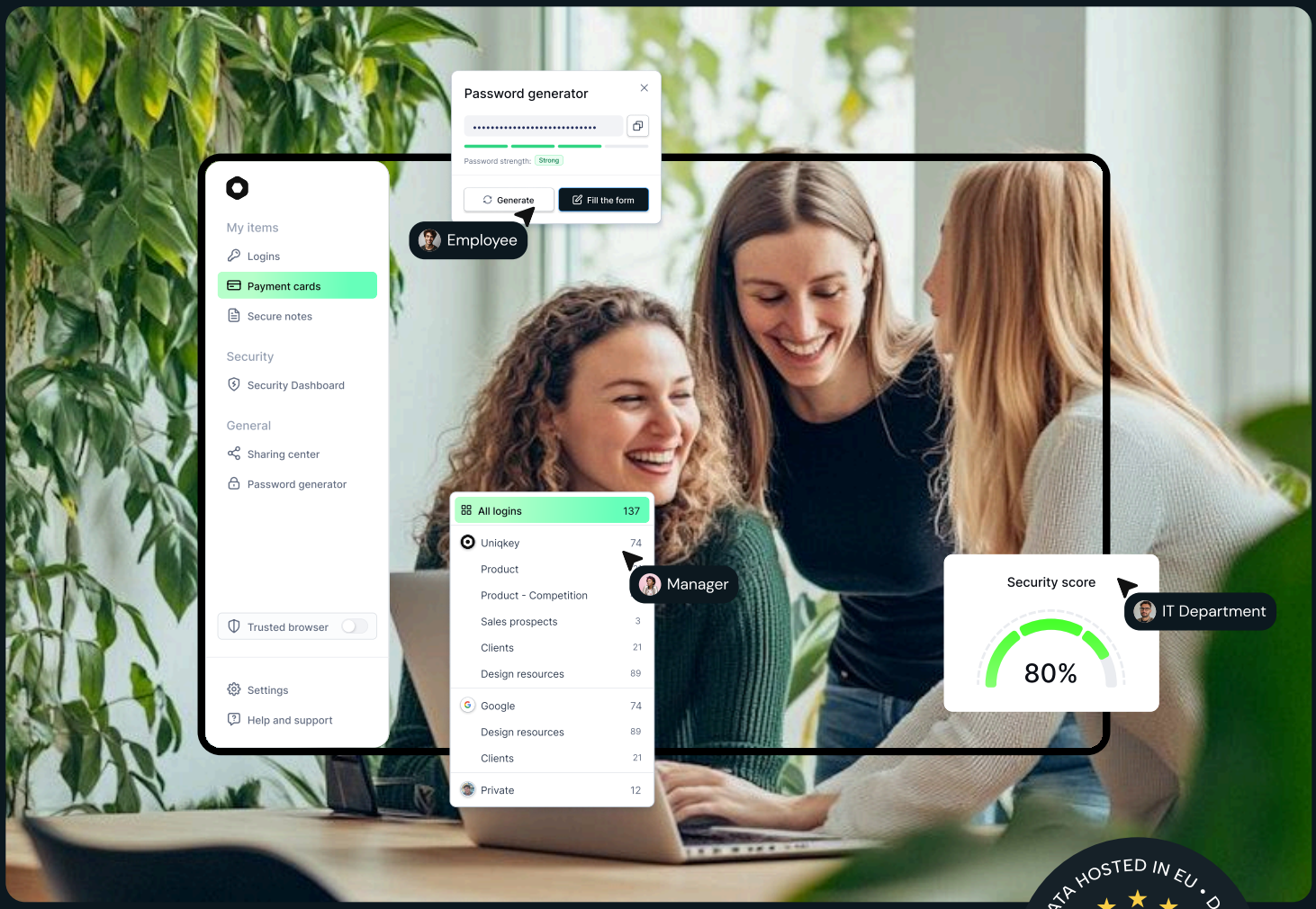


uniqkey™

The Hidden Cost of Digitalisation

Digital tools promised speed, flexibility, and growth. In practice, SaaS expansion has multiplied logins, credentials, and access friction across the workday. The hidden cost of digitalisation is the productivity you lose without noticing.

WINTER 2026 Best Est. ROI MID-MARKET

WINTER 2026 Easiest Admin MID-MARKET

WINTER 2026 Easiest To Use MID-MARKET

WINTER 2026 Fastest Implementation MID-MARKET

WINTER 2026 EMEA High Performer SMALL BUSINESS

WINTER 2026 High Performer

Where productivity disappears in modern organisations

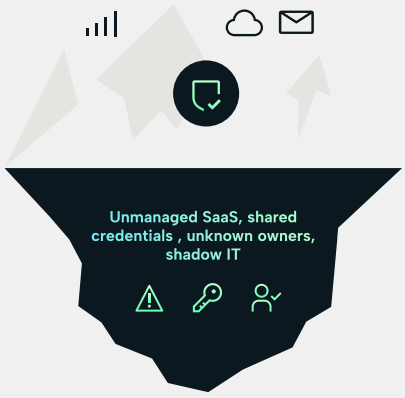
The modern workplace runs on SaaS, remote access, and constant authentication. Employees switch between dozens of systems every day, often across devices and networks. What used to be a simple login is now a repeated sequence of passwords, one time codes, approvals, and recovery steps.

Most IT teams recognise the pattern. A single missing credential, a locked account, or another prompt in an authenticator app does not just slow one person down. It creates interruptions, support tickets, and compliance effort that scale across the organisation.

As digitalisation accelerates, identity and access become the operational control plane. When access is not standardised, the hidden cost shows up as lost time, manual work, and avoidable friction across employees, IT, and compliance.

The dangers of the modern workplace

130 **SaaS apps is the average number a midsize organisation relies on**	This scale amplifies credential sprawl and makes manual access control impossible to sustain.
30% **of SaaS licenses purchased by companies go unused**	It represents significant waste, not only financially, but also by increasing security exposure, compliance risk, and operational friction.
81% **of breaches are linked to weak or reused passwords[1]**	Incidents create downtime, disruption, and unplanned work across IT, security, and the business.



65% **of SaaS is used without IT approval**

Where productivity gets lost

Employees spend 11 hours a year on passwords[2]

Password entry, resets, and recovery flows create repeated interruptions and recovery time.

Businesses spend 7.5 hours a week on security compliance[3]

A significant portion is evidence gathering, access validation, and audit follow up.

20–50% of help desk calls are password resets[4]

Password resets are a recurring operational cost and a common cause of lost working time.

Password resets cost companies up to $1M/ year[5]

These costs are symptoms of weak access standardisation. When identity controls are inconsistent across systems, the organisation spends time compensating with tickets, manual checks, and reactive reporting.

(1) 2020 Verizon Data Breach Investigations Report
(2) World Economic Forum, Passwordless Authentication, 14 January 2020
(3) Vanta, "Introducing Vanta Trust Center and the State of Trust Report", 8 Nov 2023
(4) Dark Reading states that Gartner has reported between 20% and 50% of help desk calls are for password resets
(5) Uniqkey, Ensure Better User Connectivity and Avoid Malicious Passwords, Uniqkey Resources page

One platform. Three outcomes.

Uniqkey strengthens the access layer by reducing credential friction while increasing control and visibility. It helps organisations standardise secure behaviour without adding burden to employees.

Employee

Friction free access that keeps work moving

Employees lose time when authentication becomes a repeated interruption. Secure access should remove steps, not add them.

- Autofill reduces manual credential entry and eliminates copy paste behaviour
- Integrated 2FA reduces switching and interruptions
- Secure sharing removes the back and forth in hybrid work

Employees stay in flow and follow secure practice by default, without extra effort.

IT

Operational control with less manual access handling

Identity workload is often hidden inside tickets, access requests, and on/offboarding tasks. When access is inconsistent across apps, IT compensates manually.

- Reduce password reset and account recovery overhead by removing daily credential friction
- Standardise onboarding and offboarding actions through centralised access management patterns
- Gain visibility into shared access activity, including who shared what and when, to reduce unmanaged credential use
- Reduce shadow IT discovery work by improving access visibility and control across services
- Enable the transition towards passkey based and phishing resistant authentication models

IT reduces operational overhead while improving access visibility and governance across the organisation.

Legal and Compliance

Audit evidence without the scramble

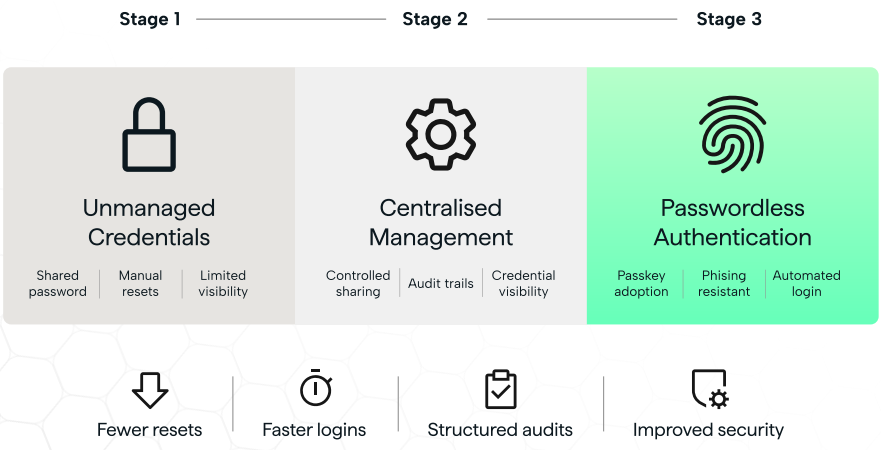
Compliance effort increases when access data is fragmented across systems and teams must reconstruct events manually.

- Clear, timestamped access activity supports faster evidence collection
- Repeatable reporting reduces audit follow ups and reduces time spent validating access history
- Better access visibility supports regulatory expectations linked to access control, incident readiness, and accountability

Reporting becomes structured and repeatable, which reduces time spent preparing audits and responding to compliance questions.

Identity Maturity Roadmap

From password sprawl to passwordless control



Make secure behaviour the easiest behaviour.

The productivity impact

Employees log in up to four times faster with autofill and integrated 2FA

This reduces repeated micro interruptions across the workday.

Password resets and access related tickets reduce

Lower reset volume reduces downtime for employees and frees IT capacity for higher value work.

Companies save 9.8 hours per employee per year from faster logins[6]

Companies save €480 per employee on password resets and up to 37% software license costs by reducing unused license.[7]

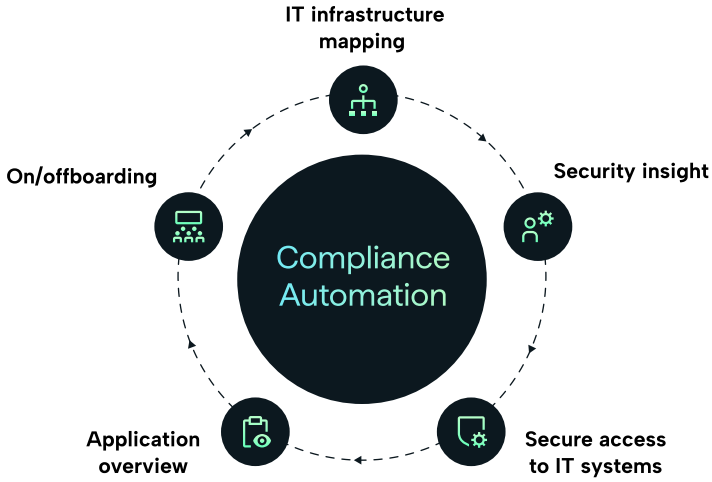
1,000 hours reclaimed per year in a 100 person organisation.

> The automatic insertion of One-Time Passwords (OTP) has significantly reduced the hassle of 2FA for users.
>
> – Sigurd Felix, IT Manager CROP

Compliance made simple and faster

Modern IT teams lose capacity to repetitive assingments related to access management and compliance work. Onboarding, offboarding, access management, security overview and mapping of it-infrastructure. Uniqkey creates an instant overview of all services used across the organisation and provides centralised access management, saving hundreds of operational hours annually.

Security improves not because of compliance pressure, but because resilience is built into daily operations.



> The ease of creating shared vaults and assigning users has improved access speed to our 1,000+ password entries
>
> – Rob De Zwaan, CISO Van Gogh Museum Amsterdam

Rethinking productivity in a digital first environment

Digitalisation will continue to increase the number of applications, identities, integrations, and regulatory obligations organisations must manage. Productivity gains will not come from adding more tools, but from standardising the identity and access layer across them.

Forward looking organisations are shifting their mindset:

- From password management to identity governance
- From reactive resets to phishing resistant authentication
- From manual evidence collection to structured, real time visibility

In the coming years, access will define both operational efficiency and regulatory resilience. The organisations that treat identity as infrastructure rather than administration will move faster with less risk.

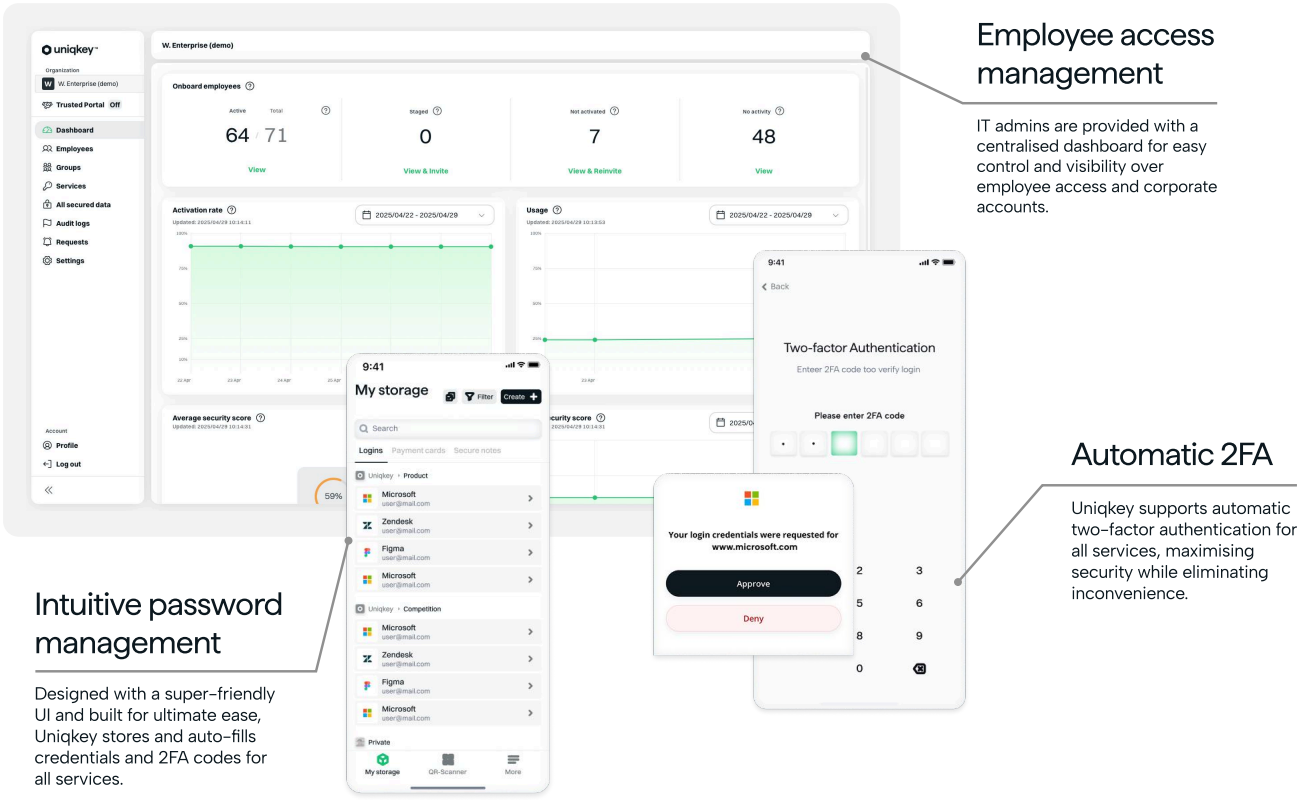
(6) Based on 20 logins per day, saving 8 seconds per login, across 220 working days
(7) Based on yearly cloud spend and avg. monthly salary.

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.

Reclaim productivity without trading away control

Uniqkey helps organisations move faster by reducing daily access friction, lowering reset volume, speeding up onboarding and offboarding, and improving visibility across unmanaged services. Built and hosted in Europe, Uniqkey supports organisations that need strong security outcomes and operational efficiency under European jurisdiction.

DATA HOSTED IN EU • DATA HOSTED IN EU • DATA HOSTED IN EU •

Talk to an expert or request a demo at Uniqkey.eu

Protect every login. Access with confidence.

Uniqkey is Europe's trusted password and access management platform – purpose-built for companies that demand security, simplicity, and control.

Engineered by European cybersecurity experts, our platform combines military-grade encryption with an effortless user experience. We remove complexity from everyday workflows, helping employees stay secure without slowing them down. From auto-filling 2FA codes to streamlining access across your cloud environment, Uniqkey keeps security frictionless and productivity high.

With real-time visibility across your entire infrastructure, IT teams gain complete control over access rights, employee activity, and security scores – empowering them to defend against threats and drive compliance with confidence proactively.

Seamlessly integrated with Microsoft and other core systems, Uniqkey makes provisioning and offboarding fast, automated, and secure.

Technical specifications

- ISAE 3402 type 2 certified based on ISO 27001 controls
- ISAE 3000 type 2 GDPR Certified
- Uses Zero-knowledge Proof & Quantum Encryption
- All data is encrypted offline and locally on the employees' phones
- Data is protected by AES 256 and Argon2id encryption
- 99.9% stable SLA uptime
- Has third-party Certification and Audit from PWC
- 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 · Nestved · Kristene Grenes Handelskompagni · hordijk

Raseborg Raasepori · AVEX · Caljan · CROP

uniqkey™

Email: hello@uniqkey.eu
Tel no.: +45 88 74 29 29
www.uniqkey.eu