

# Identitäts- und Zugriffsmanagement in der Cloud: Machen Sie es sich einfach

Da Unternehmen zunehmend Anwendungen und Vorgänge in die Cloud verlagern, ist es wichtig, den Zugriff auf diese Ressourcen zu sichern – und zwar so, dass sich jeder auf die Verfolgung von Geschäftszielen in der Cloud konzentrieren kann, anstatt sich mit Zugriffsproblemen zu befassen. Aus diesem Grund benötigen Sie ein leistungsfähiges Identitäts- und Zugriffsmanagement, das flexible Auswahlmöglichkeiten und eine adaptive Authentifizierung bietet, um den Weg zur Cloud Ihres Unternehmens zu unterstützen. Wenn Sie über Authentifizierung und andere IAM-Funktionen in der Cloud nachdenken, sollten Sie Folgendes beachten.

## **Solide Zuverlässigkeit, über die Sie nicht lange nachdenken müssen**

Sie benötigen eine Authentifizierung, die immer und überall funktioniert, damit Ihre Mitarbeiter in der Cloud verbunden und produktiv bleiben. Das bedeutet, dass die Technologie nachweislich hochverfügbar ist und es mehr Möglichkeiten gibt, in Verbindung zu bleiben - einschließlich der Option, auf andere Weise mit der Cloud verbunden zu bleiben, falls die Internetverbindung unterbrochen wird.

## **Flexible Möglichkeiten für die Anbindung an die Cloud**

Heutzutage verbinden sich die Mitarbeiter Ihres Unternehmens von vielen Orten außerhalb der traditionellen Unternehmensumgebung und verwenden dazu eine Vielzahl von Geräten und Plattformen. Sie möchten, dass die Authentifizierung gleichermaßen einfach ist, unabhängig davon, ob jemand einen firmeneigenen Laptop oder ein privates Gerät verwendet. Und Sie brauchen ein breites Angebot an modernen Authentifizierungsmethoden, die sowohl den Präferenzen als auch den Umständen des Unternehmens und des Nutzers gerecht werden.

## **Adaptive Authentifizierung für einen sicheren und dennoch bequemen Zugriff**

Ressourcen zu schützen und gleichzeitig den Nutzern den Zugriff zu erleichtern, ist in der Cloud genauso wichtig wie anderswo. Stellen Sie sicher, dass Sie die Messlatte senken können, wenn das Zugriffsrisiko gering ist, und sie anheben können, wenn ein Benutzer oder ein Gerät ein höheres Risiko darstellt. Suchen Sie nach einer Multi-Faktor-Authentifizierung, die sich dem Risiko anpasst und nur dann zu einem höheren Authentifizierungsfaktor übergeht, wenn Verhaltensanalysen und andere erweiterte Funktionen auf ein Risiko hinweisen, das diese Maßnahme rechtfertigt.

**Sie benötigen ein leistungsfähiges Identitäts- und Zugriffsmanagement, das flexible Auswahlmöglichkeiten und eine adaptive Authentifizierung bietet, um den Weg zur Cloud Ihres Unternehmens zu unterstützen.**

## SecurID: Alles, was Sie für das Identitäts- und Zugriffsmanagement in der Cloud benötigen

Mit SecurID erhalten Sie zuverlässige Leistung, flexible Auswahlmöglichkeiten und den erforderlichen adaptiven Authentifizierungsansatz, um den Zugriff auf Ressourcen in der Cloud zu sichern.

**99,95 % Verfügbarkeit** in Verbindung mit einer einzigartigen Failover-Authentifizierungsfunktion vor Ort, die es ermöglicht, dass SecurID-Implementierungen vor Ort den Zugriff nahtlos fortsetzen, wenn die Internetverbindung unterbrochen wird

**Technologieintegrationen**, entwickelt und gründlich auf Interoperabilität getestet, so dass SecurID zur Verbesserung der Authentifizierung in Cloud-Umgebungen für alle Bereiche von der geschäftlichen Zusammenarbeit bis hin zur Verwaltung von Diensten verwendet werden kann

Fähigkeit zur **einfachen, nahtlosen und schrittweisen Ausweitung von On-Premise-SecurID-Funktionen** in die Cloud - entsprechend Ihrem Tempo und Ihrer Cloud-Strategie

**Multi-Faktor-Authentifizierungsoptionen in der Cloud**, die auf Benutzerumgebungen, Benutzer-/Geräte-Risikoprofile und organisatorische Präferenzen zugeschnitten sind - einschließlich Biometrie, Einmalpasswort (OTP), Push-to-Approval und passwortlose Authentifizierung

**Risikobasierte Authentifizierung**, die die Authentifizierung nur dann verschärft, wenn das Zugriffsrisiko dies, basierend auf einer erweiterten Analyse des Benutzer- und Geräteverhaltens, rechtfertigt

**Identitäts- und Zugriffsmanagement für die Cloud** die es Administratoren leicht macht, angemessene Zugriffsebenen zu gewährleisten, mit Einblick in den Zugriff über gemischte Cloud- und On-Premises-Bereitstellungen hinweg

**Erfahren Sie mehr** darüber, wie das Identitäts- und Zugriffsmanagement von SecurID Sie auf Ihrem Weg in die Cloud unterstützt .

### 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. Mit SecurID können Unternehmen in einer digitalen Welt erfolgreich sein und verfügen über umfassende Funktionen für moderne Authentifizierung, Lebenszyklusmanagement und Identity Governance. Ob in der Cloud oder On-Premise – SecurID verbindet Menschen mit den digitalen Ressourcen, von denen sie abhängig sind, wo immer sie leben, arbeiten und spielen. Weitere Informationen finden Sie unter [securid.com](https://securid.com).

