

# Wie Cloud-basierte Identitäten Ihre Kunden schützen



Immer mehr Unternehmen verlassen sich auf moderne Customer-Identity-Lösungen, um die Daten Ihrer Kunden besser zu schützen – und von Interaktion zu Interaktion mehr Vertrauen zu gewinnen. Hier fünf Gründe, wie das gelingt:

## In 5 Schritten zur identitätsbasierten Zero-Trust-Lösung

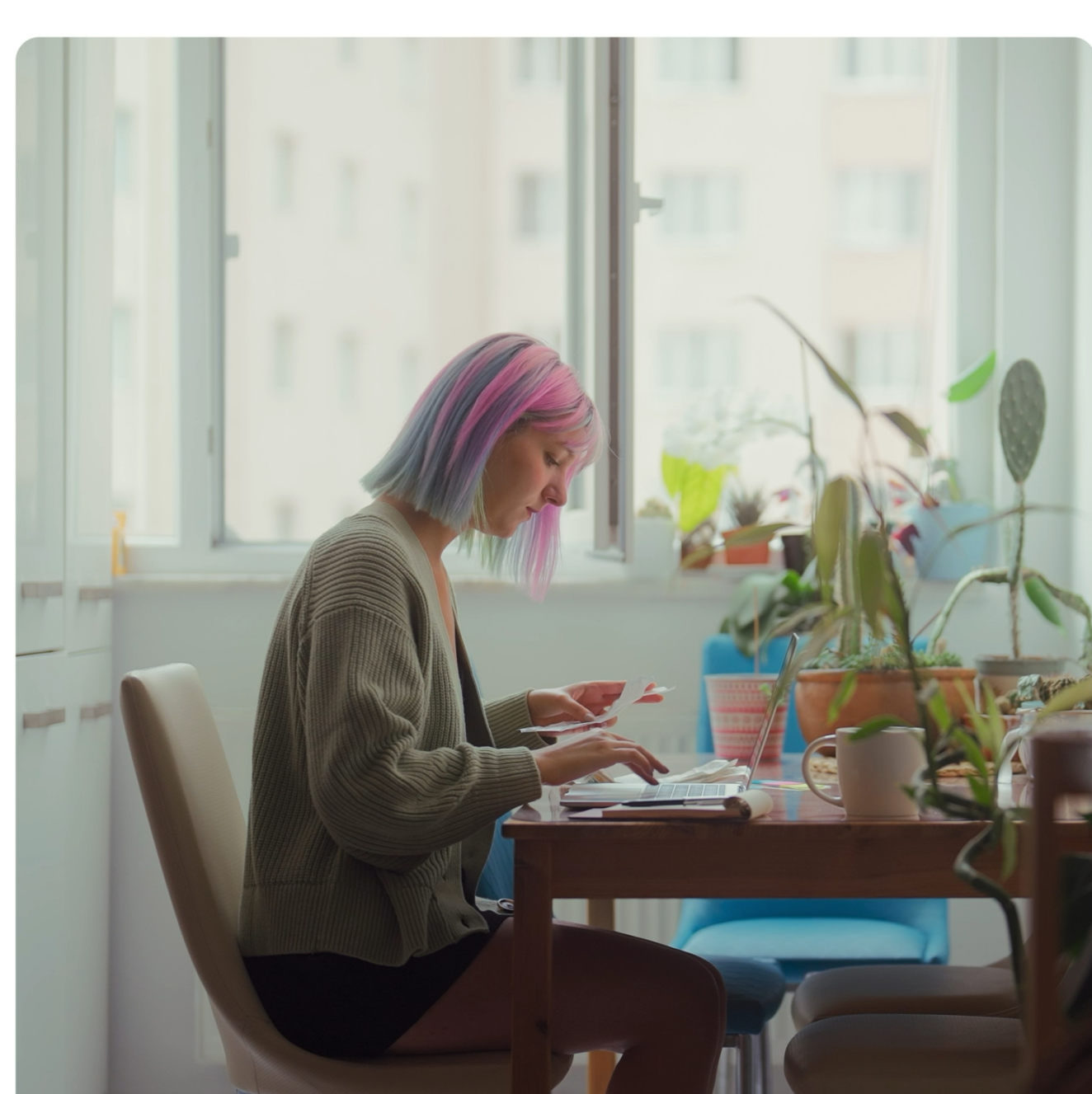
### 1. Starke Identitäten verhindern, dass Angreifer gestohlene Zugangsdaten missbrauchen.

Suchen Sie automatisch nach kompromittierten Passwörtern – und benachrichtigen Sie Ihre Kunden, wenn ihre Daten an eine dritte Quelle weitergegeben werden sollten.

80 %

aller Angriffe auf Webanwendungen lassen sich auf gestohlene Zugangsdaten zurückführen.

Quelle: [Verizon Data Breach Investigation Report 2022](#)



### 2. Sie ermöglichen eine sichere, passwortlose Verifizierung.

Ersetzen Sie die klassische Authentifizierung mit Benutzername und Passwort durch sichere Verifizierungs-Apps, und erweitern Sie diese um starke Multi-Faktor-Authentifizierung für zusätzlichen Schutz.

90 %

der Kunden weltweit machen sich Gedanken über die Sicherheit ihrer Passwörter.

Quelle: [Avast, Cybersecurity: Reality Check](#)

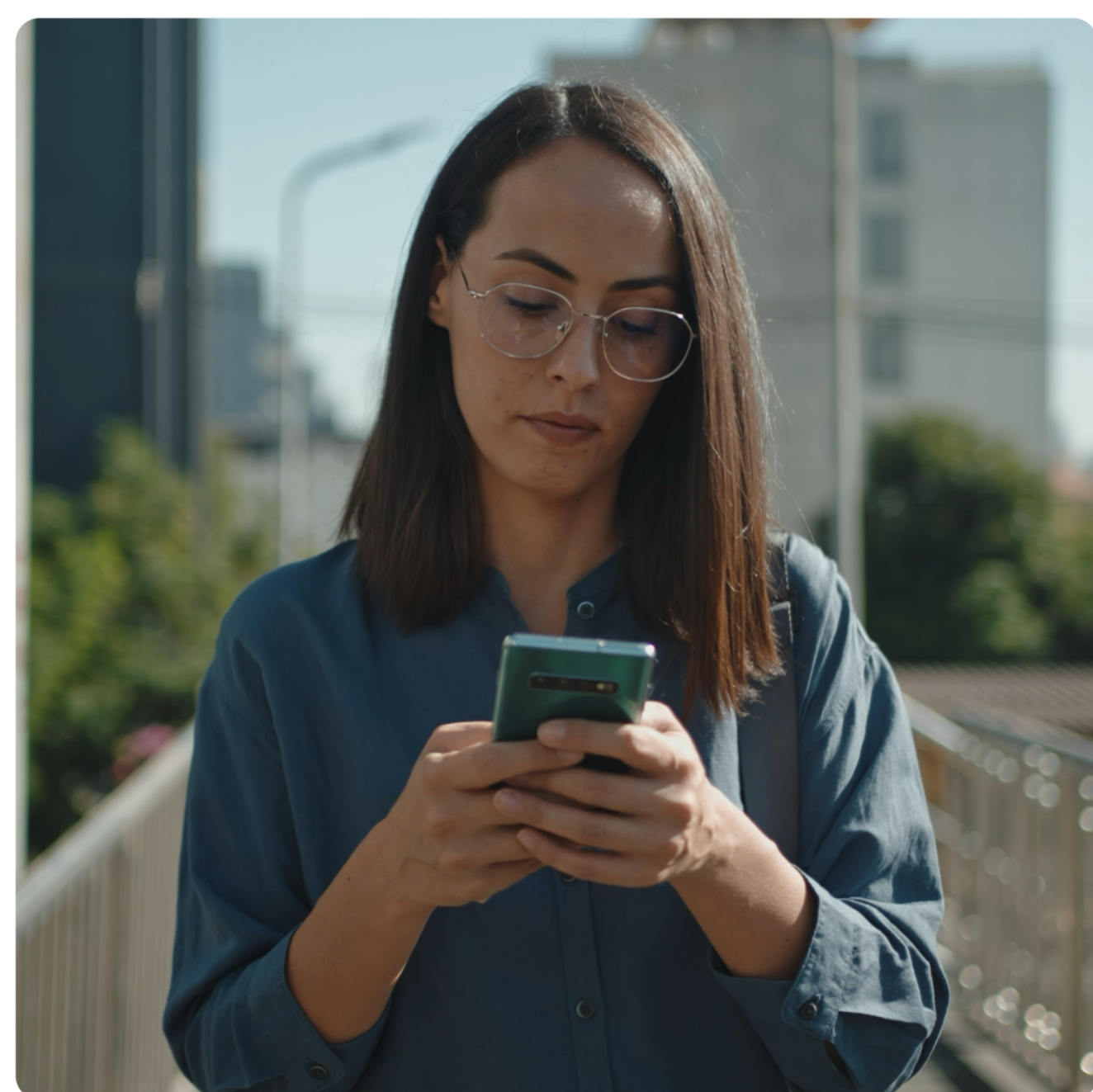
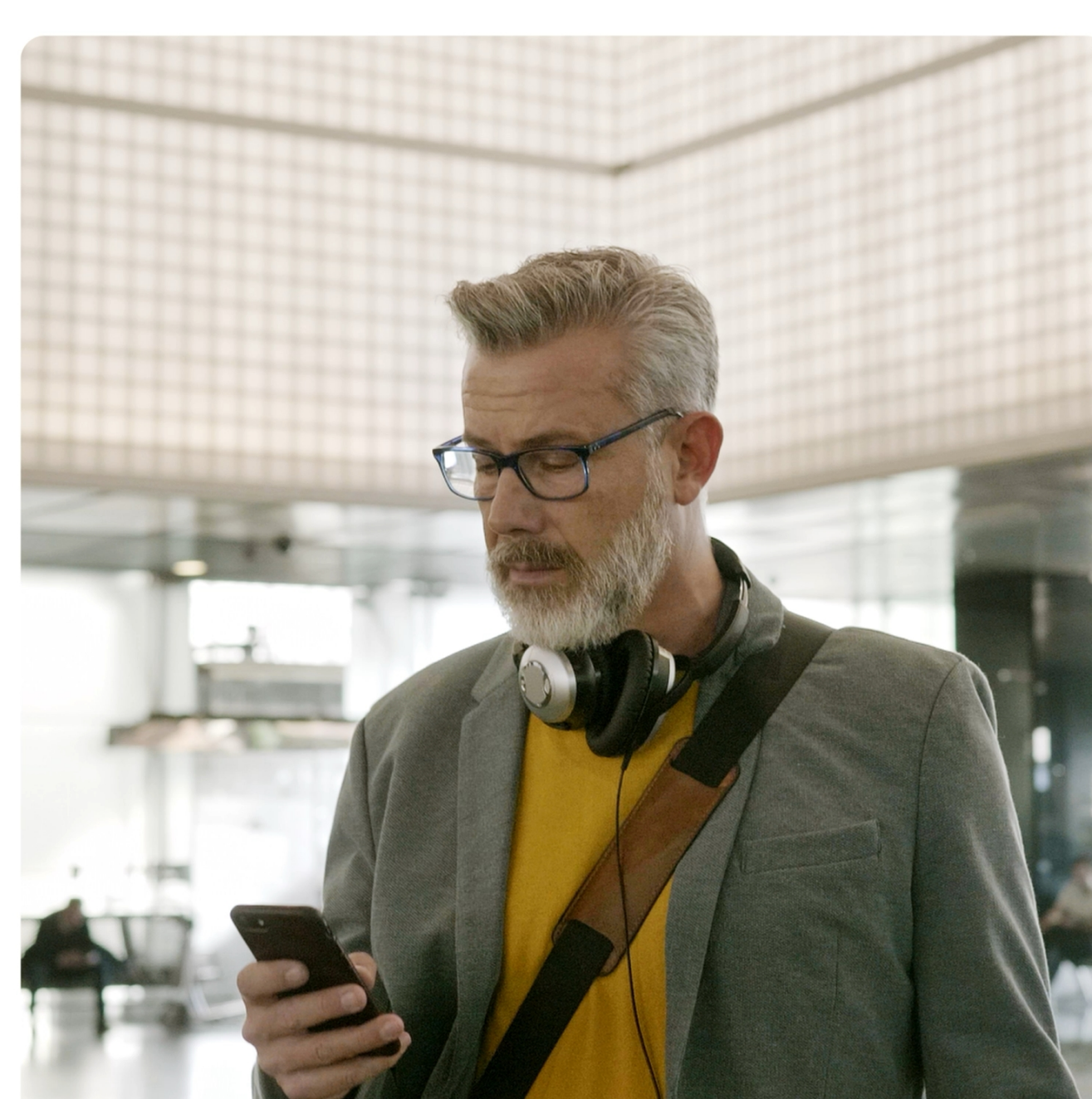
### 3. Sie bieten das richtige Gleichgewicht zwischen Komfort und Sicherheit.

Ermöglichen Sie es Ihren Kunden, vorhandene Anmeldeinformationen aus sozialen Netzwerken wie Facebook, Twitter oder Google zu verwenden – und bieten Sie ihnen so eine einfachere und sicherere Möglichkeit, sich zu registrieren und auf Ihre Website oder App zuzugreifen

50 %

aller Kunden melden sich am liebsten per Social Login an, wenn sie online mit einem Unternehmen interagieren.

Quelle: [Okta Customer Identity Trends 2023 Report](#)



### 4. Sie erkennen Anfragen, die mit hoher Wahrscheinlichkeit von Bots stammen.

Identifizieren Sie automatisch auffällige Traffic-Muster und stoppen Sie automatisierte Anfragen gefährlicher Bots, bevor diese den Accounts Ihrer Kunden schaden können.

27,7 %

des gesamten Internet-Traffics geht auf schädliche Bots zurück.

Quelle: [2022 Imperva Bad Bot Report](#)

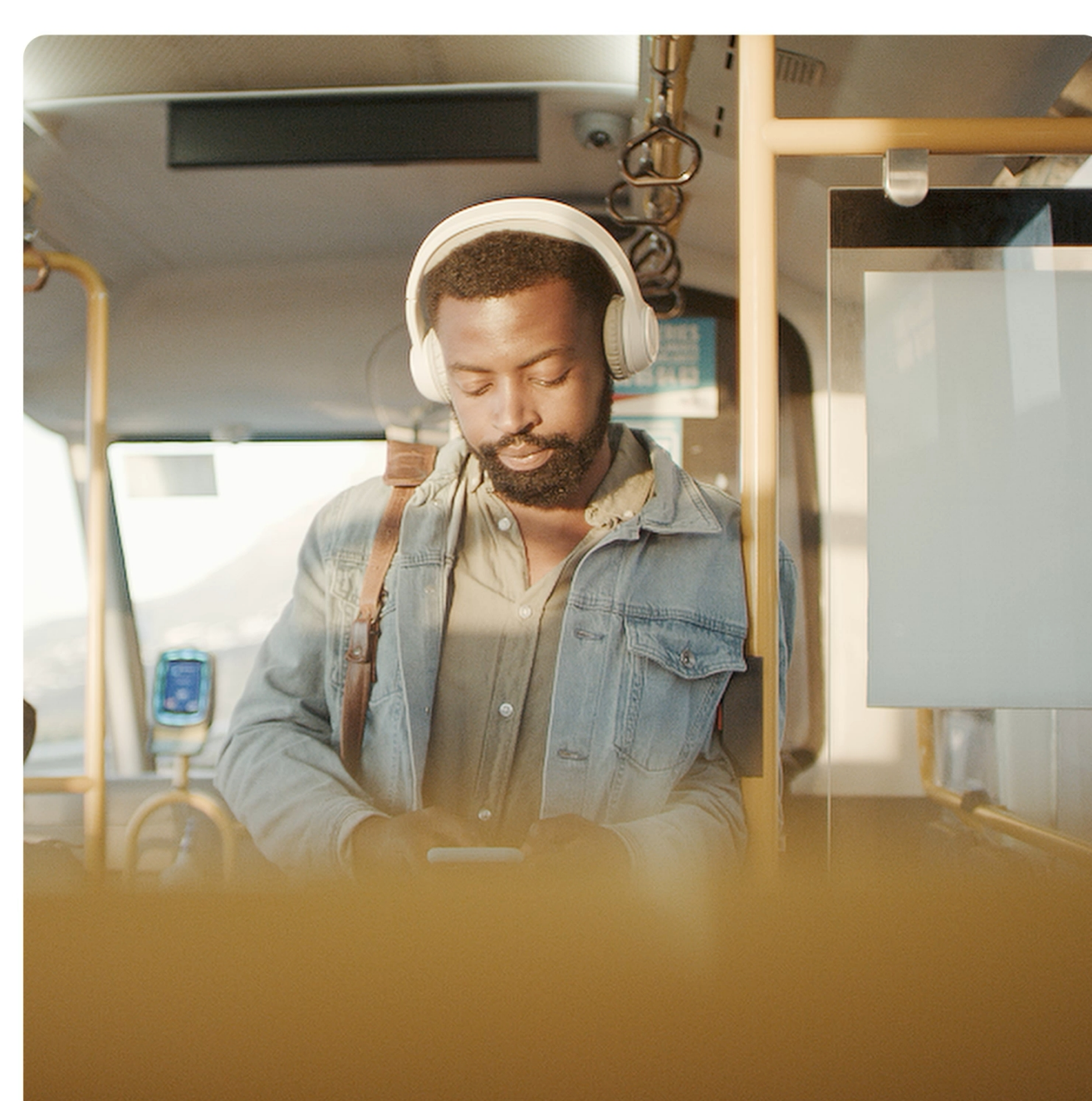
### 5. Sie blockieren Traffic von jeder IP-Adresse, die zu schnell zu viele Anmeldeversuche initiiert.

Stoppen Sie Zugriffe verdächtiger IPs, um Ihre Kunden-seitigen Anwendungen vor High-Velocity-Angriffen zu schützen, die multiple Accounts gleichzeitig ins Visier nehmen.

Über 15 Millionen

infiizierte IP-Adressen werden aktuell weltweit für DDoS-Angriffe missbraucht.

Quelle: [A10, 2022 A10 Networks DDoS Threat Report](#)



Schützen Sie mit robusten Identitäten die Daten Ihrer Kunden.



Wenn Sie mehr darüber wissen möchten, wie zeitgemäße Customer-Identity-Lösungen die Daten Ihrer Kunden schützen, eine hochwertige Experience garantieren und **jeder Interaktion mehr Vertrauen gewinnen, holen Sie sich unser E-Book [Security vs. Usability: Wie Sie Vertrauen schaffen, ohne Abstriche bei der Sicherheit in Kauf zu nehmen.](#)**

Um mehr darüber zu erfahren, wie Customer-Identity-Lösungen den Unternehmen in ganz Europa dabei helfen, geschützte, sichere und hochwertige digitale Experiences zu bieten, die Kunden heute erwarten, holen Sie sich den [Okta Customer Identity Trends 2023 Report.](#)