

3 Reasons Credential Stuffing Attacks are on the Rise

(and How Your Organization Can Stop Them)



Financially motivated attackers have found credential stuffing attacks and account takeovers (ATOs) against online, consumer-facing businesses to be a highly effective, highly scalable way to commit fraud.

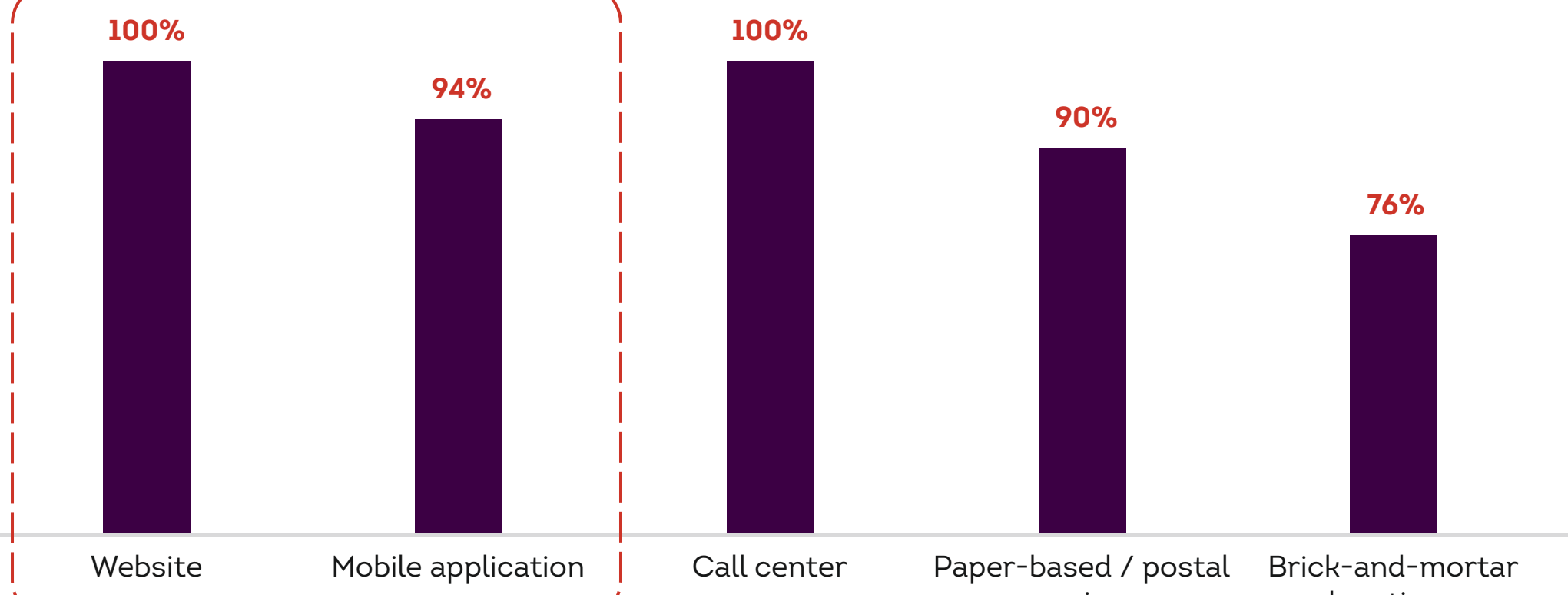
With a focus on 10 selected business-to-consumer (B2C) categories, Aberdeen's research and quantitative analysis demonstrates how the consequences of successful ATOs have grown from a "cost of doing business," to a financially material business risk.

How can your organization effectively address this risk?

Three reasons why credential stuffing attacks against B2C organizations represent such a rich opportunity for financially motivated attackers:

1 Attackers gain unauthorized access to user accounts by exploiting weak or compromised credentials.

How long-term, account-based relationships with consumers are managed



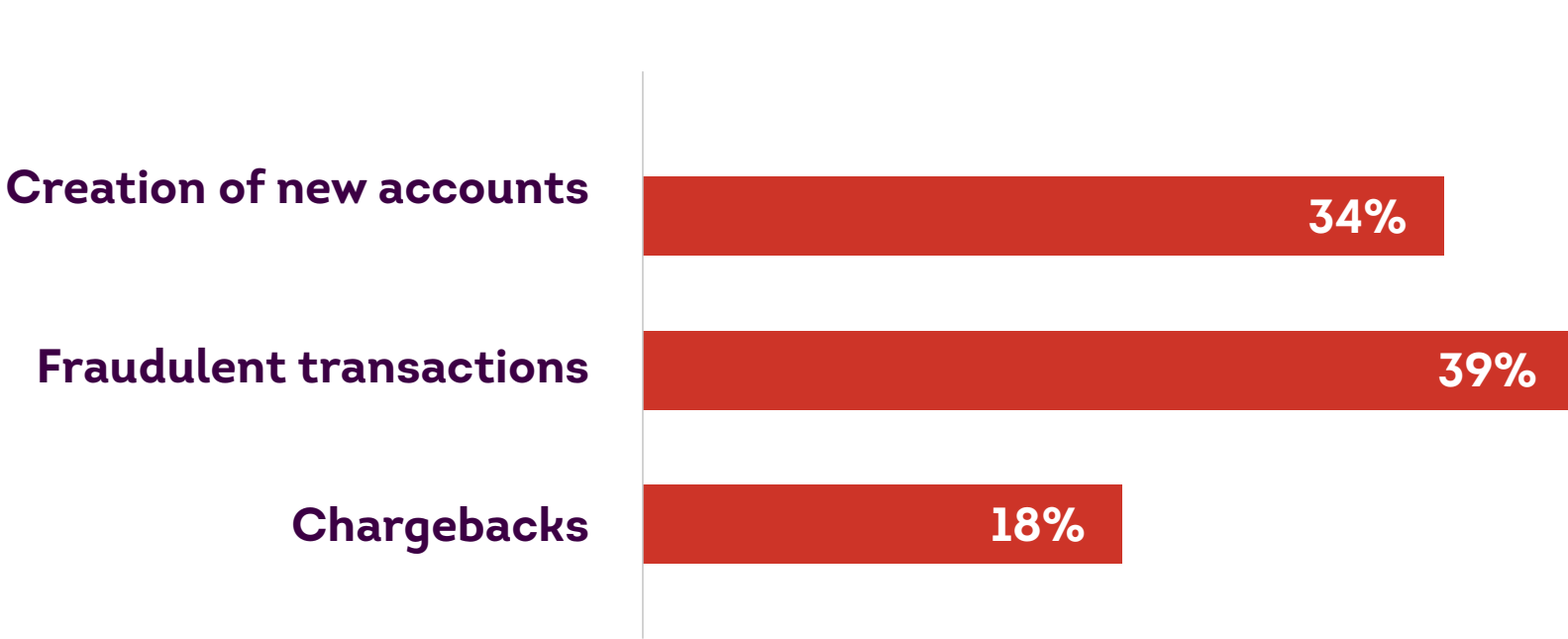
2 Credential stuffing attacks have become significantly easier for attackers to automate, at very large speed and scale.



User credentials derived from multiple mega-breaches (e.g., LinkedIn, Netflix, Gmail, Microsoft, Yahoo, Bitcoin) as of early 2021 were uploaded into a well-organized, searchable database of nearly 3.3 billion unique username / password pairs as of early 2021.

3 Financially motivated attackers are making successful account takeovers pay off, in several ways.

Consequences of successful ATOs experienced by 10 selected B2C categories

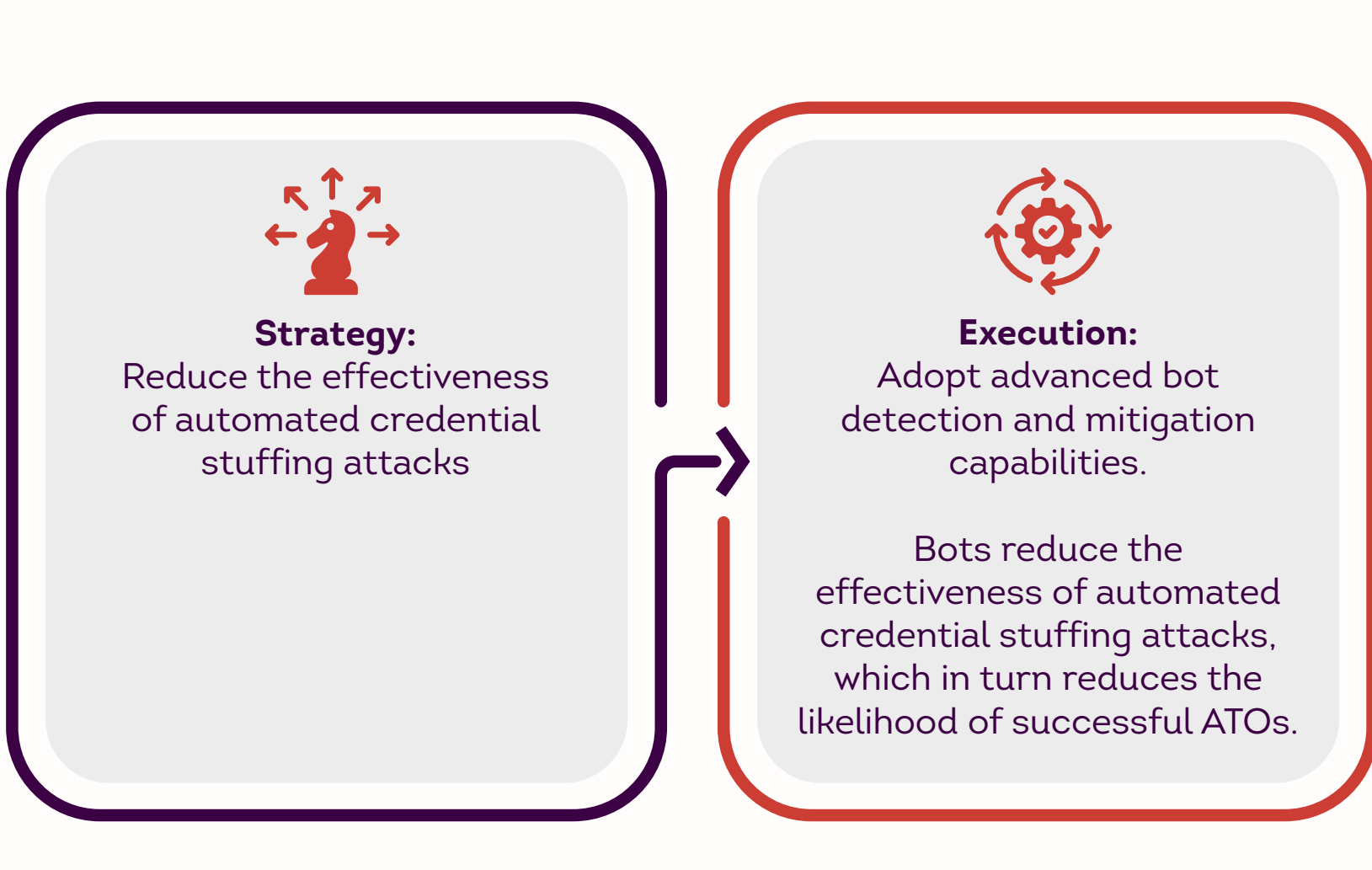


The consequences of successful account takeovers have impacted most consumer-focused organizations, driving them to proactively adopt solutions that will mitigate their risk.

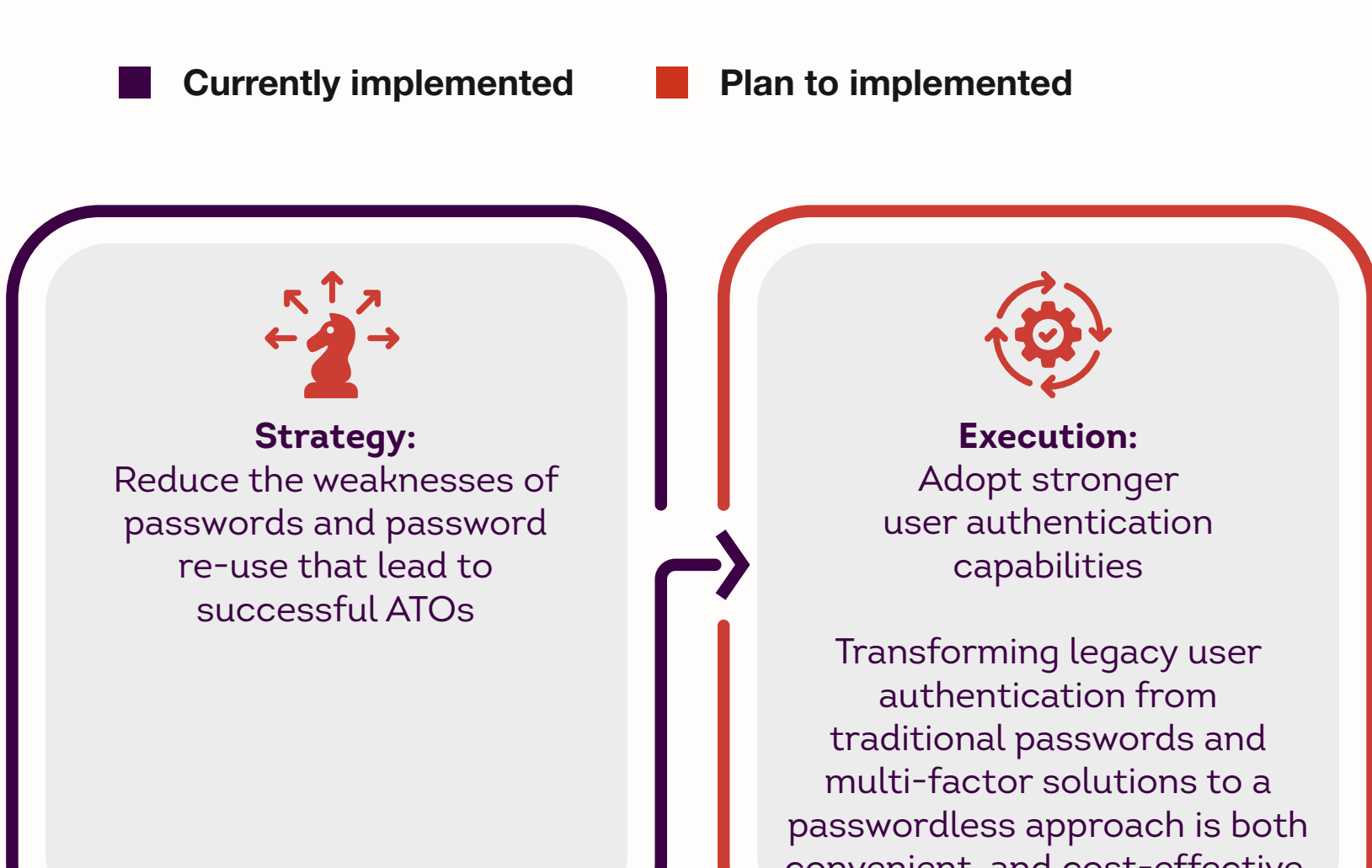
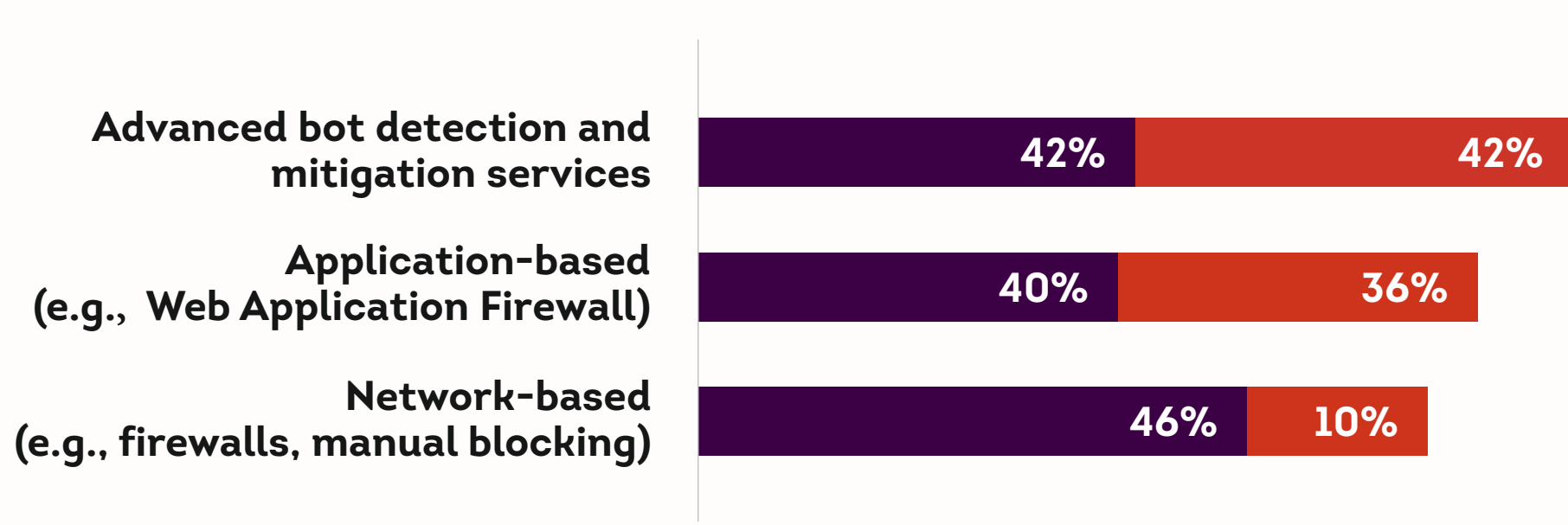
More than three-quarters (76%) of all respondents reported that some number of their online users had experienced a successful account takeover in the previous 12 months.

Consumer-facing organizations are making incremental investments in security technologies, designed to help address the issue of credential stuffing.

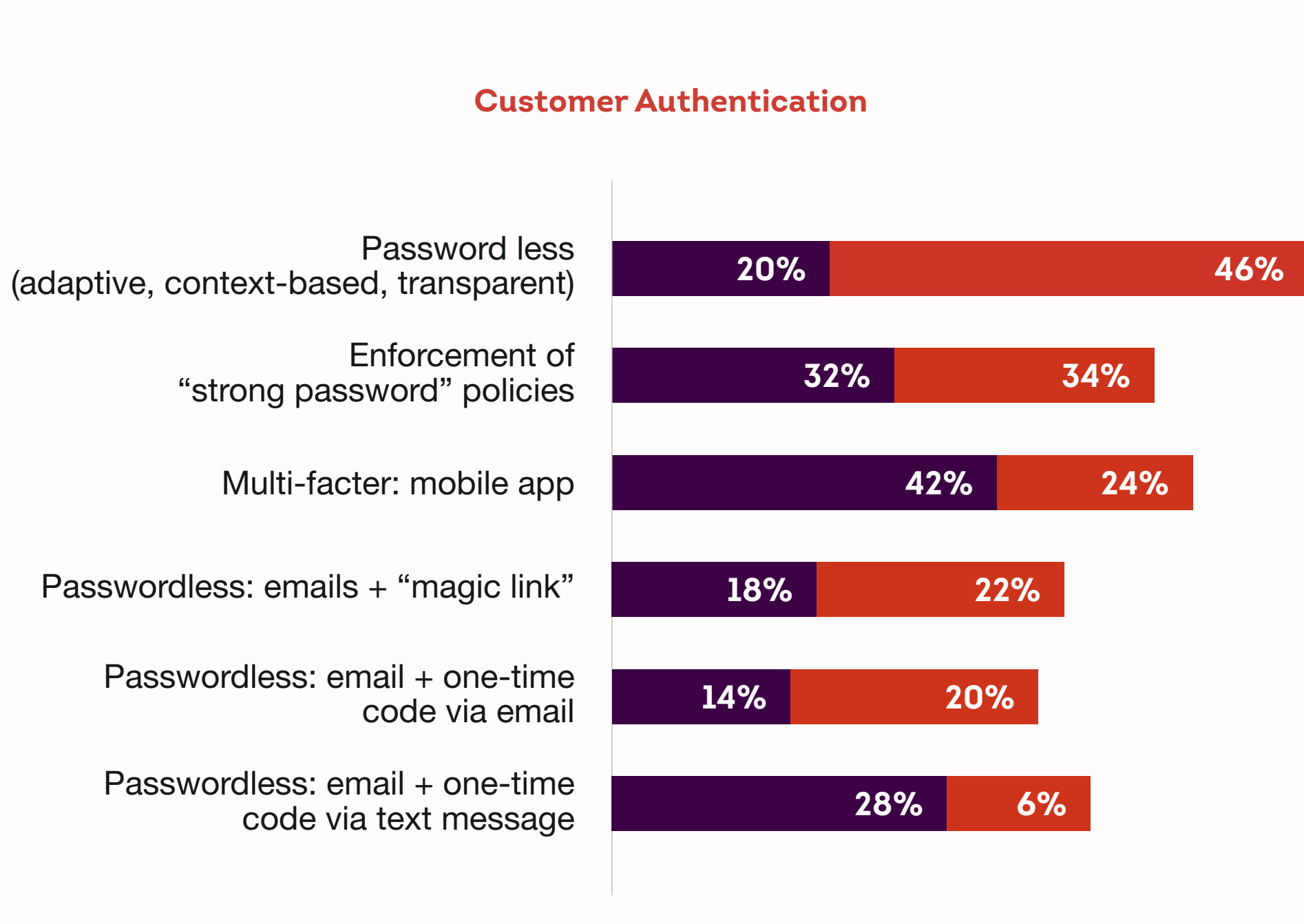
Top two technology strategies that address the growing issue of credential stuffing and account takeovers:



Technical Capabilities Being Adopted



Customer Authentication



For a deeper dive into how credential stuffing and ATOs are impacting your industry

[Read the full report](#)

Aberdeen Strategy & Research, a division of Spiceworks Ziff Davis, with over three decades of experience in independent, credible market research, helps illuminate market realities and inform business strategies.

Our fact-based, unbiased, and outcome-centric research approach provides insights on technology, customer management, and business operations, to inspire critical thinking and ignite data-driven business actions.

For more information,

info@aberdeen.com www.aberdeen.com