IDENTITY AUTOMATION

DATASHEET

RapidIdentity SafeID, Powered By SpyCloud

The use of stolen credentials remains the #1 way criminals gain access to networks and the sensitive information within, making them attractive targets for criminals.[1] Even with strong password policies in place, bad user password habits can put an organization at risk. However, keeping tabs on users' account security poses a substantial burden for IT teams.

RapidIdentity SafeID enables academic institutions to stay ahead of account takeovers and targeted attacks, like ransomware, by detecting and resetting compromised passwords— before criminals have a chance to use them. With SafeID, digital identity credentials are continuously monitored for passwords known to be compromised in previous breaches. When compromised credentials are detected, SafeID automatically alerts the institution, and the user can then be enrolled in a multi-factor authentication (MFA) policy until their password is safely changed and the threat is removed.

Best-in-Breed Protection via SpyCloud

RapidIdentity SafeID enables academic institutions to monitor multiple domains for exposed employee logins and PII. Each set of credentials is checked against SpyCloud's proprietary repository, the world's largest database of breach data, to identify and reset passwords that have been exposed.

Shorten Your Exposure Window

80% of account takeover losses occur early in the breach timeline.[2] SpyCloud researchers infiltrate criminal communities to recover breach data early in the breach timeline, providing quicker notice that passwords have been exposed—often months or even years before a breach becomes public.

Detect & Remediate Compromised Passwords

RapidIdentity SafeID alerts security teams of vulnerable accounts for swift action to remediate. Whether that is to kill an active session, force a password reset, or enroll the user in MFA until their password is reset, institutions can take immediate action to minimize the risk.

RapidIdentity SafeID is designed to address the unique needs of your academic institution with features including:

ACCOUNT TAKEOVER PREVENTION
Identify credential exposure up to 6-18 months before a data breach is made public and added to open-source databases.

CONTINUOUS MONITORING
Achieve constant data surveillance to prevent user account takeovers, with peace of mind that SpyCloud researchers collect an estimated one billion new breach assets per month.

PROACTIVE RISK NOTIFICATION
Provide IT instant notification as soon as an identity is deemed to be compromised due to their credentials being discovered in an external breach.

EASY ACCOUNT REMEDIATION
Mitigate the threat quickly with streamlined identification and remediation of exposed identities, which are automatically included in a reporting dashboard and delegated administration view.

SURGICAL REMEDIATION
Evaluate the credentials used by a specific identity to understand and set appropriate remediation paths based on the actual risk, instead of implementing a blanket blacklist.

NIST PASSWORD ALIGNMENT
Align with NIST password standards by checking both new and existing passwords against billions of previously-exposed passwords.

SOURCE
1. https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report
2. https://spycloud.com/products/consumer-ato-prevention/

IDENTITY AUTOMATION

FOR MORE INFORMATION CONTACT:
sales@identityautomation.com
877.221.8401
www.identityautomation.com