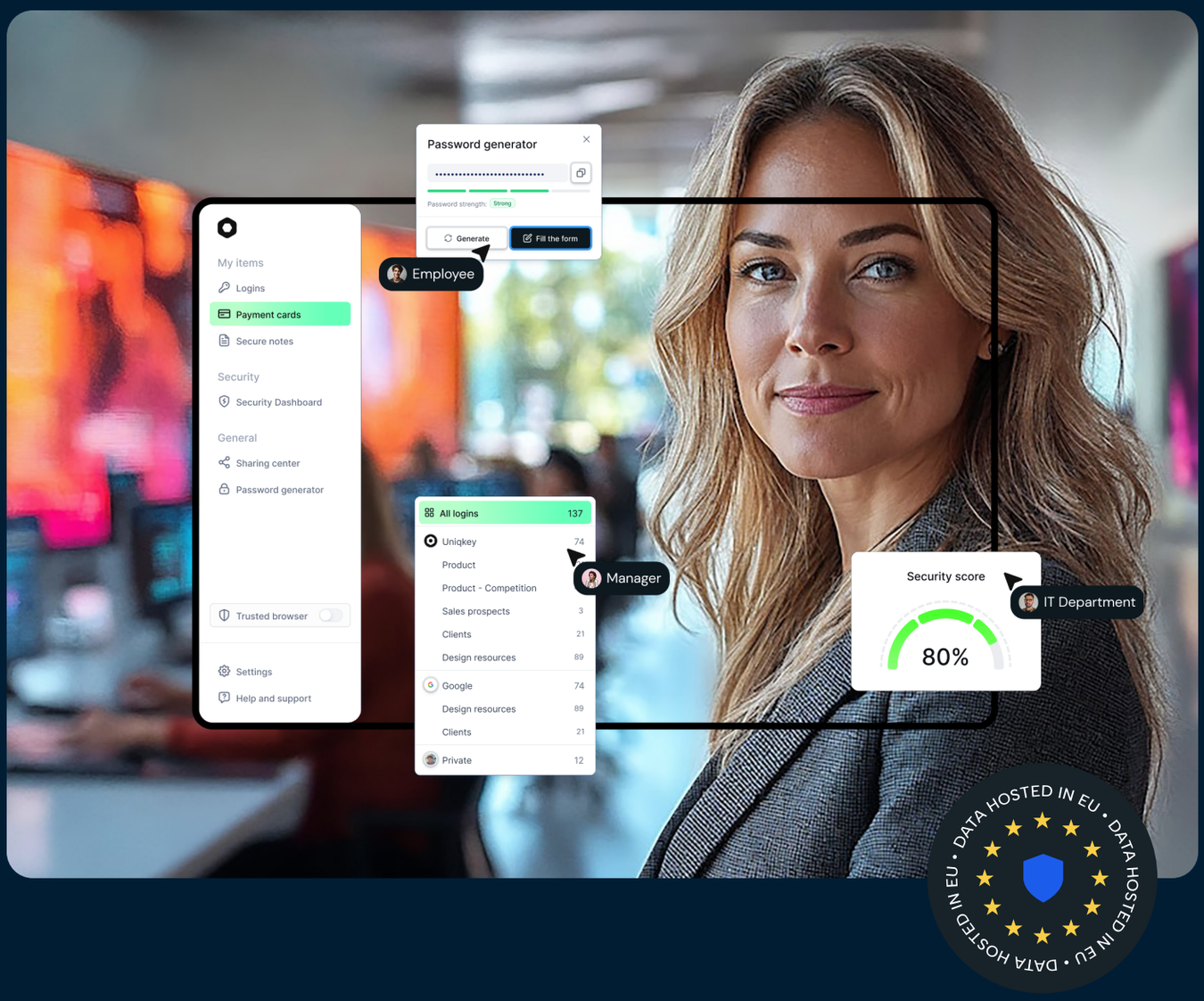


uniqkey™

Protect every login.
Access with confidence.

Smart password and access management with strong security, simplified for your entire organization. Fully compliant and trusted by Europes leading enterprises.

Users Love Us

Easiest Admin Mid-Market WINTER 2025

High Performer EMEA WINTER 2025

Best Support WINTER 2025

Fastest Implementation Mid-Market WINTER 2025

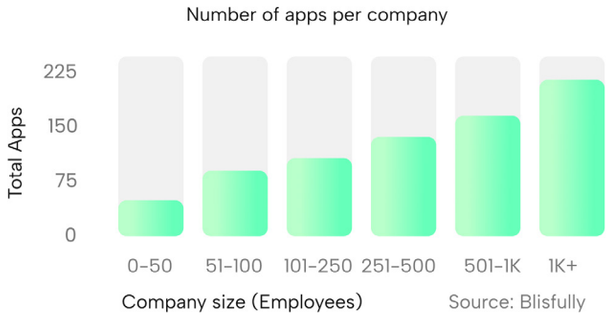
Best Est. ROI Mid-Market WINTER 2025

Why cybersecurity needs to be a top-priority
for companies in 2024 and beyond

Cyberattacks have become an existential threat to organizations
Fueled by a surge in global cloud adoption, digital transformation and remote work, cybercrime has grown to become the biggest threat facing organizations today. According to TechJury (1), 64% of companies worldwide have experienced at least one form of cyberattack, with damages ranging from ruined brand reputation and broken customer trust to severe financial costs.
This alarming trend puts great pressure on companies – particularly in Europe as Europe is one of the most digitized areas of the world – to invest heavily in cybersecurity or to deal with the business-crippling costs of an inevitable cyber incident.

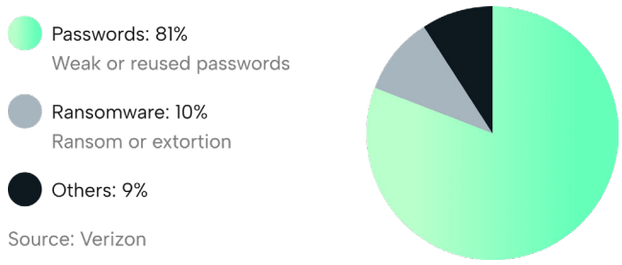
> "Cybercrime represents the biggest economic wealth transfer in history, totaling $10.5 trillion in annual costs by 2025."
> – Cybersecurity Ventures (2)

More services. More passwords. More risk.
While rapid cloud and desktop service adoption and VPN-enabled remote work is propelling productivity and business innovation, these circumstances are also introducing new serious cyber risks as companies begin to lose control and oversight of their growing digital presence. To give you an idea of how rampant this problem is, an average company with 251-500 employees manages over 123 different business apps.



Digital transformation is not a problem in and of itself.
With more services comes more logins and passwords that employees need to remember, and thus each new service added is also a new potential entry point for hackers – and a very popular one. In 2020 for instance, Remote Desktop targeted attacks increased by 768% (3).

According to Verizon's 2023 Data Breach Investigations Report, poor password security contributes to 81% of all data breaches. Considering this fact, the risks associated with this new expanding attack surface should not be ignored



Many companies try to mitigate the risk of passwords by implementing Single Sign On (SSO). Yet, while SSO simplifies logins, it doesn't necessarily boost security as it only covers a certain range of apps and services. Best security practice has always been to apply long, unique passwords for each service, but this historically has been difficult to put into action.

Poor password management is only one part of the problem. Another thing that is jeopardizing companies' security is a lack of overview and control of who has access to what. If you can't control which employees have access to which systems it becomes increasingly difficult to uphold security standards across your organization.

The dark side of digital transformation
The main problem with digital transformation is that most businesses security infrastructure is not designed to protect cloud and desktop services. Worse yet, many companies are unaware of their "digital footprint", resulting in a rise of unknown cloud, desktop and SaaS use, known as Shadow IT.

> "80% of workers admit to using SaaS applications at work without getting approval from IT."
> – Microsoft 2022

How to stay safe in a digital world
Today, anyone can start using off-premise services, which makes it difficult for IT managers to manage and maintain a high security level across the organization. Only protected by a username and a password, these services all share the same breach vulnerability.
Today, to mitigate the risk of these new attack surfaces, companies need to improve their access security. And the most impactful way to achieve this is to reclaim control and overview of all digital assets, spread the use of 2FA and enforce better password security org-wide. While great in theory, these initiatives are hard to implement in today's fast-paced digital work environment. In such an environment, relying on flawless human behaviour to stay secure is a plan doomed to fail because human error is involved in 95% of all cyber incidents (5). Instead, to succeed, companies need a solution that removes as much of the human factor from the equation as possible.

(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

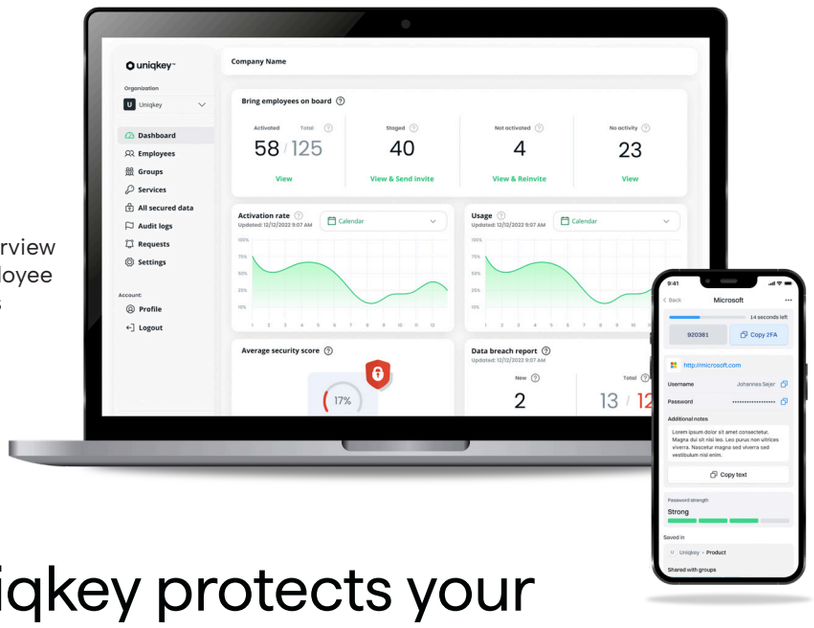
Uniqkey helps companies stay safe in a digital world by simplifying cybersecurity

In a time of exploding cloud, SaaS and desktop use, employees are drowning in passwords and companies have lost their digital overview. Uniqkey protects companies against 81% of all data breaches by automating password-use in the workplace, while giving admins the overview and control they need to keep the organization protected and productive.

A simple solution for a complex problem
By combining human-friendly password managent, automatic 2FA and a centralized access management platform, Uniqkey delivers a simple solution to a complex cybersecurity problem.
The risks of poor password hygiene, shadow IT and lacking visibility is instantly reduced as your company takes back control of your passwords and services, and turn your employees into your greatest strength with a solution that makes it easy for people to do the right thing for security.

Gain full visibility into services used

Access Management platform gives full overview and control of all employee accesses and services



Store and manage passwords safely

The Password Manager remembers and stores private and work passwords safely

How Uniqkey protects your cloud, desktop & mobile services

For admins

Identity & Access Management
On Uniqkey's centralized IAM platform, admins have full overview and granular control of the company's services, accounts and employee accesses.

Compliance-enabling Audit Log
Compliance is made easy with Uniqkey's Audit Log. Here, admins can oversee all login activity, spot suspicious activity and oversee shared logins.

Licenses, Onboarding & Offboarding
Onboarding and offboarding can be messy. With Uniqkey, admins can assign users the relevant access rights in a few clicks – and vice versa.

Customizable Access Restrictions
To maximize security, all user access privileges can be customized to include IP, geo and time-specific restrictions.

For employees

Automatic 2FA
With auto-fill of credentials and automatic 2FA authentication, log in 4x faster, and can apply 2FA on all logins without adding friction to their login flow.

Intuitive Password Manager
Uniqkey's Password Manager securely stores and saves employee's passwords and auto-fills them for them when they need to use them.

Integrated Password Generator
Equipped with a password generator, employees can upgrade their password-security by generating high-strength passwords in an instant.

Easy & Secure Password Sharing
With Uniqkey, individuals and departments can share passwords with each other without revealing the password in the process – and for a limited duration.

About Uniqkey.

Uniqkey is a Danish cybersecurity company helping hundreds of European companies guard themselves against password-related cyberattacks. Founded in 2017, Uniqkey now employs more than 50 talented individuals from 6 nationalities across 3 different European countries.

Security architects and senior advisors from HSBC Bank, VISA, UK Parliament, and NNIT are behind the success of Uniqkey's infrastructure and security. With many years of experience, the foundation of Uniqkey is based on state-of-the-art technology specializing in infrastructure, hosting, security, and encryption, which led to Deloitte naming Uniqkey "cybersecurity entrepreneur of the year" in 2018.

All data is locally encrypted and protected with the user's master password and stored on their phone. Uniqkey does not have access to data or passwords and cannot decrypt user or company data. Our solution is tested by customers through thorough POV courses.

Technical specifications

- ISAE 3402 certified based on ISO 27001 controls
- ISAE 3000 GDPR Certified
- Uses Zero-knowledge Proof & Secure Remote Password Protocol
- All data is encrypted offline and locally on the employees' phones
- Data is protected by AES 256 and SHA-3 encryption
- Uniqkey does not store personal and sensitive data from customers.
- 99.9% stable SLA uptime
- Has third-party Certification and Audit.
- Uniqkey regularly reviews audits and evaluates security processes through external consultants.
- Full support for both IT responsible and employees

A selection of European businesses who trust Uniqkey

St Helena Government · Van Gogh Museum Amsterdam · Omnicom MediaGroup · Sunset Boulevard

KMD · Næstved · Søstrene Grene All Over the World · hordijk

Raseborg Raasepori · AVEX · CALJAN · CROP

uniqkey™

Leading the next era of European security compliance.

Email: hello@uniqkey.eu
Tel no.: +45 7196 9967

To learn more or request a free business trial go to www.uniqkey.eu