

# Multi-Faktor-Authentifizierung: Vergewissern Sie sich, dass es genauso flexibel wie sicher ist

Die Sicherung des Zugriffs auf Daten, Anwendungen und andere Ressourcen ist viel schwieriger, wenn eine Person Zugriff von außerhalb des traditionellen Netzwerks beantragt, was in der heutigen digitalen Welt zunehmend der Fall ist. Da Unternehmen immer mehr Ressourcen und Vorgänge in die Cloud verlagern und Arbeit und Handel praktisch überall dort stattfinden, wo eine Internetverbindung besteht, wächst die Herausforderung der Zugriffssicherung zunehmend. Gefordert ist eine stärkere Authentifizierung, was die **Multi-Faktor-Authentifizierung (MFA)** zu einem Muss macht. Ihr Unternehmen braucht eine MFA, die nicht nur Sicherheit bietet, sondern sich auch leicht an unterschiedliche Benutzerbedürfnisse und an die Veränderungen und das Wachstum Ihres Unternehmens anpassen lässt. Sorgen Sie für das richtige Gleichgewicht, indem Sie die folgenden Grundsätze beachten:

## Je mehr Möglichkeiten zur Authentifizierung es gibt, desto besser für alle

Suchen Sie nach einer einzigen MFA-Lösung mit verschiedenen Möglichkeiten zur Authentifizierung von Benutzern, unabhängig davon, wer sie sind, wo sie arbeiten oder welche Art von Gerät oder Betriebssystem sie verwenden. Beispielsweise bietet sich die mobilbasierte Gesichtserkennung für Vertriebsteams an, die für den Zugriff auf Smartphones angewiesen sind. Im Gegenzug ist ein FIDO-basierter Sicherheitsschlüssel für Personen besser, die in sicheren Umgebungen arbeiten, in denen der Zugriff auf Mobilgeräte eingeschränkt ist. Und wenn Sie darüber nachdenken, die Authentifizierung auch auf Kunden auszuweiten, wird wahrscheinlich eine noch größere Vielfalt an Bedürfnissen und Präferenzen aufkommen.

## Wohin die Cloud Sie auch führt, Ihre MFA-Lösung sollte Sie begleiten

Alle Unternehmen befinden sich auf einer Art Weg zur Cloud, aber jeder Weg zur Cloud ist anders. Für jedes Unternehmen, das alles auf die Cloud setzt, gibt es ein anderes, das methodisch und Schritt für Schritt dorthin gelangt. Die richtige MFA-Lösung passt sich dem Moment Ihres Weges zur Cloud und auch Ihrer weiteren Reise an. Stellen Sie sicher, dass die von Ihnen gewählte Lösung während der Reise und ohne Überraschungen oder andere Unterbrechungen skaliert werden kann.

## Ortsunabhängige Authentifizierung sollte genau das sein, auch ohne Internetverbindung

Die Frustration, auf Ressourcen zugreifen zu müssen, wenn es keine Möglichkeit gibt, eine Verbindung zum Internet herzustellen, betrifft alle - von den Benutzern oder Kunden, die keine Verbindung zu den benötigten Ressourcen herstellen können, bis hin zu den Unternehmen, die aufgrund der fehlenden Verbindung Produktivitäts- oder Umsatzeinbußen hinnehmen müssen. Wählen Sie eine reibungslos funktionierende MFA, selbst wenn die sich authentifizierende Person keinerlei Zugriff auf das Internet hat.

Da Unternehmen immer mehr Ressourcen und Vorgänge in die Cloud verlagern und Arbeit und Handel praktisch überall dort stattfinden, wo eine Internetverbindung besteht, wächst die Herausforderung der Zugriffssicherung zunehmend.

## SecurID: Multi-Faktor-Authentifizierung für mehr Menschen an mehr Orten

SecurID ist die am weitesten verbreitete MFA-Lösung der Welt und ihre umfassenden, komfortablen Sicherheitsfunktionen und -fähigkeiten lassen leicht erkennen, warum:

### **Authentifikator-Auswahl zur Erfüllung verschiedener Benutzeranforderungen**

und organisatorischer Anforderungen, einschließlich biometrischer Verfahren, Push-to-Approve, One-Time Password(OTP)-Biometrie (Fingerabdruck und Gesichtserkennung), FIDO-basierte Authentifizierung, „Bring your own Authenticator“ und Hardware-Token

### **Möglichkeit zur späteren einfachen Erweiterung der On-Premise-**

**Authentifizierung bei SecurID** in die Cloud in Ihrem eigenen Tempo, basierend auf der Cloud-Strategie Ihres Unternehmens

Permanente starke Authentifizierung mit **99,95% iger Verfügbarkeit** und eine einzigartige „No-Fail“-Funktion für Windows und macOS, die einen sicheren und bequemen Zugriff auch bei unterbrochener Netzwerkverbindung gewährleistet

RSA-fähige **Technologieintegrationen**, um eine gründlich getestete, dokumentierte und interoperabilitätszertifizierte Authentifizierung für spezifische Zugriffsumgebungen bereitzustellen – plus offene Standards zur Unterstützung zusätzlicher Integrationen

**Erfahren Sie mehr** darüber, wie Sie einen sicheren und bequemen Zugriff auf Ressourcen vor Ort oder in der Cloud mit der SecurID-Multi-Faktor-Authentifizierung bereitstellen können.

## Informationen über SecurID

SecurID, ein RSA-Unternehmen, ist eine Identitätsplattform, der bereits 13.000 Unternehmen auf der ganzen Welt vertrauen. Sie verwaltet 50 Millionen Identitäten und bietet 30 Millionen Benutzern einen sicheren und bequemen Zugriff. SecurID ermöglicht es Unternehmen, in einer digitalen Welt erfolgreich zu sein, mit umfassenden Funktionen für moderne Authentifizierung, Lebenszyklusmanagement und Identitätsverwaltung. Ob in der Cloud oder On-Premise – SecurID verbindet Menschen mit den digitalen Ressourcen, auf die sie angewiesen sind, wo immer sie leben, arbeiten und spielen. Weitere Informationen finden Sie unter [securid.com](https://securid.com).

