherheit für Identitäten, indem mindestens zwei Methoden für eine vollständige Authentifizierung benötigt werden. Diese Methoden umfassen drei Kategorien:

- Etwas, das der Benutzer oder die Benutzerin kennt: Dies könnte eine Captcha-Frage sein.
- Etwas, was der Benutzer oder die Benutzerin besitzt: Dabei kann es sich um einen Code handeln, der an das Smartphone des Benutzers oder der Benutzerin gesendet wird.
- Etwas, das den Benutzer oder die Benutzerin auszeichnet: Diese erfolgt in der Regel anhand biometrischer Eigenschaften, z. B. über einen Fingerabdruck oder einen Gesichtsscan.

Mehrstufige Authentifizierung erhöht die Sicherheit Ihrer Identität, indem die Auswirkungen der Offenlegung von Anmeldeinformationen (z. B. gestohlene Benutzernamen und Kennwörter) eingeschränkt werden. Wenn mehrstufige Authentifizierung aktiviert ist, benötigt ein Angreifer, der über das Kennwort eines Benutzers verfügt, außerdem dessen Smartphone oder Fingerabdruck, um sich vollständig zu authentifizieren.

Vergleichen Sie mehrstufige Authentifizierung mit einstufiger Authentifizierung. Bei einstufiger Authentifizierung benötigt ein Angreifer nur einen Benutzernamen und Ihr Kennwort, um sich zu authentifizieren. Mehrstufige Authentifizierung sollte nach Möglichkeit aktiviert werden, da sie enorme Sicherheitsvorteile bietet.

# Was ist die Multi-Faktor-Authentifizierung von Microsoft Entra?

Die Multi-Faktor-Authentifizierung von Microsoft Entra ist ein Microsoft-Dienst, der Funktionen für die Multi-Faktor-Authentifizierung bereitstellt. Mit der Multi-Faktor-Authentifizierung von Microsoft Entra können Benutzer\*innen während der Anmeldung eine zusätzliche Form der Authentifizierung auswählen, z. B. einen Telefonanruf oder eine Benachrichtigung über eine mobile App.

## Was ist die kennwortlose Authentifizierung?

Features wie die Multi-Faktor-Authentifizierung (Multi-Factor Authentication, MFA) bieten hervorragende Möglichkeiten, Ihre Organisation zu schützen. Allerdings ist es für Benutzer\*innen oft lästig, sich nicht nur ihre Kennwörter merken, sondern zusätzlich noch weitere Sicherheitsmaßnahmen durchführen zu müssen. Menschen halten am ehesten Vereinbarungen ein, wenn es einfach und bequem ist. Kennwortlose Authentifizierungsmethoden sind bequemer, weil das Kennwort entfällt und durch etwas ersetzt wird, das Sie haben, plus etwas, das Sie auszeichnet oder das Sie wissen.

Die kennwortlose Authentifizierung muss zunächst auf einem Gerät eingerichtet werden. Ihr Computer ist beispielsweise etwas, das Sie besitzen. Nachdem er registriert wurde, weiß Azure, dass er Ihnen zugewiesen ist. Da der Computer jetzt bekannt ist, können Sie sich über die kennwortlose Authentifizierung anmelden, sobald Sie etwas eingeben, was Sie wissen oder was Sie auszeichnet (z. B. eine PIN oder einen Fingerabdruck).

Jede Organisation hat unterschiedliche Anforderungen in Bezug auf die Authentifizierung. Globales Microsoft Azure und Azure Government bieten die folgenden drei Optionen für die kennwortlose Authentifizierung, die mit Microsoft Entra ID integriert werden können:

- Windows Hello for Business
- Microsoft Authenticator-App
- FIDO2-Sicherheitsschlüssel

## Windows Hello for Business

Windows Hello for Business eignet sich ideal für Information-Worker, die über einen eigenen Windows-PC verfügen. Die biometrischen und PIN-basierten Anmeldeinformationen sind direkt mit dem PC des Benutzers verknüpft, wodurch verhindert wird, dass jemand anderes als der Eigentümer Zugriff erhält. Mit PKI-Integration (Public Key-Infrastruktur) und integrierter Unterstützung für einmaliges Anmelden (Single Sign-On, SSO) bietet Windows Hello for Business eine praktische Methode für den nahtlosen Zugriff auf Unternehmensressourcen lokal und in der Cloud.

## Microsoft Authenticator-App

Sie können auch das Smartphone von Mitarbeitern als kennwortlose Authentifizierungsmethode zulassen. Möglicherweise verwenden Sie die Microsoft Authenticator-App bereits als praktische Multi-Faktor-Authentifizierungsoption zusätzlich zu einem Kennwort. Sie können auch die Authenticator-App als kennwortlose Option verwenden.

Die Authenticator-App wandelt jedes iOS- oder Android-Telefon in sichere kennwortlose Anmeldeinformationen um. Benutzer\*innen können sich bei jeder beliebigen Plattform oder jedem beliebigen Browser anmelden, indem sie eine Benachrichtigung auf ihrem Telefon erhalten, eine

auf dem Bildschirm angezeigte Zahl mit der Zahl auf dem Telefon abgleichen und dann ihre biometrischen Daten (Fingerabdruck oder Gesichtsscan) oder ihre PIN zur Bestätigung verwenden. Weitere Informationen zur Installation finden Sie unter Herunterladen und Installieren der Microsoft Authenticator-App.

## FIDO2-Sicherheitsschlüssel

Die FIDO-Allianz (Fast IDentity Online) fördert offene Standards für die Authentifizierung und trägt zur Reduzierung der Verwendung von Kennwörtern als Authentifizierungsmethode bei. FIDO2 ist der aktuelle Standard, der den Webauthifizierungsstandard (WebAuthn) beinhaltet.

FIDO2-Sicherheitsschlüssel sind eine Phishing-resistente, standardbasierte Methode zur kennwortlosen Authentifizierung, die in jedem Formfaktor verfügbar sein kann. Fast Identity Online (FIDO) ist ein offener Standard für die kennwortlose Authentifizierung. Dank FIDO können Benutzer\*innen und Organisationen den Standard nutzen, um sich ohne Benutzername oder Kennwort mit einem externen Sicherheitsschlüssel oder einem in ein Gerät integrierten Plattformschlüssel bei ihren Ressourcen anzumelden.

Benutzer können einen FIDO2-Sicherheitsschlüssel registrieren und dann auf dem Anmeldebildschirm als Hauptauthentifizierungsmethode auswählen. Bei diesen FIDO2-Sicherheitsschlüsseln handelt es sich in der Regel um USB-Geräte, es können aber auch Bluetooth- oder NFC-Geräte sein. Mit einem Hardwaregerät, das für die Authentifizierung sorgt, erhöht sich die Sicherheit eines Kontos, da es kein Kennwort gibt, das verfügbar gemacht oder erraten werden kann.



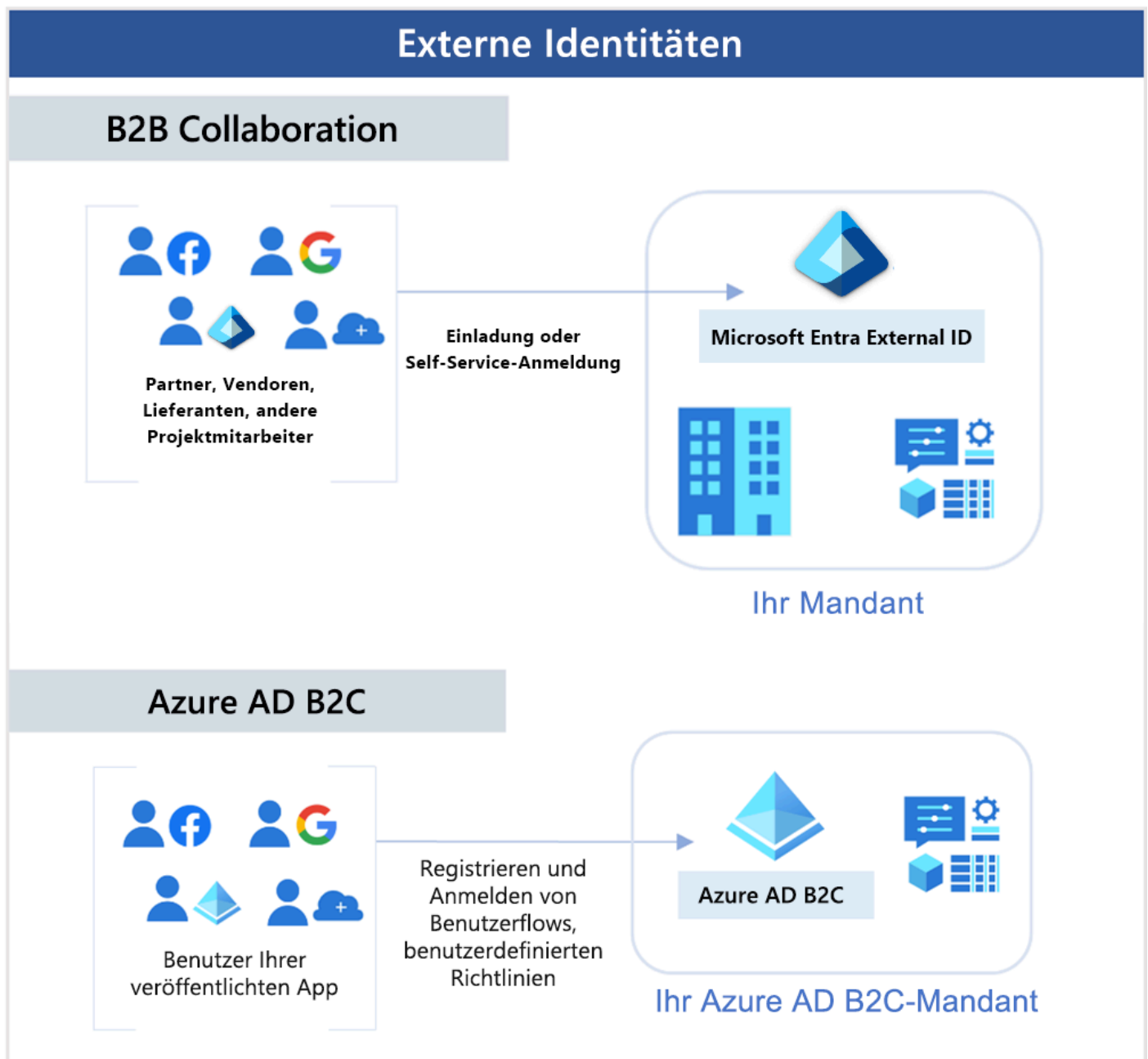
# Grundlegendes zu externen Identitäten in Azure

100 XP

3 Minuten

Eine externe Identität ist beispielsweise eine Person, ein Gerät oder ein Dienst außerhalb Ihrer Organisation. Microsoft Entra External ID umfasst alle Möglichkeiten zur sicheren Interaktion mit Benutzer\*innen außerhalb Ihres Unternehmens. Wenn Sie mit Partnern, Händlern, Lieferanten oder Anbietern zusammenarbeiten möchten, können Sie Ihre Ressourcen gemeinsam nutzen und festlegen, wie Ihre internen Benutzer auf externe Organisationen zugreifen können. Als Entwickler von Consumer-Apps können Sie die Identitätsfunktionen für Ihre Kunden verwalten.

Externe Identitäten können ähnlich wie die einmalige Anmeldung klingen. Mit External Identities können externe Benutzer ihre eigenen Identitäten nutzen (Bring Your Own Identity, BYOI): Unabhängig davon, ob sie über eine von Unternehmen oder Behörden ausgegebene digitale Identität oder über eine nicht verwaltete Social Media-Identität (z. B. für Google oder Facebook) verfügen, können sie sich mit ihren eigenen Anmeldedaten anmelden. Der Identitätsanbieter für externe Benutzer\*innen verwaltet deren Identität, und Sie verwalten den Zugriff auf Ihre Apps mit Microsoft Entra ID oder Azure AD B2C, um Ihre Ressourcen zu schützen.



External Identities umfasst die folgenden Funktionen:

- **B2B Collaboration (Business-to-Business):** Arbeiten Sie mit externen Benutzer\*innen zusammen, indem Sie ihnen die Möglichkeit geben, sich mit ihrer bevorzugten Identität bei Ihren Microsoft-Anwendungen oder anderen Unternehmensanwendungen (SaaS-Apps, individuell entwickelte Apps usw.) anzumelden. B2B Collaboration-Benutzer werden in Ihrem Verzeichnis üblicherweise als Gastbenutzer angezeigt.
- **Direkte B2B-Verbindung** – Richten Sie eine gegenseitige bidirektionale Vertrauensstellung zu einer anderen Microsoft Entra-Organisation ein, um eine nahtlose Zusammenarbeit zu ermöglichen. Direkte B2B-Verbindung unterstützt derzeit freigegebene Teams-Kanäle, sodass externe Benutzer in ihren eigenen Instanzen von Teams aus auf Ihre Ressourcen zugreifen können. Benutzer mit direkter B2B-Verbindung werden in Ihrem Verzeichnis nicht dargestellt, sind jedoch im freigegebenen Teams-Kanal sichtbar und können in Admin Center-Berichten für Teams überwacht werden.
- **Microsoft Azure Active Directory B2C (Business-to-Consumer)** – Veröffentlichen Sie moderne SaaS-Apps oder individuell entwickelte Apps (mit Ausnahme von Microsoft-Apps) für Consumer und Kunden, und nutzen Sie dabei Azure AD B2C für die Identitäts- und Zugriffsverwaltung.

Je nachdem, wie Sie mit externen Organisationen interagieren möchten und welche Arten von Ressourcen Sie freigeben müssen, können Sie eine Kombination dieser Funktionen verwenden.

Mit Microsoft Entra ID und der Funktion Microsoft Entra B2B können Sie problemlos die Zusammenarbeit über Organisationsgrenzen hinweg ermöglichen. Gastbenutzer von anderen Mandanten können von Administratoren oder anderen Benutzern eingeladen werden. Dies gilt auch für soziale Identitäten wie z.B. Microsoft-Konten.

Sie können auch auf einfache Weise sicherstellen, dass Gastbenutzer über entsprechenden Zugriff verfügen. Hierzu können Sie die Gäste selbst oder einen Entscheidungsträger bitten, an einer Zugriffsüberprüfung teilzunehmen und den Zugriff des Gasts erneut zu zertifizieren (oder zu „bescheinigen“). Basierend auf Vorschlägen von Microsoft Entra ID können die Prüfer\*innen die Notwendigkeit des weiteren Zugriffs der einzelnen Benutzer\*innen abwägen. Nach Abschluss einer Zugriffsüberprüfung können Sie dann Änderungen vornehmen und Zugriffsrechte für Gäste entfernen, die diese nicht mehr benötigen.

# Grundlegendes zum bedingten Zugriff in Azure

100 XP

3 Minuten

Bedingter Zugriff ist ein Tool, das Microsoft Entra ID verwendet, um Zugriff auf Ressourcen auf der Grundlage von Identitätssignalen zuzulassen (oder zu verweigern). Diese Signale beinhalten, wer der Benutzer ist, wo sich der Benutzer befindet und von welchem Gerät der Benutzer Zugriff anfordert.

Bedingter Zugriff unterstützt IT-Administratoren bei den folgenden Aufgaben:

- Befähigen von Benutzern, überall und jederzeit produktiv zu sein.
- Schützen der Ressourcen der Organisation.

Der bedingte Zugriff bietet auch eine präzisere Erfahrung mehrstufiger Authentifizierung für Endbenutzer. Beispielsweise wird von Benutzern möglicherweise nicht der zweite Authentifizierungsfaktor angefordert, wenn sie sich an einem bekannten Ort befinden. Allerdings kann ein zweiter Authentifizierungsfaktor angefordert werden, wenn ihre Anmeldesignale ungewöhnlich sind oder der Benutzer sich an einem unerwarteten Ort befindet.

Während der Anmeldung erfasst der bedingte Zugriff Signale vom Benutzer, trifft Entscheidungen auf Grundlage dieser Signale und erzwingt diese Entscheidung dann durch das Zulassen oder Verweigern der Zugriffsanforderung oder verlangt eine Antwort von der mehrstufigen Authentifizierung.

Dieser Flow wird im folgenden Diagramm veranschaulicht:



Hier kann das Signal der Standort oder das Gerät des Benutzers sein bzw. die Anwendung, auf die er zugreifen möchte.

Basierend auf diesen Signalen kann die Entscheidung darin bestehen, Vollzugriff zuzulassen, wenn sich der Benutzer von seinem normalen Standort aus anmeldet. Wenn sich der Benutzer von einem ungewöhnlichen Ort oder einem Standort anmeldet, der als hohes Risiko eingestuft wird, wird der Zugriff möglicherweise vollständig blockiert oder ggf. erst dann erteilt, nachdem der Benutzer eine zweite Form der Authentifizierung bereitgestellt hat.

Erzwingung ist die Aktion, die die Entscheidung ausführt. Die Aktion besteht beispielsweise darin, den Zugriff zu erlauben oder vom Benutzer eine zweite Form der Authentifizierung zu verlangen.

## Wann kann ich bedingten Zugriff verwenden?

Bedingter Zugriff ist nützlich, wenn Folgendes erforderlich ist:

- Die Multi-Faktor-Authentifizierung (MFA) ist erforderlich, um je nach Rolle, Standort oder Netzwerk des Anforderers auf eine Anwendung zuzugreifen. Beispielsweise könnten Sie MFA von Administrator\*innen, aber nicht von normalen Benutzer\*innen oder Personen anfordern, die von außerhalb Ihres Unternehmensnetzwerks eine Verbindung herstellen.
- Erfordern des Zugriffs auf Dienste nur über genehmigte Clientanwendungen. Sie können beispielsweise einschränken, welche E-Mail-Anwendungen eine Verbindung mit Ihrem E-Mail-Dienst herstellen können.
- Erfordern, dass Benutzer nur von verwalteten Geräten aus auf Ihre Anwendung zugreifen können. Ein verwaltetes Gerät ist ein Gerät, das Ihre Standards bezüglich Sicherheit und Konformität erfüllt.
- Blockieren des Zugriffs von nicht vertrauenswürdigen Quellen, z. B. Zugriff von unbekannten oder unerwarteten Orten.

# Beschreiben der rollenbasierten Zugriffssteuerung in Azure

100 XP

5 Minuten

Wie können Sie bei mehreren IT- und Entwicklungsteams steuern, welchen Zugriff die Teammitglieder auf die Ressourcen in ihrer Cloudumgebung besitzen? Das Prinzip der geringsten Rechte besagt, dass nur diejenigen Zugriffsberechtigungen gewährt werden sollten, die für das Ausführen einer Aufgabe auch benötigt werden. Ist beispielsweise für einen Speicher-Blob nur Lesezugriff erforderlich, sollten Sie für diesen Speicher-Blob auch nur Lesezugriff erteilen. Gewähren Sie weder Schreibzugriff für diesen Blob, noch Lesezugriff für andere Speicher-Blobs. Diese Sicherheitsregel hat sich bewährt.

Es wäre jedoch sehr mühsam, diese Art von Berechtigungen für ein ganzes Team zu verwalten. Anstatt detaillierte Zugriffsanforderungen für jede einzelne Person zu definieren und die Zugriffsanforderungen zu aktualisieren, sobald neue Ressourcen erstellt oder neue Teammitglieder hinzugefügt werden, bietet Ihnen Azure die Möglichkeit zur rollenbasierten Zugriffssteuerung (Role-Based Access Control, Azure RBAC).









Azure bietet integrierte Rollen, mit denen allgemeine Zugriffsregeln für Cloudressourcen beschrieben werden. Sie können außerdem eigene Rollen definieren. Jede Rolle verfügt über einen zugeordneten Satz von Zugriffsberechtigungen, die sich auf diese Rolle beziehen. Wenn Sie einer Rolle Personen oder Gruppen zuweisen, erhalten diese alle zugeordneten Zugriffsberechtigungen.

Wenn Sie also einen Entwickler oder eine Entwicklerin der Azure RBAC-Gruppe für Entwickler neu hinzufügen, erhalten diese die gleichen Zugriffsberechtigungen wie die anderen Mitglieder der Gruppe. Analog dazu erhalten alle Mitglieder der Azure RBAC-Gruppe für neu hinzugefügte Ressourcen die gleichen Berechtigungen wie für die vorhandenen Ressourcen, wenn Sie mit Azure RBAC darauf verweisen.

## Wie wird rollenbasierte Zugriffssteuerung auf Ressourcen angewendet?

Rollenbasierte Zugriffssteuerung wird auf einen Bereich angewendet. Dabei handelt es sich um eine Ressource oder eine Gruppe von Ressourcen, für die dieser Zugriff gilt.

Die folgende Abbildung zeigt die Beziehungen zwischen Rollen und Bereichen. Sie können die Besitzerrolle einer Verwaltungsgruppe, einem Abonnement oder einer Ressourcengruppe zuweisen, was mit einer erhöhten Kontrolle und Verantwortung verbunden ist. Für denselben Bereich können Sie Beobachtern die Leserrolle zuweisen, da diese keine Aktualisierungen vornehmen sollen, sondern die Verwaltungsgruppe, das Abonnement oder die Ressourcengruppe überprüfen oder beobachten.

		Rolle				
		Leser	Ressourcen-spezifisch	Benutzerdefi...	Mitwirkender	Besitzer
Bereich	 Verwaltungsgruppe	 Beobachter	 Benutzer, die Ressourcen verwalten			 Administr...
	 Abonnement					
	 Ressourcengruppe					
	 Ressource	 Automatisierte Prozesse				

Zu Bereichen gehören:

- Eine Verwaltungsgruppe (eine Sammlung mehrerer Abonnements).
- Ein einzelnes Abonnement.
- Eine Ressourcengruppe.
- Eine einzelne Ressource.

„Beobachter“, „Benutzer, die Ressourcen verwalten“, „Administratoren“ und „Automatisierte Prozesse“ stellen die Arten von Benutzer\*innen oder Konten dar, die den verschiedenen Rollen in der Regel zugewiesen werden.

Da Azure RBAC hierarchisch aufgebaut ist, werden Zugriffsberechtigungen, die für einen übergeordneten Bereich erteilt wurden, von allen untergeordneten Bereichen geerbt. Beispiel:

- Wenn Sie die Rolle Besitzer einem Benutzer im Verwaltungsgruppenbereich zuweisen, kann dieser Benutzer alles in allen Abonnements innerhalb der Verwaltungsgruppe verwalten.
- Wenn Sie die Rolle Leser einer Gruppe im Abonnementbereich zuweisen, können die Mitglieder dieser Gruppe jede Ressourcengruppe und Ressource innerhalb des Abonnements anzeigen.

## Wie wird Azure RBAC erzwungen?

Azure RBAC wird für jede Aktion erzwungen, die für eine Azure-Ressource initiiert wird, die Azure Resource Manager durchläuft. Resource Manager ist ein Verwaltungsdienst, der eine Möglichkeit bietet, Ihre Cloudressourcen zu organisieren und zu sichern.

In der Regel greifen Sie auf Resource Manager über das Azure-Portal, Azure Cloud Shell, Azure PowerShell und die Azure CLI zu. Azure RBAC erzwingt keine Zugriffsberechtigungen auf Anwendungs- oder Datenebene. Die Anwendungssicherheit muss von Ihrer Anwendung gewährleistet werden.

Azure RBAC verwendet ein Zulassungsmodell. Wenn Ihnen eine Rolle zugewiesen wurde, können Sie im Geltungsbereich dieser Rolle Aktionen ausführen. Wenn Ihnen durch eine Rollenzuweisung Leseberechtigungen für eine Ressourcengruppe und durch eine andere Rollenzuweisung Schreibberechtigungen für dieselbe Ressourcengruppe erteilt wurden, verfügen Sie über Lese- und Schreibberechtigungen für diese Ressourcengruppe.

---

# Beschreiben des Zero-Trust-Modells

3 Minuten

100 XP

Zero Trust ist ein Sicherheitsmodell, bei dem vom schlimmsten Fall ausgegangen wird und die Ressourcen entsprechend geschützt werden. Beim Zero Trust-Modell wird von einer Sicherheitsverletzung ausgegangen, und jede Anforderung wird dann so überprüft, als stamme sie von einem nicht kontrollierten Netzwerk.

Organisationen benötigen heutzutage ein neues Sicherheitsmodell, das sich effektiv an die Komplexität der modernen Umgebung anpassen lässt, mobile Mitarbeiter\*innen einbezieht und ortsunabhängigen Schutz für Personen, Geräte, Anwendungen und Daten bietet.

Um dieser neuen Welt der Datenverarbeitung gerecht zu werden, empfiehlt Microsoft dringend das Zero Trust-Sicherheitsmodell, das auf diesen Leitprinzipien basiert:

- **Führen Sie eine explizite Verifizierung durch:** Ziehen Sie zur Authentifizierung und Autorisierung immer alle verfügbaren Datenpunkte heran.
- **Verwenden Sie den Zugriff mit den geringsten Rechten:** Beschränken Sie den Benutzerzugriff mit Just-In-Time- und Just-Enough-Access (JIT/JEA), risikobasierten adaptiven Richtlinien und Datenschutz.
- **Gehen Sie von einer Sicherheitsverletzung aus:** Minimieren Sie Auswirkungsradius und Segmentzugriff. Überprüfen Sie die End-to-End-Verschlüsselung. Nutzen Sie Analysen, um Transparenz zu erlangen, die Erkennung von Bedrohungen voranzutreiben und Abwehrmaßnahmen zu verbessern.

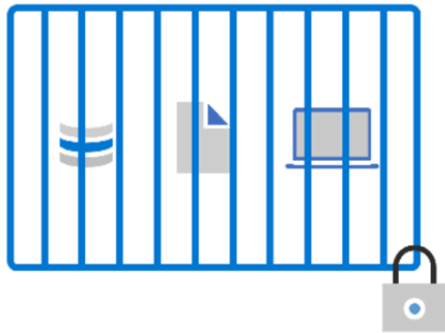
## Anpassen an Zero Trust

Unternehmensnetzwerke wurden bisher eingeschränkt, geschützt und im Allgemeinen für sicher gehalten. Nur verwaltete Computer konnten dem Netzwerk beitreten, VPN-Zugriff wurde streng kontrolliert, und persönliche Geräte wurden häufig eingeschränkt oder blockiert.

Das Zero-Trust-Modell geht von einem anderen Szenario aus. Anstatt davon auszugehen, dass ein Gerät sicher ist, weil es sich innerhalb des Unternehmensnetzwerks befindet, muss sich jede\*r authentifizieren. Dann wird basierend auf der Authentifizierung anstelle des Speicherorts Zugriff gewährt.

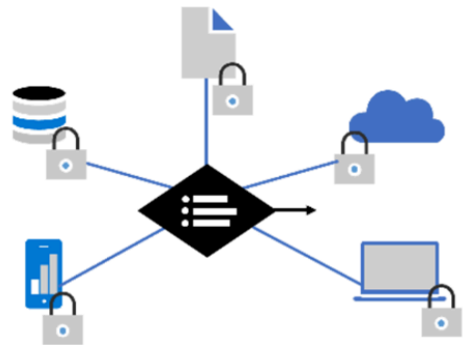
# Mit Zero Trust Ressourcen überall schützen

Für eine einfachere und effektivere Sicherheit



## Klassischer Ansatz

Alles auf ein „sicheres“ Netzwerk einschränken



## Zero Trust

Ressourcen überall mit zentralen Richtlinien schützen

---

## Nächste Lektion: Beschreiben von Defense-in-Depth

[Vorherige](#)



# Beschreiben von Defense-in-Depth

4 Minuten

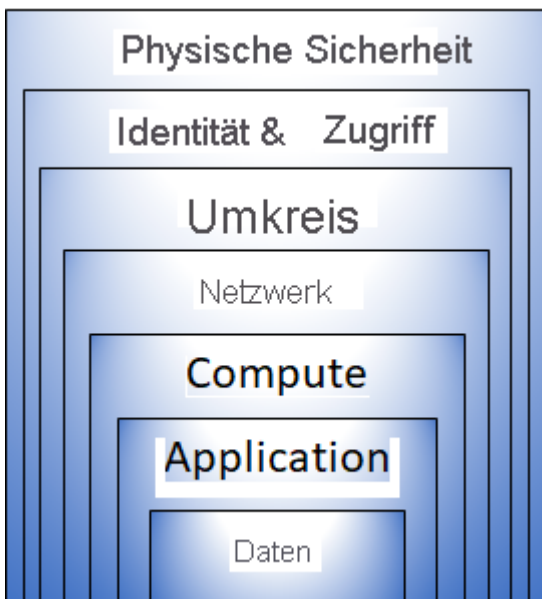
100 XP

Der Defense-in-Depth-Ansatz soll Informationen schützen und Diebstahl durch Personen verhindern, die nicht zum Zugriff darauf berechtigt sind.

Defense-in-Depth-Strategien verwenden zahlreiche Mechanismen, um das Ausmaß von Angriffen abzdämpfen, durch die unberechtigter Zugriff auf Daten erlangt werden soll.

## Schichten von Defense-in-Depth

Sie können sich Defense-in-Depth als Schichten vorstellen, wobei die Daten im Zentrum stehen, und alle anderen Schichten diese zentrale Datenschicht schützen.



Jede Ebene bietet Schutz, sodass beim Passieren einer Ebene die nachfolgende Ebene eine weitere Bedrohung verhindert. Dieser Ansatz beseitigt die Abhängigkeit von einer einzelnen Schutzebene. Er verlangsamt Angriffe und bietet Warnungsinformationen, auf die Sicherheitsteams automatisch oder manuell reagieren können.

Im Folgenden wird die jeweilige Rolle der einzelnen Schichten kurz erläutert:

- Die Schicht Physische Sicherheit ist die erste Verteidigungslinie und schützt die Computinghardware im Rechenzentrum.
- Die Schicht Identität und Zugriff steuert den Zugriff auf die Infrastruktur und die Änderungssteuerung.
- Die Schicht Umkreis verwendet einen Schutz vor verteilten Denial-of-Service-Angriffen (DDoS), um umfangreiche Angriffe abzufangen, bevor diese einen Denial of Service für den Benutzer verursachen können.
- Die Schicht Netzwerk schränkt die Kommunikation zwischen Ressourcen durch Segmentierung und Zugriffssteuerung ein.
- Die Schicht Compute schützt den Zugriff auf virtuelle Computer.
- Die Schicht Anwendung stellt sicher, dass Anwendungen sicher sind und keine Sicherheitsrisiken aufweisen.
- Die Schicht Daten steuert den Zugriff auf Geschäfts- und Kundendaten, die Sie schützen müssen.

Diese Schichten stellen eine Orientierung für Sie dar, die Ihnen bei Entscheidungen im Zusammenhang mit der Sicherheitskonfiguration in allen Schichten Ihrer Anwendungen hilft.

Azure bietet Sicherheitstools und -features für jede Schicht des Defense-in-Depth-Konzepts. Im Folgenden werden die einzelnen Schichten näher betrachtet:

## Physische Sicherheit

Die physische Sicherung des Zutritts zu Gebäuden und die Kontrolle des Zugangs zu Computinghardware im Rechenzentrum bilden die erste Verteidigungslinie.

Bei der physischen Sicherheit geht es darum, physische Schutzmaßnahmen gegen den Zugriff auf Ressourcen zu treffen. Diese Schutzmaßnahmen stellen sicher, dass andere Ebenen nicht umgangen werden können und dass auf Verlust oder Diebstahl angemessen reagiert wird. Microsoft verwendet in den Cloudrechenzentren verschiedene physische Sicherheitsmechanismen.

## Identität und Zugriff

Bei der Schicht „Identität & Zugriff“ geht es darum, die Sicherheit von Identitäten zu gewährleisten, nur erforderlichen Zugriff zu gewähren sowie Anmeldeereignisse und Änderungen zu protokollieren.

Bei dieser Schicht ist Folgendes wichtig:

- Steuern Sie den Zugriff auf die Infrastruktur und die Änderungssteuerung.
- Verwenden Sie SSO (Single Sign-On, einmaliges Anmelden) und mehrstufige Authentifizierung.
- Überwachen Sie Ereignisse und Änderungen.

## Umkreis

Der Netzwerkperimeter schützt vor Angriffen auf Ihre Ressourcen aus dem Netzwerk. Die Identifizierung dieser Angriffe, die Beseitigung ihrer Auswirkungen und das Warnen bei ihrem Auftreten sind wichtige Mechanismen zum Sichern Ihres Netzwerks.

Bei dieser Schicht ist Folgendes wichtig:

- Aktivieren Sie einen Schutz vor DDoS-Angriffen, um umfangreiche Angriffe abzufangen, bevor sie die Verfügbarkeit eines Systems für Endbenutzer beeinträchtigen können.
- Verwenden Sie Umkreisfirewalls, um böswillige Angriffe auf Ihr Netzwerk zu erkennen und zu melden.

## Netzwerk

Bei dieser Schicht liegt der Schwerpunkt darauf, die Netzwerkkonnektivität für alle Ressourcen einzuschränken, um nur Erforderliches zuzulassen. Durch Einschränken dieser Kommunikation verringern Sie das Risiko der Ausbreitung eines Angriffs auf andere Systeme in Ihrem Netzwerk.

Bei dieser Schicht ist Folgendes wichtig:

- Schränken Sie die Kommunikation zwischen Ressourcen ein.
- Verweigern Sie Aktionen standardmäßig.
- Schränken Sie nach Möglichkeit eingehenden Zugriff über das Internet und ausgehenden Zugriff ein.
- Implementieren Sie eine sichere Verbindung mit lokalen Netzwerken.

# Compute

Schadsoftware sowie nicht gepatchte oder nicht ordnungsgemäß geschützte Systeme machen Ihre Umgebung anfällig für Angriffe. Bei dieser Schicht liegt der Schwerpunkt darauf, sicherzustellen, dass Ihre Computerressourcen sicher und die notwendigen Kontrollen eingerichtet sind, um Sicherheitsprobleme zu minimieren.

Bei dieser Schicht ist Folgendes wichtig:

- Gewährleisten Sie den sicheren Zugriff auf virtuelle Computer.
- Implementieren Sie Endpunktschutz auf Ihren Geräten, und halten Sie alle Systeme gepatcht und auf dem neuesten Stand.

# Application

Integrieren Sie Sicherheit in den Anwendungsentwicklungszyklus, um die Anzahl von Sicherheitsrisiken im Code zu verringern. Alle Entwicklungsteams sollten sicherstellen, dass ihre Anwendungen standardmäßig sicher sind.

Bei dieser Schicht ist Folgendes wichtig:

- Stellen Sie sicher, dass Anwendungen sicher sind und keine Sicherheitsrisiken aufweisen.
- Speichern Sie vertrauliche Anwendungsgeheimnisse auf einem sicheren Speichermedium.
- Erklären Sie Sicherheit zu einer Entwurfsanforderung für alle Anwendungsentwicklungen.

# Daten

Personen, die Daten speichern und den Zugriff darauf steuern, müssen sicherstellen, dass diese Daten ordnungsgemäß geschützt sind. Häufig schreiben gesetzliche Vorgaben die Regelungen und die Prozesse vor, die zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit von Daten erforderlich sind.

In der Regel zielen Angriffe auf folgende Daten ab:

- Daten, die in einer Datenbank gespeichert sind
- Daten, die auf einem Datenträger eines virtuellen Computers gespeichert sind
- Daten, die in einer Software-as-a-Service-Anwendung (SaaS) gespeichert sind, z. B. in Office 365
- Daten, die über Cloudspeicher verwaltet werden

---

## Nächste Lektion: Beschreiben von Microsoft Defender für Cloud

[Vorherige](#)

# Beschreiben von Microsoft Defender für Cloud

100 XP

6 Minuten

Defender für Cloud ist ein Überwachungstool für die Verwaltung des Sicherheitsstatus und den Bedrohungsschutz. Ihre Cloudumgebungen, ob lokal, hybrid oder Multi-Cloud, werden überwacht, um Tipps und Benachrichtigungen zur Verbesserung Ihres Sicherheitsstatus bereitzustellen.

Defender für Cloud bietet die Tools, die Sie benötigen, um Ihre Ressourcen zu schützen, Ihren Sicherheitsstatus zu verfolgen, sich vor Cyberangriffen zu schützen und die Sicherheitsverwaltung zu optimieren. Die Bereitstellung von Defender für Cloud ist einfach, denn der Dienst ist nativ in Azure integriert.

## Schutz für jede Bereitstellung

Da Defender für Cloud ein nativer Azure-Dienst ist, werden viele Azure-Dienste überwacht und geschützt, ohne dass eine Bereitstellung erforderlich ist. Wenn Sie jedoch auch über ein lokales Rechenzentrum verfügen oder auch in einer anderen Cloudumgebung tätig sind, ergibt die Überwachung durch Azure-Dienste möglicherweise kein vollständiges Bild Ihrer Sicherheitssituation.

Bei Bedarf kann Defender für Cloud automatisch einen Log Analytics-Agent bereitstellen, um sicherheitsbezogene Daten zu sammeln. Bei Azure-Computern erfolgt die Bereitstellung direkt. Für Hybrid- und Multi-Cloud-Umgebungen werden die Microsoft Defender-Pläne mithilfe von Azure Arc auf Nicht-Azure-Computer ausgeweitet. CSPM-Features (Cloud Security Posture Management) werden auf Multi-Cloud-Computer ausgeweitet, ohne dass hierzu Agents benötigt werden.

## Nativer Azure-Schutz

Defender für Cloud unterstützt Sie bei der Erkennung von Bedrohungen für:

- **Azure-PaaS-Dienste:** Erkennen Sie Bedrohungen, die auf Azure-Dienste wie Azure App Service, Azure SQL, Azure Storage-Konten und weitere Datendienste abzielen. Sie können Ihre Azure-Aktivitätsprotokolle auch mithilfe der nativen Integration in Microsoft Defender für Cloud Apps (vormals bekannt als Microsoft Cloud App Security) auf Anomalien untersuchen.
- **Azure-Datendienste:** Defender für Cloud enthält Funktionen, mit denen Sie Ihre Daten automatisch in Azure SQL klassifizieren können. Sie können auch Bewertungen für potenzielle Sicherheitsrisiken für Azure SQL- und Storage-Dienste sowie Empfehlungen zu ihrer Entschärfung erhalten.
- **Netzwerke:** Mit Defender für Cloud können Sie die Anfälligkeit für Brute-Force-Angriffe verringern. Wenn Sie den Zugriff auf VM-Ports einschränken, indem Sie den Just-In-Time-Zugriff auf VMs nutzen, können Sie die Sicherheit für Ihr Netzwerk erhöhen, weil unnötige Zugriffsvorgänge verhindert werden. Sie können für ausgewählte Ports Richtlinien für den sicheren Zugriff festlegen, damit der Zugriff nur für autorisierte Benutzer, zulässige IP-Quelladressen oder IP-Adressbereiche und einen begrenzten Zeitraum möglich ist.

## Schutz Ihrer Hybridressourcen

Zusätzlich zum Schutz Ihrer Azure-Umgebung können Sie Ihrer Hybrid Cloud-Umgebung Defender für Cloud-Funktionen hinzufügen, um Ihre Nicht-Azure-Server zu schützen. Damit Sie

sich auf das Wesentliche konzentrieren können, erhalten Sie maßgeschneiderte Bedrohungsdaten und priorisierte Warnmeldungen basierend auf Ihrer spezifischen Umgebung.

Um den Schutz auf lokale Computer auszuweiten, stellen Sie Azure Arc bereit und aktivieren die erweiterten Sicherheitsfunktionen von Defender für Cloud.

## Schutz von Ressourcen, die in anderen Clouds ausgeführt werden

Defender für Cloud kann auch Ressourcen in anderen Clouds (z. B. AWS und GCP) schützen.

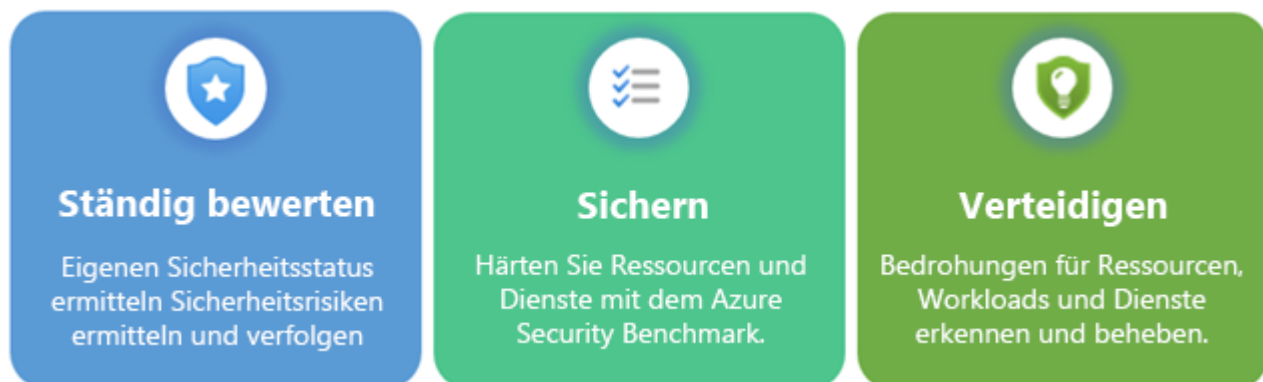
Wenn Sie beispielsweise ein AWS-Konto (Amazon Web Services) mit einem Azure-Abonnement verbunden haben, können Sie die folgenden Schutzfunktionen aktivieren:

- Die CSPM-Features von Defender für Cloud werden auf Ihre AWS-Ressourcen ausgeweitet. Dieser Plan ohne Agent bewertet Ihre AWS-Ressourcen gemäß AWS-spezifischen Sicherheitsempfehlungen und bezieht die Ergebnisse in Ihre Sicherheitsbewertung ein. Die Ressourcen werden auch auf Einhaltung integrierter AWS-spezifischer Standards (AWS CIS, AWS PCI-DSS und AWS Foundational Security Best Practices) bewertet. Die Seite Bestandsverzeichnis von Defender für Cloud ist eine Multi-Cloud-Funktion, die Ihnen hilft, Ihre AWS-Ressourcen zusammen mit Ihren Azure-Ressourcen zu verwalten.
- Mit Microsoft Defender for Containers werden die Containerbedrohungserkennung und erweiterten Schutzmaßnahmen auf Ihre Amazon EKS Linux-Cluster ausgeweitet.
- Microsoft Defender for Servers stattet Ihre Windows- und Linux-EC2-Instanzen mit Bedrohungserkennung und erweiterten Schutzmaßnahmen aus.

## Bewerten, Schützen und Verteidigen

Defender für Cloud erfüllt drei wichtige Anforderungen, wenn Sie die Sicherheit Ihrer Ressourcen und Workloads in der Cloud und lokal verwalten:

- Kontinuierliche Bewertung: Kennen Sie Ihren Sicherheitsstatus. Ermitteln und verfolgen Sie Sicherheitsrisiken.
- Schützen: Härten Sie Ressourcen und Dienste mit dem Azure Security Benchmark.
- Verteidigen: Erkennen und beheben Sie Bedrohungen für Ressourcen, Workloads und Dienste.



## Kontinuierliche Bewertung

Defender für Cloud hilft Ihnen, Ihre Umgebung kontinuierlich zu bewerten. Defender für Cloud umfasst Lösungen zur Sicherheitsrisikobewertung für Ihre VMs, Containerregistrierungen und SQL

## Server-Instanzen.

Microsoft Defender für Server umfasst eine automatische, native Integration in Microsoft Defender für Endpunkt. Wenn diese Integration aktiviert ist, haben Sie Zugriff auf die Sicherheitsrisikobewertung durch das Bedrohungs- und Sicherheitsrisikomanagement von Microsoft.

Zwischen der Ausführung dieser Bewertungstools finden regelmäßige, ausführliche Scans auf Sicherheitsrisiken statt, die Ihre Computerressourcen, Daten und Infrastruktur abdecken. Sie können die Ergebnisse dieser Scans in Defender für Cloud überprüfen und auf diese reagieren.

## Sicher

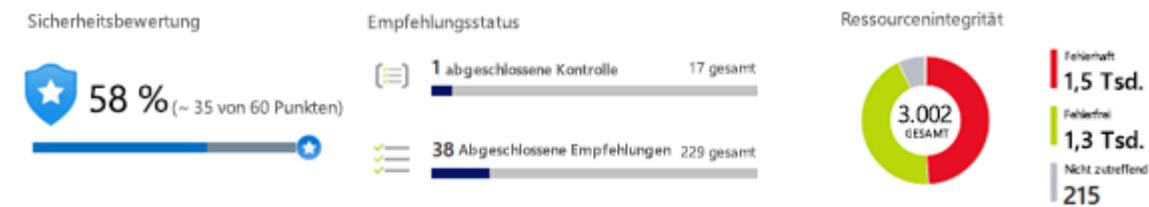
Von Authentifizierungsmethoden über Zugriffssteuerung bis hin zum Zero-Trust-Konzept – die Sicherheit in der Cloud ist eine wichtige Grundlage, bei der keine Fehler unterlaufen dürfen. Schutz in der Cloud bedeutet, dass Ihre Workloads geschützt werden. Um Ihre Workloads zu schützen, benötigen Sie Sicherheitsrichtlinien, die auf Ihre Umgebung und Ihre Situation zugeschnitten sind. Da die Richtlinien in Defender für Cloud auf Azure Policy-Kontrollen basieren, können Sie vom vollen Funktionsumfang und der Flexibilität einer erstklassigen Richtlinienlösung profitieren. In Defender für Cloud können Sie Ihre Richtlinien so festlegen, dass sie für Verwaltungsgruppen, abonnementübergreifend und sogar für einen gesamten Mandanten ausgeführt werden.

Einer der Vorteile des Wechsels in die Cloud ist die Möglichkeit, bei Bedarf neue Dienste und Ressourcen hinzuzufügen und zu skalieren. Defender für Cloud überwacht neu bereitgestellte Ressourcen ständig – und das für sämtliche Workloads. Defender für Cloud bewertet, ob neue Ressourcen entsprechend den Best Practices für die Sicherheit konfiguriert werden. Falls nicht, werden sie markiert, und Sie erhalten eine nach Prioritäten geordnete Liste mit Empfehlungen zur Bereinigung. Mithilfe der Empfehlungen können Sie die Angriffsfläche jeder einzelnen Ressource verringern.

Die Liste der Empfehlungen wird durch den Azure-Sicherheitsvergleichstest aktiviert und unterstützt. Bei diesem Vergleichstest handelt es sich um einen von Microsoft erstellten Satz mit Azure-spezifischen Richtlinien zu Best Practices in Bezug auf Sicherheit und Compliance, die auf allgemeinen Complianceframeworks beruhen.

Dadurch können Sie mithilfe von Defender für Cloud nicht lediglich Sicherheitsrichtlinien festlegen, sondern außerdem Standards für die sichere Konfiguration Ihrer gesamten Ressourcen anwenden.

Damit Sie besser nachvollziehen können, wie wichtig die einzelnen Empfehlungen für den gesamten Sicherheitsstatus sind, werden die Empfehlungen von Defender für Cloud in Sicherheitskontrollen gruppiert, und jedem Sicherheitskontrollelement wird eine Sicherheitsbewertung hinzugefügt. Die Sicherheitsbewertung gibt auf einen Blick Aufschluss über die Integrität Ihres Sicherheitsstatus. Die Kontrollmechanismen erstellen hingegen eine Liste der Faktoren, die hinsichtlich Ihrer Sicherheitsbewertung und Ihres allgemeinen Sicherheitsstatus verbessert werden können.



Steuerelemente	Potenzielle Bewertungssteigerung	Fehlerhafte Ressourcen	Ressourcenintegrität
> Sicherheitsrisiken entschärfen	+ 10 % (6 Punkte)	171 von 219 Ressourcen	
> Verschlüsselung ruhender Daten aktivieren	+ 5 % (3 Punkte)	147 von 231 Ressourcen	
> Zugriff und Berechtigungen verwalten	+ 5 % (3 Punkte)	20 von 36 Ressourcen	
> Sicherheitskonfigurationen bereinigen	+ 4 % (3 Punkte)	134 von 212 Ressourcen	
> Anwendungen vor DDoS-Angriffen schützen	+ 3 % (2 Punkte)	14 von 156 Ressourcen	
> Daten während der Übertragung verschlüsseln	+ 3 % (2 Punkte)	135 von 331 Ressourcen	
> Systemupdates anwenden	+ 3 % (2 Punkte)	57 von 212 Ressourcen	
> Adaptive Anwendungssteuerung anwenden	+ 2 % (1 Punkt)	75 von 165 Ressourcen	
> Verwaltungsports schützen	+ 2 % (1 Punkt)	14 von 151 Ressourcen	
> Datenklassifizierung anwenden	+ 2 % (1 Punkt)	16 von 53 Ressourcen	
> Nicht autorisierten Netzwerkzugriff einschränken	+ 1 % (1 Punkt)	48 von 241 Ressourcen	
> Endpoint Protection aktivieren	+ 1 % (1 Punkt)	75 von 192 Ressourcen	
> Überwachung und Protokollierung aktivieren	+ 1 % (1 Punkt)	134 von 180 Ressourcen	
> Bewährte Sicherheitsmethoden implementieren	+ 0 % (0 Punkte)	168 von 797 Ressourcen	
> Erweiterten Bedrohungsschutz aktivieren	+ 0 % (0 Punkte)	8 von 11 Ressourcen	
> Benutzerdefinierte Empfehlungen	+ 0 % (0 Punkte)	1033 von 2183 Ressourcen	
> MFA aktivieren <span>✓ Abgeschlossen</span>	+ 0 % (0 Punkte)	Keine	

## Verteidigen

Die ersten beiden Bereiche haben sich auf die Bewertung, Überwachung und Wartung Ihrer Umgebung konzentriert. Defender für Cloud hilft Ihnen mithilfe von Sicherheitswarnungen und erweiterten Features für den Bedrohungsschutz auch bei der Verteidigung Ihrer Umgebung.

## Sicherheitswarnungen

Wenn Defender für Cloud eine Bedrohung in einem Bereich Ihrer Umgebung erkennt, wird eine Sicherheitswarnung generiert. Sicherheitswarnungen:

- enthalten Details zu den betroffenen Ressourcen
- schlagen Korrekturschritte vor
- enthalten in manchen Fällen eine Option zum Auslösen einer Logik-App als Reaktion

Sie können Warnungen unabhängig davon, ob sie von Defender für Cloud generiert oder von Defender für Cloud von einem integrierten Sicherheitsprodukt empfangen wird, exportieren. Der Bedrohungsschutz von Defender für Cloud umfasst die Fusion-Kill-Chain-Analyse, die automatisch Warnungen in Ihrer Umgebung auf der Grundlage der Cyber-Kill-Chain-Analyse korreliert, damit Sie das ganze Ausmaß einer Angriffskampagne, ihren Ausgangspunkt und ihre Auswirkungen auf Ihre Ressourcen besser verstehen können.

## Erweiterter Schutz vor Bedrohungen

Defender für Cloud bietet erweiterte Features für den Bedrohungsschutz, von denen viele bereitgestellte Ressourcen profitieren, zum Beispiel virtuelle Computer, SQL-Datenbanken, Container, Webanwendungen und Netzwerke. Die Schutzmaßnahmen umfassen das Absichern der Verwaltungsports Ihrer VMs mit Just-In-Time-Zugriff und adaptive Anwendungssteuerungen zum Erstellen von Positivlisten, die festlegen, welche Apps auf Ihren Computern ausgeführt werden dürfen und welche nicht.

---

## Nächste Lektion: Wissensbeurteilung