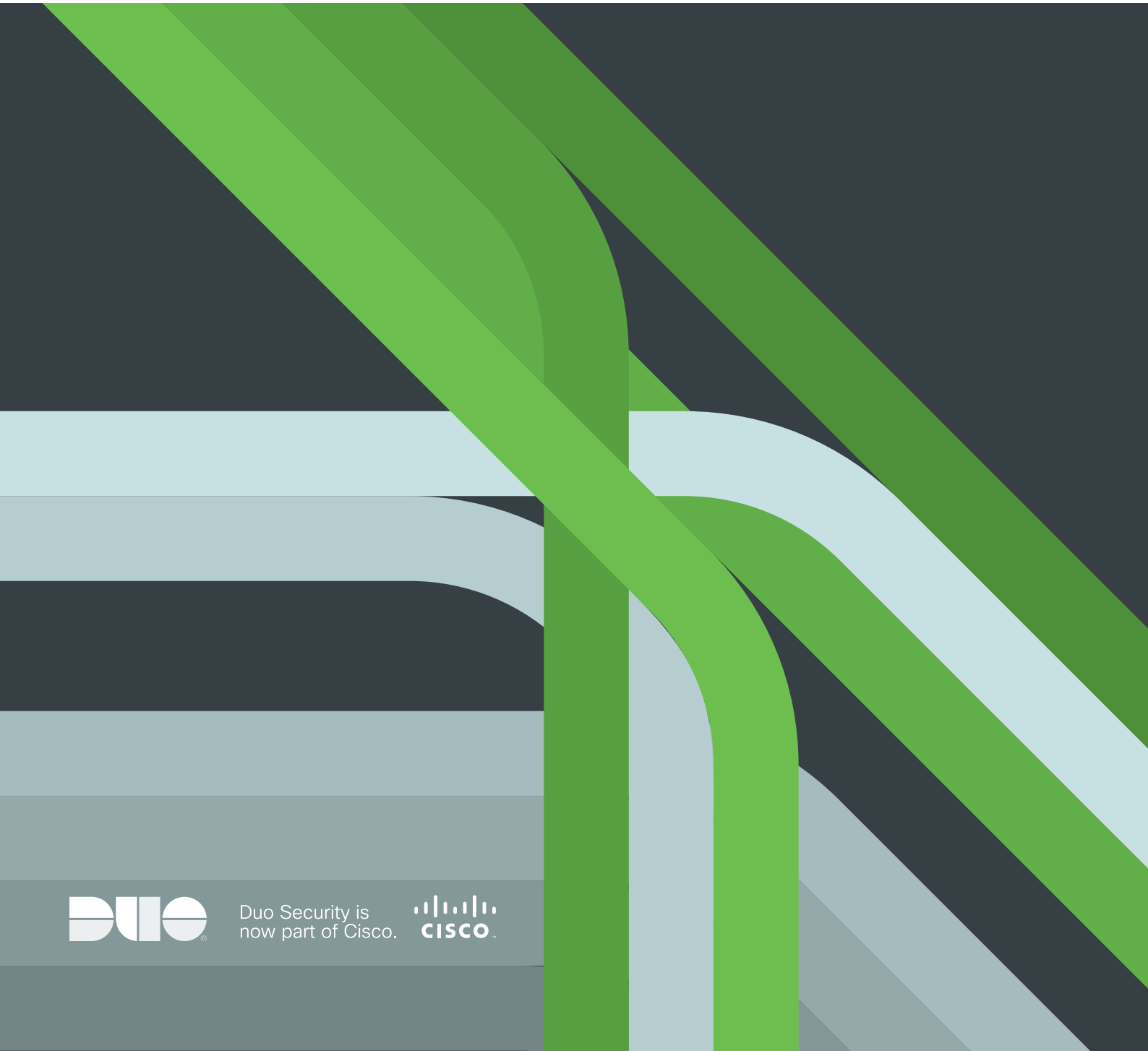
# Zero Trust Evaluierungsleitfaden

## Für die Belegschaft



Duo Security is now part of Cisco.

# CONTENTS

**Heutzutage hat die Zunahme von Mitarbeitern, die mit der Cloud verbunden sind sowie mobil und entfernt arbeiten, dazu geführt, dass die Sichtbarkeit und Kontrolle von Benutzern und Geräten außerhalb des Unternehmens liegt.**

# Warum **Zero Trust**?

**LIEFERANTEN & VERTRAGSPARTNER**

**PERSÖNLICHE & MOBILE GERÄTE**

## ORIGINAL PERIMETER

**ENDPUNKTE**
**ON-SITE BENUTZER**
**SERVER**
**APPLIKATIONEN**
**DATENZENTREN**

## NEUE IDENTITÄTS-PERIMETER

**REMOTE MITARBEITER**

**CLOUD-INFRASTRUKTUR & APPLIKATIONEN**

Der Umkreis hat sich über Unternehmenswände erweitert, was es für Sicherheits- und IT-Teams erschwert die Benutzeridentitäten sowie die Vertrauenswürdigkeit von Geräten zu überprüfen, bevor Sie beiden Zugang zu Unternehmensanwendungen und -daten gewähren.

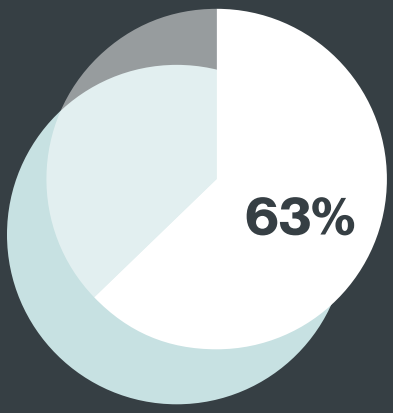
Das neue Arbeitskräftemodell erfordert heute ein ebenso erweitertes Sicherheitsmodell. **Der erweiterte Umkreis ist jetzt zentriert und um die Benutzeridentität und ihre Geräte.** Das erweiterte Sicherheitsmodell für Arbeitskräfte muss in der Lage sein, Geräte- und Benutzervertrauen zu schaffen, unabhängig davon, wo sich der Benutzer befindet, und zwar unabhängig von der Art des Netzwerks, von dem aus sie sich verbinden.

Zero Trust behandelt jeden Zugriffsversuch so als ob er von einem nicht vertrauenswürdigen Netzwerk ausgeht. **Ein vertrauenszentriertes Modell steht im Mittelpunkt zur Authentifizierung jedes Benutzers und Geräts, bevor der Zugriff auf irgendeine Anwendung gewährt wird.**

Ein Zero Trust Ansatz benötigt keine völlige Neuerfindung Ihrer Infrastruktur. Die erfolgreichsten Lösungen sollten auf einer Hybrid-Umgebung aufbauen und diese unterstützen, ohne dass sie bestehende Investitionen vollständig ersetzt.

## NEUE RISIKEN IM IDENTITÄTS PERIMETER

Kompromittierte Zugangsdaten sind vorrangig Ziel der Angreifer, welche ungeschützten Zugriff aufgrund von Phishing, roher Gewalt oder Passwortangriffen leicht ermöglichen. In einer Analyse von simulierten Phishing-Angriffen fand ***Duo's 2018 Trusted Access Report*** heraus, dass mehr als die Hälfte (63 Prozent) erfolgreich entwendete Benutzerdaten waren.



# Andere Zero Trust Modelle

Das Konzept des Null-Vertrauens zeigt sich im **Gartner's CARTA** – durchgehend adaptive Risiko- und Vertrauensbewertung. Dies erfordert eine Abkehr von einmaligen, binären Zugriffsentscheidungen hin zu kontextuellen, risiko- und vertrauensbasierten Entscheidungen. Bei diesem Modell geht es darum, den Benutzern gerade genug Vertrauen zu schenken, auch nach der Authentifizierung, um die beantragte Aktion durchzuführen.

**Forrester's Zero Trust eXtended (ZTX)** bezieht sich auf das Aufbrechen 'monolithischer Perimeter' in eine Reihe von Mikroperimetern oder Netzwerksegmente zur Anwendung granularer Sicherheitskontrollen um sie herum. Aber sie erkennen auch an, dass es viel mehr ist als nur Netzwerksegmentierung - es ist ein ganzheitlicher Ansatz zur Sicherung von Daten, Netzwerken, Geräten, Workloads und Belegschaften.

**Google's BeyondCorp** ist die Implementierung einer Zero Trust Architektur welche die sichere Identifikation von Benutzern und Geräten voraussetzt und das Vetrauen vom Netzwerk nimmt und damit eine Externalisierung von Anwendungen und Workflows, und eine Implementierung von inventarbasierten Zugriffskontrollen möglich macht.

All diese Modelle erfordern mehr Kontrollen rund um die Identität als der neue Perimeter – Benutzer und ihre Geräte beim Zugriff auf Anwendungen und Dienstleistungen. Es gibt viele verschiedene Komponenten eines Zero Trust  Modells die die Sicherung unterschiedlicher Arbeitsabläufe erfordern:

## Belegschaft

Sicherung der Benutzer und ihre Geräte während sie auf Anwendungen zugreifen.

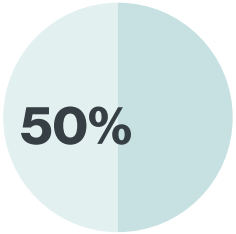
## Workload

Sichern Sie alle Verbindungen zwischen Ihren Apps, über die Multi-Cloud

## Arbeitsplatz

Sichern Sie alle Verbindungen über Ihr Netzwerk, einschließlich dem Internet der Dinge (IoT)

**Ein Ansatz besteht darin, mit dem Schutz von Benutzern und Geräten zu beginnen; Ihre Mitarbeiter – die Grundlage eines Zero Trust Modells.** Dieser Leitfaden konzentriert sich auf die Bewertung der Kriterien eines vertrauensbasierten Sicherheitsansatzes für die Belegschaft.




**Gartner** sagt voraus, dass Sicherheit als Dienstleistung auf mindestens 50 Prozent der Lieferung von Sicherheitssoftware bis 2020 darstellen wird.

# Zero Trust:
# Für die Belegschaft

Der Anwendungsbereich dieses Leitfadens konzentriert sich auf Zero Trust in Bezug auf die Sicherung Ihrer ***Belegschaft*** – d.h. die Benutzer und die Geräte die sie für den Zugriff auf Arbeitsanwendungen verwenden. Benutzer können Mitarbeiter und Partner sein,Verkäufer, Auftragnehmer und viele andere, was die Kontrolle über Geräte und Zugriffe erschwert.

Ein Zero Trust Ansatz für die Belegschaft sollte einer Organisation die Werkzeuge zur Verfügung stellen um Entscheidungen auf der Grundlage spezifischer risikobasierter Kontext auswerten und zugänglich machen zu können.

Zum Beispiel:

+ **Wird der Benutzer mittels Multi-Faktor Authentifizierung (MFA) verifiziert?**
+ **Sind ihre Geräte vertrauenswürdig und/oder verwaltet?**
+ **Erfüllen ihre Geräte Ihre Sicherheitsanforderungen?**

Sicherheitsteams müssen diese Fragen beantworten können um Vertrauen in die Benutzer und Geräte zu schaffen die auf die Anlagen einer Organisation zugreifen. Sie müssen es auch mit einem Ansatz tun, der ein Gleichgewicht zwischen Sicherheit und Benutzerfreundlichkeit schafft.

Dieser vertrauenszentrische Sicherheitsansatz für das erweiterte Perimeter erschwert es Angreifern oder unauthorisierten Benutzern Zugriff auf Anwendungen zu erhalten, ohne bestimmte Identitäts-, Geräte- und anwendungsbezogene Kriterien zu treffen.

Ziehen Sie die folgenden Schritte in Betracht, die Sie auf Ihrem Weg zum Zero Trust zur Sicherung Ihrer Belegschaft unternehmen sollten:

## Benutzervertrauen schaffen

**Können Sie überprüfen, ob Ihre Benutzer die sind, für die sie sich ausgeben? Benutzen Sie eine skalierbare, reibungslose MFA-Lösung?** Die Verwendung von MFA und die Schaffung von Vertrauen der Benutzer ist der erste Schritt zum Aufbau eines Zero Trust  Modells und zum Schutz gegen komprommittierte Zugangsdaten, Phishing und andere kennwortbasierte Angriffe.

## Einsicht in Benutzergeräte schaffen

**Haben Sie einen detaillierten Einblick in jede Art von Gerät, das auf Ihre Anwendungen zugreift, auf allenvPlattformen?** Die Transparenz in jedem Endpunkt ermöglicht es Ihnen, welche ein Risiko für Ihre Umgebung darstellen können – veraltete Software kann Sicherheitslücken enthalten, die von Angreifern ausgenutzt werden können.

## Gerätevertrauen schaffen

**Können Sie die Sicherheitslage und das Vertrauen aller Benutzergeräte überprüfen, die auf Ihre Anwendungen zugreifen? Können Sie alle Geräte und BYOD (bring your own device) sicher unterstützen- sowohl Firmen- als auch Geräte in persönlichem Besitz?** Prüfen Sie zum Zeitpunkt der Anmeldung die Vertrauenswürdigkeit des Benutzergeräts zur Bestimmung ihrer Sicherheitsaufstellung, ganz gleich wer das Gerät verwaltet oder die Kontrolle über das Gerät hat.

## Adaptive Richtlinien durchsetzen

**Können Sie granulare, kontextbezogene Richtlinien durchsetzen, die auf Benutzer, Gerät und Standort zum Schutz des Zugriffs auf spezifische Anwendungen beruhen?** Durch die Durchsetzung kontextbezogener Zugriffsrichtlinien, die das Risiko bewerten basierend auf Attributen wie Standort, Benutzerrolle, Gerät Typ, etc., können Sie eine dynamischere Kontrolle haben über wer und was auf bestimmte Anwendungen zugreifen kann – und somit nur das erforderliche Mindestmaß an Zugang erlauben damit ein Benutzer seine Arbeit erledigen kann.

## Sicheren Zugang zu allen Apps schaffen

**Können Sie Ihren Benutzern eine sichere und konsistente Login-Erfahrung sowohl vor Ort als auch in Cloud-Anwendungen geben?** Implementieren Sie MFA und Geräteeinsicht um einen sicheren Zugang zu allen Arten von Anwendungen, Diensten und Plattformen zu schaffen. Die Kombination von einem vertrauenswürdigen Benutzer und einem vertrauenswürdigen Gerät macht es schwieriger für einen nicht autorisierten Benutze, sich als eine legitime Anmeldung bei Ihren Anwendungen auszugeben.

Dieser Leitfaden wird jeden Schritt betrachten und Ihnen helfen, Ihre Kriterien und Anforderungen an die Technologie und Lösungen zur Bereitstellung von sicherem vertrauenswürdigen Zugriff von Ihren Benutzern und deren Geräten auf Arbeitsanwendungen zu formen.

01.

# Benutzervetrauen schaffen

Der erste Schritt zum Errichten von Zero Trust für Ihre Belegschaft ist die Verifizierung der Identitäten Ihrer Benutzer zum Zeitpunkt der Anmeldung in der Cloud oder Onsite-Arbeitsanwendungen, Dienste und Plattformen.

Können Sie Ihren Benutzern vertrauen, dass sie die sind, für die sie sich ausgeben? Und wie verringert man die Bedrohung durch kompromittierte Berechtigungsnachweise und Geräte, die durch Phishing, Malware und andere Vektoren verursacht werden - bei gleichzeitiger Einhaltung der datenrechtlichen Compliance-Anforderungen für die Zugangssicherheit?

# Multi-Factor Authentication

Verifizieren Sie die Identitäten Ihrer Benutzer mit einer skalierbaren, reibungsfreien Multi-Faktor Authentifizierungslösung (MFA).

## Unterstützen Sie jeden Benutzer

Bietet Ihre MFA-Lösung flexible Authentifizierungsoptionen an passend für eine Bandbreite an Benutzern, Sicherheitsprofilen und technische Hintergründe? Stellen Sie sicher, dass Ihre Lösung Mitarbeiter, Vielreisende, Auftragnehmer, Lieferanten, Kunden, Partner usw. unterstützt.

Sie sollten in der Lage sein, anzupassen und durchzusetzen, welche MFA-Methoden verwendet werden können. Für einen sichereren Zugang zu risikoreiche Anwendungen, verpflichten Sie den Einsatz von:

Benutzerfreundliche, mobile Out-of-Band-Push Benachrichtigungen

Phishing-sicherer **Universal 2nd Factor (U2F)** Sicherheitsschlüssel

Biometrie-basierter **WebAuthn**

## Erleichterung der Verwaltung

Ist Ihre MFA-Lösung für Administratoren einfach einzusetzen? Wählen Sie eine Cloud-basierte Lösung, die minimale Infrastruktur und Personaleinsatz erfordert zur Reduzierung der Belastung Ihres Teams.

Bietet es Benutzerregistrierung und skalierbare Bereitstellungsoptionen während Ihre Organisation wächst?
Zum Beispiel:

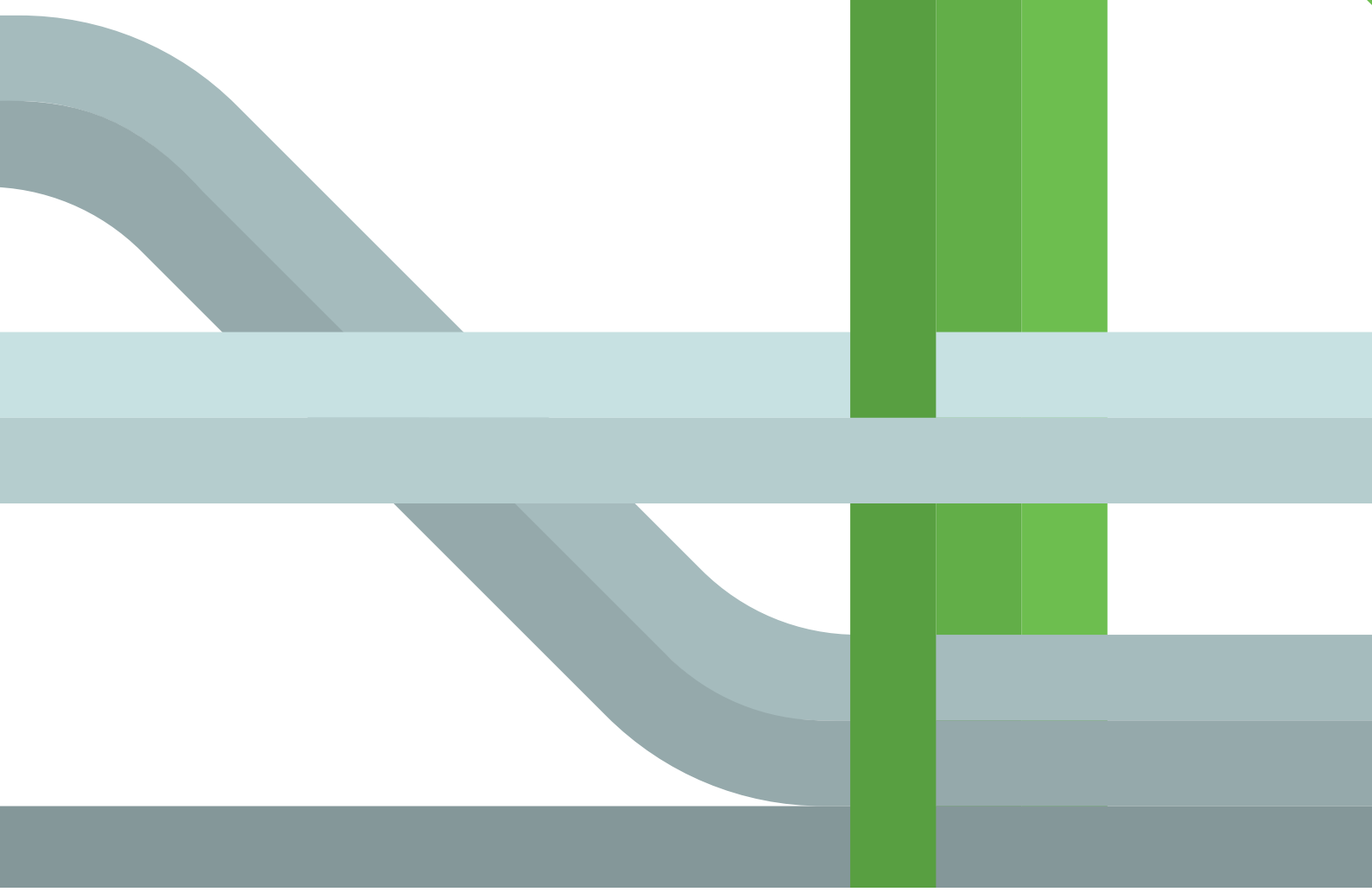
Automatische Einschreibung

Administrative APIs für eine skalierbare Benutzerbereitstellung

Option zur Synchronisierung von Benutzern aus bestehenden Verzeichnissen, wie z.B. Active Directory und Azure AD

Sparen Sie bei Trainings, Support und laufenden Help Desk Tickets mit Selbstregistrierung und Selbstbedienung.
– Lassen Sie Ihre Benutzer sich in MFA einschreiben und verwalten Sie ihre eigene Authentifizierungsgeräte ohne administrative Unterstützung.

Reduzieren Sie Risiken mit einem flexiblen, Benutzerfreundlichen und setzen sie eine Multi-Faktor-Authentifizierungslösung ein.



02.

# Einsicht in Geräte erhalten

Als nächstes evaluieren Sie, ob Ihre Lösung Einsicht in Geräte bietet die auf Ihre Anwendungen und Daten zugreifen und die Sie nutzen können, um den Zugriff zu kontrollieren, basierend auf der Gesundheit Ihrer Gerätesicherheit.

Haben Sie Sichtbarkeit für jede Art von Endbenutzergerät - mobil, Desktop und Laptops? Gibt es ein Werkzeug, das die Authentifizierung und die Endpunktdaten zentralisiert über verschiedene Geräteplattformen hinweg? Können Sie sich leicht einen Überblick über Ihre Benutzer, Endpunkte und Authentifizierungsaktivität bekommen?

# Gerätesichtbarkeit

Als nächstes evaluieren Sie, ob Ihre Lösung Einsicht in Geräte bietet die auf Ihre Anwendungen und Daten zugreifen und die Sie nutzen können, um den Zugriff zu kontrollieren, basierend auf der Gesundheit Ihrer Gerätesicherheit.

## Über alle Plattformen hinweg

Manche Gerätesichtbarkeitslösungen geben nur bedingt Einblick in bestimmte Plattformen und Betriebssysteme, wie etwa nur solche die Windows betreiben oder Desktops. Reduzieren Sie den Bedarf daran, auf verschiedene Datensysteme mit einem zentralisierten Dashboard die Admins einen Überblick verschaffen über:

### ALLE DESKTOPS, LAPTOPS & MOBILE GERÄTE

Ob Firmen- oder Privatbesitz

### BROWSER

Chrome, Firefox, Edge, Internet Explorer, etc. (Versionen, Anzahl der veralteten Geräte)

### BETRIEBSSYSTEME

Windows, Mac, iOS, Android, etc. (Versionen, Anzahl der veralteten Geräte)

### PLUGINS

Java und Flash (Versionen, Anzahl der veralteten Geräte, aktiviert, deaktiviert oder deinstalliert)

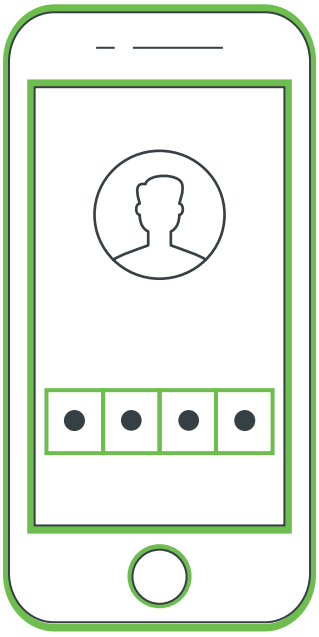
> "Zero trust demands that security teams retain visibility and control across their entire digital business ecosystem, regardless of location, device, user population or hosting model."
>
> **—Forrester Zero Trust eXtended (ZTX)**

# Unterstützen Sie BYOD & Mobile Geräte

Der erweiterte Perimeter stellt neue Herausforderungen um die Sicherung von BYOD (bring your own device). Ein Zero Trust Modell sollte auch mit Ihrer bestehenden Infrastruktur reibungslos funktionieren und jede Art von Gerät unterstützen.

Sie sollten in der Lage sein, Einblick in persönliche und Geräte im Unternehmensbesitz zu erhalten, inklusive mobile Geräte. BYO-Geräte können Ihren Sicherheitsanforderungen nicht entsprechen oder können ältere Software betreiben die anfällig für Schwachstellen ist.

Eine umfassende Lösung zur Gerätesichtbarkeit sollte es Ihnen erlauben aktivierte oder deaktivierte mobile Geräte mit bestimmten Sicherheits-Features und ihrer Sicherheitsaufstellung zu identifizieren:



**BETRIEBSSYSTEM**
iOS oder Android-Version

**DISK ENCRYPTION**

**SCREEN LOCK**

**BIOMETRIE**
Fingerabdruck, Touch oder Face ID

**GERÄTESTATUS**
Jailbroken, gerooted oder manipuliert

# Geräteprotokolle & Berichte

Viele Compliance-Vorschriften und Auditoren verlangen Protokolle und Berichte zu Benutzeraktivitäten und Gerätesicherheit. Kann Ihre Lösung für die Gerätesichtbarkeit Ihnen Zugang zu Detaillierten Berichten über Benutzerverhalten und riskante Geräte geben - alles in einem Dashboard? Integriert es sich gut mit jeder bestehenden SIEM (security information and event management) software?

Stellen Sie sicher, dass Ihre Admins leichten Zugang zu exportierbaren Berichten für Auditoren haben, mit Einsicht in Authentifizierungen, Benutzer, Admins, Richtlinien und mehr.

03.

# Gerätevertrauen schaffen

Überprüfen Sie beim Login die Gerätegesundheit aller Geräte welche versuchen auf Ihre Anwendungen zuzugreifen. Vertrauen schaffen geht über die Verwaltung des Status der Geräte hinaus für die Inspektion und Zugangskontrolle auf der Grundlage mobiler und persönlicher Geräte.

Können Sie Endpunktkontrollen für riskante Geräte oder Geräte in Unternehmensbesitz durchsetzen? Wie etablieren Sie vertrauen in mobile Geräte? Sind Sie in der Lage, automatisch Benutzer über veraltete Software zu benachrichtigen, um Ihre Helpdesk-Tickets zu reduzieren?

# Endpunktkontrollen durchsetzen

Durch die Nutzung der Sichtbarkeit von Geräten, die sich mit Ihren Anwendungen verbinden (wie in Vorherigen besprochen), sollten Sie in der Lage sein, gerätegestützte Zugriffsrichtlinien zu schaffen, um den Zugriff riskanter oder nicht vertrauenswürdiger Geräte auf Ihre Anwendungen zu verhindern.

## Risikobasierter Gerätezugriff

Für den Zugang zu risikoreichen Anwendungen muss ein Gerät womöglich im Besitz des Unternehmens sein oder von einem IT-Team Ihrer Organisation verwaltet werden. Beispiele für risikoreiche Anwendungen sind etwa elektronische Gesundheitsdatensysteme (EHR) wie Epic die die Gesundheitsdaten von Patienten enthalten; Cloud-Infrastruktur wie Microsoft Azure und Google Cloud Platform; und viele andere.

Können Sie Zugriffsrichtlinien durchsetzen, die auf dem Anwendungsrisiko oder ob es sich um ein Firmengerät handelt oder in persönlichem Besitz ist? Und können Sie dies tun, ohne dass Endpunkt-Zertifikate erforderlich sind?

Zusätzlich benötigen Sie möglicherweise MFA für den Zugang zu Sensibleren Anwendungen für ein höheres Maß an Sicherheit für die Identitäten Ihrer Benutzer. Können Sie Ihre Benutzer zu Push-Benachrichtigungen, U2F-Sicherheitsschlüssel oder biometrisch-basiertes WebAuthn verpflichten, bevor sie Zugang zu bestimmten Anwendungen gewähren?

## Vertrauen in mobile Geräte schaffen

Stellen Sie sicher, dass Ihre Lösung es Ihnen ermöglicht, mobiles Gerätevertrauen mit oder ohne Verwendung einer mobilen Gerätemanagement-Software (MDM) zu schaffen.

Benutzer können Einwände gegen die Installation von MDMs auf ihren persönlichen Geräten aufgrund von Datenschutzbedenken haben, was zu einer insgesamt niedrigeren Annahme und verringerte Einsicht in ihre Gerätesicherheit führt. Und manchmal liegt es außerhalb der Möglichkeiten Ihres IT-Teams einen Agenten auf dem persönlichen Gerät Dritter zu installieren, die auf Ihre Anwendungen zugreifen müssen.

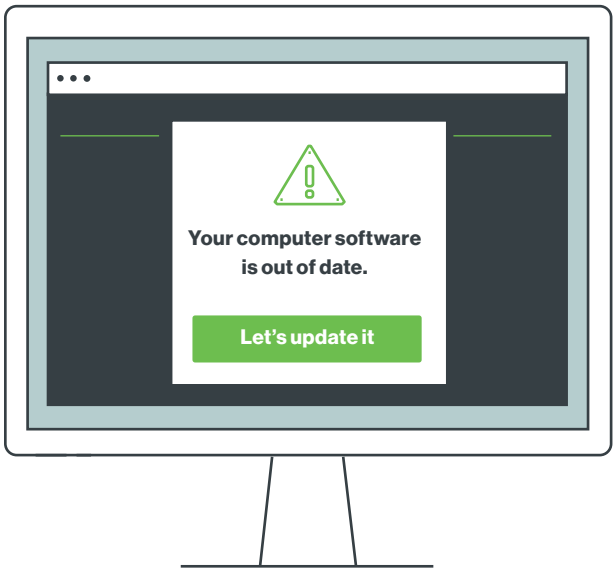
Ob Sie eine MDM-Lösung haben oder nicht, Sie sollte in der Lage sein, Geräte für den Zugriff auf Ihre Anwendungen zu blockieren, basierend auf:

+ O S, Browser und Plugin-Versionen und wie veraltet sie sind
+ Status der aktivierten Sicherheitsfunktionen (konfiguriert oder deaktiviert)
+ Full disk encryption
+ Biometrie für mobile Geräte (Face ID/Touch ID)
+ Screen lock
+ Manipuliert (jailbroken, rooted oder failed
+ Google's SafetyNet)

# Benutzer zum Update von riskanten Geräten auffordern

Ermöglicht Ihre Lösung Ihren Benutzern die Verwaltung ihrer eigenen Geräte? Wählen Sie eine Lösung, die ältere Software-Versionen feststellt und dann die Benutzer benachrichtigt, wenn ihr Gerätesoftware veraltet ist.

Fordern Sie Benutzer zu Updates ihrer Software auf ihren eigenen Geräten beim Login auf um die Arbeit Ihres Help Desk Support Teams zu erleichtern. Ein Selbstbedienungsportal ermöglicht ihnen auch ihre eigenen Authentifizierungsgeräte einfach zu verwalten ohne ein Helpdesk-Ticket einzureichen.




Setzen Sie Kontrollen und Richtlinien durch, um riskante Endpunkte vom Zugriff auf Ihre Anwendungen abzuhalten.

04.

# Adaptive Richtlinien durchsetzen

Setzen Sie kontextbezogene Zugangsrichtlinien durch die den Zugang zu Ihren Anwendungen mit Benutzer-, geräte- und standortbasierten Kontrollen erlauben. Der Kontext umfasst verschiedene Aspekte von Ihren Login-Versuchen - wo sie sich befinden, welche Rolle sie in Ihrer Organisation haben, welche Art von Gerät die sie benutzen, etc.

Beschränken Sie den Zugriff nur auf das, was Ihre Benutzer für ihre Arbeit benötigen und fügen Sie strengere Kontrollen für den Zugang zu sensibleren Anwendungen hinzu - ohne negative Auswirkungen auf Benutzer-Workflows. Können Sie Richtlinien basierend auf auf Benutzer, Benutzergruppen oder Benutzerort anpassen? Oder fordern Sie Benutzer zu einer sichereren MFA-Methode auf, basierend auf den Anwendungen, auf die sie zugreifen?

# Kontextuelle Zugangsrichtlinien

Passen Sie Richtlinien an, um strengere Sicherheit zu erlauben, zu verweigern oder zu fordern, basierend auf benutzerspezifischen Rollen und Verantwortungen, Geräte und Anwendungen – bei gleichzeitiger Abwägung von Sicherheit und Benutzerfreundlichkeit.

## Rollenbasierende Zugangsrichtlinien

Nicht alle Benutzer benötigen Zugang zu allen Anwendungen - können Sie den Zugang basierend auf der Benutzergruppe anpassen? Geben Sie Auftragnehmern oder Drittanbietern Befristeten und eingeschränkten Zugang zu nicht-sensiblen Anwendungen oder Systemen.

Sie sollten in der Lage sein, Richtlinien zur Gewährung einer höheren Zugriffsebene für Administratoren und privilegierte Benutzer durchzusetzen, wobei sichergestellt wird, dass nur Entwickler Zugriff auf Ihre Produktionsumgebungen und Cloud-Infrastruktur haben.

Prüfen Sie, ob Ihre Admins:

+ Richtlinien basierend auf dem Benutzer, der Gruppe oder deren spezifische Rollen und Verantwortlichkeiten anpassen können
+ Benutzerdefinierter Richtlinien basierend auf der Authentifizierungsmethode festlegen können
+ Benutzern nur die Authentifizierung mit bestimmten Methoden erlauben
+ Einfache Verwendung von Active Directory- oder Azure AD-Benutzergruppenrichtlinien

## Anwendungsspezifische Richtlinien

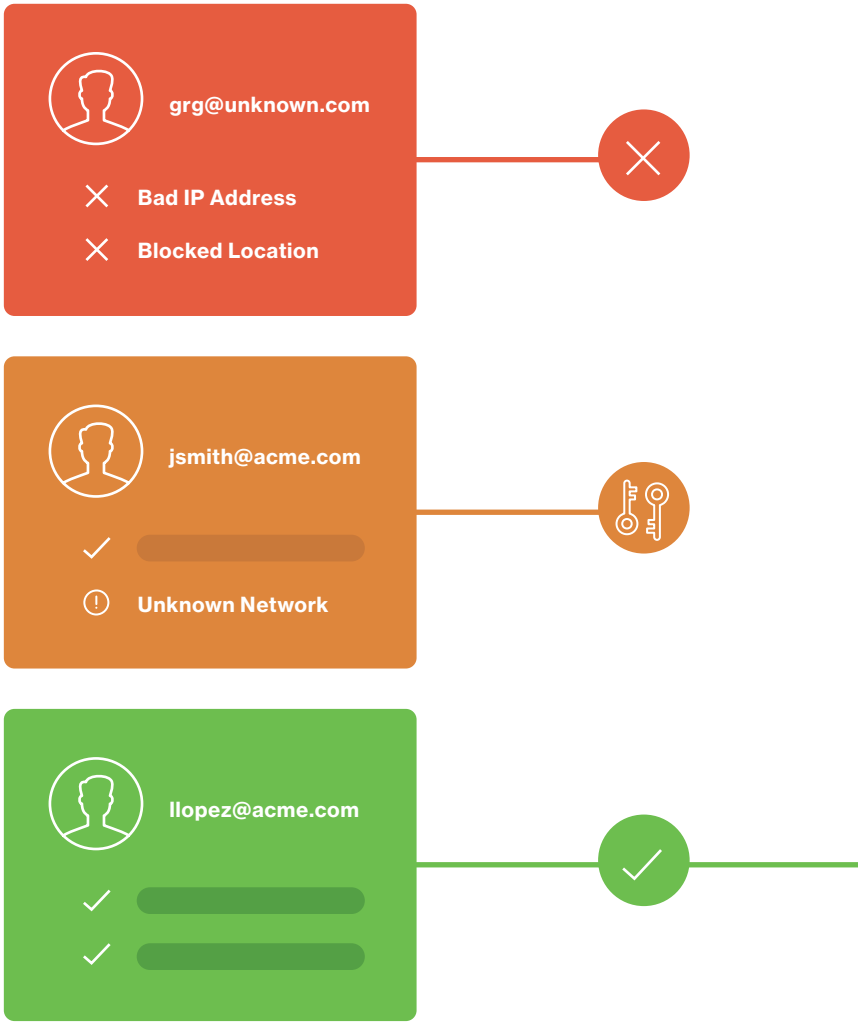
Setzen Sie die Nutzung von sichereren MFA-Methoden für den Zugang zu geschäftskritischen Anwendungen und Diensten durch um das Risiko von unauthorisiertem Zugriff zu reduzieren.

Ihre Administratoren sollten in der Lage sein, app-spezifische Richtlinien zu konfigurieren um zur Nutzung von Push-basierten oder U2F-Sicherheitsschlüsseln zu verpflichten um die Indentität Ihrer Benutzer zu verifizieren bevor Sie Zugriff auf diese Anwendungen gewähren. Die verpflichtende Nutzung von ausschließlich sicheren Methoden bietet ein höheres Maß an Sicherung der Benutzeridentität; eine Stärkung der Zugriffskontrolle für Ihre sensibleren Anwendungen und Daten.

# Standort der Benutzer

Verhindern Sie unautorisierten Zugang von jedem geographischen Standort mit Benutzerbasierten Zugriffsrichtlinien. Wenn Sie in bestimmten Ländern keine Geschäfte machen, sollten Sie in der Lage sein Zugriffsversuche aus diesen Regionen zu blockieren..

Admins sollten auch in der Lage sein, Authentifizierungsversuche zu blockieren auf der Grundlage eines Satzes von IP-Adressbereichen oder solche, die von anonymen Netzwerken wie Tor oder Proxies kommen. Nicht blockierte IP-Adressen implizieren jedoch nicht dass der Zugriff erlaubt ist - dies ist nur ein zu prüfendes Attribut im weiteren Kontext eines Zugangsantrags.




> "Shift from 'good' versus 'bad' macro decisions, toward a context-based set of smaller decisions. Give just enough trust to entities like users – even once they've been authenticated - to complete the action being requested."
>
> **—Gartner's Continuous Adaptive Risk & Trust Assessment (CARTA)**

05.

# Aktivieren Sie sicheren Zugang zu allen Apps

Geben Sie Benutzern sicheren und konsistenten Zugriff auf alle Anwendungen, Dienste und Plattformen, unabhängig davon, wo sie gehostet werden.

# Schützen Sie Ihre Investitionen

Vielleicht sind Sie eine Cloud-forward-Organisation oder ein großes Unternehmen mit einer Komplexen Mischung aus Cloud- und vorhandener Infrastruktur vor Ort und Anwendungen. Was auch immer es ist, stellen Sie sicher, dass Sie den Zugang zu allem mit MFA, kontextabhängigen Zugriffsrichtlinien sowie Sichtbarkeit und Kontrolle der Geräte schützen können.

## Fernzugriff

Der Wechsel zur Cloud-Infrastruktur hat es zu einer Herausforderung gemacht für Organisationen, stärkere Zugangskontrollen in Hybrid- und Multi-Cloud-Umgebungen anzuwenden.

Ihre Lösing sollte die Login-Erfahrung für ihre Benutzer vereinfachen und vereinheitlichen, egal wo Benutzer sich befinden, wenn sie sich mit verschiedenen Systemen und Anwendungen verbinden, die in verschiedenen Clouds gehostet werden.

Vergewissern Sie sich, dass Sie den Zugriff darauf sichern können:

- Multi-Cloud-Umgebungen, wie z.B. Azure, AWS und Google-Cloud-Plattform
- Infrastruktur, dev/DevOps Umgebungen und interne Linux-Server
- HTTPS-Webanwendungen und SSH-Server
- Virtual Private Network (VPN) und Remote-Access-Anwendungen

## Cloud/Identity Zugang

Sicherer Zugriff auf alle Ihre Cloud-Anwendungen wie Office 365, Google, Box, Dropbox, Slack, und mehr, sowie Zugang zu jedem bestehenden Single Sign-On (SSO), Identitätsanbieter und Verbandsdienste. Stellen Sie sicher, dass Ihre Lösung sicheren Zugriff auf jede SAML 2.0-fähige Cloud-Anwendung bietet.

Best Practices empfehlen, den Zugang zu diesen Apps durch Trennung Ihrer primären Authentifizierung Methode aus Ihrer Sekundarstufe (mit MFA) zu sichern. Entfernen Sie sich von einer Abhängigkeit von primärer Authentifizierung um um einen anbieterbezogenen Verstoß zu vermeiden, der das Risiko der Offenlegung von sowohl der primären als auch der sekundären Authentifizierung darstellt.

Setzen Sie strengere Sicherheitskontrollen durch, um nur zu verwalteten und aktualisierten Geräten Zugang zur Infrastruktur und Entwicklerumgebungen zu verschaffen.

# Sicherer Single Sign-On (SSO)

Für ein einheitliches Anmeldeerlebnis lassen Sie Ihre Benutzer sich einmal einloggen, um auf ihre gesamte Cloud und interne Arbeitsanwendungen mit einem sicheren Single Sign-On (SSO) Lösung zugreifen zu können.

Schützen Sie Ihr SSO mit MFA und kontextbezogenem Zugriffsrichtlinien, und überprüfen Sie die Sicherheit der Geräte Ihrer Benutzer jedes Mal, bevor der Zugang gewährt wird.


Sicheren Sie Zugang zu allen Anwendungen, Diensten und Plattformen - ob Multi-Cloud, On-Prem, Benutzerdefiniert, Fernzugriff oder VPN.

# Duo's Zero Trust für die Belegschaft

Duo liefert die Grundlage für eine Zero Trust Sicherheitsmodell durch Bereitstellung von Benutzer- und Gerätevertrauen bevor der Zugang zu Anwendungen gewährt wird - und gewährleistet Zugang für jeden Benutzer und jedes Gerät, das sich mit einer beliebigen Anwendung verbindet, von überall her.

Bei jedem Login in eine Anwendung wird das Vertrauen in die Identität und die Sicherheit der Geräte von Duo überprüft, bevor der Zugang zu den benötigten Anwendungen gewährt wird. Duo bietet Ihnen anpassungsfähige Richtlinien und Kontrollen, um Zugriffsentscheidungen auf der Grundlage des Benutzers, Geräts und Anwendungsrisikos zu treffen.

# Benutzervertrauen schaffen

Überprüfen Sie die Identität Ihrer Benutzer mit starker Multi-Faktor-Authentifizierung die eine flexible, breite Abdeckung für jede Art von Benutzer bietet.

## Multi-Factor Authentication

Beseitigen Sie die Bedrohung durch Angriffe die auf kompromittierten Zugangsdaten beruhen mit Duo's einfacher und effektiver **multi-factor authentication**. Duo's intuitive MFA macht die Anmeldung und einfaches Einloggen sicherer für Benutzer und reduziert die Reibung in Ihrem Workflow. Benutzer können schnell auf eine Taste auf einer **Duo Push** Benachrichtigung klicken die auf ihr Smartphone über die **Duo Mobile** Authentifizierungsapp zur Überprüfung ihrer Identität gesendet wird.

## Für alle Arten von Benutzern

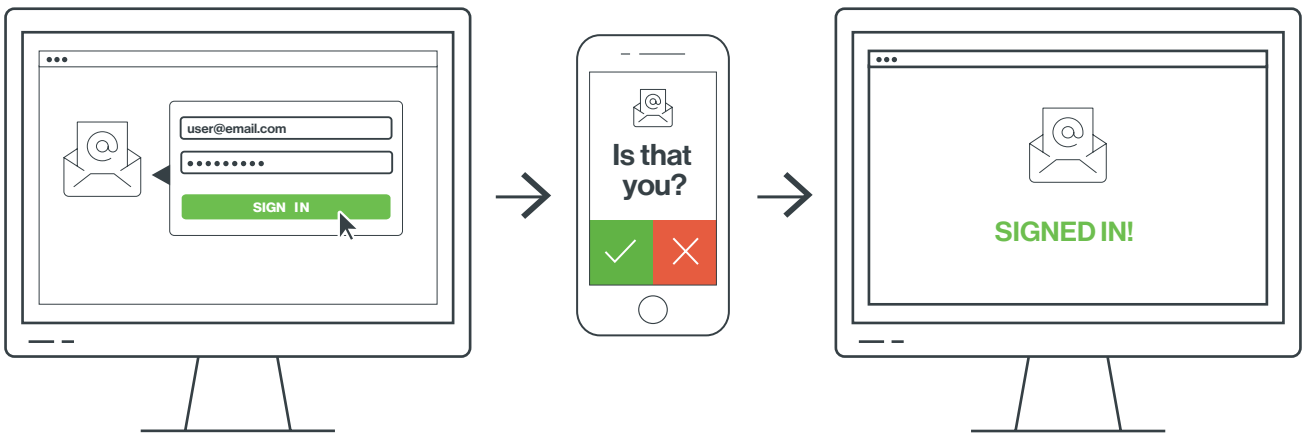
Duo's MFA funktioniert gut mit allen Benutzergruppen im Unternehmen, wie Mitarbeiter, Vertragspartner, Händler, Partner etc., durch die Unterstützung von gruppenspezifischen Zugangsrichtlinien.

Konzipiert zur Unterstützung jedes Szenarios der Benutzeranmeldung vom Offline- zum eingeschränkten Zelldienst und Internet-Konnektivität bietet Duo viele verschiedene **MFA Methoden**, inklusive Mobil-Apps, Push-Benachrichtigungen, Offline-Optionen, **Biometrie-basiertes WebAuthn**, Sicherheitsschlüssel und mehr.

Zusätzlich können Ihre Admins zur Nutzung von bestimmten Methoden für den Zugang zu sensibleren Daten verpflichten um die Identitäten Ihrer Benutzer genauer zu überprüfen.

## Leicht zu implementieren

Admins profitieren von Duo's nativer Integrationen, einfacher Cloud-basierte Einrichtung und wartungsarmer Lösung. Duo's automatisierte Anmeldungsoptionen wie **Benutzer-Selbstregistrierungs** und Active Directory-Synchronisierungsoptionen ermöglichen skalierbare Benutzer-Bereitstellung. Zur Reduzierung von Helpdesk-Tickets und Verwaltung ermöglicht das **Self-Service-Portal** von Duo Benutzern schnell und einfach die Nutzung ihrer eigenen Authentifizierungsgeräte.



# Erhalten Sie Einsicht in Benutzergeräte

Erhalten Sie detaillierte Einsicht in die Geräte Ihrer Benutzer mit Duo's **Endpunkt-Einsicht** und einer einzelnen Ansicht des gesamten **Sicherheitsstatus** mit Duo's Admin Panel das riskante Geräte markiert.

## Auf jeder Plattform

Erhalten Sie **vollständige Einsicht** in mobile, Laptop, Desktop and PC-Geräte auf jeder Plattform (Windows, Mac, iOS, Android und Chrome). Identifizieren und überwachen Sie Geräte in Unternehmens- und Privatbesitz, um Einblicke in ihre Sicherheitslage zu erhalten.

## Unterstützen Sie BYOD & Mobile Geräte

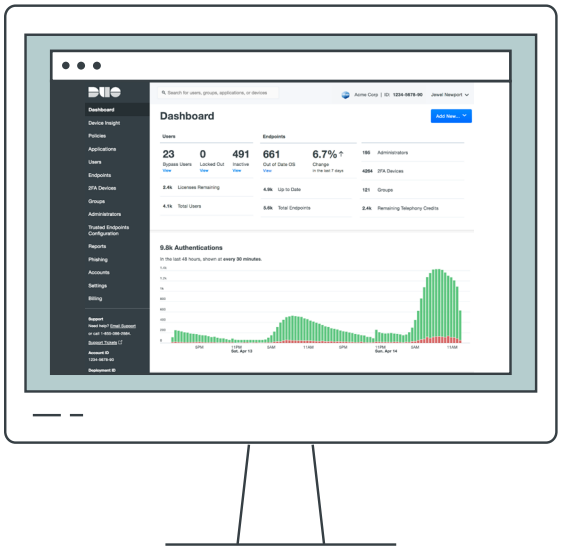
Erhalten Sie größere Einsicht in BYOD-Geräte und Kontrollen mit Duo's Plattform welche jedes Gerät erkennt was auf geschützte Anwendungen zugreifen will, inklusive Desktop-, Laptop- and mobile Geräte - ohne einen Agenten zu verwenden.

Identifizieren Sie sowohl durch Unternehmens-IT-geführte als auch private Geräte mit Duo's **vertrauenswürdigen Endpunkten**. Nutzen Sie bestehende Gerätemanagementinfrastruktur um Gerätevertrauen herzustellen und durchzusetzen mit Duo's Integrationen mit Active Directory, Airwatch, Google, Jamf, Landesk, MobileIron und Sophos ohne eine komplexe PKI-Zertifikatsinfrastruktur verwalten zu müssen.

## Zentralisiertes Dashboard

Admins erhalten ein zentralisiertes, intuitives Interface um einfach Benutzer, Geräte und Richtlinien global verwalten zu können, sowie Sicherheitsberichte und Protokolle für Konformitätsprüfungen.

Die **detaillierten Berichte** von Duo geben den Admins Daten zum Benutzerverhalten und risikoreichen Geräten, sowie Benutzer-, Admin- und Telefondaten – alle leicht integrierbar mit vorhandenen Sicherheitsinformationen und Ereignisverwaltungs (SIEM)-Systemen.



# Gerätevertrauen schaffen

Duo stellt Einsicht in Benutzer und Geräterisiken bereit und bietet die Möglichkeit, Kontrollen anzuwenden, Bedrohungen verhindern und riskante Geräte vom Zugriff auf sensible Anwendungen und Daten abzuhalten.

## Risikobasierter Gerätezugriff

Admins können die Richtlinien der BYOD unterstützen, indem sie Endpunkte als **vertrauenswürdig oder nicht vertrauenswürdig** markieren, und gleichzeitig Richtlinien durchsetzen die stärkere Sicherheit benötigen oder den Zugang von nicht vertrauenswürdigen Geräten beschränken.

## Vertrauen in mobile Geräte schaffen

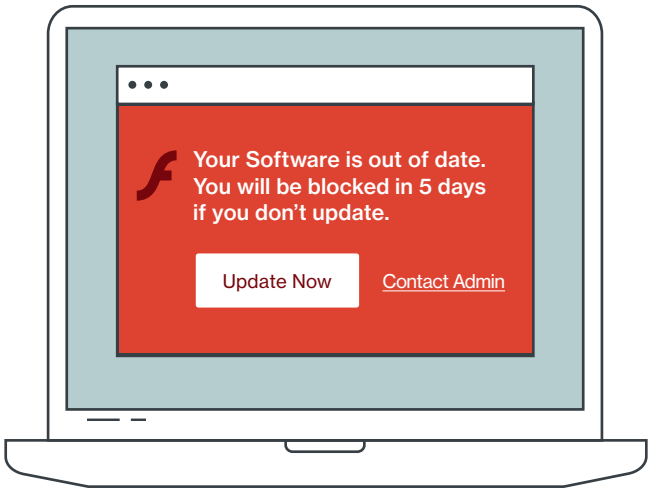
Mit **Duo Mobile für vertrauenswürdige Endpunkte** können Sie Geräte vom Zugriff auf Ihre Anwendungen blockieren, auf Basis von:

+ Betriebssystem-, Browser- und Plugin-Versionen und wie lange sie veraltet sind
+ Status der aktivierten Sicherheitsmerkmale (konfiguriert oder deaktiviert):
+ Full disk encryption
+ Biometrie für mobile Geräte (Gesichts-ID/ Touch-ID)
+ Screen lock
+ Manipuliert (jailbroken, geortet oder failed Googles Sicherheitsnetz)

Die Duo Mobile-Anwendung, die auf den Telefonen Ihrer Benutzer installiert ist kann als Ihr Android/ iOS-verwaltetes Verifizierungswerkzeug dienen.

## Benutzer zur Aktualisierung von risikoreichen Geräten benachrichtigen

Um Ihr Helpdesk-Team zu entlasten und Support-Tickets reduzieren benachrichtigt und unterstützt Duo's **Self-Remediation** Benutzer bei der Aktualisierung veralteter Geräte. Informieren Sie die Benutzer darüber, dass ihnen der Zugang verweigert wird in eine bestimmte Anzahl von Tagen, sofern sie nicht aktualisiert werden, und bieten Sie eine direkte Verbindung zur Aktualisierung ihrer Software an, um Sicherheitslücken schneller zu schließen.



# Adaptive Richtlinien durchsetzen

Duo bietet Ihnen die Kontrollmöglichkeiten, um den Zugriff risikobehafteter Endpunkte und Benutzer auf Anwendungen auf der Grundlage des bedingten Risikos zu beschränken (adaptive Authentifizierung).

## Rollenbasierte Zugangsrichtlinien

Das Prinzip des geringsten Privilegs bedeutet Beschränkung des Zugangs zu Daten und Anwendungen durch Personen, die Zugang brauchen um ihre Arbeit zu tun. Duo ermöglicht es Ihnen, rollenbasierte Zugangskontrollen festzulegen und den Zugang zu Anwendungen zu beschränken, die auf den Rollen und Aufgaben der Benutzer basieren.

Sie können zum Beispiel die Duo-Richtlinien verwenden um sicherzustellen, dass nur Entwickler Zugang zu kritischer Infrastruktur gehostet in AWS erhalten - und dass sie nur mit von Unternehmen ausgegebenen Geräten darauf zugreifen können, mit dem neuesten Betriebssystem, unter Verwendung der sicheren MFA-Methode Duo-Push.

## App-spezifische Richtlinien

Setzen Sie die Verwendung von sichereren MFA Methoden (Duo-Push, U2F, etc.) durch für den Zugang zu risikoreichen Anwendungen und Diensten (z.B. in den Bereichen Finanzen, Gesundheit, HR oder andere sensible Daten) für eine höhere Ebene der Sicherung der Identität Ihrer Benutzer. Benutzer müssen sich für jede neue Sitzung authentifizieren, die Benutzer werden nach einer festgelegten Zeitspanne dazu aufgefordert.

## Standort des Benutzers

Zur Einhaltung der regionalen Datenschutzgesetze, müssen Sie möglicherweise Zugriffsrichtlinien basierend auf dem Standort durchsetzen. Um dies zu tun lässt Duo Richtlinien für die Gewährung oder Verweigerung des Zugriffs auf Ihre Anwendungen einrichten, aufgrund von woher der Benutzer/das Gerät kommt (ein Satz von IP-Adressbereichen).

Sie können MFA auch für bestimmte Standorte festlegen.  Plus, Duo ermöglicht es Ihnen Authentifizierungsversuche an Ihre Anwendungen von anonymen Netzwerken wie Tor und Proxies zu blockieren.

# Sicheren Zugriff auf alle Apps ermöglichen

Duo bietet **breite Abdeckung für jede Anwendung,** mit Out-of-the-box-Integrationen für eine einfache Einrichtung mit allen Arten von Anwendungen – von legacy bis moderne und kundenspezifische Tools. Für Benutzerdefinierte Anwendungen bietet Duo auch APIs, WebSDKs und Unterstützung für andere Protokolle, um es Ihnen zu ermöglichen die Sicherheitsplattform von Duo zu erweitern, um proprietäre Dienste zu schützen.

Duo bietet flexiblen, reibungslosen Zugang zu Hybrid- und Multi-Cloud-Umgebungen, die es Ihnen erlaubt, einen Zero Trust Sicherheitsansatz für Fernzugriff auf Cloud-Infrastruktur und Unternehmensanwendungen anzuwenden.

## Remote-Zugriff

Schützen Sie sich vor kompromittierten Zugangsdaten und sichern Sie den Zugriff auf Ihre Remote Gateway Provider mit Duo's Integration für Virtual Private Networks (VPNs), Virtual Desktop Infrastructure (VDI) und Proxies wie etwa Cisco AnyConnect, Juniper, F5, Citrix und andere.

## Cloud/Identity Zugang

Da Organisationen ihre Anwendungen und Infrastruktur in die Cloud migrieren, kann Duo sowohl eine Hybrid- als auch eine Multi-Cloud-Umgebung vollständig schützen. Duo bietet Benutzern einen konsistenten Fernzugriff auf Multi-Cloud- und hybride Umgebungen, einschließlich Cloud-Infrastrukturanbieter, sowie vor Ort und Cloud-Anwendungen.

Duo unterstützt Anwendungsfälle für den Cloud-Zugriff, wie zum Beispiel Entwickler, die auf Amazon Web Services (AWS) zugreifen und Auftragnehmer, die Fernzugriff auf interne Anwendungen benötigen. Der MFA von Duo ist auch mit anderen SSOwie Ping, Azure, Okta, Orakel und Shibboleth integriert; er bietet Identitätsintegration mit AD und SAML.

## Secure Single Sign-On (SSO)

Benutzer erhalten eine einheitliche Anmeldeerfahrung mit Duo's Single Sign-On, das den zentralen Zugriff auf beide Vor-Ort- und Cloud-Anwendungen bietet. Reduzieren Sie Passwortermüdung und steigern Sie die Produktivität der Anwender, indem Sie es Ihren Benutzern erlauben sich nur einmal bei Duo's **Single Sign-On (SSO)** anmelden um auf alle ihre Apps zuzugreifen. Duo's sicherer SSO überprüft die Gerätesicherheit jedes Mal, bevor der Zugriff auf jede Anwendung erlaubt wird.

## Tech Partner

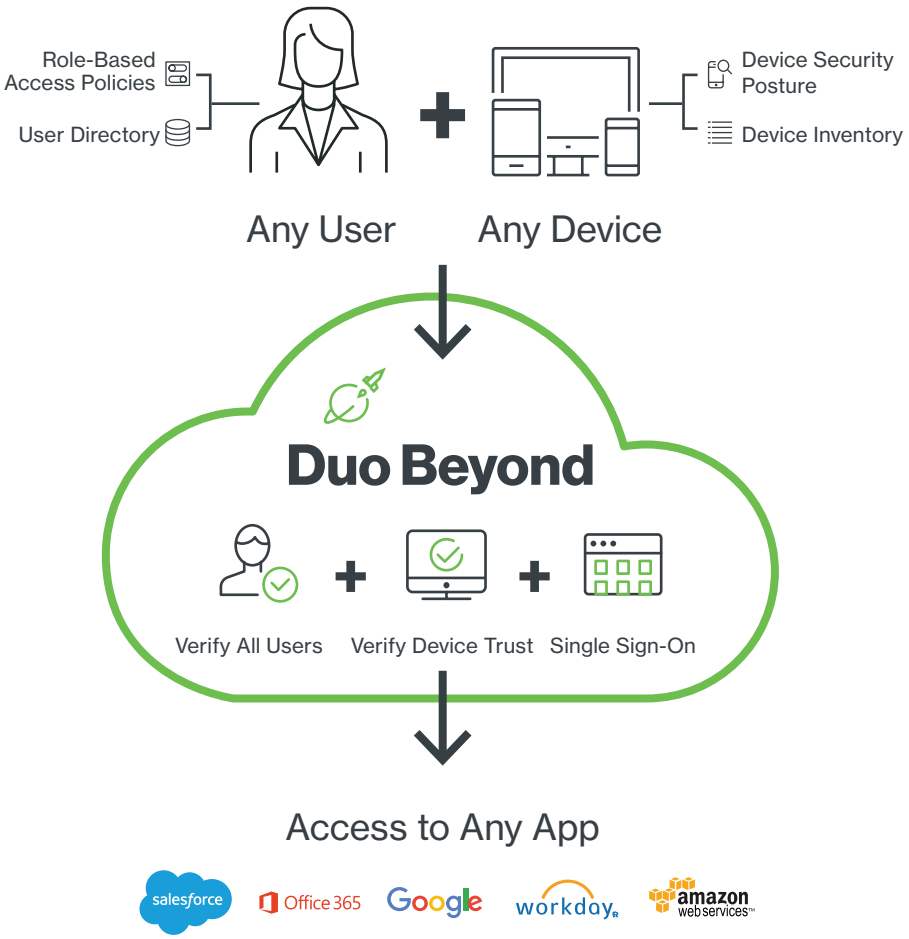
Duo's Partnerschaften in den Bereichen **Technologie und Sicherheit** geben Ihnen die vereinfachte Möglichkeit Komplexität zu beseitigen und gleichzeitig Ihre bestehenden IT-Investitionen zu schützen. Unsere technischen Partner (Microsoft, Cisco, Workday, Citrix, VMware und viele andere) decken Identitäts- und Zugangsmanagement ab; Netzwerk und Fernzugriff; Endpunktverwaltung und -sicherheit; Erkennung und Reaktion; sowie beliebte Geschäftsanwendungen.

# Beginnen Sie Ihre Zero Trust Erfahrung mit Duo Beyond

# Duo Beyond

In **Duo Beyond**, erhalten Sie:

**Voll ausgestattete Zwei-Faktor Authentifizierung für jede Organisation:**




- Geschützte Logins mit **Duo's MFA**
- Einblick in eine Übersicht **der Sicherheitshygiene der Geräte**
- Verwalten der Duo-Lösung mit **Admin-APIs**
- Duo's sicherer **Single Sign-On (SSO)** bietet einen konsistenten Workflow für die Benutzeranmeldung über alle Anwendungen hinweg
- Schützen Sie den Zugang sowohl zu den Räumlichkeiten vor **Ort als auch Cloud-Anwendungen**

## Unentbehrliches Sicherheitspaket für Cloud-, BYOD- und mobile Risiken:

- Vollständige Transparenz sowohl für mobile als auch Desktops, einschließlich von **Unternehmen verwalteter und nicht verwalteter** (in persönlichem Besitz) Geräte zur Unterstützung der BYOD-Richtlinien
  - Überblick über mobile Geräte mit Sichtbarkeit in aktivierte Sicherheitsfunktionen und **manipulierte oder unverschlüsselte Geräte**
- Setzen Sie Regeln durch bezüglich w**er auf welche Anwendungen unter welchen Bedingungen zugreifen kann** (adaptive Authentifizierung)
- Das Durchsetzen einer Richtlinie, die **nur verwalteten Geräten** Zugriff auf sensible Anwendungen gewährt
- Bereitstellung eines modernen Fernzugriffs auf Multi-Cloud Umgebungen (On-site, Azure, AWS, Google Cloud Plattform) bei gleichzeitiger Durchsetzung von Zero Trust Prinzipien
- **Benutzer benachrichtigen**, ihre Geräte zu aktualisieren müssen,
- basierend auf Richtlinien für den Gerätezugriff
- Identifizieren Sie Benutzer, die für Phishing durch **Phishing-Kampagnen anfällig sind**
- Vollständig ausgestattete Dashboards und Benutzerdefinierte Berichte für **Konformitätsprüfungen** und Erleichterung der administrativen Verwaltung

Learn more about Duo Beyond in our **documentation**.

# Duo Security

Duo ist eine Cloud-basierte Sicherheitsplattform, die Zugang zu allen Anwendungen schützt, für jeden Benutzer und jedes Gerät, von überall her. Es ist so konzipiert, dass es sowohl einfach zu bedienen und bereitzustellen ist und gleichzeitig eine vollständige Endpunkttransparenz und Kontrolle bietet.

Duo verifiziert Benutzeridentitäten mit starkem Multi-Faktor-Authentifizierung. Gepaart mit tiefer Einsicht in die Geräte Ihrer Benutzer bietet Duo die Richtlinien und Kontrollen die Sie für das Begrenzen von Zugang benötigen, basierend auf dem Endpunkt und dem Benutzerrisiko. Benutzer erhalten eine einheitliche Anmeldeerfahrung mit Duo's Single Sign-On, das einen zentralen Zugang zu sowohl standortbasierte als auch Cloud-Anwendungen liefert.

Mit Duo können Sie sich vor kompromittierten Zugangsdaten und riskanten Geräten schützen, ebenso vor ungewolltem Zugriff auf Ihre Anwendungen und Daten. Die Kombination von Benutzer- und Gerätevertrauen stellt ein starkes Fundament für ein Zero Trust Sicherhetsmodell dar.

Erhalten Sie eine **kostenlose Testversion für 30 Tage** und schützen Sie schnell alle Benutzer, Geräte und Anwendungen. Oder **kontaktieren Sie** uns.

# Cisco Trusted Access

Mit dem vertrauenszentrierten Modell von Cisco erhalten Sie einen Praktischen Zero Trust Ansatz für Sicherheit. Sichern Sie Ihre Belegschaft unterwegs, Workloads in vielen Clouds, und Geräte außerhalb Ihrer Kontrolle. Cisco Trusted Access macht es einfach und sicher, Zugang zu gewähren und einzuschränken durch Vertrauensbildung und softwaredefiniertem Zugriff auf der Grundlage eines dynamischen Kontexts.

Cisco Trusted Access hilft Ihnen drei primäre Bedürfnisse zu befreidigen:

**Belegschaft**
Überprüfung der Benutzeridentität und der Gerätehygiene vor der Erteilung von Zugriff auf Ihre Cloud- und On-Premises-Anwendungen.

**Arbeitsplatz**
Überprüfen Sie konforme Geräteprofile vor der Erteilung von Softwaredefiniertem Zugang zu Ihrem segmentierten Netzwerk..

**Workload**
Verifizieren des Anwendungsverhaltens zur Implementierung von Mikro-Segmentierung über das firmeninterne Rechenzentrum und Multi-Cloud-Infrastruktur.

Erfahren Sie mehr über **Cisco Trusted Access**