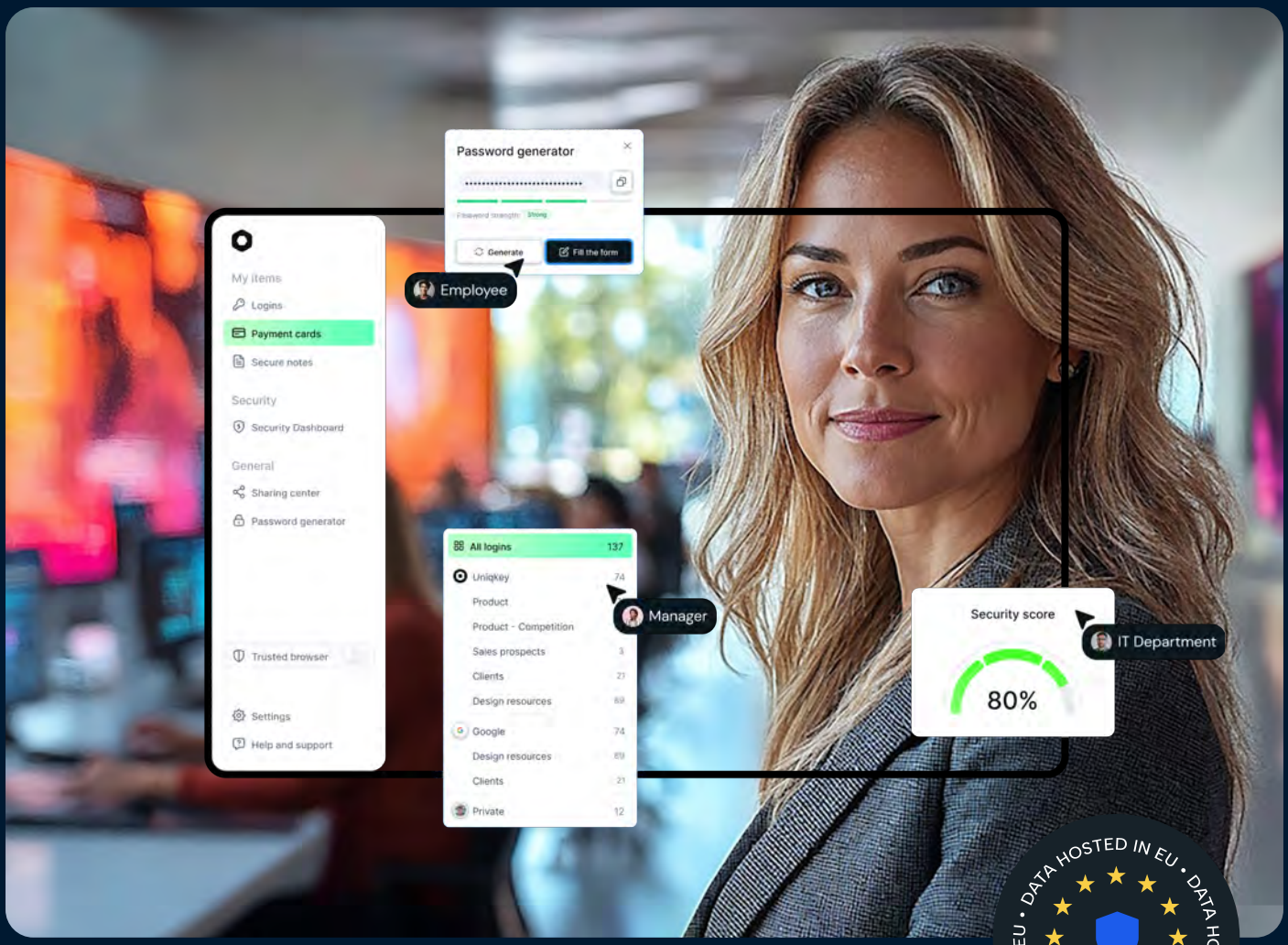
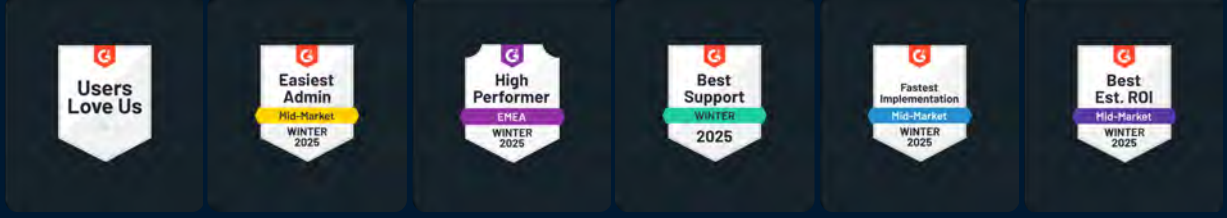


uniqkey™

Schützen Sie jeden Login. Greife mit Vertrauen zu.

Intelligentes Passwort- und Zugriffsmanagement mit starker Sicherheit – vereinfacht für Ihr gesamtes Unternehmen. Vollständig konform und von Europas führenden Unternehmen vertraut.

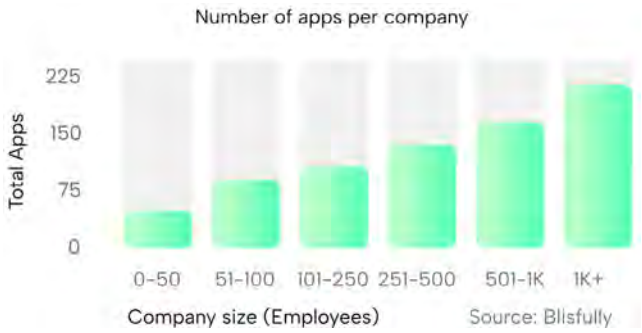


Warum Cybersicherheit für Unternehmen oberste Priorität haben muss.

Cyberangriffe sind zu einer existenziellen Bedrohung für Unternehmen geworden
Angetrieben durch zunehmende globale Cloud-Nutzung, digitale Transformation und Remote-Arbeit ist Cyberkriminalität zur größten Bedrohung für Unternehmen geworden. Laut TechJury (1) haben 64 % der Unternehmen weltweit mindestens einen Cyberangriff erlebt – mit Schäden von ruinierter Markenreputation über gebrochenes Kundenvertrauen bis zu erheblichen finanziellen Verlusten. Dieser Trend setzt Unternehmen – besonders in Europa, einer der digitalisiertesten Regionen der Welt – stark unter Druck, massiv in Cybersicherheit zu investieren oder die geschäftsgefährdenden Folgen eines Cybervorfalls zu tragen.

> "Cyberkriminalität stellt die größte Vermögensverschiebung in der Geschichte dar und wird bis 2025 jährliche Kosten von 10,5 Billionen US-Dollar verursachen."
> – Cybersecurity Ventures (2)

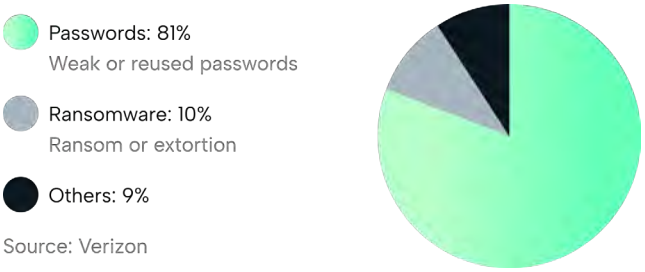
Mehr Dienste. Mehr Passwörter. Mehr Risiko.
Während die rasante Einführung von Cloud- und Desktop-Services sowie VPN-gestützter Remote-Arbeit die Produktivität und Innovation steigert, bringen diese Entwicklungen auch erhebliche neue Cyberrisiken mit sich, da Unternehmen zunehmend die Kontrolle und Übersicht über ihre wachsende digitale Präsenz verlieren. Um Ihnen eine Vorstellung von der Dimension des Problems zu geben: Ein durchschnittliches Unternehmen mit 251 bis 500 Mitarbeitenden verwaltet über 123 verschiedene Business-Apps.



Die digitale Transformation ist an sich kein Problem.
Mit mehr Diensten kommen jedoch auch mehr Logins und Passwörter, die sich Mitarbeitende merken müssen – und jeder neue Dienst wird so zu einem potenziellen Einstiegspunkt für Hacker – und das ist ein sehr beliebter Angriffsvektor. Im Jahr 2020 stiegen beispielsweise die Angriffe auf Remote-Desktop-Verbindungen um 768 % (3).

Laut dem Data Breach Investigations Report 2023 von Verizon trägt eine mangelhafte Passwortsicherheit zu 81 % aller Datenpannen bei. Angesichts dieser Tatsache sollten die Risiken, die mit dieser wachsenden Angriffsfläche einhergehen, nicht unterschätzt werden.

(1) TechJury "How Many Cyber Attacks Per Day In 2022?", 2022
(2) Cybersecurity Magazine, 2020
(3) ESET's Q4 2020 Threat Report, 2020
(4) Microsoft, 2022
(5) Global Risks Report 2022, World Economic Forum, 2018



Viele Unternehmen versuchen, das Passwortrisiko durch die Implementierung von Single Sign-On (SSO) zu minimieren. Doch obwohl SSO Logins vereinfacht, erhöht es die Sicherheit nicht zwangsläufig, da es nur einen bestimmten Bereich von Apps und Diensten abdeckt. Best Practice für Sicherheit war schon immer, für jeden Dienst lange und einzigartige Passwörter zu verwenden, was in der Praxis jedoch historisch schwer umsetzbar war.

Schlechtes Passwortmanagement ist nur ein Teil des Problems. Ein weiteres Problem, das die Sicherheit von Unternehmen gefährdet, ist der fehlende Überblick und die mangelnde Kontrolle darüber, wer auf welche Systeme Zugriff hat. Wenn Sie nicht steuern können, welche Mitarbeitenden auf welche Systeme zugreifen dürfen, wird es zunehmend schwieriger, Sicherheitsstandards im gesamten Unternehmen aufrechtzuerhalten.

Die Schattenseite der digitalen Transformation
Das Hauptproblem der digitalen Transformation besteht darin, dass die Sicherheitsinfrastruktur der meisten Unternehmen nicht darauf ausgelegt ist, Cloud- und Desktop-Dienste zu schützen. Noch schlimmer ist, dass viele Unternehmen sich ihrer „digitalen Fußabdrücke" nicht bewusst sind, was zu einer Zunahme unbekannter Cloud-, Desktop- und SaaS-Nutzung führt – bekannt als Schatten-IT.

> "80 % der Mitarbeitenden geben zu, SaaS-Anwendungen bei der Arbeit zu nutzen, ohne die IT-Abteilung zu informieren."
> – Microsoft 2022

Wie Sie in einer digitalen Welt sicher bleiben
Heutzutage kann jeder problemlos Off-Premise-Dienste nutzen, was es IT-Verantwortlichen erschwert, ein hohes Sicherheitsniveau im Unternehmen zu gewährleisten. Nur durch Benutzername und Passwort geschützt, teilen diese Dienste alle dieselbe Schwachstelle für Sicherheitsverletzungen.
Um das Risiko neuer Angriffsflächen zu minimieren, müssen Unternehmen ihre Zugriffssicherheit verbessern. Der wirkungsvollste Weg ist, die Kontrolle über alle digitalen Ressourcen zurückzugewinnen, Zwei-Faktor-Authentifizierung (2FA) stärker einzusetzen und die Passwortsicherheit unternehmensweit zu erhöhen.
Doch diese Maßnahmen sind in der schnellen digitalen Arbeitswelt schwer umzusetzen. Auf fehlerfreies menschliches Verhalten zu setzen, ist zum Scheitern verurteilt, denn menschliches Versagen ist an 95 % aller Cybervorfälle beteiligt (5). Unternehmen brauchen daher eine Lösung, die den menschlichen Faktor so weit wie möglich ausschließt.

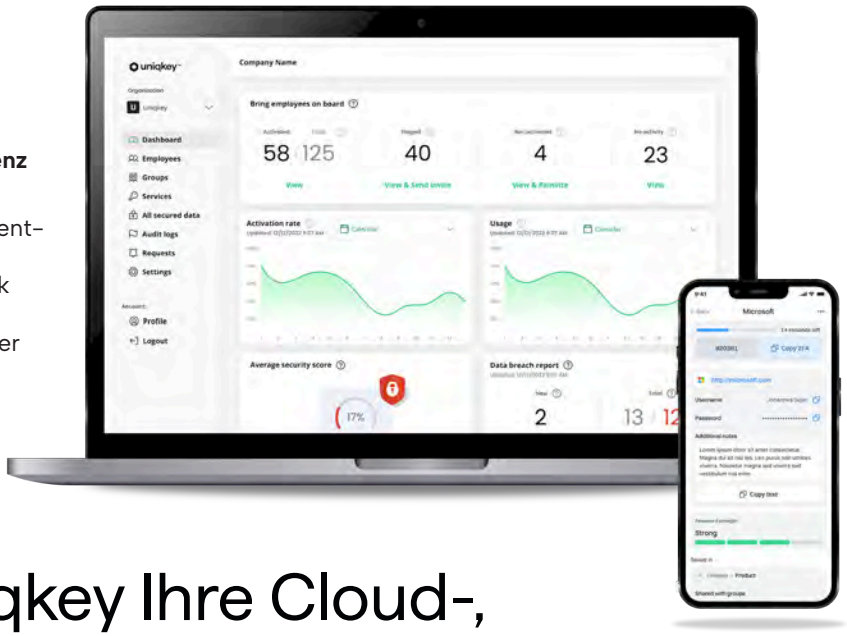
Uniqkey hilft Unternehmen, indem es Cybersicherheit vereinfacht.

In Zeiten explodierender Cloud-, SaaS- und Desktop-Nutzung ertrinken Mitarbeitende in Passwörtern, und Unternehmen haben den Überblick über ihre digitale Infrastruktur verloren. Uniqkey schützt Unternehmen vor 81 % aller Datenpannen, indem es die Passwortnutzung am Arbeitsplatz automatisiert und Administratoren die Übersicht und Kontrolle gibt, die sie benötigen, um die Organisation sicher und produktiv zu halten.

Eine einfache Lösung für ein komplexes Problem
Durch die Kombination von benutzerfreundlichem Passwortmanagement, automatischer 2FA und einer zentralen Plattform für Zugriffsmanagement bietet Uniqkey eine einfache Lösung für ein komplexes Cybersicherheitsproblem.
Die Risiken durch schlechte Passworthygiene, Shadow IT und fehlende Transparenz werden sofort reduziert, während Ihr Unternehmen die Kontrolle über Passwörter und Dienste zurückgewinnt und Ihre Mitarbeitenden mit einer Lösung unterstützt, die es einfach macht, das Richtige für die Sicherheit zu tun.

Erhalten Sie vollständige Transparenz über genutzte Dienste

Die Access-Management-Plattform bietet vollständigen Überblick und Kontrolle über alle Zugriffe und Dienste der Mitarbeitenden.



Passwörter sicher speichern und verwalten

Der Passwort-Manager merkt sich private und berufliche Passwörter und speichert sie sicher.

Wie Uniqkey Ihre Cloud-, Desktop- und mobilen Dienste schützt

Für Admins

Identity & Access Management
Auf Uniqkeys zentraler IAM-Plattform haben Administratoren vollständigen Überblick und detaillierte Kontrolle über die Dienste, Konten und Zugriffe der Mitarbeitenden.

Compliance-fähiges Audit-Log
Compliance wird mit Uniqkeys Audit-Log ganz einfach. Hier können Administratoren alle Login-Aktivitäten überwachen, verdächtige Vorgänge erkennen und geteilte Logins im Blick behalten.

Lizenzen, Onboarding und Offboarding
Onboarding und Offboarding können chaotisch sein. Mit Uniqkey können Administratoren Nutzern mit wenigen Klicks die relevanten Zugriffsrechte zuweisen – und auch wieder entziehen.

Individuell anpassbare Zugriffsbeschränkungen
Zur Maximierung der Sicherheit können alle Nutzerzugriffsrechte individuell angepasst und um IP-, Geo- und zeitspezifische Beschränkungen ergänzt werden.

Für Mitarbeitende

Automatische 2FA
Mit Auto-Fill von Zugangsdaten und automatischer 2FA-Authentifizierung erfolgt der Login viermal schneller, und 2FA kann bei allen Logins angewendet werden, ohne den Anmeldeprozess zu verlangsamen.

Intuitiver Password Manager
Uniqkeys Passwort-Manager speichert die Passwörter der Mitarbeitenden sicher und füllt sie bei Bedarf automatisch aus.

Integrierter Passwort-Generator
Mit einem integrierten Passwort-Generator können Mitarbeitende ihre Passwortsicherheit erhöhen, indem sie in Sekundenschnelle starke Passwörter erstellen.

Einfaches und sicheres Teilen von Passwörtern
Mit Uniqkey können Einzelpersonen und Abteilungen Passwörter miteinander teilen, ohne das Passwort offenzulegen – und nur für eine begrenzte Dauer.

Über Uniqkey.

Uniqkey ist ein dänisches Cybersecurity-Unternehmen, das Hunderten von europäischen Unternehmen hilft, sich gegen passwortbezogene Cyberangriffe zu schützen. Gegründet im Jahr 2017 beschäftigt Uniqkey heute mehr als 50 talentierte Mitarbeitende aus 6 Nationalitäten in 3 verschiedenen europäischen Ländern.

Sicherheitsarchitekten und Senior Advisors von HSBC Bank, VISA, dem britischen Parlament und NNIT stehen hinter dem Erfolg von Uniqkeys Infrastruktur und Sicherheit. Mit langjähriger Erfahrung basiert die Grundlage von Uniqkey auf modernster Technologie mit Spezialisierung auf Infrastruktur, Hosting, Sicherheit und Verschlüsselung. Dies führte dazu, dass Deloitte Uniqkey im Jahr 2018 zum „Cybersecurity Entrepreneur of the Year" ernannte.

Alle Daten werden lokal verschlüsselt und mit dem Master-Passwort der Nutzer geschützt und auf deren Smartphone gespeichert. Uniqkey hat keinen Zugriff auf Daten oder Passwörter und kann weder Nutzer- noch Unternehmensdaten entschlüsseln. Unsere Lösung wird von Kunden in umfangreichen Proof-of-Value-Tests geprüft.

Technische Spezifikationen

- ISAE 3402-zertifiziert auf Basis der ISO-27001-Standards
- ISAE 3000 DSGVO-zertifiziert
- Verwendet Zero-Knowledge-Proof und Secure Remote Password Protocol
- Alle Daten werden offline und lokal auf den Smartphones der Mitarbeitenden verschlüsselt
- Daten sind durch AES-256- und SHA-3-Verschlüsselung geschützt
- Uniqkey speichert keine personenbezogenen oder sensiblen Daten von Kunden
- 99,9 % stabile SLA-Verfügbarkeit
- Verfügt über externe Zertifizierungen und Audits
- Uniqkey überprüft, auditiert und bewertet die Sicherheitsprozesse regelmäßig durch externe Berater
- Umfassender Support für IT-Verantwortliche und Mitarbeitende

Eine Auswahl europäischer Unternehmen, die Uniqkey vertrauen

St Helena Government · Van Gogh Museum Amsterdam · Omnicom MediaGroup · Sunset Boulevard · KMD · Nestved · Søstrene Grenes All Over the World Handelsromantikere · hordijk · Raseborg Raasepori · AVEX · Caljan · CROP

uniqkey™

Vorreiter der nächsten Ära europäischer Sicherheits-Compliance.

Für weitere Informationen oder eine kostenlose Testinstanz für Unternehmen kontaktieren Sie uns unter: info@interscale.ch