ENZOIC

THE CITY OF PASO ROBLES TAPS ENZOIC FOR PASSWORD PEACE OF MIND

The City of Paso Robles, located in San Luis Obispo County, California, is famous for its award-winning wines and relaxed atmosphere. As such, it's no surprise that the City is a popular tourist destination, with Paso Robles included in Travel and Leisure magazine's "25 Top Places to Visit for the Holidays" in 2015 and 2016. Located halfway between San Francisco and Los Angeles, the City is also a thriving residential community with over 30,000 residents.

Protecting city resources from a cyberattack is of critical importance for Paso Robles, particularly as threat actors are increasingly targeting smaller municipalities. For example, in February 2021, a Florida city was hit with an attack attempting to poison its water supply. Poor employee password habits were one of the vulnerabilities exploited by the threat actors, underscoring the importance of securing the password layer in combating municipal cyberthreats. David McCue, Information Technology Manager for the City of Paso Robles, knew it needed to modernize its approach to password management and began looking for a solution that would enable it to thwart credential stuffing, password spraying, brute force and other password-based attacks.

WHAT WOULD YOU WANT TO TELL SOMEONE CONTEMPLATING IMPROVING THEIR PASSWORD SECURITY?

"Employees will always find the easiest way to use their passwords so you should implement solutions that prevent threat actors from exploiting the resulting vulnerabilities. Enzoic is a great tool that ensures password security without needing any additional employee training or adding an administrative burden on IT.

Now that I know our employees are utilizing more secure passwords, I sleep better at night!"

David McCue
Information Technology Manager

WHAT TYPE OF PASSWORD POLICY AND AUTHENTICATION TOOL DID YOU HAVE BEFORE ADDING ENZOIC?

We used the built-in Windows Active Directory security to force password complexity. When our employees created new passwords, the policy required the inclusion of different character types—for example, a combination of upper-and-lowercase letters along with symbols and numbers. However, even with these settings in place, our employees were still creating easy to guess passwords and those commonly found on the web.

After doing some research, we learned this is relatively normal with default Windows security settings and other legacy password policies. In fact, the National Institute of Standards and Technology (NIST), recently revised its guidance and came out against complexity requirements, due to the fact that these policies don't actually strengthen password security. If anything, the opposite is true, as people tend to create weak passwords when they are mandated to use a combination of different characters and symbols. In light of NIST's new recommendations and our own anecdotal evidence, we began looking for an alternative that would ensure password security and lessen the likelihood of an attack.

ENZOIC

THE CITY OF PASO ROBLES TAPS ENZOIC FOR PASSWORD PEACE OF MIND

WHY / HOW DID YOU SELECT ENZOIC? WHAT SET THEM APART FROM YOUR ALTERNATIVES?

Unlike other solutions, Enzoic does not require a GINA to implement but instead uses a password DLL filter. This really helped us reduce installation complexity as we didn't have to install an agent on every employee's workstation or upgrade any infrastructure. In addition, Enzoic ensures password security is enforced throughout the entire environment in contrast to GINA, which only addresses password changes done through Windows.

Another feature that stood out to us was Enzoic's database. Containing multiple billions of exposed passwords sourced from the internet, Dark Web, and private sources, their database is updated several times daily without any involvement from our side. Finally, we were impressed by Enzoic's ability to ingest the JSON event logs into our SIEM and the automated messaging to both our employees and admins. The solution made it so easy to automate reporting and notifications and has given us hours back into our week.

HOW DID THE TECHNICAL DEPLOYMENT GO?

Our Enzoic deployment was really easy--it took under an hour! The team provided excellent technical documentation that clearly walked us through each step of the installation and configuration. They also made themselves available for any questions we had and ensured we felt supported throughout the entire process.

WHAT CAPABILITIES OF ENZOIC DO YOU FEEL HAVE BEEN MOST BENEFICIAL?

Automatically checking for weak or exploited passwords before they are saved in Active Directory has been a gamechanger. Before Enzoic, we had to manually scan or attempt to crack passwords to check for weakness and then notify employees to change them. Not only was this time-intensive, it also did little to strengthen credentials. It wasn't uncommon for employees to only change one or two characters, addressing the built-in Windows security requirements but still resulting in a relatively weak password.

Enzoic has allowed us to eliminate this vulnerability. With the solution, passwords are automatically checked at their creation and on an ongoing basis against Enzoic's database, which is always being updated. Because this checking happens entirely on the backend, employees are only aware if a compromise is detected at which time we can automate the appropriate action. This gives us peace of mind that password security is addressed without impacting employee productivity or efficiency.

CITY OF EL PASO DE ROBLES
INCORPORATED
1889