Centrify

5 REASONS TO TURN TO MULTI-FACTOR AUTHENTICATION EVERYWHERE

Combat Data Breaches, Weak Passwords, and Phishing Attacks with MFA

To minimize exposure to credential-based cyber-attacks, cybersecurity experts as well as a growing number of industry standards and government regulations (e.g., PCI, HIPAA, NYDFS, NIST) recommend augmenting usernames and passwords with multi-factor authentication (MFA) to add an additional layer of security for access control. The following five reasons drive the need for MFA:

1. **80%** of data breaches involve stolen, weak, default, or otherwise **compromised Privileged Credentials**
   Forrester Research

2. **90%** of **verified phishing emails** were found in environments using secure email gateways
   Cofense

3. **61%** of people **use the same password** across multiple services and/or applications
   Lastpass

4. **47%** of organizations **still rely solely on username** and **password**
   Javelin Strategy & Research

5. **99.9%** An account is 99.9% less likely to be compromised **if using MFA**
   Microsoft