

2022 Authentication Survey



Methodology

- Survey Goal:** To better understand the authentication environment and challenges facing Security/IT professionals in large organizations
- Participants:** 252 Security/IT Professionals, Director and above, at U.S. Companies with 2500+ employees across a broad cross section of sectors
- Methodology:** Respondents were surveyed about the various factors and requirements comprising their organization's authentication environment. The survey was conducted by Censuswide between August 12-22, 2022. Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct which is based on the ESOMAR principles

Key Findings

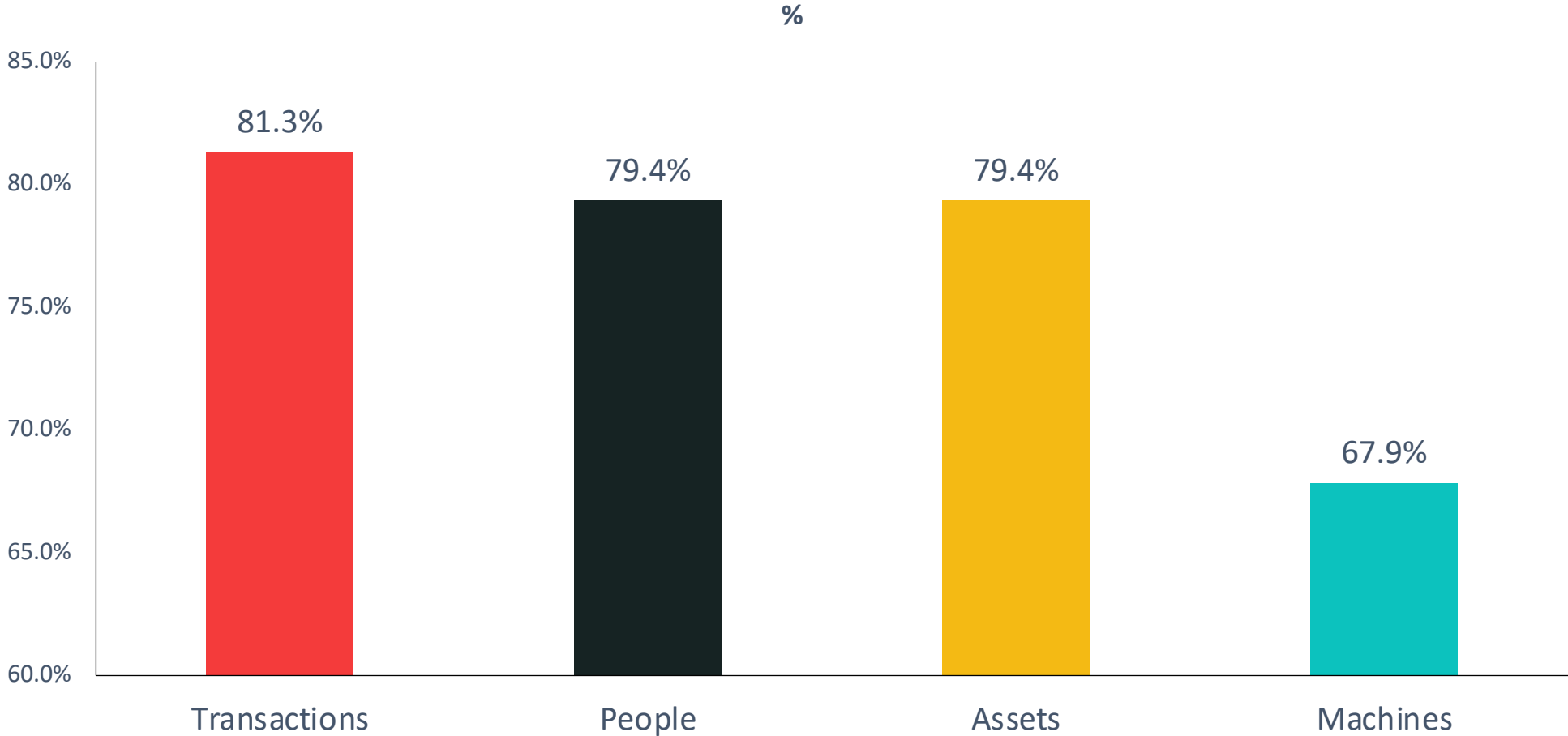
Organizations Are Struggling with Authentication Due to Underlying Complexity

- 79% said it was critical to secure people, 68% said machines are critical
- 89% use 3 or more authentication methods and 60% use more than 5
- 70% have 3 or more IAM ecosystems in place and 52% have more than 4
- 83% said they must authenticate against at least 2 operating systems
- More than half (54%) must comply with four or more regulatory requirements

70% of respondents said they are overwhelmed by the complexity of their authentication systems

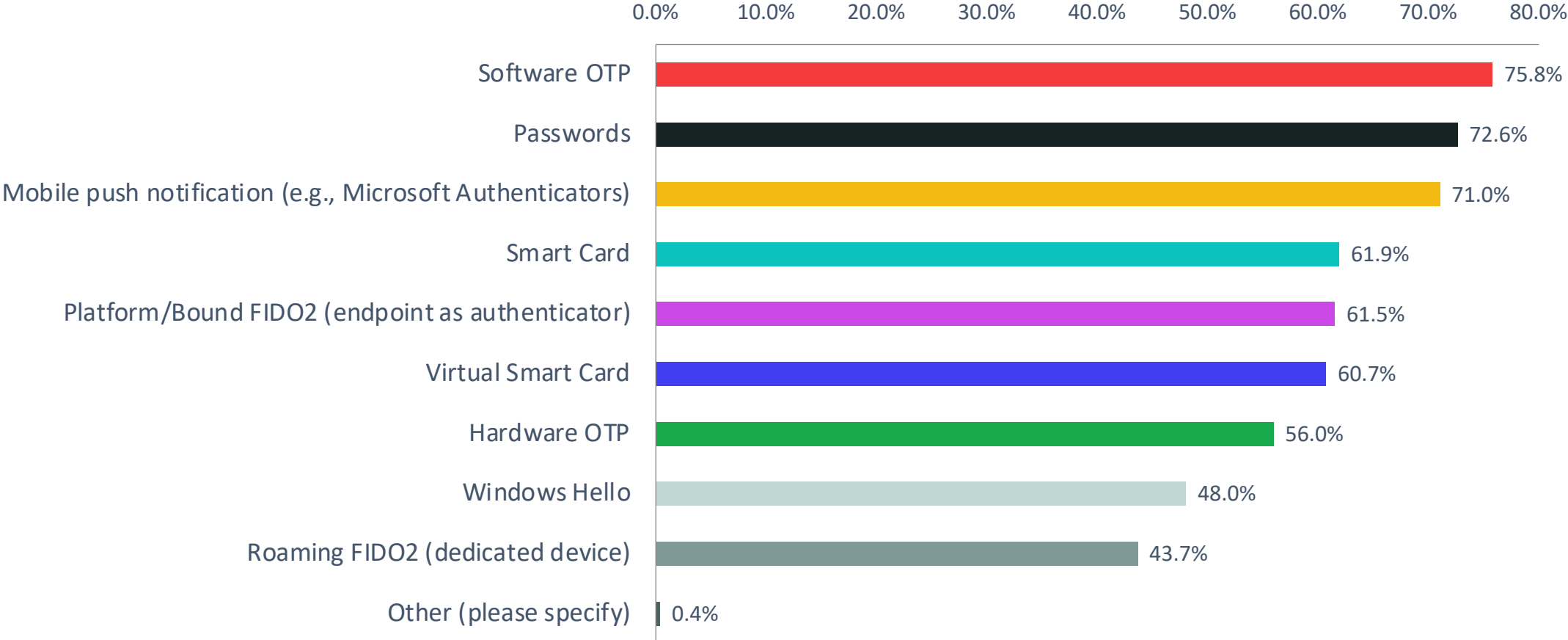
Authentication Goes Beyond People

What targets are critical when you think about securing digital interactions based on identities? (check all that apply)



89% of organizations use 3 or more authentication methods and 60% use more than 5

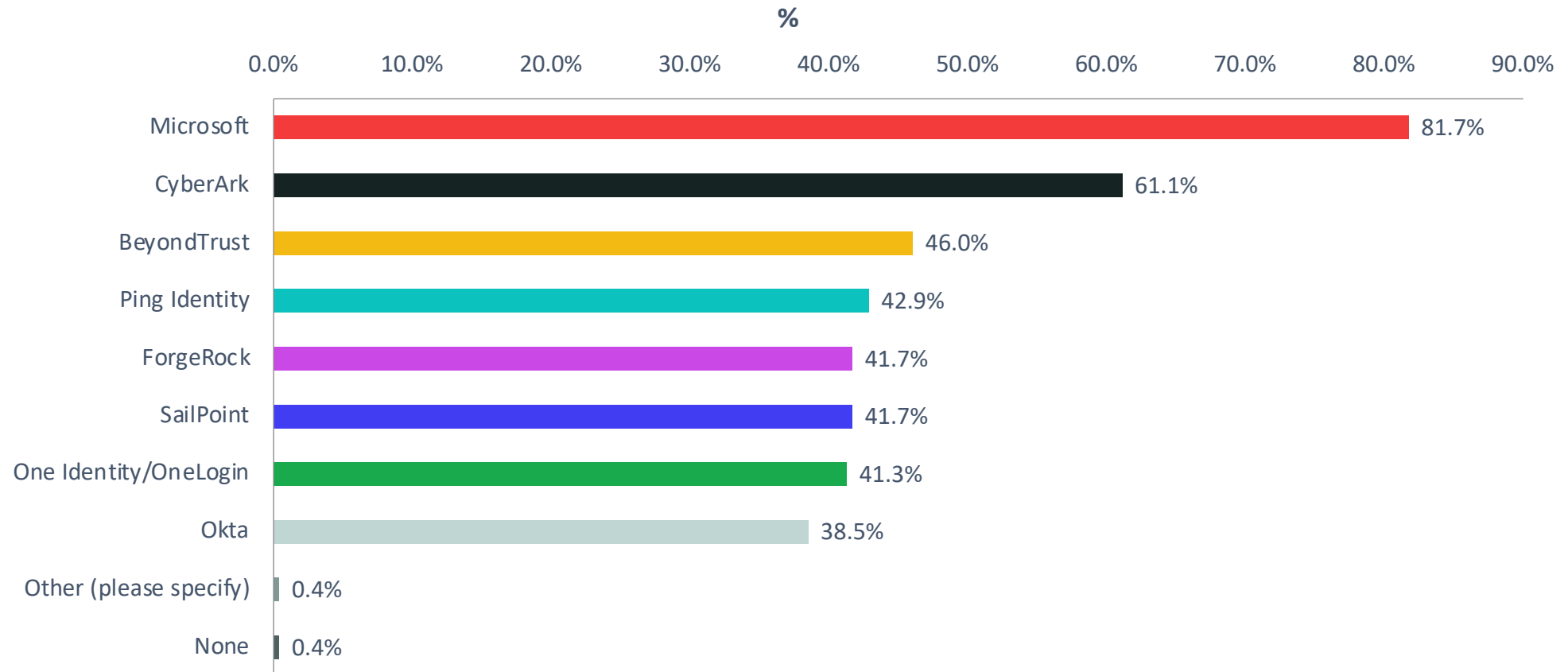
What authentication methods, if any, does your security/IT team manage across your enterprise? (Select all that apply)



More than a third (35%) use 7 different authentication methods across their organization

70% of organizations use at least 3 IAM vendors and 52% use 4 or more

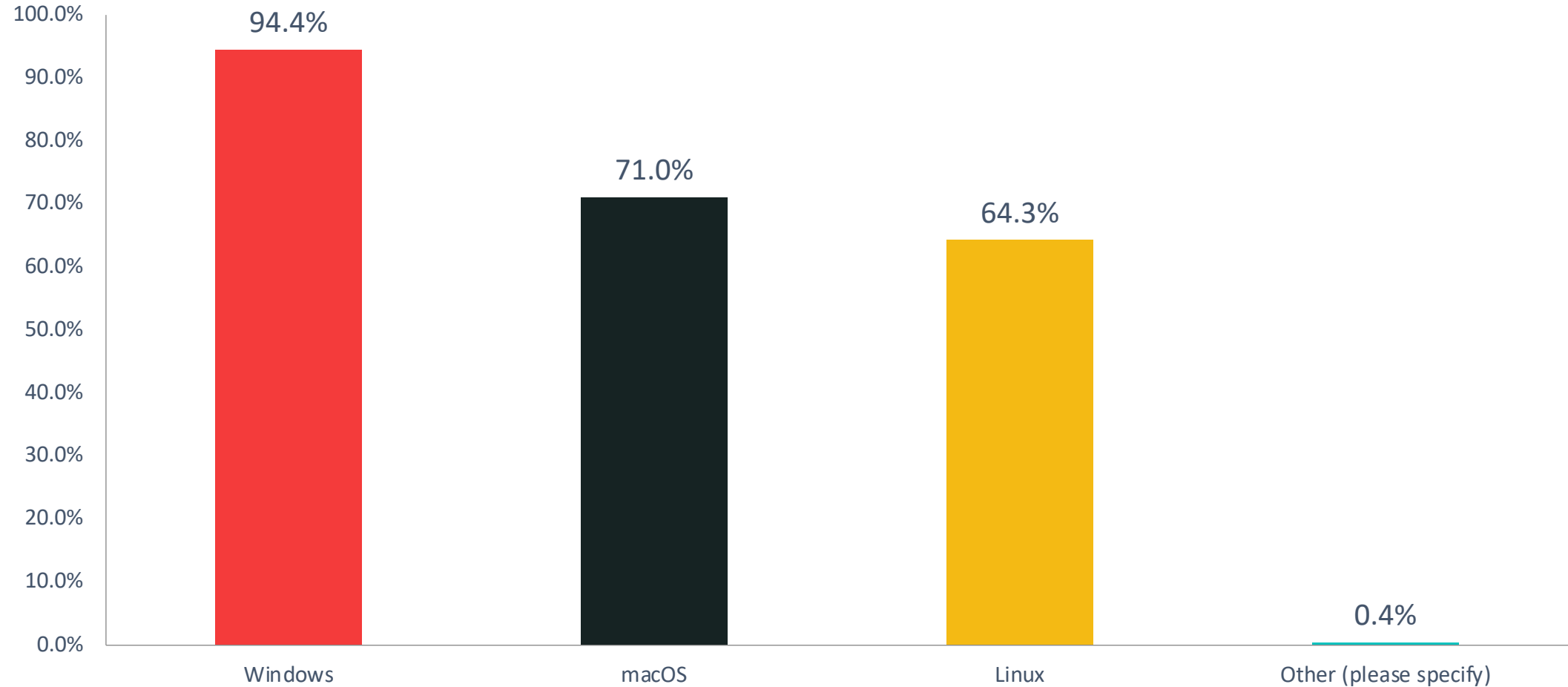
What IAM vendors, if any, do you currently have in house? (Select all that apply)



More than a fifth (21%) work with six or more IAM vendors

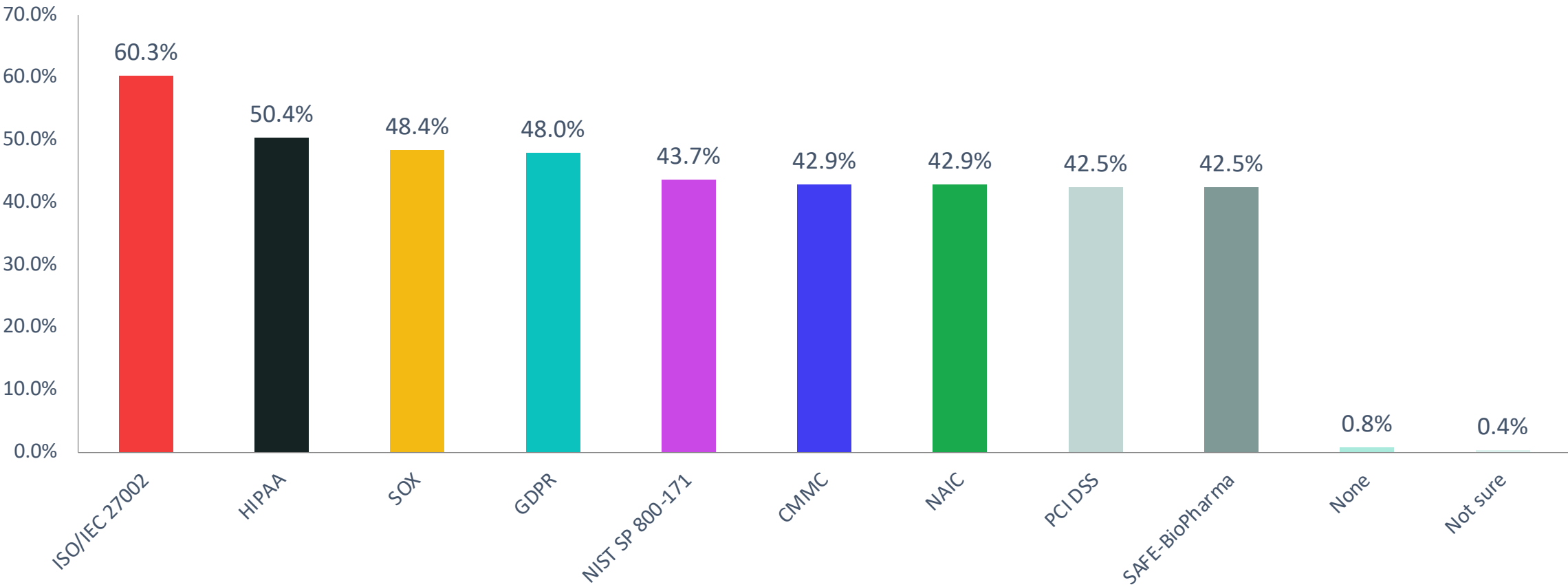
83% of organizations have at least 2 operating systems in place and almost half (46%) have 3

What operating systems are in use at your organization? (Select all that apply)



54% of respondents must comply with 4 or more regulatory requirements and 38% must comply with 5 or more

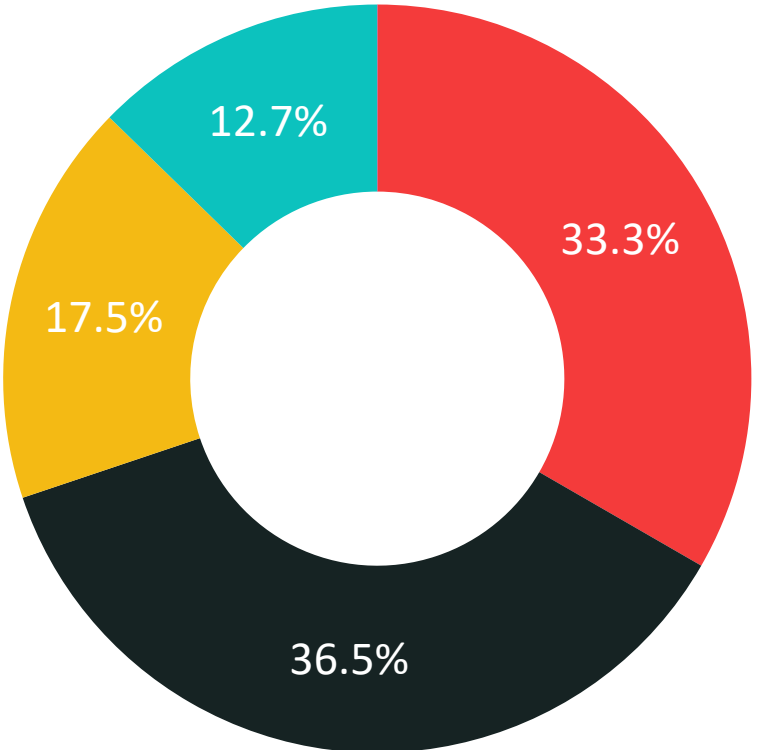
What regulatory and compliance requirements, if any, must your company comply with, that relates to authentication?



70% of security and IT pros are overwhelmed by their organization's authentication complexity*

How overwhelmed are you, if at all, by the complexity of your authentication systems?

■ Very overwhelmed ■ Somewhat overwhelmed ■ Not very overwhelmed ■ Not at all overwhelmed

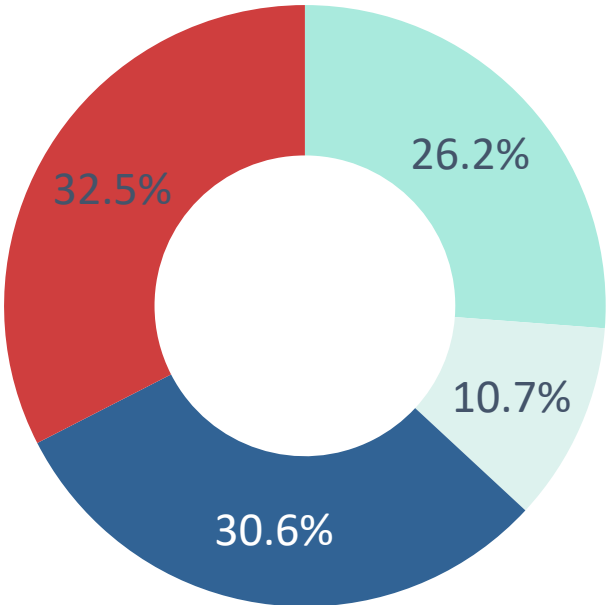


*'Very overwhelmed' and 'Somewhat overwhelmed' answers combined

Participant Demographics

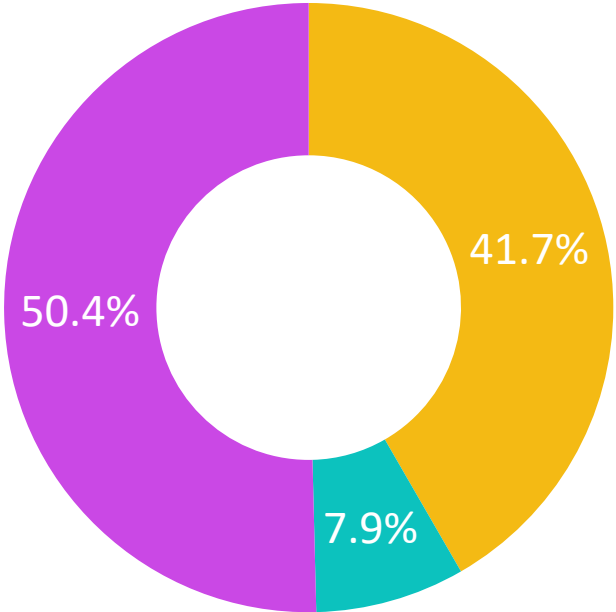
Company Size

- 2,500 – 2,999 employees
- 3,000 – 3,999 employees
- 4,000 – 4,999 employees
- 5,000 or more employees



Job Level

- Director
- VP
- C-Suite



About Axiad

Axiad delivers organization-wide passwordless orchestration to secure users, machines and transactions for organizations that must optimize their cybersecurity posture while navigating underlying IT complexity. The company's flagship offering, Axiad Cloud, is a comprehensive, secure and integrated authentication platform that allows customers to move to a passwordless future without the friction and risk of fragmented solutions. Axiad supports the widest range of credentials including FIDO, mobile MFA, AD CBA, Windows Hello for Business, YubiKeys, smart cards, TPM and biometrics, and is trusted by public sector organizations and Fortune 500 companies across aerospace & defense, financial services, insurance, healthcare, oil & energy and more.

For more information visit www.axiad.com