

Forging Effective Security with Password Enforcement

PASSWORDS ARE THE WEAKEST LINK IN ENTERPRISE SECURITY

Users Employ Poor Password Practices

90% of businesses support users who utilize the same password for multiple accounts



21% of business users are in violation of their organization's password reset policies

Businesses Fail to Enforce Strong Password Requirements

35% of organizations do not place any restrictions on password strength

57% of organizations allow users to share their passwords with others

52% of organizations do not regularly review passwords to ensure they are compliant

41% of organizations do not have a minimum password length

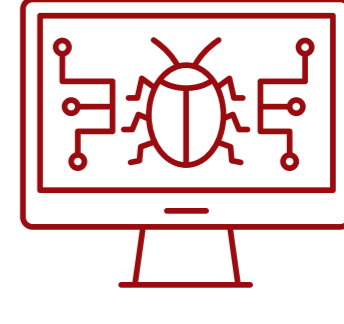
40% of organizations allow users to reuse previously set passwords



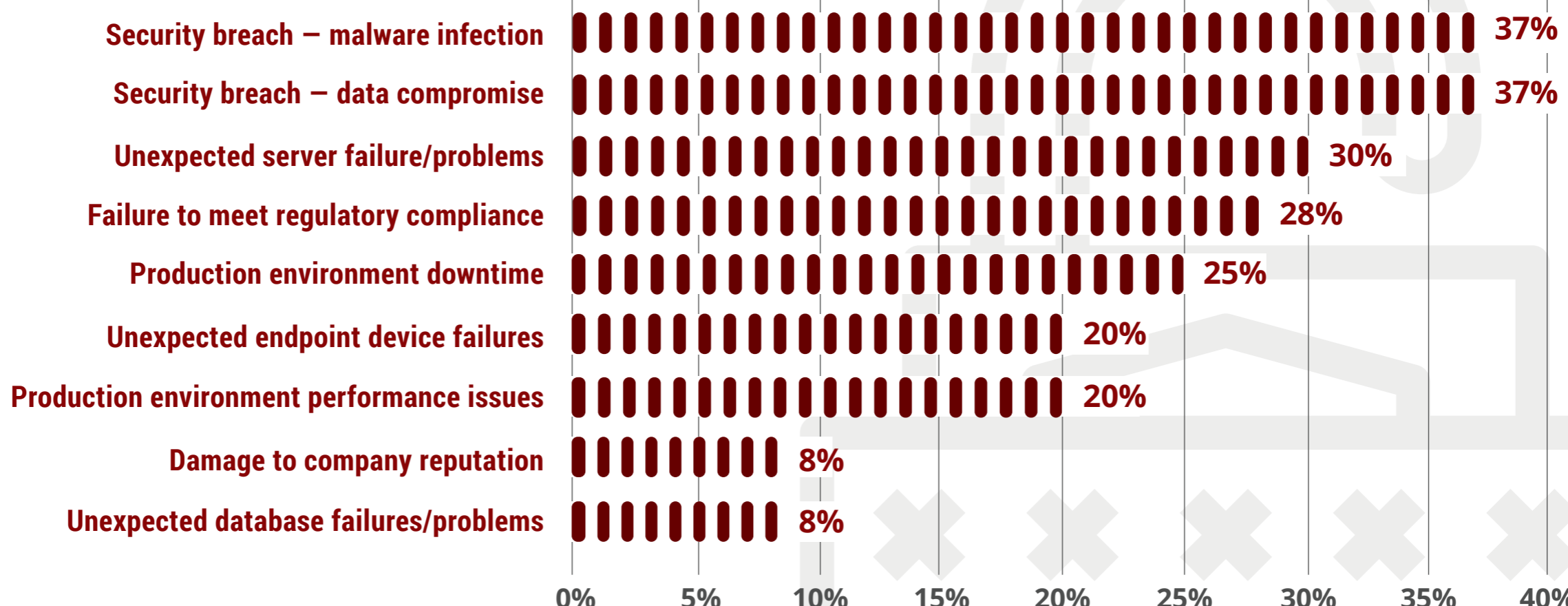
Compromised passwords are sold on the dark web, granting criminals access to businesses' most sensitive applications and data

Violations of Password Policies Result in Significant Consequences to Businesses

99% of surveyed organizations are able to directly correlate password breaches to business-impacting consequences



REAL-WORLD CONSEQUENCES THAT WERE ATTRIBUTED TO A PASSWORD POLICY INFRACTION:



\$5,580 Average amount businesses spend repairing damage caused by each violation of password policies

Key Elements Needed for Strengthening Password Controls

- ✓ **Monitor the dark web to identify compromised passwords**
Immediately close the gaps on vulnerabilities
- ✓ **Enforce the use of strong passwords at the time they are created**
Block the use of any compromised password strings
- ✓ **Unify and centralize password policies**
Enabling adaption to changing conditions in real-time

Continuous password enforcement reinforces the weak point in enterprise security to forge an unbreakable chain of access controls

Forging Effective Passwords with Enzoic for Active Directory

Leading IT industry analyst firm, Enterprise Management Associates (EMA), recommends the adoption of Enzoic for Active Directory to ensure sustained confidence in password effectiveness



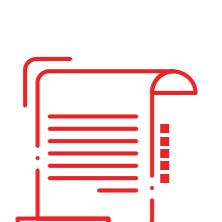
Screens for passwords in a cracking dictionary and common passwords



Provides continuous password protection
Checks for password vulnerabilities at the time they are created and every day after they are in use



Installed as a plug-in to Active Directory
Providing easy deployment while working with existing identity technologies



Aids in satisfying current NIST digital identity guidelines (NIST 800-63)

FOR MORE INFORMATION ABOUT ENZOIC FOR ACTIVE DIRECTORY, GO TO:
www.enzoic.com/active-directory/