ENZOIC

DETECT AND BLOCK
COMPROMISED CREDENTIALS

CASE STUDY

LEADING HEALTHCARE ORGANIZATION STRENGTHENS PASSWORD SECURITY WITH ENZOIC

OVERVIEW

The healthcare industry is increasingly in hackers' crosshairs, with over 725 breaches reported in the sector in 2023–resulting in the exposure of more than 133 million records. Many of these attacks are fueled by poor password security, with compromised credentials behind over 80% of data breaches. In this environment, one leading regional network of healthcare providers was seeking a means of strengthening the password layer and eliminating credentials as a threat vector while also reducing the burden on IT.

TIME-INTENSIVE PROCESSES LEAVING SECURITY GAPS

The organization's legacy approach to password management was cumbersome and took at least 10 hours per week. The IT team would manually run password audits and send individual emails to all users found to have weak credentials.

Because the company had no system to enforce robust password policies, its users were often simply swapping out a character or adding an additional letter or number to the same root phrase. In addition, the IT team was concerned about the prevalence of password reuse opening the organization up to additional threats. It was also seeking a way to ensure compliance with NIST password guidelines, which emphasize the importance of screening credentials for exposure.

sales@enzoic.com 720-773-4515 3800 Arapahoe Avenue I Boulder CO

ENZOIC

DETECT AND BLOCK
COMPROMISED CREDENTIALS

> "ENZOIC'S COMPREHENSIVE THREAT INTELLIGENCE DATABASE, COUPLED WITH THE EASE OF INTEGRATION, MADE IT THE LOGICAL CHOICE."

A MODERN APPROACH TO PASSWORD SECURITY

The organization began seeking a solution that would address these requirements and free its IT team from much of the password management burden. Two providers emerged as frontrunners in its search—Specops and Enzoic. After comparing the offerings the company ultimately selected the latter, stating, "Enzoic's comprehensive threat intelligence database, coupled with the ease of integration, made it the logical choice."

Enzoic for Active Directory vets all username and password pairs against its dynamic database, powered in real-time by a combination of human and automated threat intelligence. The screening occurs at the initial creation and on an ongoing basis thereafter, ensuring that compromised credentials are kept out of Active Directory. Should a previously safe password become compromised down the road, Enzoic offers a range of automated remediation actions up to and including the immediate disabling of the account. This was a particular benefit for the network of healthcare providers, as it meant the IT team no longer had to email affected employees.

STRONGER CREDENTIALS WITH MINIMAL USER FRICTION

As they put it, "What Microsoft provides in terms of Active Directory security is pretty limited, so we're very impressed with how seamlessly Enzoic fills this gap." Because the solution runs automatically in the background, employees are unaware that the screening is occurring unless a compromise is detected. In addition to this friction-free experience, the IT team appreciates how Enzoic enables them to enforce password best practices throughout the organization rather than manually emailing users.

PASSWORD SECURITY PEACE OF MIND

The organization's Enzoic implementation was easy, with users immediately reporting positive feedback. According to the IT team, "Humans are always the weakest link, and it takes just one compromise to bring down your network. Enzoic is an important piece in our efforts to ward off this threat, and the support that we received was stellar. Quite simply, we love the product."

sales@enzoic.com 720-773-4515 3800 Arapahoe Avenue I Boulder CO