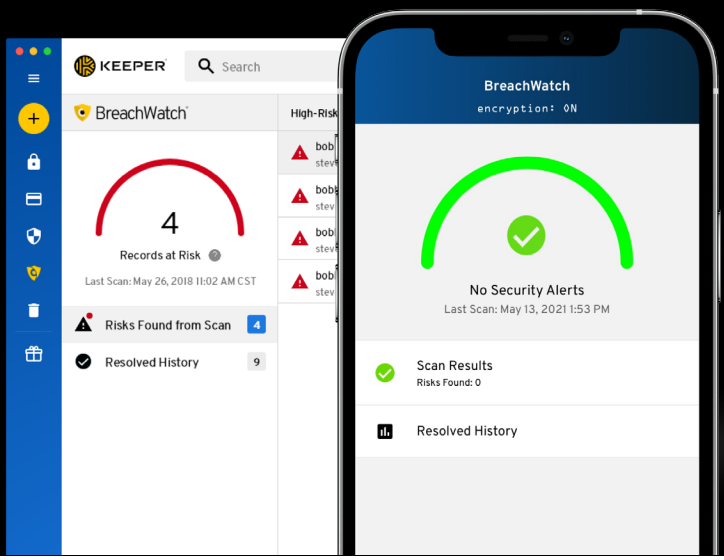
KEEPER

DATASHEET: BREACHWATCH

Protect Your Company from Credential-Stuffing and Account Takeover Attacks

BreachWatch



Nearly ¾ of adults reuse passwords at least some of the time[1], and nearly half of them reuse passwords across personal and work accounts.[2] 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.[3]

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 (EPM) 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[4]

44% of consumers reuse passwords across personal and work accounts[5]

101 Days average time for an organization to discover they've been breached[6]

Key Features

- ✓ 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
- ✓ Rapid deployment on all devices, with no upfront equipment or installation costs
- ✓ Personalized onboarding and 24/7 support and training from a dedicated support specialist
- ✓ Support for RBAC, 2FA, auditing, event reporting, and multiple compliance standards, including HIPAA, DPA, FINRA, and GDPR
- ✓ Provision secure shared folders, subfolders, and passwords for teams
- ✓ Provision users for either SSO or Master Password authentication
- ✓ Enable offline vault access when SSO is not available
- ✓ Dynamically provision vaults through SCIM
- ✓ Configure for High Availability (HA)

Prevent Employees From Engaging in Risky Password Habits

BreachWatch is an add-on to Keeper's zero-knowledge EPM, 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 Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cybertheft and data breaches. Keeper is the leading provider of zero-knowledge security and encryption software covering enterprise password management, role-based access control, event tracking, dark web monitoring, secure file storage, secrets management and encrypted messaging. Named PC Magazine's Best Password Manager (2019, 2020, 2021) & Editors' Choice (2019, 2020,2021), U.S. News & World Report's Best Overall Password Manager (2021), and the Publisher's Choice Cybersecurity Password Management InfoSec Award (2020), Keeper is trusted by millions of people and thousands of businesses to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2, FIPS 140-2 and ISO 27001 Certified. Keeper protects businesses of all sizes across every major industry sector.

Sources: [1,2,3] Ibid [4] Uk.pcmag.com [5] Keeper Workplace Password Malpractice Report [6] Darkreading.com