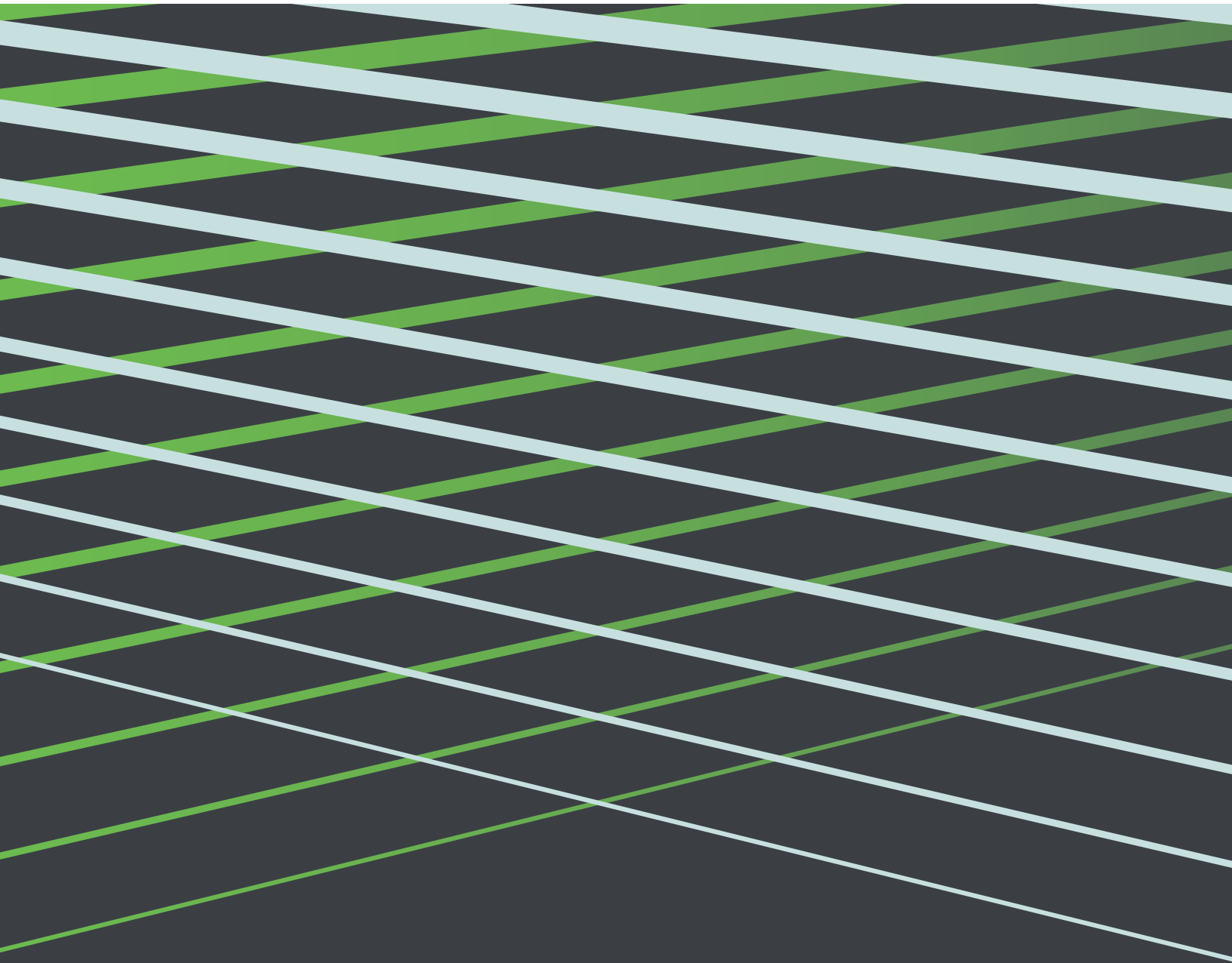
Ein essentieller Leitfaden zu

# Zero Trust für Microsoft Anwendungen



Duo Security is now part of Cisco.

**In den letzten Jahren ist ein neues Sicherheitsmodell entstanden, das jeden Zugriffsversuch so behandelt, als stamme er aus einem nicht vertrauenswürdigen Netzwerk.**

## In einer Welt geprägt von Cloud- und mobilen Anwendungen

können Organisationen sich nicht auf traditionelle Sicherheitsarchitekturen zur Sicherung des Perimeters und dem Zugang zu Anwendungen verlassen. Heute greifen Benutzer direkt aus der Entfernung auf Unternehmensanwendungen zu ohne durch Firewalls und VPN's zu gehen.

Da Benutzer traditionelle Sicherheitskontrollen und Regelungen umgehen benötigen Unternehmen neue Sicherheitsmodelle um sensible Date zu schützen, unabhängig davon wo der Benutzer sich aufhält und welche Geräte für den Zugang zu Anwendungen benutzt werden.

In den vergangenen Jahren ist ein neues Sicherheitsmodell entstanden welches jeden Zugangsversuch so behandelt als komme er von einem nicht vertrauenswürdigen Netzwerk. Dieses Modell konzentriert sich auf die Authentifizierung von Benutzern und die Kontrolle der Sicherheitslage von Geräten bevor ein Zugriff auf Anwendungen erlaubt wird. Dieses Modell ist bekannt als Zero Trust für Mitarbeiter.

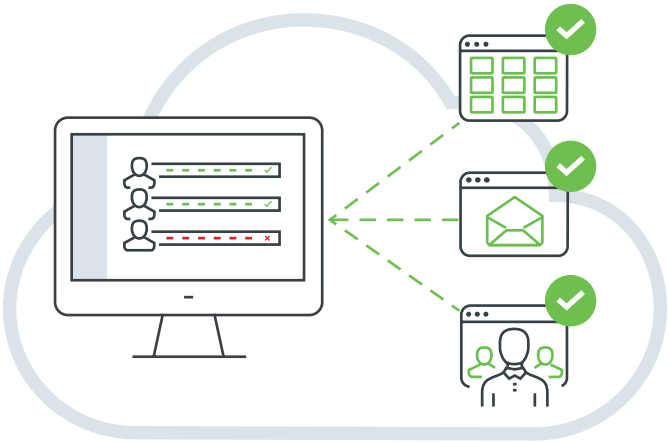
Durch das Hinzufügen eines Zero Trust Sicherheitsmodells zu der bestehenden Sicherheitsinfrastruktur können Unternehmen ihre Zugangssicherheit verbessern. Obwohl ein umfangreiches Zero Trust Sicherheitsmodell Benutzer, Geräte und das Internet der Dinge (IoT) Geräte und Workloads umfasst, möchten wir in diesem White Paper einen Überblick darüber verschaffen wie Unternehmen Zero Trust Prinzipien umsetzen können um ihre Microsoft Anwendungen zu schützen.

Microsoft Anwednungen stellen das Rückgrat für tausende Organisationen dar. Viele Unternehmen wechseln gegenwärtig von On-Premises zur Cloud. Diesen Organisationen kann ein Zero Trust Zugang helfen die Risiken von unerlaubtem Zugriff und von Datenschutzverletzungen zu reduzieren. Gleichzeitig kann so sichergestellt werden, dass die Benutzerproduktivität beim Zugriff auf Anwendungen nicht betroffen ist.

In diesem Leitfaden werden einige wesentliche Tipps für Administratoren besprochen, um Zero Trust Zugangssicherheit für drei wesentliche Microsoft-Suiten sicherzustellen: Office 365, Windows und Azure.

ZERO TRUST FÜR

# Office 365



Viele Unternehmen wechseln zügig ihr Productivity Suite zu Office 365. Trotz verschiedener Kosten- und Produktivitätsvorteile gibt es Risiken die Administratoren beachten und reduzieren sollten wenn sie vorhaben kritische Daten in die Cloud zu verschieben. Administratoren können die Zugangsentscheidungen basierend auf spezifischen Risikokontexten entscheiden. Zum Beispiel: *ist der Benutzer bestätigt? Wird das Gerät verwaltet?*

## Ziehen Sie die folgenden Schritte in Betracht, um Office 365 zu sichern:

## Benutzervertrauen schaffen

Benutzervertrauen zu schaffen ist der erste Schritt zu Zero Trust. Können sie ihre Benutzer indentifizieren und von wo sie zugreifen möchten? Administratoren können starke Authentifizierung mit einer Multi-Faktor Authentifizierung (MFA) schaffen. MFA hilft das Risiko des Diebstahls von Zugangsdaten, von roher Gewalt oder anderen passwortbasierten Angriffen zu reduzieren.  Desweiteren, da Office 365 alle Mitarbeiter einer Organisation betrifft, sollten Administratoren weitere Optionen zur Authentifizierung anbieten und es Benutzern erlauben basierend auf ihrer Umgebung zu wählen.
Diese Authentifizierungsmethoden können Push-Benachrichtigungen, Einmal-Passwörter (OTP), Telefon-Rückruf sowie Universal Second Factor (U2F) Sicherheitsschlüssel umfassen.

## Sichtbarkeit im BYOD schaffen

Benutzer können auf Cloud-Anwendungen wie Office365 von überall und auf jedem Gerät zugreifen. Zero Trust Lösungen sollten Einblicke in die Sicherheit der Geräte geben, die sich bei Office 365 anmelden. Mit diesen Einblicken können Administratoren beurteilen, ob zugreifende Geräte potenziell anfällig sind für Missbrauch und Angriffe. Eine Zero-Trust-Lösung sollte alle Plattformen von Endbenutzergeräten unterstützen - Windows, Mac, iOS und Android.

# Lernfähige Richtlinien durchsetzen

Moderne Zero Trust Lösungen sollten in der Lage sein Sicherheitsrichtlinien für Benutzer und die Geräte mit denen auf Office 365 zugegriffen wird durchzusetzen. Administratoren sollten für jeden Zugriffsversuch bestimmen können ob ein Sicherheitsrisiko akzeptabel ist.
Zum Beispiel: wenn sich Benutzer bei Office 365 mit einem Gerät mit einem veralteten Browser anmelden möchten, dann sollte dieser Versuch blockiert werden. Ein veralteter Browser kann verschiedene Sicherheitslücken bedeuten, die noch nicht behoben wurden. Zudem sollten Administratoren in der Lage sein den Zugriff basierend auf Geolokalisierung, IP's und Sicherheitsaufstellung des Geräts zu verwalten.

# Rollenbasierte Zugangskontrolle

Benutzer in funktionalen Bereichen, wie etwa Finanzen, Buchhaltung und Recht, erhalten Zugriff auf mehr sensible Daten in Office 365 Dokumenten oder Tabellen als in anderen Gruppen.
Administratoren sollten in der Lage sein strengere Regeln für Benutzer mit Zugriff auf sensible Daten einzurichten, basierend auf der Vertrauenswürdigkeit ihrer Geräte um sicher zu gehen, dass kompromittierte Geräte nicht auf sensible Daten zugreifen können.

# Compliance-Richtlinien durchsetzen

Organisationen, die Office 365 einsetzen, müssen in der Cloud Datenschutz und Sicherheit gewährleisten. Zum Beispiel: HIPAA Omnibus verpflichtet Benutzer mit Zugriff auf Gesundheitsdaten zur Nutzung von verschlüsselten Geräten mit Passwortschutz. Eine Zero-Trust-Lösung sollte Compliance-Anforderungen ermöglichen, die in PCI, NIST, GDPR und CCPA veröffentlicht werden und sicherstellen, dass Administratoren diese Richtlinien durchsetzen können um die Compliance zu erreichen.

# Sicherheitsrichtlinien für alle Cloud-Anwendungen erweitern

Organisationen können mehrere Cloud-Anwendungen haben um spezifische Anwendungsfälle und Anforderungen abzudecken. Jede Zero Trust Sicherheitslösung sollte in der Lage sein ihre Sicherheitsrichtlinien für Office 365 auf andere Cloud-Anwendungen zu erweitern. Desweiteren sollten Admins in der Lage sein die Zugangskontrollen für jede Cloud-Anwendung anzupassen, basierend auf dem Daten- und Anwendungsrisiko.

ZERO TRUST FÜR

# Windows

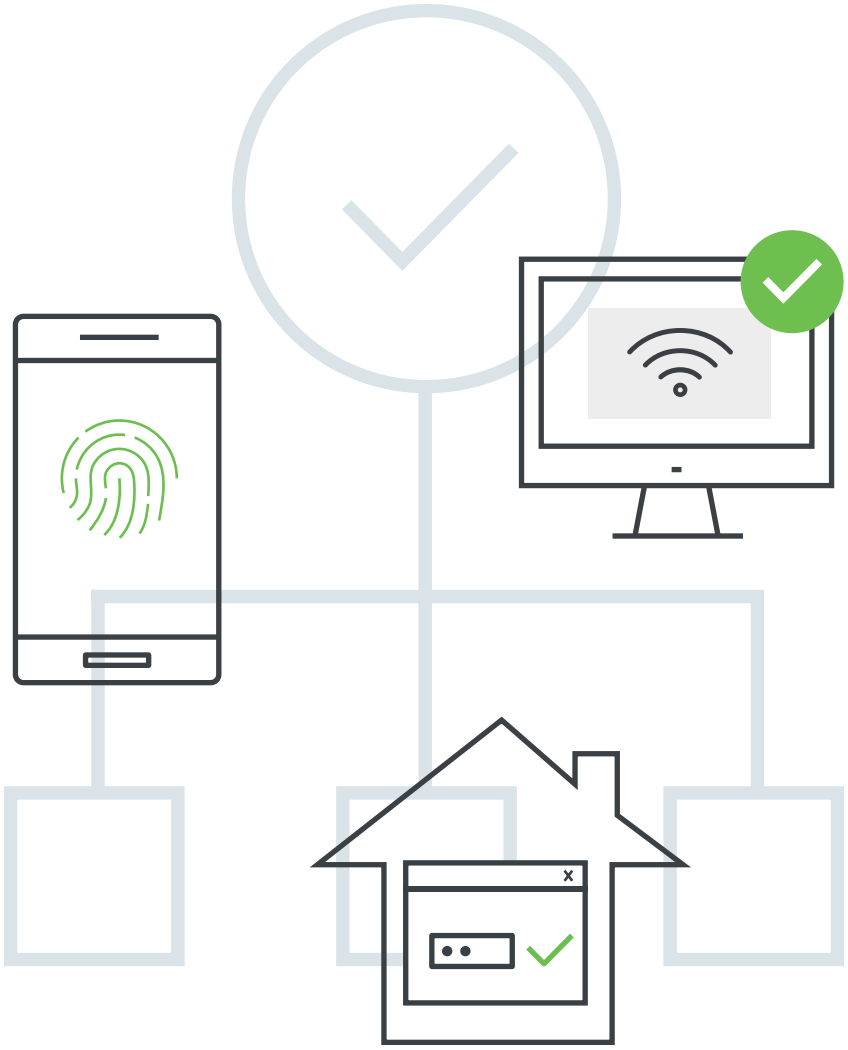
Die meisten Organisationen haben einen großen Einsatz der Windows-Infrastruktur in ihrem Umfeld. Dies beinhaltet Laptops, Desktops und Server. Üblicherweise verwalten Administratoren verschiedene Versionen von Windows-Betriebssystemen auf den laufenden Anwendungen. Jede Zero Trust Zugangslösung sollte alle gängigen Windows-Versionen um eine beständige Zugangssicherheit in der gesamten Organisation zu gewährleisten.

## Benutzervertrauen herstellen

Zunächst sollten die Administratoren in der Lage sein eine starke Benutzer-Authentifizierung mit MFA für jeden Windows-basierten Betriebssystem-Login zu schaffen, egal ob lokal oder remote. Eine Zero-Trust-Lösung sollte Remote Desktop Protocol (RDP) und Remote Desktop Gateway (RDG) für Remote-Anmeldungen zulassen.
Desweiteren sollten Administratoren in der Lage sein sicher auf lokale Maschinen zuzugreifen, auch wenn diese offline sind.
Dies stellt sicher, dass böswillige Benutzer das Authentifizierungs-Workflow nicht umgehen können wenn eine Maschine sich nicht mit dem Netzwerk verbinden kann.

## Anpassungsrichtlinien durchsetzen

Da Windows-Server auch für die Nutzung von anderen, geschäftsentscheidenden Anwendungen eingesetzt werden können sollten Admins den Zugriff auf Server mit stärkeren Formen von Authentifizierung schützen. Beispielsweise sollten Admins den Zugriff auf Windows-Server durch MFA-Methoden wie U2F und Biometrik wie etwa TouchID und FaceID schützen.
Die Anwendung von weniger sicheren Arten der Authentifizierung, wie etwa SMS, sollte vermieden werden.
Administratoren sollten in der Lage sein die Authentikatoren für jeden Server basierend auf dem Risikoprofil der in der jeweiligen Anwendung gespeicherten Daten anzupassen.



# Rollenbasierte Zugangskontrolle

Sicherheitsverletzungen sind erfolgreich wenn Benutzer zuviel Zugang haben.  Angreifer verletzen eine Anwendung und können lateral auf andere Anwendungen oder Server zugreifen. Eine Zero-Trust-Sicherheitslösung würde die Angriffsoberfläche durch die Umsetzung von rollenbasierten Zugangsrichtlinien reduzieren um sicherzustellen, dass Benutzer nur Zugriff auf Windows Workstations habe zu denen sie authorisiert sind.

ZERO TRUST FÜR

# Hybrid Azure Environments

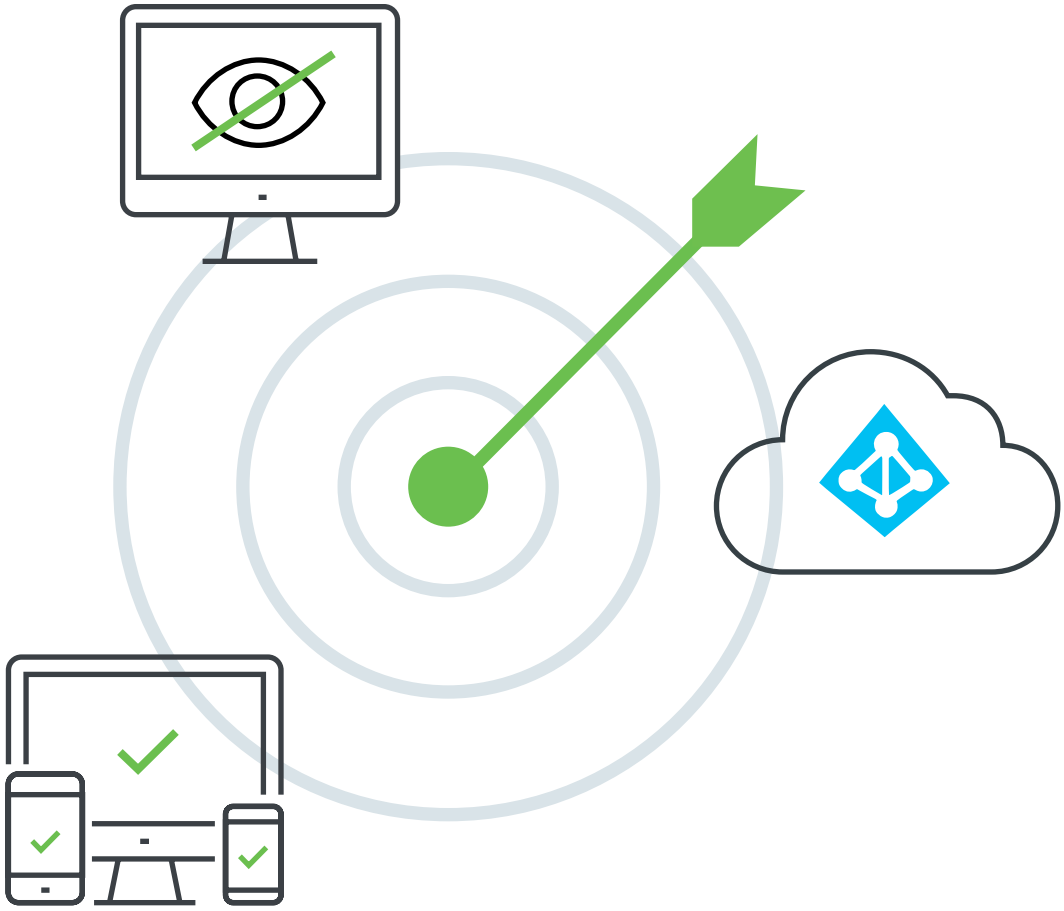
Viele Organisationen betreiben eine Hybrid-Infrastruktur mit einer Mischung von Anwendungen die Onsite oder in der Azure Cloud sind. Administratoren müssen sicherstellen, dass einheitliche Sicherheitsrichtlinien für den Zugriff bestehen, egal von wo aus diese eingesetzt werden. Eine Zero Trust Lösung sollte in jeder Umgebung Sicherheitskontrollen anbieten: onsite, in der Cloud oder hybrid.

## Vertrauen in Benutzer und Geräte schaffen

Eine Zero Trust Sicherheitslösung ermöglicht den Benutzern Remote-Zugriff auf alle Anwendungen die durch Azure eingesetzt werden. Dies verbessert die Benutzerproduktivität ohne die Sicherheit zu kompromittieren.Administratoren können starke Authentifizierung mit MFA schaffen um die Sicherheitsaustellung von Geräten zu überprüfen bevor der Zugriff erteilt wird.

## BYOD sichtbar machen

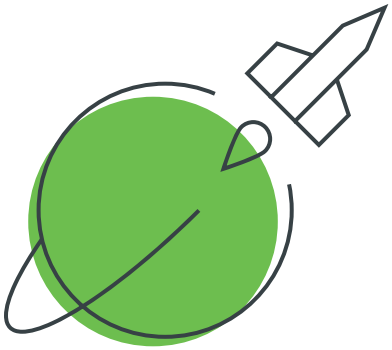
Wenn Administratoren Remote-Zugriff erlauben können Benutzer von überall her auf die Anwendungen zugreifen, durch die Nutzung eines einzigen Geräts. Eine Zero-Trust Lösung soll Einblicke in die Sicherheit eines jeden Geräts welches auf Azure zugreift. Mit diesen Einblicken in die Sicherheit können Administratoren bewerten ob einzelne Geräte potentiel risikobelastet sind bezüglich Missbrauch und Angriffe.



# Anpassungsfähige Richtlinien durchsetzen

Veraltete und ungeschützte Geräte können ein großes Sicherheitsrisiko für durch Azure bereitgestellte Anwendungen darstellen.
Angreifer können ungeschützte Geräte für den Zugriff auf Anwendungen ausnutzen und somit Datenschutzverletzungen erhöhen. Administratoren sollten in der Lage sein gerätebasierte Richtlinien durchzusetzen um riskante und ungeschützte Geräte am Zugriff auf Anwendungen zu hindern.

Da Organisationen vermehrt Microsoft-Anwendungen einsetzen und übernehmen kann eine Zero Trust Lösung dabei helfen das Risiko von Datenschutzverletzungen verhindern. Allerdings werden heute verschiedene Zero Trust Lösungen am Markt angeboten. Admins können diesen Ratgeber nutzen um eine Sicherheitslösung ausfindig zu machen die das Minimum an Merkmalen und Funktionalitäten für jede Anwendungs-Suite besitzt um ein Gleichgewicht zwischen Benutzerfreundlichkeit und Sicherheit zu schaffen.



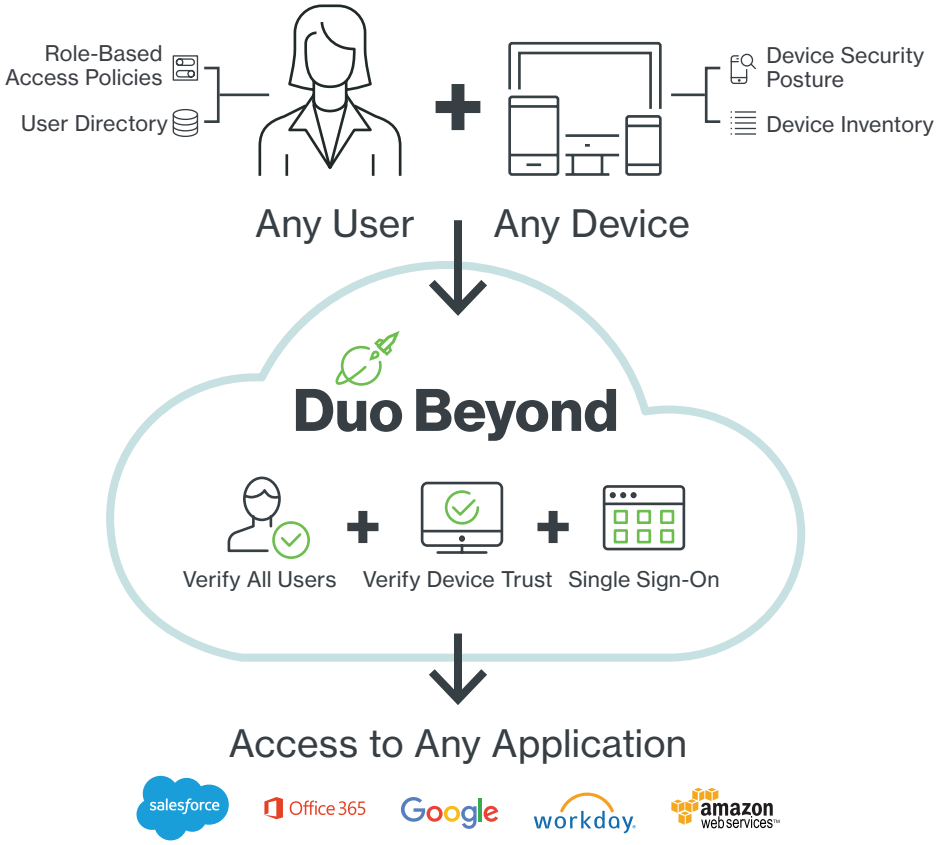
# Duo Beyond

## Zero Trust für die Belegschaft

Mit **Duo Beyond**, erhalten Sie:

### Umfassende Zwei-Faktor-Authentifizierung für jede Organisation:

- Schützt Logins mit **Duo's MFA**
- Einsicht in einen Überblick über die **Sicherheitshygiene von Geräten**
- Verwaltung von Duo's Lösung mit **Admin APIs**
- Duo's sicherer **Single Sign-on (SSO)**
- stellt einen beständigen Benutzer-Login-Workflow über **alle Anwendungen** bereit
- Schützt den Zugriff auf sowohl **Onsite- als auch Cloud-Anwendungen**




### Essentielle Zugangssicherheits-Suite um Cloud-, BYOD- und mobile Risiken anzusprechen:

- Vollständige Einsicht in sowohl mobile Geräte als auch Desktops, inklusive **firmenverwalteter und unverwalteter Geräte** (in persönlichem Besitz) um BYOD-Richtlinien zu unterstützen
- Aufgliederung von mobilen Geräten mit Einblick in die freigeschalteten Sicherheitsmerkmale sowie **in eingegriffene und unverschlüsselte Geräte.**
- Regeln durchsetzen bezüglich wer **unter welchen Umständen auf Anwendungen zugreifen kann** (adaptive Authentifizierung)
- Eine Richtlinie durchsetzen, dass **nur verwaltete Geräte Zugang** zu sensiblen Anwendungen haben
- **Modernen Remote-Zugriff zu Multicloud-Umgebungen** bereitstellen (Onsite, Azure, AWS, Google Cloud Platform) und gleichermaßen die Zero Trust Sicherheitsprinzipien durchsetzen.
- **Benutzer** zum Update ihrer Geräte **auffordern**, basierend auf den Gerätezugangsrichtlinien
- Vollständige Dashboards und Benutzerdefinierte Berichte für **Konformitätsprüfungen** und eine Erleichterung der administrativen Verwaltung

Erfahren Sie mehr über Duo Beyond in unserer **Dokumentation**.

# Duo Security

Duo ist eine Cloud-basierte Sicherheitsplattform die den Zugang zu allen Anwendungen schützt, für jeden Benutzer und jedes Gerät, egal von wo her. Es wurde entwickelt für eine einfache Anwendung mit der Option von vollständiger Endpunkt-Sichtbarkeit und Kontrolle.

Duo überprüft die Identitäten von Benutzern mit einer starken Multi-Faktor-Authentifizierung. Zusammen mit einem tiefen Einblick in die Benutzergeräte gibt ihnen Duo die Richtlinien und die Kontrolle um Zugriff zu kontrollieren, basierend auf dem Endpunkt oder dem Benutzerrisiko. Benutzer erhalten eine einheitliche Login-Erfahrung mit Duo's Single-Sign-On. Dieser liefert zentralisierten Zugriff auf Onsite- sowie Cloud-Anwendungen.

Mit Duo können Sie sich vor kompromittierten Zugangsdaten und risikobehafteten Geräten schützen, sowie vor ungewolltem Zugriff auf ihre Anwendungen und Daten.  Diese Kombination aus Benutzer- und Gerätevertrauen bildet ein starkes Fundament für ein Zero-Trust-Sicherheitsmodell.

Starten Sie Ihre **kostenlose Testversion für 30 Tage** und schützen Sie schnell alle Benutzer, Geräte und Anwendungen.

Oder **kontaktieren Sie uns**.

# Cisco Zero Trust

Cisco Zero Trust stellt einen umfassenden Ansatz zur Sicherung des Zugriffs auf alle ihre Anwendungen und ihrer Umgebung bereit, für jeden Benutzer, jedes Gerät und jeden Ort. Es schützt ihr Personal, ihre Workloads und ihren Arbeitsplatz.

+ Cisco stellt sicher, dass ausschließlich die richtigen Benutzer und sichere Geräte auf ihre Anwendungen zugreifen können um ihr Personal zu schützen.
+ Cisco sichert alle Verbindungen mit ihren Anwendungen über die Multi-Cloud um ihre Workloads zu schützen.
+ Cisco sichert alle Benutzer und Geräteverbindungen, inklusive IoT, in ihrem Netzwerk um ihren Arbeitsplatz zu schützen.

Dieses vollständige Zero Trust Sicherheitsmodell erlaubt eine Abminderung, Erkennung und Antwort auf Risiken in ihrem gesamten Umfeld.

Erfahren Sie mehr über **Cisco Zero Trust**