



Protect your company from credential-stuffing and account takeover attacks.

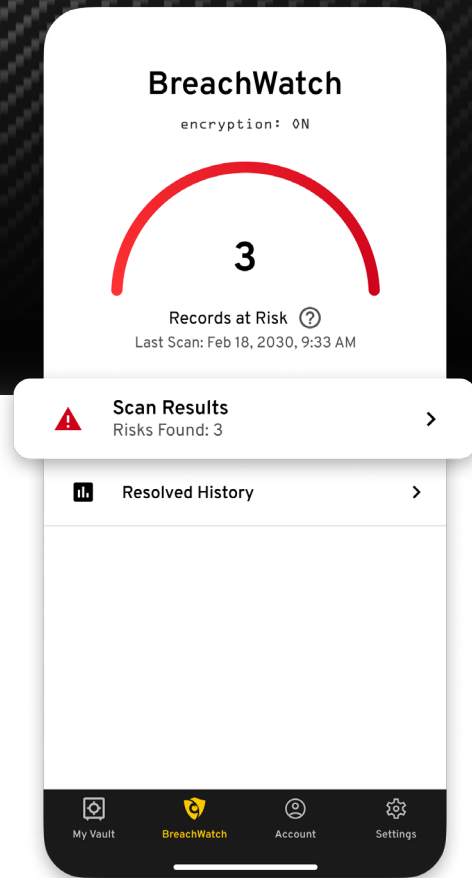
Nearly  $\frac{3}{4}$  of adults reuse passwords at least some of the time<sup>1</sup> and nearly half of them reuse passwords across personal and work accounts.<sup>2</sup> Cybercriminals know this. That's why, when they get hold of a set of user credentials that work on one website or app, they try to use them everywhere: banking and credit card sites, shopping sites – and organizational networks.

If your employees are reusing passwords across accounts and one of their other accounts is breached, cybercriminals can use the stolen credentials to access your network and data – long before the other company even knows they've been breached. On average, it takes a breached organization over three months to detect the intrusion.<sup>3</sup>

Once an organization has detected a breach, they may not promptly disclose the attack or notify compromised users. Cybercriminals don't hesitate. When they get a set of working login credentials, they put them to use very quickly, either by launching their own attacks or by putting them up for sale on the Dark Web.

### Find Out Right Away if an Employee's Password Has Been Compromised

Keeper BreachWatch™ for Business makes sure you're not the last one to find out that one of your employee's passwords has been compromised. BreachWatch for Business doesn't depend on public breach notifications.



It scans Dark Web forums and notifies organizations in real-time if any employee passwords have been compromised. This allows IT administrators to force password resets right away, minimizing the risk of cybercriminals using them to breach company systems.

BreachWatch seamlessly integrates with Keeper's Advanced Reporting and Alerts Module (ARAM) for drill-down reports and real-time alerts of BreachWatch-related alerts.

Just like Keeper's top-rated enterprise password management platform, BreachWatch for Business is affordable, easy to set up and manage and offers enterprise-level protection that scales with your business.

# 70%

of adults reuse passwords at least some of the time<sup>4</sup>

# 44%

of consumers reuse passwords across personal and work accounts<sup>5</sup>

# 101 days

average amount of time an organization takes to discover they've been breached<sup>6</sup>

## Key Features

- 01** Exclusive, proprietary zero-knowledge security model; all data in transit and at rest is encrypted; it cannot be viewed by Keeper Security employees or any outside party
- 02** Provision secure shared folders, subfolders and passwords for teams
- 03** Dynamically provision vaults through SCIM
- 04** Support for RBAC, 2FA, auditing, event reporting and multiple compliance standards, including HIPAA, DPA, FINRA and GDPR
- 05** Rapid deployment on all devices, with no upfront equipment or installation costs
- 06** Configure for High Availability (HA)
- 07** Personalized onboarding and 24/7 support and training from a dedicated support specialist
- 08** Provision users for either SSO or Master Password authentication
- 09** Enable offline vault access when SSO is not available

## Prevent Employees From Engaging in Risky Password Habits

BreachWatch is an add-on to Keeper's zero-knowledge password management, which provides organizations with comprehensive protection against password-related cyberattacks. With data breach costs rising and stolen login credentials the number-one threat vector, it's more important than ever for organizations to ensure that their employees are following good password security practices, such as using strong, unique passwords for every account and enabling multi-factor authentication (2FA) wherever it's supported.

Keeper gives IT administrators complete visibility into employee password practices, enabling them to monitor employee password habits and enforce password security policies organization-wide.

## About Us

Keeper Security is transforming cybersecurity for people and organizations globally. Keeper's intuitive solutions are built with end-to-end encryption to protect every user, on every device, in every location. Trusted by millions of individuals and thousands of organizations, Keeper is the leader for password, passkey and secrets management, privileged access, secure remote access and encrypted messaging.