okta

Wie Sie die Zero-Trust-Einführung beschleunigen

Immer mehr IT- und Security-Entscheider verlassen sich auf Zero-Trust-Strategien, bei denen das Identity- und Access-Management im Mittelpunkt steht. Erfahren Sie, wie Sie mit einem solchen Ansatz Ihre hybride Workforce schützen, dynamische Cyberthreats stoppen und die Weichen für einen sicheren Wechsel in die Cloud stellen.

99 %

der Unternehmen weltweit bezeichnen Identity als kritischen Bestandteil ihrer Zero-Trust-Strategie

Quelle: Zero Trust Security 2021

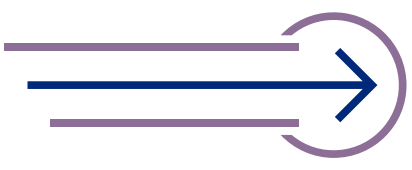
1 Beschleunigen Sie die Digitalisierung

Weltweit wollen Unternehmen immer schneller in die Cloud wechseln – doch die Sicherheit der Zugriffe zu gewährleisten, ist oft alles andere als einfach. Moderne Identity-Plattformen unterstützen out-of-the-box schlüsselfertige Integrationen für geschäftskritische Anwendungen – und ermöglichen es IT-Entscheidern so, ihren Mitarbeitern schnell und sicher alle benötigten Tools an die Hand zu geben.

97 %

der Entscheider sind überzeugt, dass die Pandemie die Digitalisierung ihrer Unternehmen beschleunigt hat

Quelle: COVID-19 Digital Engagement Report, Twilio



2 Schützen Sie Ihre hybride Workforce

Mitarbeiter wollen heute selbst entscheiden können, wo sie am liebsten und am produktivsten arbeiten. Moderne Identity-Lösungen ermöglichen es Ihnen, die Zugriffsrechte für jeden Anwender über alle Cloud- und On-Prem-Anwendungen hinweg zentralisiert zu managen. So haben alle User jederzeit sicheren Zugang zu benötigten Ressourcen – wann und wo sie diese auch brauchen.

89 %

der Mitarbeiter möchten zumindest teilweise von zuhause aus arbeiten

Quelle: PwC, Global Workforce Hopes and Fears Survey 2022

3 Stoppen Sie die gängigsten Cyberthreats

Um während der Pandemie handlungsfähig zu bleiben und den Anforderungen ihrer remote und hybrid agierenden Mitarbeiter gerecht zu werden, haben viele Unternehmen Kompromisse bei der Security in Kauf genommen. Die Einführung moderner Tools wie MFA und SSO hilft Ihnen, unsichere Passwörter zu vermeiden und Ihre Identities wesentlich besser zu schützen.

61 %

der Cyberangriffe des Jahres 2021 involvierten gestohlene oder schwache Zugangsdaten

Quelle: 2022 Data Breach Investigations Report, Verizon

4 Hyperautomatisieren Sie manuelle Provisioning-Prozesse

Cloud-Technologien können zwar zur Resilienz der IT beitragen – die Apps manuell bereitzustellen, ist aber fehleranfällig und kann Ihr Unternehmen angreifbar machen. Wenn Sie Ihr Provisioning mit starken Identities hyperautomatisieren, können Sie viele dieser Risiken vermeiden. So ermöglichen Sie es Ihrem IT-Team, sich auf andere Security-Anforderungen zu konzentrieren.

88 % **aller Data-Breaches des Jahres 2021 nutzten kompromittierte Zugangsdaten aus**

Quelle: 'Why Do People Make Mistakes?', Tessian

5 Schützen Sie Apps und APIs

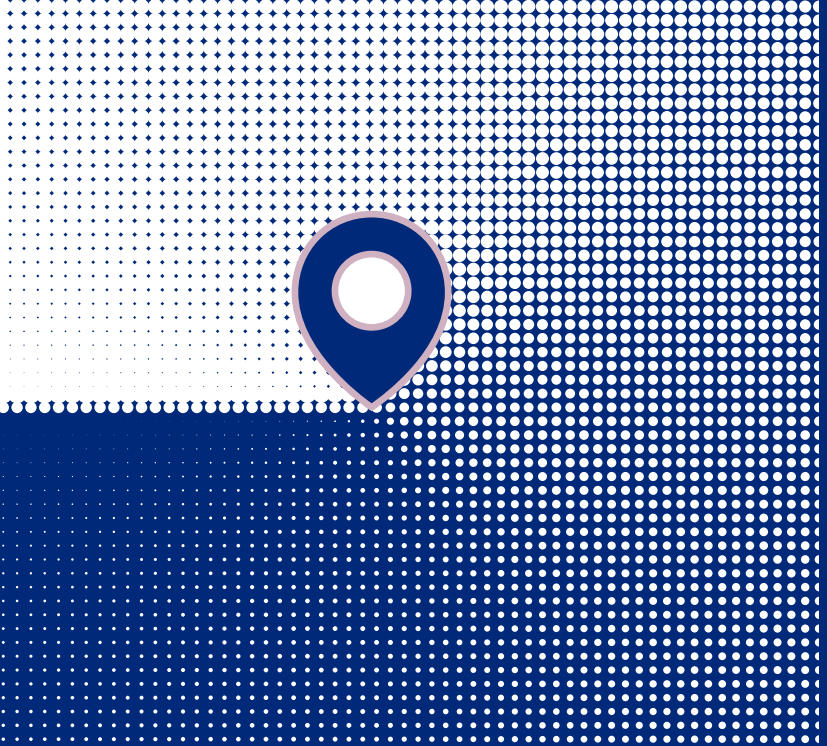
Der richtige Identity-Provider schützt nicht nur Ihre Anwendungen. Er wird Ihren Mitarbeitern auch einen sicheren Zugang zu allen Technologien bieten, auf die sie im Alltag angewiesen sind – zum Beispiel zu den APIs, die die moderne Anwendungslandschaft zusammenhalten, aber auch für Data-Breaches missbraucht werden können.

Zunahme der API-Angriffe

681 %

in den vergangenen zwölf Monaten

Quelle: State of API Security Report 2022, Salt



Wie Sie Ihre Zero-Trust-Journey beginnen können

Wenn Sie mehr darüber erfahren möchten, wie Identities Ihre Zero-Trust-Journey beschleunigen können – oder wenn Sie sich unsicher sind, wo Sie auf Ihrer Zero-Trust-Journey gerade stehen und wissen möchten, wie es weitergeht – sehen Sie sich unseren Video-Podcast mit Brian Glick, Editor-in-Chief der Computer Weekly, und Ian Lowe von Okta an.

Zum Video-Podcast