REPORT REPRINT

Coverage Initiation: Enzoic looks to make passwords more bearable

JULY 1 2020

By Garrett Bekker

The vendor believes that passwords will be with us for the foreseeable future, and has developed a set of APIs and Active Directory plug-ins that scan for weak and compromised passwords across the public internet and dark web to help avoid account takeover and credential-stuffing attacks.

 | WWW.451RESEARCH.COM

Introduction

The drawbacks of passwords are well-known – simply put, they can be hard to remember, easy to guess, and can be a general nuisance for both end users and security personnel. Not surprisingly, recent initiatives toward 'passwordless' authentication have gained a lot of attention, in part thanks to momentum of the Fast Identity Online (FIDO) alliance and new standards such as FIDO2, WebAuthn and CTAP. However, the passwordless movement is still early, and passwords remain a staple of many firms' security framework, despite the fact that the cybersecurity industry has been calling for the death of passwords for nearly for 20 years now.

Enzoic believes that passwords will be with us in some fashion for the foreseeable future, and has developed a set of APIs and Active Directory plug-ins that scan for weak and compromised passwords across the public internet and dark web, with the goal of helping to avoid account takeover (ATO) and credential-stuffing attacks.

451 TAKE

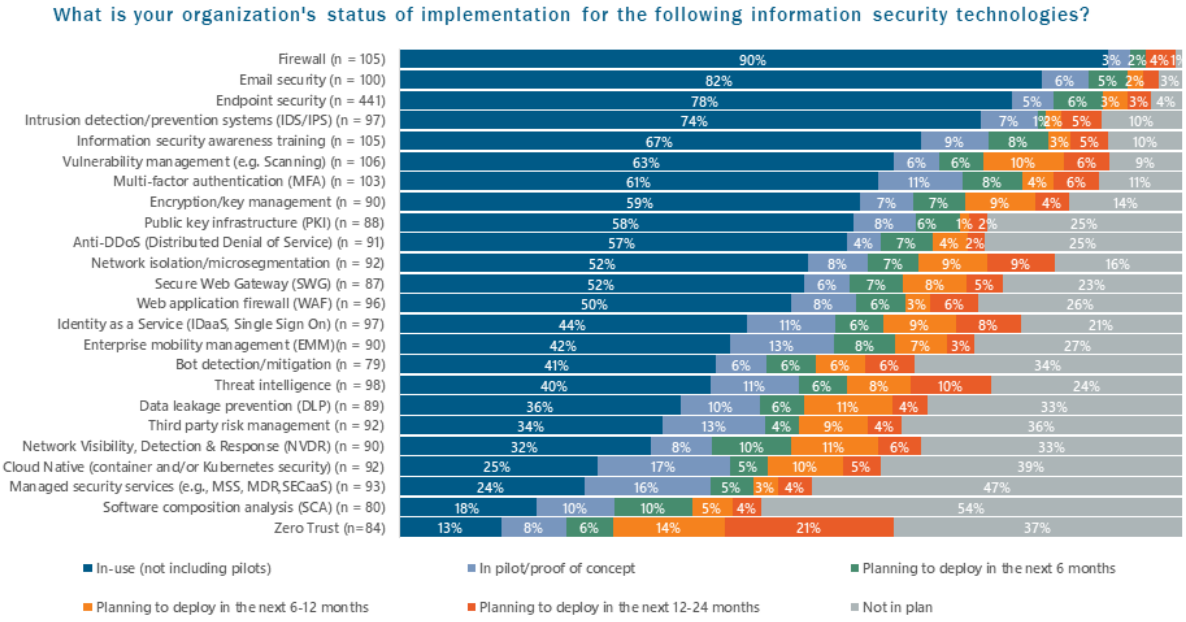
While many security practitioners are looking forward to the day when passwords have become completely obsolete, if the past 20 years are a guide, passwords are likely to stick around longer than most of us would like. Despite their shortcomings, passwords do have some benefits, mainly the fact that they are reasonably cheap and easy to understand. Factor in some of the potential issues around multi-factor authentication (MFA) deployment, and it's no wonder that the percentage of enterprises employing MFA has risen very slowly – despite the growing threat of phishing and compromised credentials. Even passwordless offerings, despite their promise, have struggled to come up with a valid account lockout and recovery capability that doesn't rely on passwords in some manner. To the extent that passwords are still a part of most firms' access control infrastructure, Enzoic provides a relatively straightforward offering that can help reduce the bigger risks of using passwords while requiring few changes to user workflows or business processes.

Context

Survey data from 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2020 study shows that just 61% of enterprises have deployed MFA – the primary alternative to passwords – well below other common security tools like firewalls (90%) and endpoint security (82%). Further, it's likely that of those 61% of organizations that do use MFA, those deployments are not enterprise-wide, but are reserved for just a subset of the total user population and for specific use cases, such as remote access VPNs, while other points of egress remain password-protected. A major reason is that most forms of MFA also suffer from their own challenges, including cost, deployment difficulties and a frequently poor user experience.

Enterprise MFA Adoption Lags Popular Security Tools

Source: 451 Research's Voice of the Enterprise: Information Security, Workloads and Key Projects 2020



Boulder, Colorado-based Enzoic was founded in 2016 by Mike Wilson (CTO), Kristen Wilson (CMO) and Josh Horwitz (COO). The latter have extensive experience at a variety of cybersecurity providers, including CA, IBM, Symantec and Webroot. The company is led by Symantec and Webroot veteran Michael Greene as CEO. Enzoic has 10-20 fulltime employees and is self-funded.

Products

Enzoic for Account Takeover started out with a password strength meter that looked for weak and compromised passwords. The meter was built upon a database of billions of leaked credentials that were discovered on dark web forums and by human threat. The company later added an API to embed the password checking into other applications. Next was another API that was capable of seeking specific combinations of username and password, which can be a better gauge of whether an account is at risk than by looking at either username or password in isolation.

More recently, Enzoic released an API with a plug-in for Microsoft's Active Directory (Enzoic for Active Directory) that screens for weak and common passwords such as root passwords ('Security123,' 'Spring2020,' etc.). The idea is to enable compliance with new NIST password guidelines that recommend dropping past best practices such as periodic password resets that typically involve substantial costs in terms of helpdesk calls, but in theory offer little in the way of enhanced security.

The 2.5 release of Enzoic added new features such as the ability to catch 'Leet speak' (e.g., 'l33t,' 'l0pht,' or '5und@y') as well as continuous password monitoring and automated daily updates to the password database that replace the previous manual update process. This allows enterprises to catch a password that is currently valid but might be compromised overnight and present a risk that might otherwise go undetected until the next manual update. When an unsafe password is flagged, automated remediation options include notifications, restricting privileges for potentially risky accounts, and requiring a password reset.

The 2.6 release introduced similarity checking to previously used passwords and root password checking to isolate the root password (e.g., 'Security' from 'Security123#!') from extraneous characters that do little to enhance security. The 2.7 release included blocking passwords containing the user's first name, last name or login name, as well as new reporting capabilities to show which users are compromised within the organization.

Strategy

Enzoic sells mostly to B2C organizations with external web and e-commerce sites. Pricing is either a monthly fee or annual subscription per user, roughly $4 per user per month on average ($3 for the AD tool).

Competition

Vendors that focus primarily on password security and most directly vie with Enzoic include nFront Security and Spycloud, both of which have features to help protect AD accounts. Providers that address ATO protection include, but are not limited to, Agari, Avanan, Barracuda, Imperva, Kount, Netacea, Proofpoint, SafePassMe, Shape Security, Spycloud, Tessian and Vericloud.

Password managers are an adjacent category that Enzoic does not consider directly competitive, but which could contend for budget dollars, in our view. Firms offering password managers include BeyondTrust (Lieberman Software), Core Security, Dashlane, Keeper, Lastpass (LogMeIn) and Roboform, while Google provides a free password manager as part of Chrome.

Enzoic could potentially complement as well as compete with a long list of MFA vendors such as RSA Security (Dell), Duo Security (Cisco), Entrust Datacard, Thales (Gemalto) and Yubico. In the realm of passwordless authentication, players include Feitian, HYPR, Nok Nok Labs, Trusona and Yubico.

SWOT Analysis

STRENGTHS

Enzoic provides a straightforward and cost-effective way to help reduce the risk of compromised passwords.

WEAKNESSES

The company relies on an AD plug-in, which implies that an organization must have Active Directory with or without Azure AD.

OPPORTUNITIES

Enzoic could target firms seeking a simple yet effective way to counter ATO and credential-stuffing attacks. New NIST guidelines require that organizations check passwords against a list of commonly used, expected and compromised passwords.

THREATS

The Covid-19 pandemic and work-from-home trends appear to have accelerated the deployment of MFA. Further, we anticipate adoption of passwordless authentication growing over time, which could place pressure on password-based offerings and constrain Enzoic's addressable market.