uniqkey™

The SSO Blind Spot

Why a Password Manager is Essential For Closing
Security Gaps

Table of Contents

uniqkey™

Introducing

For years, Single Sign-On (SSO) has been the go-to solution for organizations to secure access, mitigating most access-related risks and offering near-complete coverage.

However, the rise of SSO-incompatible cloud services is creating security gaps. For SSO reliant businesses, this means that an increasing percentage of their IT environment is now left uncovered and exposed.

This e-book shows how pairing SSO with a password manager can fill these gaps. When used together, they offer a comprehensive approach to identity and access management that maximizes coverage without sacrificing convenience. In the following pages, we'll make the case for why combining these solutions is crucial to staying secure in our digital age.

What you will learn:

01 Understand the role and limitations of SSO.

02 Discover how password managers fill the gaps left by SSO.

03 Learn How Uniqkey and SSO work together.

04 Debunk common myths about combining SSO and password management.

05 Assess the ROI of combining SSO and password managers.

uniqkey™

If You Only Have 5 Minutes

Digital Transformation Invites New Threats

The digital transformation wave has led to an unprecedented adoption of SaaS tools and cloud services. While technologies offer immense flexibility and scalability, they also introduce a myriad of new threats and attack vectors.

This means that …

As organizations adopt more cloud-based services, the complexity of securing these platforms grows, demanding a more robust and versatile set of security solutions to ensure coverage.

The Limits of SSO in Our Cloud Era

SSO systems offer a streamlined login experience across various traditional IT platforms but have limitations when it comes to modern cloud services that often doesn't support SSO by default.

This means that …

While SSO is effective for managing access to traditional IT infrastructure, it's not the cover-all solution it used to be. Additional security measures are needed for platforms that aren't SSO-compatible.

Password Managers Fill The Gaps

Password managers like Uniqkey serve as the perfect complement to SSO solutions by securely managing credentials for non-SSO compatible services.

This means that …

Password managers fill the security gaps left by SSO by securing the use of credentials for SSO-incompatible systems and apps, therefore offering a more comprehensive security architecture.

SSO + Password Management Offers More Versatility

Pairing SSO with a password manager like Uniqkey provides a balanced security ecosystem that leverages the strengths of both solutions.

This means that …

A combined approach of using SSO for what it excels at, and a password manager for what SSO can't cover, results in a robust and holistic access security framework.

Uniqkey is a Perfect Match For SSO

Uniqkey is not merely an additional tool but functions as a strong partner for SSO solutions. It does so by adding additional security layers, such as encrypted password storage and two-factor authentication for services not covered by SSO.

This means that …

When Uniqkey is combined with SSO, the resulting security setup offers comprehensive coverage across all possible digital services, improving enterprise security and IT management without sacrificing user convenience.

uniqkey™

The Dangers of The Modern Workplace

How Rapid Changes in How We Work is Inviting New Threats

The workplace has transformed dramatically over the last decade.

Shifts like the adoption of remote work, BYOD policies, and the surge in SaaS and AI tools have revolutionized the way we work. While these advancements offer incredible flexibility and efficiency, they come with a new set of security challenges that traditional tools like SSO can't fully address.

130 SaaS apps used by the average organization in 2022.

It's A Bigger Problem Than You Think

The problem goes beyond a few services falling outside of SSO's scope. A substantial portion of today's business activities operate outside the realm of SSO. This includes everything from specialized software to niche SaaS tools and personal consumer services, all which house sensitive information. And often even if services do support SSO, the feature is only available in paid plans. When these systems go unprotected and undetected by IT, they pose serious risks that can impact an entire organization.

As we delve further, we'll discuss why pairing SSO with password management has transitioned from a 'nice-to-have' to an absolute necessity for navigating the complexities and risks of the modern work environment. But first, let's explore the factors behind SSO's rise in popularity.

"Cybercrime is the greatest threat to every company in the world."

– Ginni Rometty, CEO of IBM.

The Rise of SSO

A Strong Solution That is Now Facing Challenges

SSO has been part of the tech toolkit for a while. However, its significance has skyrocketed due to the massive shift towards cloud–based apps and services.

Originally designed to reduce password fatigue and simplify the login process, SSO has become a cornerstone in the modern IT landscape. It lets users sign in once to access various services, simplifying life for both employees and IT staff. For employees, it eliminates the hassle of remembering multiple passwords; for IT, it reduces the number of password reset calls.
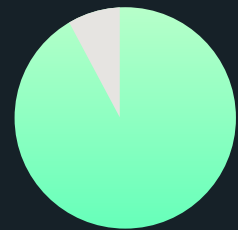
However, while SSO excels in convenience, changes in the modern business landscape mean that it's no longer the cover–all solution it used to be.

The adoption of remote work policies, Bring Your Own Device (BYOD) strategies, and the explosion of SaaS platforms have introduced nuances that SSO was not initially designed to address.

SSO Deployment

80%

of companies in the EMEA region have deployed SSO.

Estimated global SSO market size by 2023 — **$ 8.4B**

uniqkey™

The Strengths and Limitations of SSO

Uncovering Why Using SSO is Smart, But Has Critical Gaps

SSO brings ease and efficiency to IT teams and users alike, but it's not without its draw backs and security concerns. Let's explore its strengths and weaknesses

The Strengths of SSO

Lowers IT load
Implementing SSO means fewer passwords reset requests and less time spent on managing multiple authentication systems. This allows IT departments to focus on more strategic tasks.

Increased admin control
Centralized authentication via SSO provides administrators with a unified view of user activity. This makes it easier to enforce security policies, monitor suspicious activities, and even conduct audits.

Improves user experience
SSO eliminates the hassle of remembering multiple usernames and passwords. Users can access a range of services, from email to internal databases, all with a single login. This streamlined process improves user satisfaction and productivity.

Reduces password overload
With fewer passwords to remember, users are less likely to resort to insecure practices such as using overly simple passwords or reusing the same password across multiple services.

Simplifies on/offboarding
When a new employee joins or an existing one leaves, SSO makes it easier to enable or disable access to all connected systems. This speeds up onboarding and ensures that offboarding is secure and comprehensive.

SSO Strenghts

- Simplifies Access
- Lowers IT load
- Reduces password overload

- Streamlines onboarding
- Centralizes administration

uniqkey™

The Limitations of SSO

No full coverage
The biggest disadvantage to using standalone SSO is that many new SaaS tools and services aren't built to support SSO by default. This makes SSO inadequate for agile and modern businesses that increasingly rely on the use of SaaS and cloud services.

Single point of failure
SSO's centralized nature means that if it's compromised, all linked services are at risk. If your SSO provider experiences an outage or breach, your users could be locked out of all integrated systems, disrupting business operations.

Incomplete solution
While SSO simplifies the login process, it doesn't solve everything. It doesn't help your users generate strong passwords, enforce your password policies or help ease password rotations.

Not right for every use case
SSO is not suited for businesses that rely on the use of shared accounts.

The "SSO Tax"
Some vendors require premium subscriptions for SSO features. This means that relying on SSO alone could be a very expensive decision.

SSO Limitations

- Gaps in coverage
- Single point of failure
- No password security
- Doesn't support sharing
- Often require paid subscription

uniqkey™

The Role of Password Managers

Understanding The Need for Password Management in a Cloud-first Age

While SSO excels at streamlining the login process across multiple platforms, it doesn't cover all the bases when it comes to comprehensive security. This is where password managers come into play.

What Password Managers Do That SSO Doesn't

Password Managers fill the gaps left by SSO in several key areas:

- **Universal compatibility**
  Password managers cover all services by default, including those without SSO support.

- **Creating strong passwords**
  Generating strong, unique passwords for every service is easy with a password manager.

- **Enforcing password policies**
  Password managers help enforce password policies and facilitate regular password changes, features lacing in SSO solutions.

Main Benefits of Password Manager

1. Main Benefits of Password Manager
2. Improves password security
3. Increases productivity

Security Features Unique to Password Managers

Password managers also bring their own set of unique security features to the table:

Two-factor authentication
Many password managers support 2FA, adding an extra layer of security to the login process.

Safe password storage
Password managers keep passwords stored safely, encrypted and easily accessible on multiple devices.

Secure sharing
If you need to share a password within your team, virtually all password managers enable users to share logins while maintaining the integrity of your credentials.

uniqkey™

The Power Duo of Access Security

Exploring The Benefits of This Powerful Access Security Duo

While SSO and password managers each have their own set of benefits, their true potential is unlocked when used together. This synergy creates a more robust and comprehensive security framework

SSO leaves gaps in your security.

Pairing SSO with a password manager fills those security gaps

How SSO and Password Managers Complement Each Other:

While SSO and password managers each have their own set of benefits, their true potential is unlocked when used together. This synergy creates a more robust and comprehensive security framework:

Full visibility and control
Combined, SSO and a password manager covers all possible applications, platforms and services.

Enhanced security features
A password manager adds an extra layer of security via high-grade encryption and secure password sharing.

Stronger passwords for logins
While SSO offers login convenience, a password manager backs up every login with a strong, unique password.

Reduced risk of single point of failure
When you employ both solutions, you reduce the risk of relying on one.

Better auditing
Both SSO and password managers provide detailed audit logs, improving user and security insights.

Reduced attack surface
SSO combined with a password manager reduces the number of passwords that could potentially be compromised.

☒ SSO ☒ Password Management	☑ SSO ☒ Password Management	☑ SSO ☑ Password Management
• No visibility and control	• Partial visibility and control	• Full visibility and control
• Exposed to data breaches	• Partially exposed (when SSO isn't available)	• Limited exposure
• No proper deprovi sioning of users	• Partial deprovisioning of users	• Complete and thorough deprovisioning of users

Meet Uniqkey

The European Business Password and Access Management Solution

Uniqkey is a European-based password and access management solution tailored for businesses. Engineered with IT professionals in mind and designed for an effortless user experience, our platform streamlines password management while offering centralized access control for administrators.
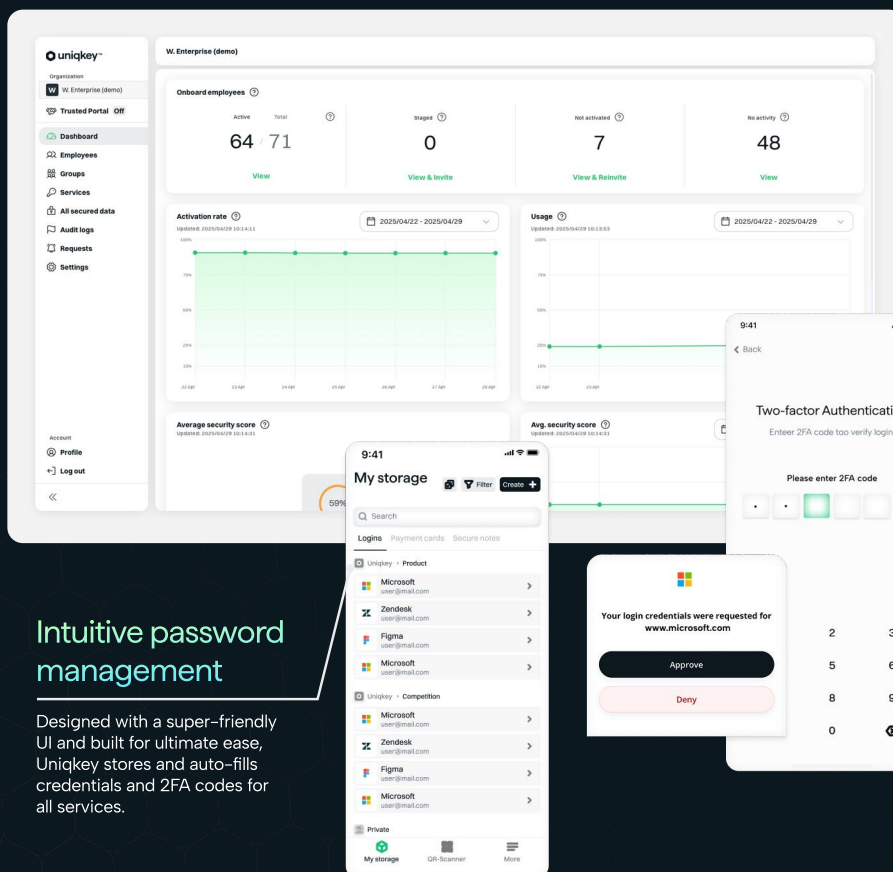
Best-in-class security
Uniqkey uses zero-knowledge architecture to store encrypted data offline on the user's device, ensuring safety even in case of a breach.

EU-approved privacy and compliance
Data is stored in Danish data centers, ensuring privacy and avoiding overseas data transfers.

Employee access management

IT admins are provided with a centralised dashboard for easy control and visibility over employee access and corporate accounts.

Automatic 2FA

Uniqkey supports automatic two-factor authentication for all services, maximising security while eliminating inconvenience.

Intuitive password management

Designed with a super-friendly UI and built for ultimate ease, Uniqkey stores and auto-fills credentials and 2FA codes for all services.

How Uniqkey and SSO work together

Achieving Seamless and Secure with Uniqkey and Single Sign-On

Now that you're familiar with what Uniqkey brings to the table, let's explore how it complements your existing Single Sign-On solution to create a robust, user-friendly, and future-proof access management setup.

Uniqkey is so user-friendly that all our users
have been willing to adopt it.

– Wim, VIB

☑ **Seamless User Experience**

Uniqkey and SSO together make logins effortless. For SSO-supported services, it's one-click access. For everything else, Uniqkey autofills credentials and 2FA codes.

☑ **Comprehensive Security**

SSO is great for quick access but lacks in password control. Uniqkey takes over here, generating and storing secure, unique passwords.

☑ **Centralized Control**

Uniqkey adds to SSO by offering a dashboard for IT to manage group and individual access, streamlining onboarding and revoking permissions.

☑ **Flexibility and Compatibility**

Not all services support SSO. Uniqkey ensures secure access to unsupported services, filling in the gaps.

☑ **EU Compliance and Data Privacy**

Uniqkey and SSO together provide a robust, EU-compliant security setup that balances privacy with organizational security needs.

uniqkey™

Skeptical?
Let's Debunk Some Myths

Debunking Common Myths

If you're skeptical about combining SSO with a password manager like Uniqkey, you're not alone. Let's tackle some myths and examine the cost-benefit aspects.

Q: Is using both SSO and a password manager like Uniqkey overkill?

A: Using both may seem excessive, but each has its unique strengths that complement each other. SSO provides quick access, while a password manager like Uniqkey covers the gaps for services not integrated with SSO

Q: Won't using both SSO and Uniqkey make things complicated

A: It's a common concern, but the experience is quite seamless. SSO handles access for some services, and Uniqkey takes care of the rest, reducing the cognitive load on the user.

Q: Doesn't using a password manager like Uniqkey make you a bigger target for hackers?

A: One might think that storing all your passwords in one place make you a more attractive target, but reality is different. Password managers like Uniqkey use robust encryption and multiple layers of security to protect your data, discouraging attacks

Doing The Cost-Benefit Analysis

Your Initial Costs

- **Purchase**
  The upfront cost of ac quiring the password manager.

- **Implementation**
  Time invested in integration the tool into your IT setup.

- **Education**
  Resources spent training your users.

Your Long-term Gains

- **Lower IT costs**
  Fewer IT hours spent on password resets means cost savings.

- **Increased security**
  More coverage and stronger passwords reduces risk of breaches.

- **Smoother workflows**
  Automated logins speed up routine tasks.

- **Higher productivity**
  Less time spent on login issues leads to more productive work.

- **Compliance benefits**
  Easier to meet industry regulations, reducing legal risks.

uniqkey™

Summary

While SSO excels at simplifying access for most of your traditional tech stack, it falls short in supporting the rise of new services adopted by teams every day. In addition, used on its own, SSO can be a single point of failure, putting all linked services at risk if compromised.

A password manager like Uniqkey complements SSO by filling these security gaps. It helps users create strong, unique passwords, supports all services by defaults, and adds an extra layer of security with features like end–to–end encryption, local password storage, and automatic two–factor authentication. Additionally, it also reduces the IT department's workload by minimizing password reset requests and enhancing overall security protocols.

When used together, SSO and a password manager like Uniqkey offer a balanced and future–proof approach to identity and access management that maximizes both user convenience and organizational security.

Key Takeaways:

01 SSO is super–effective but lacks coverage.

02 Password managers fill SSO's security gaps.

03 Together, they diversify authentication methods.

04 The combo boosts IT efficiency and cost savings.

05 Extra security offered by the duo reduces risks and exposure.

uniqkey™

Ready to Close Your SSO Gaps?

Ready to elevate your organization's security and simplify access management?

Combine Uniqkey with your existing SSO solution today and close the gaps in your security. Contact us now to get started.

→ Schedule a Demo

Contact our team on:

Email   sales@uniqkey.eu
Phone   +45 88 74 29 29