Zero Trust am Arbeitsplatz

Sorgen Sie dafür das nur die richtigen Benutzern und ihre Geräte auf freigebenen Applikationen zugreifen können.

Ein Zero-Trust-Ansatz für die Belegschaft stellt die Grundlage für ein Zero Trust Sicherheitsmodell dar. Es soll die Vertrauenswürdigkeit von Benutzern und Geräten sicherstellen bevor ihnen Zurgriff gewährt wird.

Ist ihr Gerät sicher und vertrauenswürdig?

Ist der Benutzer wer er zu sein vorgibt?

Hat der Benutzer Zugriff auf die richtigen Anwendungen?

Zero Trust am Arbeitsplatz ist eine Komponente des Zero Trust-Rahmenprogramms von Cisco. Es ist eine dreiteilige Zero Trust-Plattform, die workforce (Mitarbeiter), workloads (Arbeitsauslastung) und workplaces (Arbeitsplätze) umfasst.

Bauen Sie das Vertrauen der Nutzer auf

Überprüfen Sie die identität Ihrer Benutzer mit einer leistungsfähigen Multi-Faktor Authentifizierung (MFA), die jeden Benutzertyp flexibel und umfassend abdeckt.

- Verhindern Sie Bedrohungen wie Angriffe auf Grund von kompromittierten Anmeldeinformationen dank der einfachen und effektiven MFA Authentifizierung.
- Vereinfachen Sie die Benutzerregistrierung und sichere Anmeldung und sorgen Sie somit für einen reibungslosen Arbeitsablauf – die Benutzer bestätigen Ihre Identität Tippen auf eine Push-Benachrichtigung welche durch die Duo Mobile-App an ihr Smartphone gesendet wird.
- Unterstützen Sie gruppenspezifische Zugriffsrichtlinien für alle Benutzergruppen, einschließlich Mitarbeitern, Auftragnehmern, Anbietern, Kunden, Partnern usw.
- Unterstützen Sie alle Anmelde-Szenarios für Benutzer mit unterschiedlichen MFA-Methoden (Mobile Apps, Push-Benachrichtigungen, Offline-Optionen, biometrisch basierte WebAuthn, Sicherheitsschlüssel und mehr).
- Skalieren Sie das User-Provisioning mit automatisierten Anmeldeoptionen wie Benutzer-Selbstregistrierung und Active Directory-Synchronisierung.
- Reduzieren Sie Tickets und Management des Helpdesks über ein Self-Service-Portal zur schnellen und einfachen Verwaltung der Authentifizierungsgerate durch die Benutzer.

Transparenz von Nutzergeräten schaffen

Erhalten Sie einen detaillierten Überblick über die Geräte Ihrer Benutzer dank der Endpunkttransparenz von Duo und einer zentralen Ansicht aller Sicherheitszustände mit dem Duo-Admin-Panel, das risikobehaftete Geräte markiert.

- Schaffen Sie umfassende Transparenz auf allen Plattformen (Windows, Mac, iOS, Android und Chrome) für Mobilgeräte, Laptops, Desktops und PCs
- Erkennen und überwachen Sie unternehmenseigene sowie persönliche Geräte, und erhalten Sie einen Einblick in ihre Sicherheitsaufstellung mit den Trusted Endpoints von Duo
- Die Duo-Plattform bietet Ihnen einen umfassenderen Überblick sowie Kontrolle über BYOD, indem jedes Gerät mit Zugriff auf geschützte Anwendungen erfasst und zurückverfolgt werden kann, einschließlich Desktops, Laptops und Mobilgeräten ohne Einsatz eines mobilen Agenten.
- Ihre vorhandene Gerätemanagement-Infrastruktur kann zur Einrichtung und Durchsetzung von Gerätevertrauen mit Duo-Integrationen in Active Directory, AirWatch, Google, Jamf, Landesk, MobileIron und Sophos ohne erforderliche Bereitstellung und Verwaltung einer komplexen PKI-Zertifikatinfrastruktur genutzt werden.
- Eine zentralisierte, intuitive Benutzerschnittstelle ermöglicht ein einfaches Management von Benutzern, Geräten und Richtlinien weltweit sowie van Sicherheitsberichten und Protokollen für Compliance-Audits
- Erhalten Sie detaillierte Daten und Berichte zu Benutzerverhalten und risikobehafteten Geräten sowie Benutzer-, Administrator- und Telefoniedaten um diese problemlos mit bestehenden SIEM-Systemen (Security Information and Event Management) zu integrieren.

Device Trust einrichten

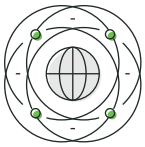
Erhalten Sie Transparenz über Benutzer- und Geräterisiken, und wenden Sie Kontrollen an, die verhindern, dass Bedrohungen und risikobehaftete Geräte Zugriff auf vertrauliche Anwendungen und Daten erhalten.

- Markieren Sie Endpunkte als vertrauenswürdig oder nicht vertrauenswürdig und folgen Sie damit BYOD-Richtlinien. Setzen Sie gleichzeitig Richtlinien für großere Sicherheit oder beschränkten Zugriff durch nicht vertrauenswürdige Geräte durch.
- Verifizieren Sie verwaltete Android- und iOS-Gerate mit der Duo Mobile-App auf den Telefonen Ihrer Benutzer.
- Mit Self Remediation von Duo lassen sich Sicherheitslücken schneller schließen und somit der Helpdesk durch reduzierte Support-Tickets entlasten. Über diese Funktion werden Benutzer benachrichtigt, ihre veralteten Geräte zu aktualisieren. Sie werden informiert, dass ihnen der Zugriff innerhalb einer bestimmten Anzahl von Tagen verweigert wird, wenn sie keine Aktualisierung vornehmen. Zudem wird ein direkter Link zur Aktualisierung der Benutzer-Software bereitgestellt.
- Blockieren Sie den Zugriff auf Ihre Anwendungen von Geräten, basierend auf:
  - Betriebssystem-, Browser- und Plugin-Versionen und darauf, wie lange diese veraltet sind
  - Status von aktivierten Sicherheitsfunktionen (konfiguriert oder deaktiviert):
    - Vollständige Festplattenverschlüsselung
    - Biometrie für Mobilgeräte (Face ID/Touch ID)
    - Bildschirmsperre
    - Manipulation (Jailbroken, Rooted oder im Google SafetyNet gescheitert)

Adaptive Richtlinien durchsetzen

Schränken Sie das Zugangsrecht für risikobehaftete Endpunkte und Benutzer auf Anwendungen ein, die bedingte Risiken aufweisen (adaptive Authentifizierung).

- Legen Sie rollenbasierte Zugriffskontrollen an, und beschränken Sie den Zugriff auf Anwendungen je nach Benutzerrolle und Zuständigkeit.
- Legen Sie die Verwendung sicherer MFA-Methoden (Duo-Push, U2F usw.) für den Zugriff auf Anwendungen und Services mit hohem Risiko (z. B. mit Finanz-, Gesundheits-, HR- oder anderen vertraulichen Daten) für eine höhere Sicherheit der Benutzeridentitäten fest.
- Verplichten Sie die Benutzer sich für jede Sitzung erneut zu authentifizieren, wozu die Benutzer nach einer bestimmten Zeitspanne aufgefordert werden.
- Durch das festlegen von standortbasierte Richtlinien kann der Zugriff auf Ihre Anwendungen je nach Herkunftsort des Benutzers bzw. Geräts (eine Reihe von IP-Adressbereichen) gewährt oder verweigert werden. Für bestimmte Standorte können Sie erforderliche MFA-Authentifizierung einführen.
- Blockieren Sie Authentifizierungsversuche für Ihre Anwendungen von anonymen Netzwerken wie Tor und Proxys.



Ermöglichen Sie sicheren Zugriff auf alle Apps

Dank der einfachen und umfassenden Anwendungsabdeckung von Duo können Sie über Out-of-the-box-Integrationen alle Arten von Anwendungen, von veralteten bis modernen und benutzerdefinierten Tools einrichten.

- Schützen Sie benutzerdefinierte Anwendungen und proprietäre Services mit APIs, WebSDKs, und unterstützen Sie andere Protokolle, um die Sicherheitsplattform von Duo zu erweitern und somit proprietäre Services zu schützen.
- Setzen Sie einen Zero Trust-Sicherheitsansatz für den Remote Access auf Cloud-Infrastrukturen und Unternehmensanwendungen mit flexiblem, reibungslosem Zugriff auf Hybrid- und Multi-Cloud-Umgebungen ein.
- Schützen Sie sich vor kompromittierten Anmeldeinformationen, sowie den Zugriff auf Ihre Remote-Access-Gateway-Provider mit Duo-Integrationen für Virtual Private Network (VPNs), Virtual Desktop Infrastructure (VDI) und Proxys wie Cisco AnyConnect, Juniper, F5, Citrix und mehr.
- Der konsistente Remote Access von Duo schützt Hybrid- und Multi-Cloud-Umgebungen, Cloud-Infrastruktur-Provider sowie OnPremises- und Cloud-Anwendungen.
- Leisten Sie Support für Cloudzugriffe, z. B. für Entwickler, die auf Amazon Web Services (AWS) zugreifen, und Auftragnehmer, die einen Remote Access auf interne Anwendungen benötigen.
- Durch eine einheitliche Benutzeranmeldung reduzieren Sie die Passwort-Ermüdung, und erhöhen Sie die Produktivität der Benutzer, indem Sie den ihnen ermöglichen, sich nur einmal anzumelden, um auf alle ihre Anwendungen mit Single Sign-on (SSO) von Duo zuzugreifen, wodurch ebenfalls die Gerätesicherheit immer überprüft wird, bevor Zugriff auf die jeweilige App gewährt wird.
- Schaffen Sie eine einfache Integration in andere bereitgestellte SSO-Services wie Ping, Azure, Okta, Oracle und Shibboleth und eine Identitätsintegration in AD und SAML über die MFA-Authentifizierung von Duo.
- Schützen Sie Ihre vorhandenen IT-Investitionen und reduzieren Sie die Komplexität dank des Technologie- und Sicherheitspartnernetzwerks von Duo. Das Netzwerk umfasst Partner (Microsoft, Cisco, Workday, Citrix, VMware und viele andere) die Identitäts- und Zugriffsmanagement, Netzwerkzugriff und Remote Access, Endpunkt-Management und -Sicherheit, Aufdeckung und Reaktion sowie beliebte Geschäftsanwendungen bereitstellen.

"Duo is the partner we rely on in our journey towards a zero-trust model."

Andrew Spenceley
Cyber Security Architect, University of Sunderland

"Duo Beyond has enabled us to push our zero-trust strategy faster."

Mike Johnson
CISO, Lyft

Starten Sie Ihre kosstenlose 30-Tage-Testversion und beschützen Sie alle Ihre benutzer, Geräte und Anwendugen auf **duo.com**.

Duo Security

Duo ist eine Cloud-basierte Sicherheitsplattform, die den Zugriff auf alle Anwendungen für jeden Benutzer und jedes Gerät von überall aus schutzt. Es ist so konzipiert, dass es sowohl einfach zu verwenden als auch bereitzustellen ist und gleichzeitig vollständige Sichtbarkeit und Kontrolle des Endpunkts bietet.

Duo überprüft die Identität der Benutzer mit einer starken Multi-Faktor Authentifizierung. Zusammen mit umfassenden Einblicken in die Geräte Ihrer Benutzer bietet Duo Ihnen die Richtlinien und die Kontrolle, die Sie benötigen, um den Zugriff basierend auf dem Endpunkt- oder Benutzerrisiko zu beschränken. Benutzer erhalten mit das Single Sign-On von Duo eine konsistente Anmeldeerfahrung, die einen zentralen Zugriff auf lokale und Cloud-Anwendungen ermöglicht.

Mit Duo können Sie sich vor gefährdeten Anmeldeinformationen und riskanten Geräten sowie vor unerwünschtem Zugriff auf Ihre Anwendungen und Daten schützen. Diese Kombination aus Benutzer- und Gerätevertrauen bildet eine solide Grundlage für ein Zero-Trust Sicherheitsmodell.