

MFA: The Brave New World of Authentication

Getting users' passwords isn't really that hard anymore. In fact, **77%** of stolen user credentials¹ are easily guessable passwords. With the exponential increase in data breaches, it is estimated that there are over **15 billion** leaked login credentials² circulating online. Adding MFA significantly enhances security by requiring a second piece of information to verify a user's identity.



So What'cha Steal

The velocity and increased sophistication of cybersecurity attacks makes it clear that passwords alone simply cannot provide the security needed to safeguard valuable enterprise assets.

86%

of breaches are caused by weak, reused, or stolen passwords³

71%

of basic web application attacks stem from stolen credentials⁴

57%

of organizations report daily or weekly phishing attempts⁵

MFA the Hard Way

Dramatic shifts in how we work, coupled with digital transformation initiatives has made the cloud the de facto business platform of choice.

As enterprises celebrate the operational and performance gains of their cloud platform, they have inadvertently made data — an extremely valuable commodity — an attractive asset to steal or ransom

82%

82% of data breaches involved data stored in cloud environments—public, private, or hybrid⁶

80% of organizations that did not employ a zero-trust architecture have experienced a breach⁷

80%

\$4.45M | 88 days

The average cost of a data breach rose to \$4.45 million USD; and breaches involving stolen or compromised credentials take an average of 88 days to resolve

Hackin' and Stealin'

The increasing frequency of cyberattacks, strict data protection regulations, investments in cloud technologies, the rise of BYOD, and the push for digital transformation all necessitate the implementation and adoption of MFA.



99%

MFA can block up to 99% of account takeover (ATO) attacks⁹

No Sleep Till MFA

The adoption of MFA is no optional for enterprises aiming to protect their sensitive data and systems.

With **StrongDM**, organizations can enhance their security posture, ensure compliance, and support their digital transformations strategy with confidence.

- Reduce Risk with Intelligent Decision Making**
Deny access to any resource, if accessed from a device that is compromised
- Continuous Compliance Against Unauthorized Access**
Consolidated view of who should be given access and who should have access removed or suspended
- Enhance Security with Active Alerts**
Review specific user activities by resources, tags, or source IP address

Get ready to secure everything and anything with StrongDM and MFA.

[Learn more](#)

1. 2024 Data Breach Investigation Report, Verizon, May 1, 2024
 2. "Global Cyber Threat Intelligence (CTI) Annual Cyber Threat Trends," Deloitte, March 28, 2024
 3. IBID, 1.
 4. IBID, 1.
 5. "161 Cybersecurity Statistics and Trends," Varonis, January 4th, 2024

6. "Cost of a Data Breach 2023" IBM Security, July 4, 2023
 7. "Multi-Factor Authentication (MFA) Statistics You Need To Know In 2024," Expert Insights, April 22, 2024
 8. IBID, 5.
 9. "Multifactor Authentication," Cybersecurity and Infrastructure Security Agency (CISA) [Accessed on June 7th, 2024].