AllCreds Compromised Credential Screening enables you to detect if compromised credentials are being used by consumers and/or employees at key events like account creation, login, and password change and to take action to avoid exposure.

AllCreds COMPROMISED CREDENTIAL SCREENING

You can use *AllCreds* to determine what actions to take based on your organization's risk appetite in concert with the best possible user experience. *AllCreds* doesn't just screen for credentials that have been breached, but ones that are actively being used. Not just for compromised passwords, but for credential pairs, to reduce false positives and unnecessary friction.

- Prevent ATO by detecting when an account uses a compromised password so the user can be directed to choose one that is secure.
- Protect users AND the user experience by targeting two factor authentication (2FA) on accounts that are high risk from using compromised passwords.
- Take action with preventative measures before an attack occurs.

35+ BILLION
unique pairs of compromised credentials in our ever-expanding database

STOP CREDENTIAL STUFFING ATTACKS

Any website or app with user accounts is susceptible to credential stuffing attacks, when credential pairs obtained from one source (such as a data breach) are used to attack other sites and systems.

Credential stuffers use automation to test large numbers of known credentials against numerous targets, typically done systematically with the use of bots. The goal of the credential stuffer is to find valid credentials—ones that can successfully access the target system. Credential stuffing is effective because 52% of consumers reuse the same passwords for multiple accounts.[1]

BUSINESS USE CASES

> Credential stuffing is to ATO what card testing is to third party fraud

Identify ATO Risk at the Login Event

Nearly 23% of logins at retail sites are account takeover (ATO) attempts.[2] A login attempt providing the correct username and password combination is far from a guarantee that it is a real account holder attempting access. You must look at other signals of risk to determine if the login attempt is legitimate. Looking at the IP address or a list of passwords compromised in data breaches up to 10 years ago casts too wide of a net. Users travel and use breached passwords in troves. *AllCreds* provides high-quality risk signals that indicate the potential for ATO. For example, a login providing the correct password coming from an unusual IP address has some indication of risk, but a login presenting a password known to be compromised and actively being tested coming from an unusual IP or proxy is a strong high-risk signal. When *AllCreds* and myNetWatchman data show there is high risk of a given login attempt being ATO, you can decide to present two factor authentication (2FA) or force a password reset.

15	MILLION NEWLY-COMPROMISED CREDENTIAL PAIRS ADDED DAILY TO OUR DATABASE
90%	DECREASE IN CREDENTIAL STUFFING ATTACKS AT FORTUNE 25 E-COMMERCE COMPANY
650	MILLION USER ACCOUNTS PROTECTED BY myNETWATCHMAN

Identify and Prevent the Use of Compromised Credentials at Account Creation or Password Change Events

Applying *AllCreds* at the account creation event and not allowing the use of compromised credential pairs prevents that compromised credential pair from being used against your organization in the future. This also applies to when users seek to change their password, username or both. User accounts are

vulnerable to credential stuffing attacks because many consumers use compromised passwords and credential pairs shared across multiple accounts. By identifying and preventing the use of compromised credential pairs at account creation, you mitigate the risk of that account falling victim to a credential stuffing attack.

> Protect internal email accounts as well as customer email acccounts

Identify Employees with Compromised Credential Pairs

Workplace accounts are susceptible to credential stuffing as well, and the stakes are even higher. Attackers may be able to access proprietary or sensitive information about your organization or its customers if they gain access to an employee or contractor's account. A prime example would be the credential stuffing attacks targeting accounts that organizations held with the cloud data warehousing platform Snowflake in May and June 2024.

You can leverage myNetWatchman's *Active Directory (AD) Audit* to get ahead of potential credential stuffing attacks against your employees by detecting and eliminating the use of shared, compromised credentials on your own systems. Just as myNetWatchman clients leverage our proprietary data repository of 35+ billion compromised credential pairs with *AllCreds*, your organization can benefit from this data by using *Active Directory (AD) Audit* to ensure internal accounts are secured.

myNetWatchman

1 Diamond Causeway
Suite 21-246
Savannah, GA 31406
+1 678-624-0924

contactus@mynetwatchman.com
mynetwatchman.tech

1 - https://services.google.com/fh/files/blogs/google_security_infographic.pdf
2 - https://internetretailing.net/40-of-traffic-to-ecommerce-sites-comes-from-bots-raising-cyber-security-threat-level/