

How Enzoic is helping West-Mark comply with NIST

West-Mark is an ISO 9001 certified manufacturer of trucks and trailers based in the western United States. Their high-quality manufacturing process helped them become an essential supplier for the US Department of Defense and the United States military. However, being in this part of the nation's supply chain makes West-Mark a potential target for cybercriminals. To manage the risk, West-Mark follows National Institute of Standards (NIST) cybersecurity guidelines. Read how Enzoic is helping West-Mark comply with NIST and keep its business secure.



WHAT PROMPTED WEST-MARK TO LOOK FOR A PASSWORD SCREENING SOLUTION?

We had multiple government contracts that required us to comply with the most current version of NIST's cybersecurity guidelines.

We knew adopting all the NIST recommendations would take time, so we started with a risk analysis. We quickly determined passwords were our most significant vulnerability. I understood that we could do whatever we wanted with firewalls and virus scanning, but our weakest point would always be our people. Human behavior, particularly around passwords, is hard to control.

We made some changes directly in Active Directory and provided users with basic security awareness training. But to enhance our authentication security, NIST 800-171 and 800-63B required we prevent compromised passwords and other policy changes that we couldn't do with existing tools.

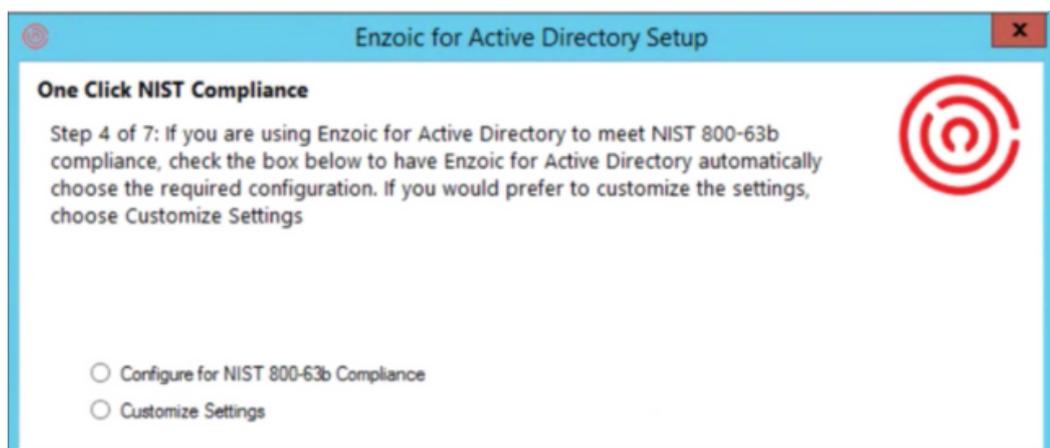


HOW WELL DID ENZOIC MEET YOUR NEEDS?

We were amazed at how well Enzoic did the job for such a modest tool. We matched each of our NIST password requirements to the features in Enzoic's service.

Some other password products we reviewed had password features NIST no longer recommends. Others included dark web monitoring that we didn't feel was relevant.

With Enzoic's continuously updated database, we could check users' passwords in real-time and know we'd be protected if they became compromised in the future.



How Enzoic is helping West-Mark comply with NIST



HOW DID YOU SECURE INTERNAL SUPPORT FOR THE INVESTMENT?

It was straightforward for me to secure support for Enzoic. We had two executives whose business strategy included going after large government contracts. I explained that we would need to comply with current NIST password requirements to make this happen and that Enzoic was the best choice.

Everyone understands the logic of password practices, but it's tough for organizations to compel good behavior. Enzoic makes it very easy to enforce good password practices that would otherwise be difficult to even monitor. So, it wasn't a hard decision to show that we had the need.

The investment has been very reasonable compared to other ways of solving this problem. Overall, I've been very comfortable with the cost and the return-on-investment.



HOW COMPLICATED WAS THE ENZOIC DEPLOYMENT?

We have a hybrid environment - Azure and on-premises deployment of Active Directory with four domain controllers. We've found Enzoic to be user-friendly and extremely easy to deploy. The settings were intuitive and even included a checkbox to comply with NIST recommended policies automatically.

Enzoic is the type of solution that you turn on and forget. As a result, password auditing and compliance couldn't be easier. We receive a daily report that tells me Enzoic is automatically running successfully. When a password is compromised, we receive an alert. When the user picks a secure password, we receive a second alert that closes the issue.



HOW DID YOUR EMPLOYEES RESPOND TO ENZOIC?

Our users like the overall changes in our passwords policy that Enzoic helped us make. For instance, we used to require a password reset every 90 days. Now, password changes only occur when they are compromised. From our employees' perspective, that's a big win.

They also liked the Windows client that informs users when they've tried to select an unsafe password. That makes choosing a new password easy for them.

"Enzoic solved the most crucial parts
of the big NIST puzzle"

David Hixson
IT Manager at West-Mark

