

CIO and CISO priorities for IAM and machine identity management

CIOs are driving innovation, while the CISO's mission is to ensure information assets and technologies are adequately protected while reducing risk. As the strategy around identity and access management (IAM) has changed and machine identity management becomes crucial, these two roles need to work together to build a comprehensive strategy.

Pulse and Keyfactor surveyed 100 CIOs and CISOs to understand their priorities around Identity and Access Management (IAM).

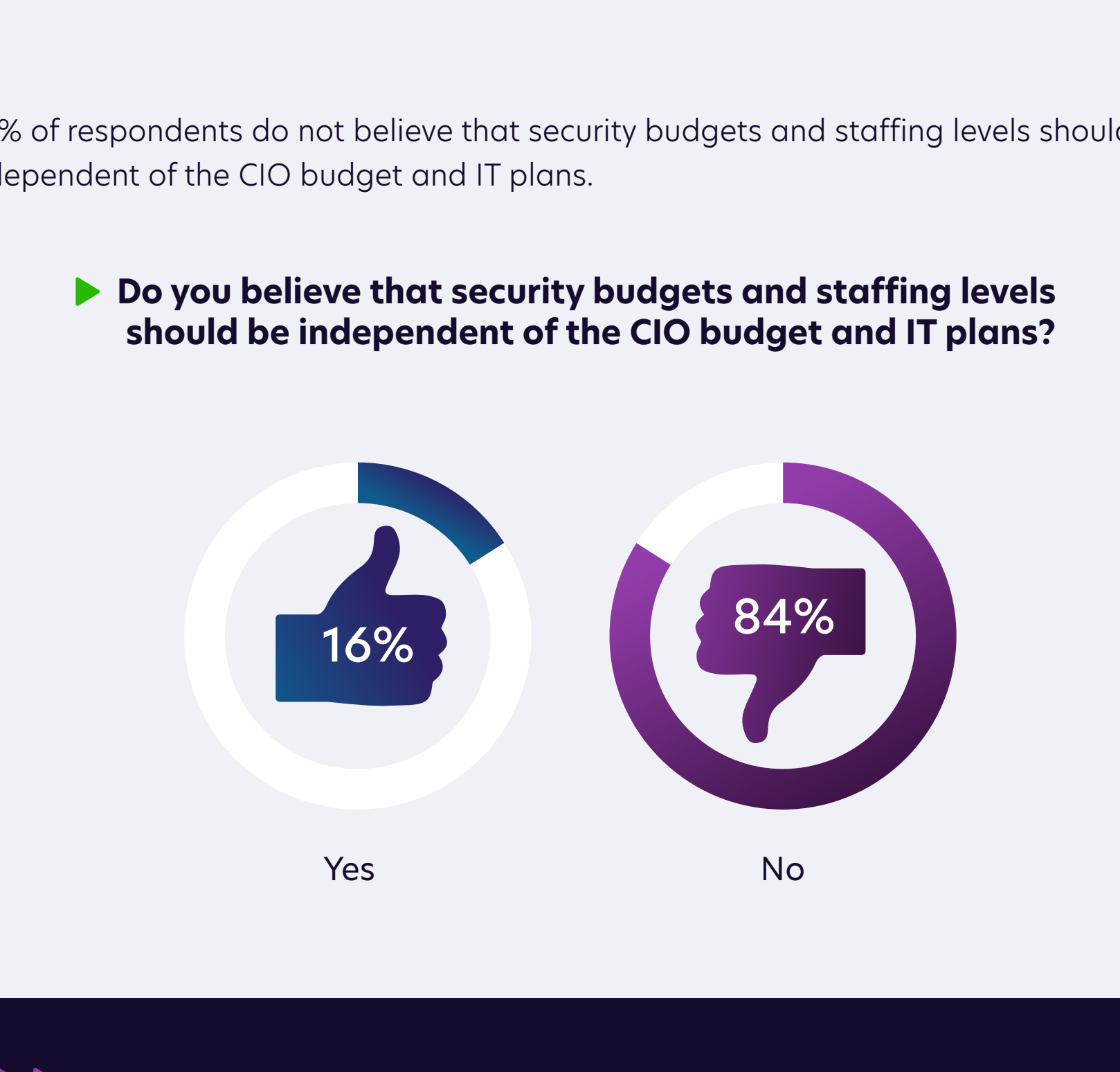
Data collected: May 6 - June 22, 2021

Respondents: 100 CIOs and CISOs

CIOs AND CISOs KNOW HOW THEIR RESPONSIBILITIES DIFFER AND BELIEVE THAT CIO BUDGET AND IT PLANS SHOULD PLAY A PART IN SECURITY BUDGETS AND STAFFING LEVELS

In general, CIOs and CISOs understand how their responsibilities and objectives differ within their company.

► To what extent do you agree with the following: "At my company, I clearly understand how the responsibilities and objectives of the CIO and CISO differ."



84% of respondents do not believe that security budgets and staffing levels should be independent of the CIO budget and IT plans.

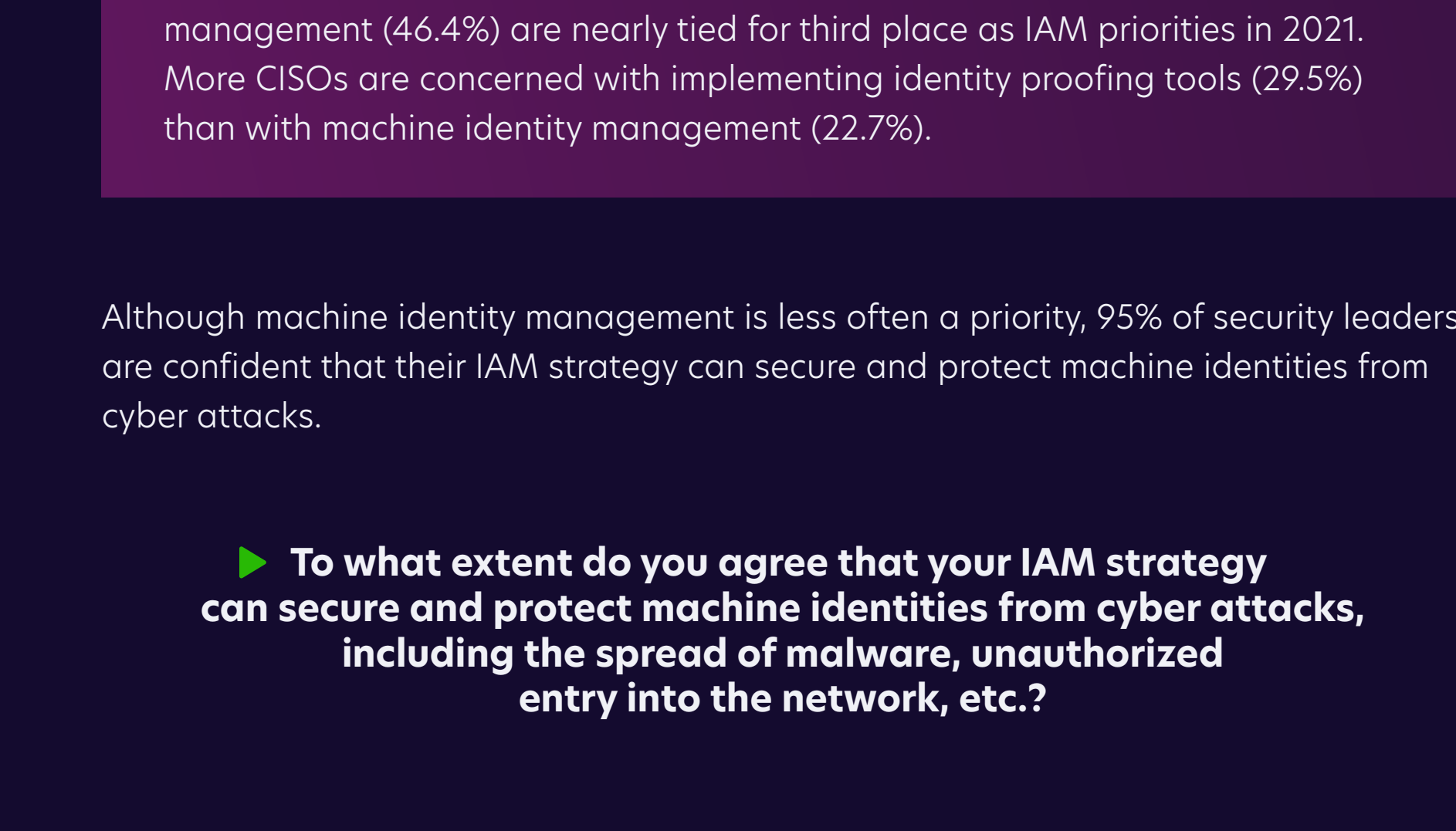
► Do you believe that security budgets and staffing levels should be independent of the CIO budget and IT plans?



MACHINE IDENTITIES REMAIN A LOWER PRIORITY IN IAM STRATEGIES FOR MOST, ESPECIALLY FOR CISOs

For most CIOs and CISOs, the top three IAM priorities for 2021 are user authentication (71%), privileged access management (62%) and cloud IAM & governance (54%).

► What are your top 3 priorities for Identity & Access Management (IAM) in 2021?



However, among CIOs, cloud IAM & governance (48.2%) and machine identity management (46.4%) are nearly tied for third place as IAM priorities in 2021. More CISOs are concerned with implementing identity proofing tools (29.5%) than with machine identity management (22.7%).

Although machine identity management is less often a priority, 95% of security leaders are confident that their IAM strategy can secure and protect machine identities from cyber attacks.

► To what extent do you agree that your IAM strategy can secure and protect machine identities from cyber attacks, including the spread of malware, unauthorized entry into the network, etc.?



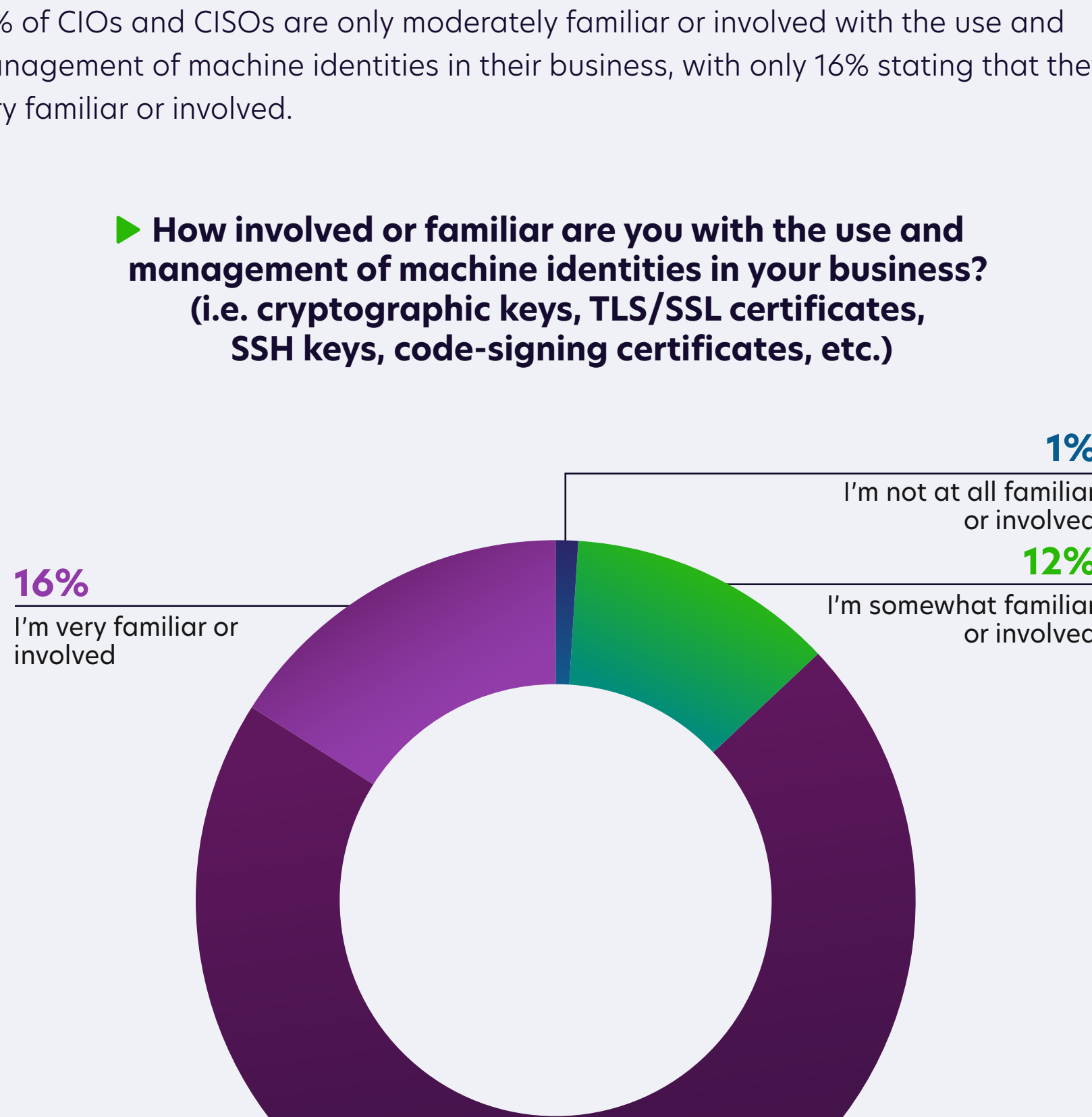
And 88% of respondents agree that they treat machine identities with the same level of policy and protection as user identities.

► To what extent do you agree with the following statement: "We treat machine identities with the same level of policy and protection as we do user identities."



But when strategic plans for IAM strategy are developed, 79% of respondents say machine identities are only sometimes included in planning, followed by 11% who say they're rarely included in planning.

► When you develop strategic plans for IAM strategy, machine identities are:



CIOs AND CISOs ARE NOT ENTIRELY FAMILIAR WITH OR INVOLVED IN MANAGEMENT OF MACHINE IDENTITIES, BUT REMAIN CONFIDENT IN THEIR TEAM'S ABILITY TO MANAGE THEM

71% of CIOs and CISOs are only moderately familiar or involved with the use and management of machine identities in their business, with only 16% stating that they're very familiar or involved.

► How involved or familiar are you with the use and management of machine identities in your business? (i.e. cryptographic keys, TLS/SSL certificates, SSH keys, code-signing certificates, etc.)



Despite this limited familiarity, 90% of respondents are confident in their team's ability to manage machine identities.

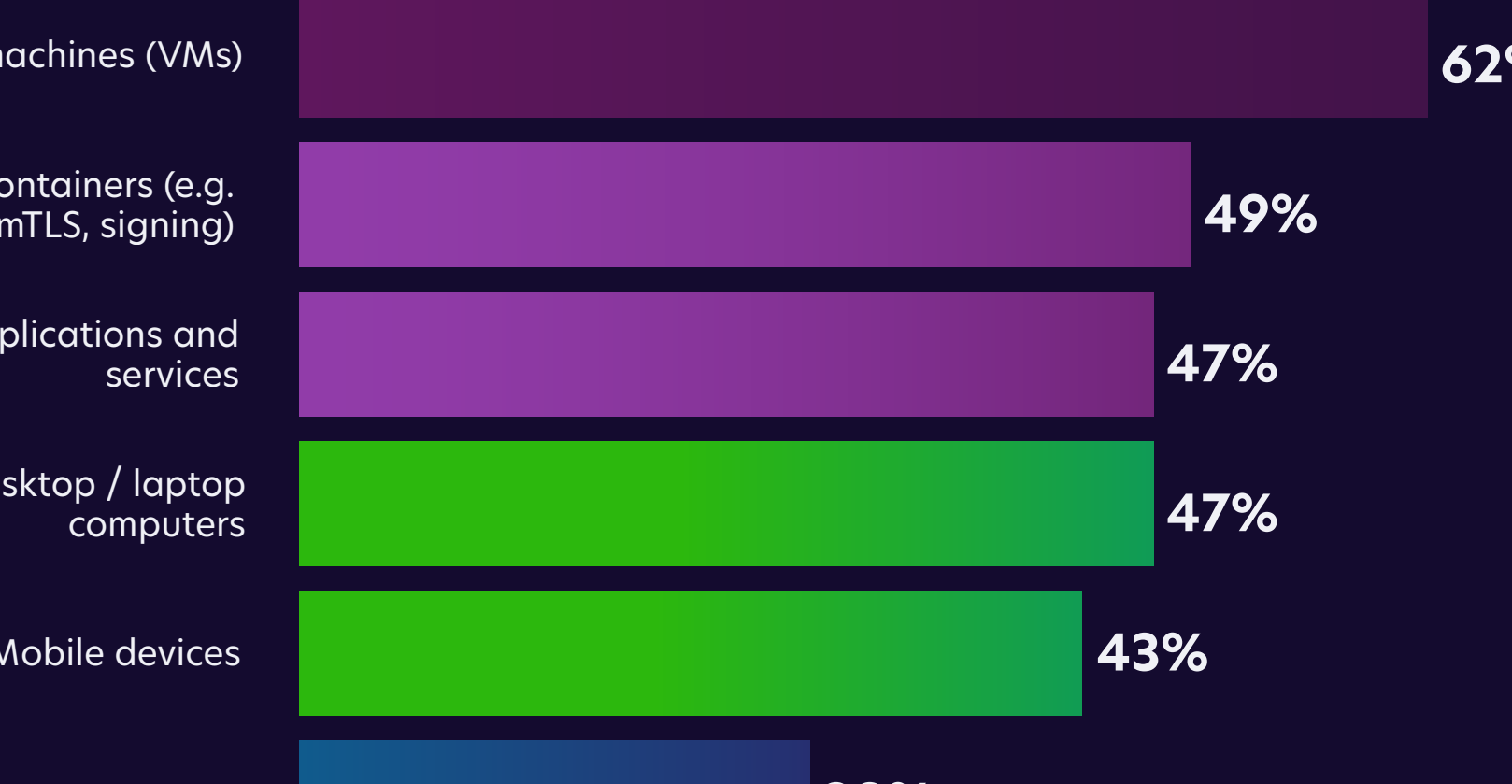
► To what extent do you agree with the following statement: "I feel confident about my team's ability to manage the increasing volume and velocity of machine identities required to support our digital business needs."



THEIR MAY BE A DESIRE TO INCREASE INVESTMENT IN MACHINE IDENTITY MANAGEMENT

The majority of respondents (73%) believe that their organization is invested correctly in securing machine identities compared to their investment in user identity and access management, but one-quarter (25%) say they are underinvested.

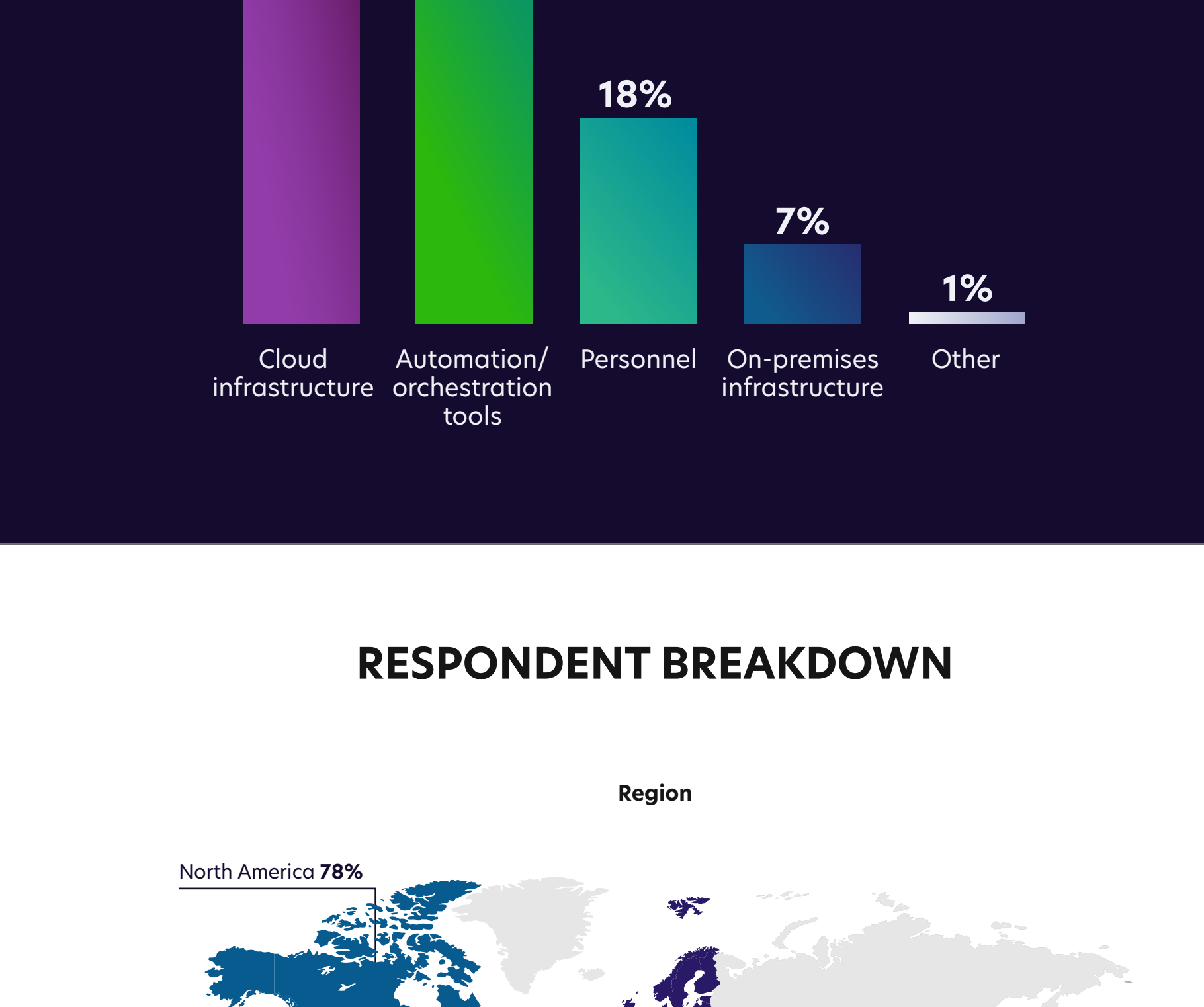
► In your opinion, compared to your investment in user identity and access management, your organization is ___ in securing machine identities:



31.8% of CISOs feel underinvested in securing machine identities compared to 19.6% of CIOs.

When it comes to devices and workloads, CIOs and CISOs are most concerned about web server infrastructure (62%), virtual machines (62%), and containers (49%).

► Of the following devices and workloads, what are you most concerned about?



Given more budget, most (40%) respondents would invest in cloud infrastructure, followed by automation and orchestration tools (34%).

► If you had more budget, what would be the top area you would invest it in?

