

# Credential-Stuffing: A Pervasive & Costly Side Effect of Data Breaches

BreachWatch<sup>®</sup> by Keeper: Enterprise-grade dark web monitoring for protecting against credential-stuffing and account takeover attacks

**30B**

login attempts due to credential-stuffing attacks in 2018<sup>1</sup>

**115M**

attempts to use stolen credentials per day<sup>1</sup>

**39%**

of adults use the same or similar passwords across online accounts<sup>2</sup>

Today's headlines are filled with news of public data breaches. However, even with all of this public awareness, the majority of individuals involved in a data breach are unaware their credentials might have been compromised. And, unfortunately, even when people are aware of a breach, they are slow to change the affected passwords.

Enter credential-stuffing. An attack where cybercriminals use passwords stolen from one breached website to attempt to break into other sites or networks via software and botnets.

As an employer, if even one of your company's employee's privileged account credentials are exposed via a public data breach, your organization is at risk.

The best way to protect your employees and your company is to detect and defend against these attacks is BreachWatch<sup>®</sup> by Keeper. It constantly scans employees' Keeper vaults for passwords that have been exposed on the dark web from a public data breach and notifies the user to take action. It also informs the administrator whether that employee has resolved the exposed password, or ignored it.


---

For more information about BreachWatch or to schedule a demo, visit <https://keepersecurity.com/breachwatch.html> or email [sales@keepersecurity.com](mailto:sales@keepersecurity.com)

---

## KEY FEATURES

- Deploys to all Keeper users and informs them of passwords breached on the dark web
- Maintains Keeper's proprietary zero-knowledge cybersecurity platform architecture
- Provides administrative oversight of users with risky passwords
- Integrates with Keeper's Advanced Reporting & Alerts Module (ARAM) for drill-down reports and real-time alerts of BreachWatch-related alerts
- Integrates with SIEM tools by sending the events from the user's device for more analysis

  
Splunk  
Sumo Logic  
Amazon S3 Bucket  
IBM QRadar SIEM

<sup>1</sup> Akami, "Credential Stuffing: Attacks and Economies", April 2019    <sup>2</sup> Pew Research Center, "Americans and Cybersecurity", January 2017