uniqkey™

Die Schwachstelle von SSO

Warum ein Passwortmanager entscheidend ist, um Lücken im Identitäts- und Zugriffsmanagement zu schließen

www.uniqkey-cloud.de

Inhaltsverzeichnis

Einleitung	1
Wenn Sie nur 5 Minuten Zeit haben	2
Die neuen Gefahren des modernen Arbeitsplatzes	3
Der Aufstieg von SSO	4
SSO verstehen: Stärken und Grenzen	5
Die Rolle von Passwortmanagern	7
Die Synergie zwischen SSO und Passwortmanagern	8
Lernen Sie Uniqkey kennen	9
Wie Uniqkey und SSO zusammenarbeiten	10
Häufige Bedenken	11
Zusammenfassung	12
Bereit, das Beste aus beiden Welten zu erleben?	13

Einleitung

Seit Jahren ist Single Sign-On (SSO) die bevorzugte Lösung für Unternehmen, um sicheren Zugriff zu gewährleisten, Zugriffsrisiken zu minimieren und nahezu vollständige Abdeckung zu bieten.

Doch der Anstieg von Cloud-Diensten, die nicht mit SSO kompatibel sind, führt zu Sicherheitslücken. Für Unternehmen, die stark auf SSO setzen, bedeutet das, dass ein wachsender Teil ihrer IT-Umgebung ungeschützt und angreifbar bleibt.

Dieses E-Book zeigt, wie die Kombination von SSO und Passwortmanagern diese Lücken schließen kann. Wenn beide gemeinsam eingesetzt werden, ermöglichen sie einen ganzheitlichen Ansatz für Identitäts- und Zugriffsmanagement, der Sicherheit gewährleistet, ohne die Benutzerfreundlichkeit einzuschränken.
In den folgenden Kapiteln werden wir darlegen, warum diese Kombination entscheidend für die digitale Sicherheit ist.

Was Sie lernen werden:

01 Verstehen Sie die Rolle und die Grenzen von SSO.

02 Erfahren Sie, wie Passwortmanager die von SSO hinterlassenen Lücken schließen.

03 Lernen Sie, wie Uniqkey und SSO zusammenarbeiten.

04 Räumen Sie mit gängigen Mythen über die Kombination von SSO und Passwortmanagement auf.

05 Bewerten Sie den ROI der Kombination von SSO und Passwortmanagern.

uniqkey™

Wenn Sie nur 5 Minuten Zeit haben

Die digitale Transformation bringt neue Bedrohungen mit sich

Die Welle der digitalen Transformation hat zu einer beispiellosen Verbreitung von SaaS-Tools und Cloud-Diensten geführt. Obwohl diese Technologien enorme Flexibilität und Skalierbarkeit bieten, bringen sie auch eine Vielzahl neuer Bedrohungen und Angriffsvektoren mit sich.

Das bedeutet ...

Mit der zunehmenden Nutzung cloudbasierter Dienste steigt die Komplexität der Absicherung dieser Plattformen. Dies erfordert robustere und vielseitigere Sicherheitslösungen, um eine umfassende Absicherung zu gewährleisten.

Die Grenzen von SSO in unserer Cloud-Ära

SSO-Systeme bieten eine vereinfachte Anmeldung über verschiedene traditionelle IT-Plattformen hinweg, stoßen jedoch an ihre Grenzen, wenn es um moderne Cloud-Dienste geht, die SSO oft nicht standardmäßig unterstützen.

Das bedeutet ...

Auch wenn SSO den Zugriff auf traditionelle IT-Infrastrukturen effektiv verwaltet, ist es nicht mehr die All-in-One-Lösung, die es einmal war. Zusätzliche Sicherheitsmaßnahmen sind erforderlich für Plattformen, die nicht SSO-kompatibel sind.

Passwort-Manager schließen die Lücken

Passwortmanager wie Uniqkey ergänzen SSO-Lösungen perfekt, indem sie Anmeldedaten für nicht SSO-kompatible Dienste sicher verwalten.

Das bedeutet ...

Passwortmanager schließen die von SSO hinterlassenen Sicherheitslücken, indem sie die Nutzung von Zugangsdaten für nicht SSO-kompatible Systeme und Anwendungen absichern und so eine umfassendere Sicherheitsarchitektur bieten.

SSO + Passwort-Manager bieten mehr Vielseitigkeit

Die Kombination von SSO mit einem Passwortmanager wie Uniqkey schafft ein ausgewogenes Sicherheitsökosystem, das die Stärken beider Lösungen vereint.

Das bedeutet ...

Ein kombinierter Ansatz, bei dem SSO für seine Stärken genutzt wird und ein Passwortmanager die Bereiche abdeckt, die SSO nicht abdecken kann, führt zu einem robusten und ganzheitlichen Sicherheitsframework.

Uniqkey passt perfekt zu SSO

Uniqkey ist nicht nur ein zusätzliches Tool, sondern ein starker Partner für SSO-Lösungen. Es bietet zusätzliche Sicherheitsebenen wie verschlüsselte Passwortspeicherung und Zwei-Faktor-Authentifizierung für Dienste, die nicht durch SSO abgedeckt sind.

Das bedeutet ...

In Kombination mit SSO bietet Uniqkey eine umfassende Absicherung aller digitalen Dienste, verbessert die Unternehmenssicherheit und das IT-Management, ohne die Benutzerfreundlichkeit einzuschränken.

Die Gefahren des modernen Arbeitsplatzes

Wie neue Arbeitsweisen neue Bedrohungen mit sich bringen

Der Arbeitsplatz hat sich in den letzten zehn Jahren grundlegend verändert.

Veränderungen wie die Einführung von Remote-Arbeit, BYOD-Richtlinien und der Boom von SaaS- und KI-Tools haben unsere Arbeitsweise revolutioniert. Auch wenn diese Entwicklungen enorme Flexibilität und Effizienz ermöglichen, bringen sie neue Sicherheitsherausforderungen mit sich, die herkömmliche Tools wie SSO nicht vollständig lösen können.

130 SaaS-Apps werden im Durchschnitt von einem Unternehmen im Jahr 2022 genutzt.

Das Problem ist größer, als Sie denken

Das Problem geht weit über ein paar Dienste hinaus, die nicht unter die Reichweite von SSO fallen. Ein erheblicher Teil der heutigen Geschäftstätigkeiten findet außerhalb des SSO-Bereichs statt. Dazu zählen sowohl spezialisierte Software als auch Nischen-SaaS-Tools und persönliche Consumer-Dienste – alle mit sensiblen Informationen. Selbst wenn ein Dienst SSO unterstützt, ist diese Funktion oft nur in kostenpflichtigen Versionen enthalten. Bleiben solche Systeme ungeschützt und unbemerkt von der IT, stellen sie ernsthafte Risiken dar, die ein gesamtes Unternehmen betreffen können.

Im weiteren Verlauf werden wir erklären, warum die Kombination aus SSO und Passwortmanagement sich von einem „Nice-to-have“ zu einer absoluten Notwendigkeit entwickelt hat, um die Komplexität und Risiken der modernen Arbeitswelt zu bewältigen. Doch zunächst werfen wir einen Blick auf die Gründe für den Aufstieg von SSO.

“Cyberkriminalität ist die größte Bedrohung für jedes Unternehmen weltweit.“

- Ginni Rometty, CEO von IBM.

Der Aufstieg von SSO

Eine starke Lösung, die nun vor Herausforderungen steht

SSO ist schon seit einiger Zeit Teil des technischen Werkzeugkastens. Doch seine Bedeutung ist stark gestiegen durch den massiven Wandel hin zu cloudbasierten Anwendungen und Diensten.

Ursprünglich entwickelt, um Passwortmüdigkeit zu reduzieren und den Anmeldeprozess zu vereinfachen, ist SSO heute ein zentraler Bestandteil der modernen IT-Landschaft. Es ermöglicht Nutzern den Zugang zu verschiedenen Diensten mit nur einer Anmeldung. Für Mitarbeiter bedeutet das weniger Aufwand beim Merken mehrerer Passwörter, für die IT-Abteilung weniger Anfragen zum Zurücksetzen von Passwörtern.

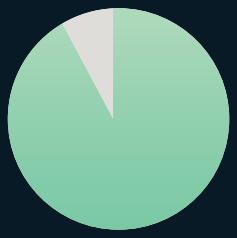
Doch obwohl SSO bei der Benutzerfreundlichkeit punktet, sorgen Veränderungen in der heutigen Arbeitswelt dafür, dass es nicht mehr die All-in-One-Lösung ist, die es einmal war.

Die Einführung von Homeoffice-Regelungen, BYOD-Strategien (Bring Your Own Device) und die zunehmende Verbreitung von SaaS-Plattformen bringen neue Herausforderungen mit sich, auf die SSO ursprünglich nicht ausgelegt war.

SSO-Einführung

80 %

der Unternehmen in der EMEA-Region haben SSO implementiert.



Geschätzte weltweite Marktgröße für SSO bis 2023

8.4 Mrd. US-Dollar

Die Stärken und Grenzen von SSO

Aufdeckung: Warum SSO klug ist, aber kritische Lücken aufweist

SSO bringt sowohl IT-Teams als auch Nutzern mehr Komfort und Effizienz, doch es gibt auch Schwächen und Sicherheitsbedenken. Werfen wir einen Blick auf die Vor- und Nachteile.

Die Stärken von SSO

Reduziert IT-Aufwand
Die Einführung von SSO reduziert Passwortanfragen und vereinfacht die Verwaltung, sodass sich die IT auf strategische Aufgaben konzentrieren kann.

Verbessert die Nutzererfahrung
SSO erspart das Merken mehrerer Benutzernamen und Passwörter. Nutzer erhalten mit nur einer Anmeldung Zugriff auf verschiedene Dienste von E-Mail bis hin zu internen Datenbanken. Dieser reibungslose Ablauf steigert Zufriedenheit und Produktivität.

Vereinfacht On- und Offboarding
Wenn neue Mitarbeiter dazukommen oder bestehende das Unternehmen verlassen, erleichtert SSO das Aktivieren oder Deaktivieren von Zugängen zu allen Systemen. Das beschleunigt den Prozess und sorgt für Sicherheit und Übersicht.

Mehr Kontrolle für Administratoren
Zentrale Authentifizierung über SSO gibt Admins einen Überblick über Nutzeraktivitäten. So lassen sich Sicherheitsrichtlinien einfacher durchsetzen, verdächtige Aktivitäten überwachen und Audits durchführen.

Weniger Passwortüberlastung
Weniger Passwörter bedeuten, dass Nutzer seltener auf unsichere Gewohnheiten zurückgreifen – wie einfache Passwörter oder die Wiederverwendung desselben Passworts über mehrere Dienste hinweg.

Stärken von SSO

- Vereinfachter Zugriff
- Geringere IT-Belastung
- Zentrale Verwaltung
- Weinger Passwortüberlastung
- Schnelleres Onboarding

Die Grenzen von SSO

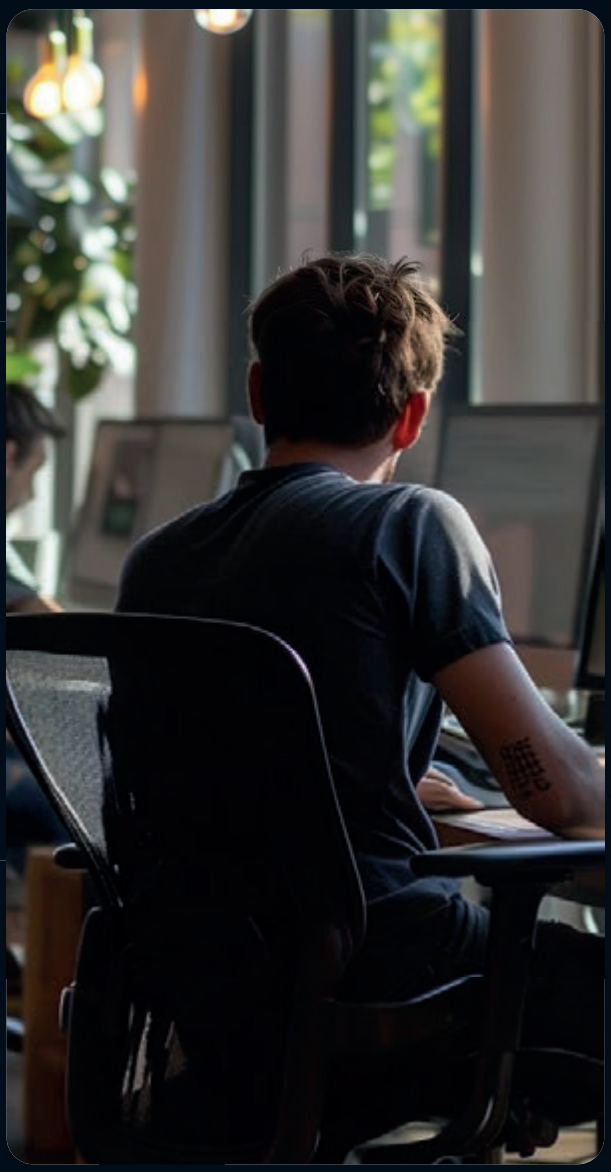
Keine vollständige Abdeckung
Der größte Nachteil von reinem SSO ist, dass viele neue SaaS-Tools und Dienste standardmäßig kein SSO unterstützen. Das macht SSO ungeeignet für agile und moderne Unternehmen, die zunehmend auf SaaS und Cloud-Dienste setzen.

Einzelner Ausfallpunkt
Die zentrale Struktur von SSO bedeutet: Wird es kompromittiert, sind alle verbundenen Dienste gefährdet. Bei einer Störung beim SSO-Anbieter könnten Nutzer von allen Systemen ausgeschlossen werden. Das beeinträchtigt den Geschäftsbetrieb.

Unvollständige Lösung
SSO vereinfacht zwar den Login-Prozess, löst aber nicht alle Probleme. Es hilft nicht beim Erstellen starker Passwörter, bei der Umsetzung von Passwort-Richtlinien oder bei Passwortwechseln.

Nicht für jeden Anwendungsfall geeignet
SSO ist nicht geeignet für Unternehmen, die auf geteilte Accounts angewiesen sind.

Die „SSO-Steuer“
Einige Anbieter verlangen Premium-Abos für SSO-Funktionen. Das bedeutet, dass alleiniger Einsatz von SSO eine teure Entscheidung sein kann.



Einschränkungen von SSO

- Lücken in der Abdeckung
- Einzelner Ausfallpunkt
- Keine Passwortsicherheit
- Oft nur mit kostenpflichtigem Abo
- Keine Unterstützung für gemeinsame Nutzung

Die Rolle von Passwortmanagern

Warum Passwortmanagement im Cloud-Zeitalter unverzichtbar ist

SSO optimiert zwar den Anmeldeprozess über verschiedene Plattformen hinweg, bietet jedoch keine vollständige Sicherheit. Genau hier kommen Passwortmanager ins Spiel.

Was Passwortmanager leisten, was SSO nicht kann

Passwortmanager schließen die Lücken, die SSO in mehreren wichtigen Bereichen hinterlässt:

- **Universelle Kompatibilität**
  Passwortmanager unterstützen standardmäßig alle Dienste, auch ohne SSO.
- **Starke Passwörter erstellen**
  Mit einem Passwortmanager lassen sich für jeden Dienst starke, einzigartige Passwörter einfach generieren.
- **Passwortrichtlinien durchsetzen**
  Passwortmanager setzen Richtlinien durch und ermöglichen Passwortwechsel, was SSO oft nicht bietet.

Hauptvorteile eines Passwortmanagers

1. Verbessert die Passwortsicherheit
2. Erhöht die Produktivität

Sicherheitsfunktionen, die nur Passwortmanager bieten

Passwortmanager bringen eigene, einzigartige Sicherheitsfunktionen mit:

Zwei-Faktor-Authentifizierung
Viele Passwortmanager unterstützen 2FA und fügen dem Login-Prozess eine zusätzliche Sicherheitsebene hinzu.

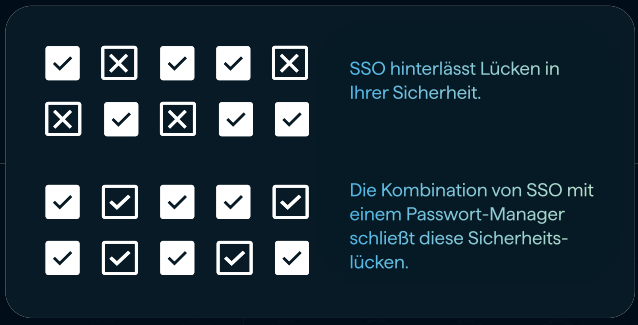
Sichere Passwortspeicherung
Passwörter werden sicher und verschlüsselt gespeichert und sind auf mehreren Geräten leicht zugänglich.

Sicheres Teilen
Wenn ein Passwort im Team geteilt werden muss, ermöglichen nahezu alle Passwortmanager eine sichere Weitergabe, ohne die Integrität der Zugangsdaten zu gefährden.

Das Power-Duo der Zugriffssicherheit

Die Vorteile dieses starken Duo für die Zugriffssicherheit entdecken

Während SSO und Passwort-Manager jeweils ihre eigenen Vorteile haben, wird ihr wahres Potenzial erst freigesetzt, wenn sie zusammen verwendet werden. Diese Synergie schafft ein robusteres und umfassenderes Sicherheits-Framework.



Wie sich SSO und Passwortmanager perfekt ergänzen

Während SSO und Passwort-Manager jeweils ihre eigenen Vorteile haben, wird ihr wahres Potenzial erst freigesetzt, wenn sie zusammen verwendet werden. Diese Synergie schafft ein robusteres und umfassenderes Sicherheits-Framework:

Volle Sichtbarkeit und Kontrolle
Kombiniert decken SSO und ein Passwortmanager alle möglichen Anwendungen, Plattformen und Dienste ab.

Reduziertes Risiko eines Ausfallpunkts
Wenn Sie beide Lösungen einsetzen, reduzieren Sie das Risiko, sich auf eine einzige zu verlassen.

Erweiterte Sicherheitsfunktionen
Ein Passwortmanager fügt eine zusätzliche Sicherheitsebene mit starker Verschlüsselung und sicherer Passwortfreigabe hinzu.

Besseres Auditing
Sowohl SSO als auch Passwortmanager bieten detaillierte Audit-Logs, die die Benutzer- und Sicherheitseinblicke verbessern.

Stärkere Passwörter für Logins
Während SSO die Login-Bequemlichkeit bietet, sichert ein Passwort-Manager jedes Login mit einem starken, einzigartigen Passwort ab.

Reduzierte Angriffsfläche
SSO kombiniert mit einem Passwortmanager reduziert die Anzahl der Passwörter, die potenziell kompromittiert werden könnten.

☒ SSO ☒ Passwort-Manager	☑ SSO ☒ Passwort-Manager	☑ SSO ☑ Passwort-Manager
• Hohes Risiko für Datenlecks • keine Sichtbarkeit und Kontrolle • keine orndnungsgemäße Deaktivierung von Benutzern	• Teilweise Angriffsfläche (wenn SSO nicht greift) • Teilweise Sichtbarkeit und Kontrolle • Teilweise orndnungsgemäße Deaktivierung von Benutzern	• Geringe Angriffsfläche • Volle Sichtbarkeit und Kontrolle • Vollständige und saubere Deaktivierung von Benutzern

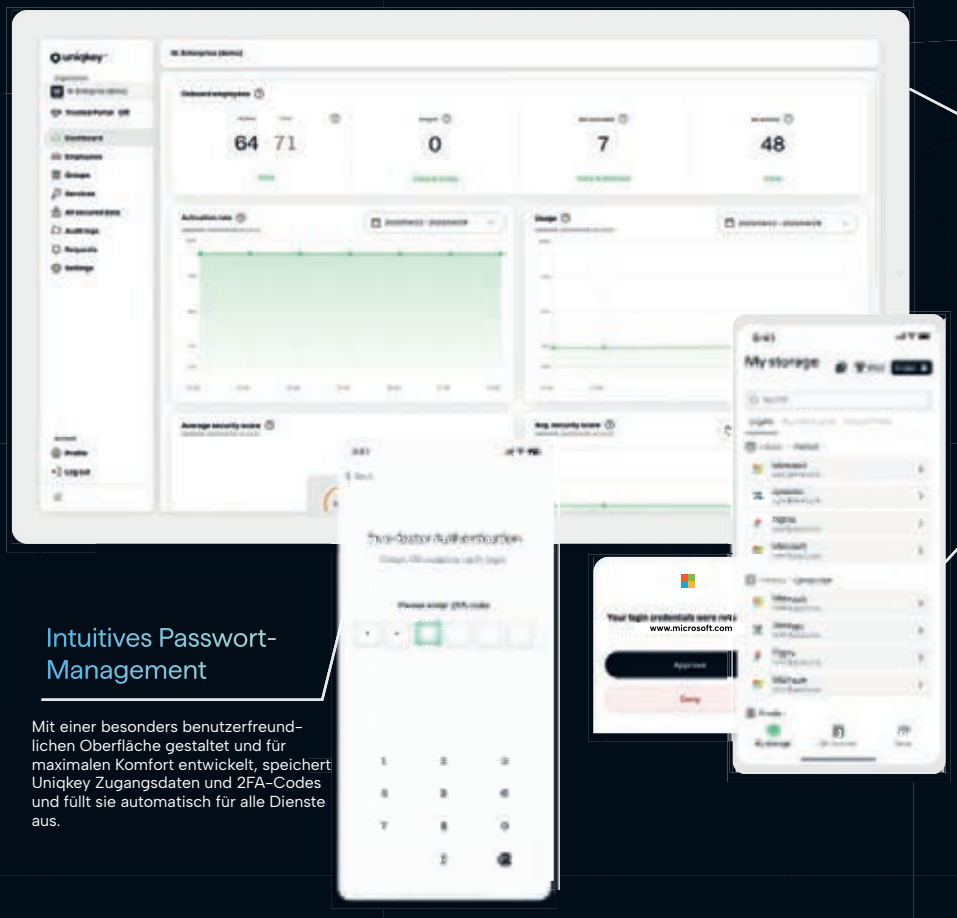
Lernen Sie Uniqkey kennen

Europas Business-Lösungen: Passwort- & Access Managementment

Uniqkey ist eine europäische Passwort- und Access Management-Lösung. Für Unternehmen und IT-Experten entwickelt, optimiert sie das Passwortmanagement, bietet müheloses Benutzererlebnis und zentralisierte Admin-Kontrolle

Erstklassige Sicherheit
Uniqkey nutzt Zero-Knowledge-Architektur, um verschlüsselte Daten offline auf dem Gerät zu speichern, was Sicherheit auch bei Datenschutzverletzung gewährleistet.

EU-genehmigte Privatsphäre & Compliance
Daten werden in dänischen Rechenzentren gespeichert, um die Privatsphäre zu gewährleisten und Datenübertragungen ins Ausland zu vermeiden.



Verwaltung von Mitarbeiterzugängen

IT-Administratoren erhalten ein zentrales Dashboard für einfache Kontrolle und Übersicht über Mitarbeiterzugriffe und Unternehmenskonten.

Automatische 2FA

Uniqkey unterstützt die automatische Zwei-Faktor-Authentifizierung für alle Dienste, maximiert die Sicherheit und beseitigt gleichzeitig Unannehmlichkeiten.

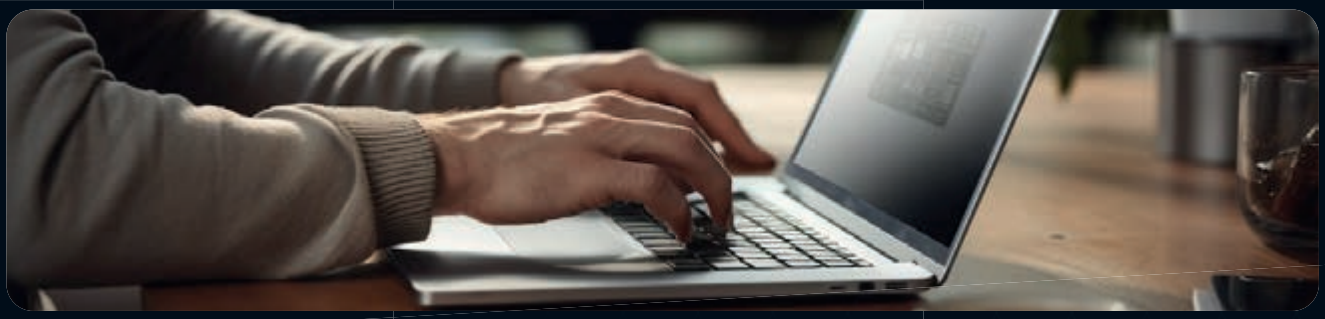
Intuitives Passwort-Management

Mit einer besonders benutzerfreundlichen Oberfläche gestaltet und für maximalen Komfort entwickelt, speichert Uniqkey Zugangsdaten und 2FA-Codes und füllt sie automatisch für alle Dienste aus.

Wie Uniqkey und SSO zusammenarbeiten

Nahtlosen und sicheren Zugriff mit Uniqkey und Single Sign-On erreichen

Nachdem Sie nun mit den Vorteilen von Uniqkey vertraut sind, lassen Sie uns untersuchen, wie es Ihre bestehende Single Sign-On-Lösung ergänzt, um eine robuste, benutzerfreundliche und zukunftssichere Zugriffsmanagement-Umgebung zu schaffen.



> Uniqkey ist so benutzerfreundlich, dass alle unsere Nutzer bereit waren, es zu übernehmen
>
> - Wim, VIB

Nahtloses Benutzererlebnis

Uniqkey und SSO zusammen machen Logins mühelos. Für SSO-unterstützte Dienste ist es ein Ein-Klick-Zugriff. Für alles andere füllt Uniqkey Anmeldeinformationen und 2FA-Codes automatisch aus.

Umfassende Sicherheit

SSO ist großartig für schnellen Zugriff, mangelt es aber an der Kontrolle über Passwörter. Uniqkey übernimmt hier, indem es sichere, einzigartige Passwörter generiert und speichert.

Zentralisierte Kontrolle

Uniqkey ergänzt SSO, indem es ein Dashboard für die IT bietet, um Gruppen- und individuellen Zugriff zu verwalten und das Onboarding sowie den Entzug von Berechtigungen zu optimieren.

Flexibilität und Kompatibilität

Nicht alle Dienste unterstützen SSO. Uniqkey gewährleistet sicheren Zugriff auf nicht unterstützte Dienste und schließt so die Lücken.

EU-Compliance und Datenschutz

Uniqkey und SSO bieten zusammen eine robuste, EU-konforme Sicherheitseinrichtung, die den Datenschutz mit den organisatorischen Sicherheitsbedürfnissen in Einklang bringt.

Skeptisch? Lassen Sie uns einige Mythen entlarven

Weitverbreitete Mythen entlarven

Wenn Sie skeptisch sind, ob die Kombination von SSO mit einem Passwort-Manager wie Uniqkey sinnvoll ist, sind Sie nicht allein. Lassen Sie uns einige Mythen angehen und die Kosten-Nutzen-Aspekte untersuchen.

F: Ist die gemeinsame Nutzung von SSO und einem Passwort-Manager wie Uniqkey übertrieben?

A: Die gemeinsame Nutzung mag übertrieben erscheinen, aber jede Lösung hat ihre einzigartigen Stärken, die sich gegenseitig ergänzen. SSO bietet schnellen Zugriff, während ein Passwort-Manager wie Uniqkey die Lücken für Dienste abdeckt, die nicht in SSO integriert sind.

F: Wird durch die Kombination von SSO und Uniqkey nicht alles komplizierter?

A: Diese Sorge ist verständlich, aber die Nutzung ist sehr reibungslos. SSO regelt den Zugriff auf viele Dienste, Uniqkey übernimmt den Rest. Das reduziert die geistige Belastung für den Nutzer.

F: Macht die Verwendung eines Passwort-Managers wie Uniqkey Sie nicht zu einem größeren Ziel für Hacker?

A: Man könnte meinen, dass das Speichern aller Passwörter an einem Ort Sie zu einem attraktiveren Ziel macht, aber die Realität ist anders. Passwort-Manager wie Uniqkey verwenden robuste Verschlüsselung und mehrere Sicherheitsebenen, um Ihre Daten zu schützen und Angriffe abzuschrecken.

Durchführung der Kosten-Nutzen-Analyse

Ihre Anfangskosten

- **Kauf**
  Die anfänglichen Kosten für die Anschaffung des Passwort-Managers.
- **Implementierung**
  Zeit, die in die Integration des Tools in Ihre IT-Umgebung investiert wird.
- **Schulung**
  Ressourcen für die Einweisung und das Training der Nutzer.

Ihre langfristigen Vorteile

- **Niedrigere IT-Kosten**
  Weniger IT-Stunden, die für Passwort-Resets aufgewendet werden, bedeuten Kosteneinsparungen.
- **Erhöhte Sicherheit**
  Mehr Abdeckung und stärkere Passwörter reduzieren das Risiko von Datenschutzverletzungen.
- **Reibungslosere Arbeitsabläufe**
  Automatisierte Logins beschleunigen Routineaufgaben.
- **Höhere Produktivität**
  Weniger Zeit, die für Login-Probleme aufgewendet wird, führt zu produktiverer Arbeit.
- **Compliance-Vorteile Einfachere**
  Einhaltung von Branchenvorschriften, wodurch rechtliche Risiken reduziert werden.

Zusammenfassung

Während SSO sich hervorragend dazu eignet, den Zugriff für den Großteil Ihrer traditionellen Technologieinfrastruktur zu vereinfachen, bleibt es bei der Unterstützung neuer, täglich von Teams genutzter Dienste zurück. Darüber hinaus kann SSO, allein verwendet, ein Single Point of Failure sein, der alle verknüpften Dienste im Falle einer Kompromittierung gefährdet.

Ein Passwort-Manager wie Uniqkey ergänzt SSO, indem er diese Sicherheitslücken schließt. Er hilft Benutzern, standardmäßig starke, einzigartige Passwörter für alle Dienste zu erstellen, und fügt eine zusätzliche Sicherheitsebene mit Funktionen wie Ende-zu-Ende-Verschlüsselung, lokaler Passwortspeicherung und automatischer Zwei-Faktor-Authentifizierung hinzu. Außerdem reduziert er die Arbeitslast der IT-Abteilung, indem er Passwort-Reset-Anfragen minimiert und die allgemeinen Sicherheitsprotokolle verbessert.

Zusammen verwendet, bieten SSO und ein Passwort-Manager einen ausgewogenen und zukunftssicheren Ansatz für Identitäts- und Zugriffsmanagement, der sowohl den Benutzerkomfort als auch die organisatorische Sicherheit maximiert.

Wichtigen Erkenntnisse:

01 SSO ist besonders effektiv, aber mangelt an Abdeckung.

02 Passwortmanager schließen die Sicherheitslücken von SSO.

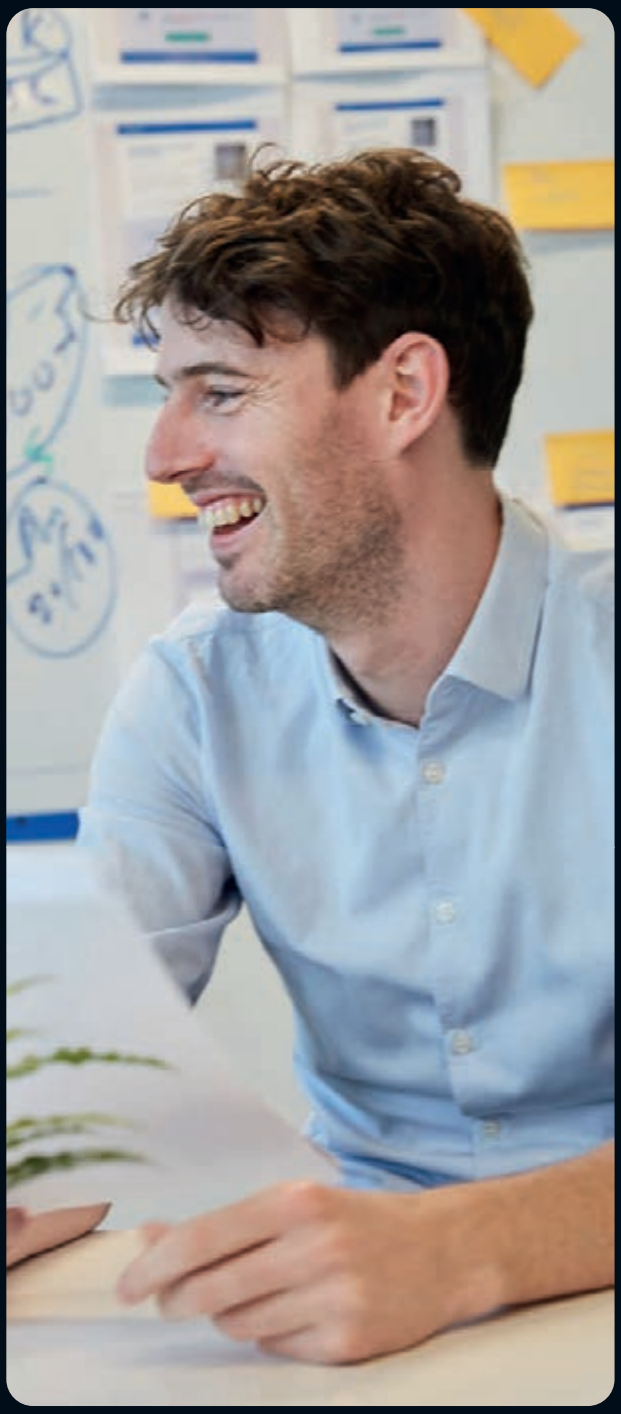
03 Zusammen diversifizieren sie die Authentifizierungsmethoden.

04 Die Kombination steigert die IT-Effizienz und Kosteneinsparungen.

05 Die vom Duo gebotene zusätzliche Sicherheit reduziert Risiken und Exposition.

uniqkey™

Bereit, Ihre SSO-Lücken zu schließen?



Bereit, die Sicherheit Ihrer Organisation zu erhöhen und das Zugriffsmanagement zu vereinfachen?

Kombinieren Sie Uniqkey noch heute mit Ihrer bestehenden SSO-Lösung und schließen Sie die Lücken in Ihrer Sicherheit. Kontaktieren Sie uns jetzt, um loszulegen.

→ Demo vereinbaren

Kontaktieren Sie unser Team:

E-Mail: info@interscale.ch
Tel.: +41 41 511 21 90