

The State of Secure Access in North America

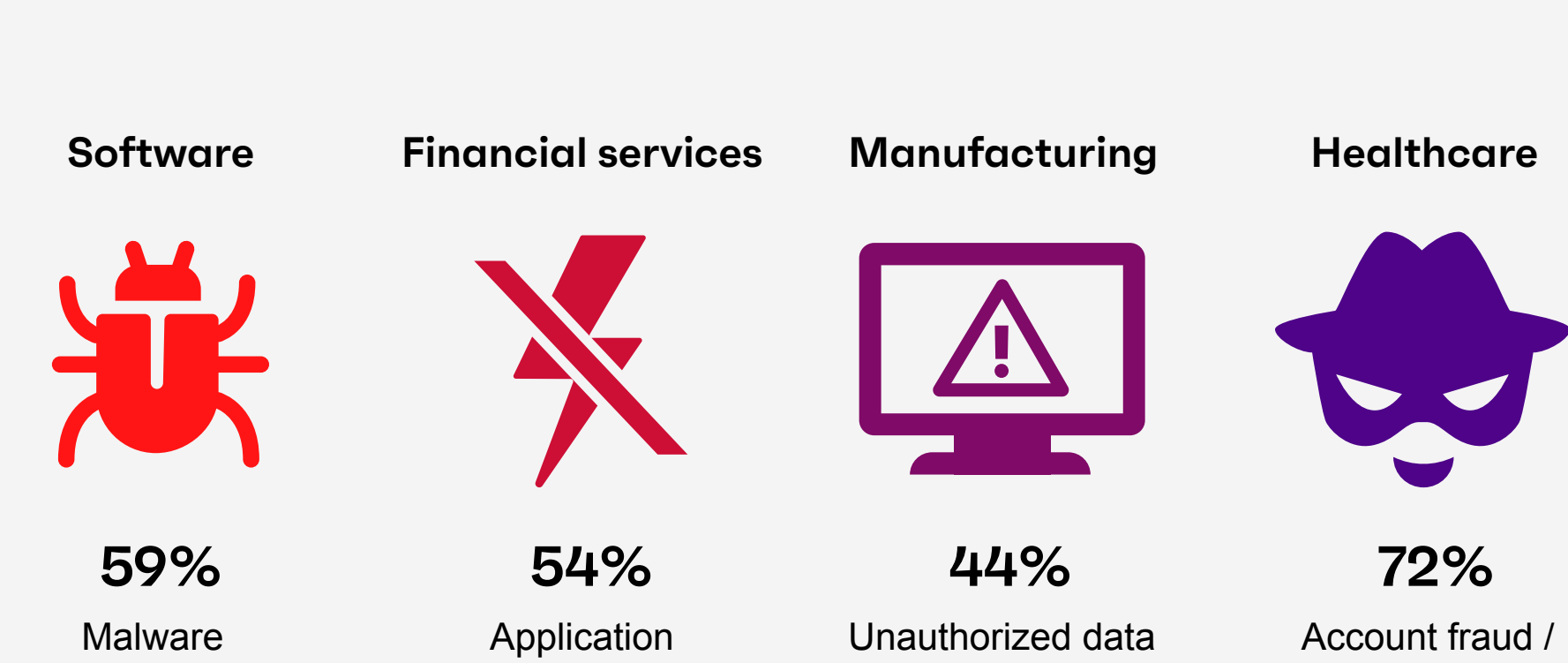
In the past 12 months, security and IT leaders in North America have experienced a number of security threats. To combat these growing challenges, they're prioritizing a number of secure access initiatives, and are planning to align them against a Zero Trust protocol. But among different industries—namely software, financial services, manufacturing, and healthcare—those priorities differ.

Ivanti and Pulse surveyed 275 North American IT and security leaders to uncover their secure access priorities for the next 12 months, and discover how they'll be used to reduce the frequency of security challenges.

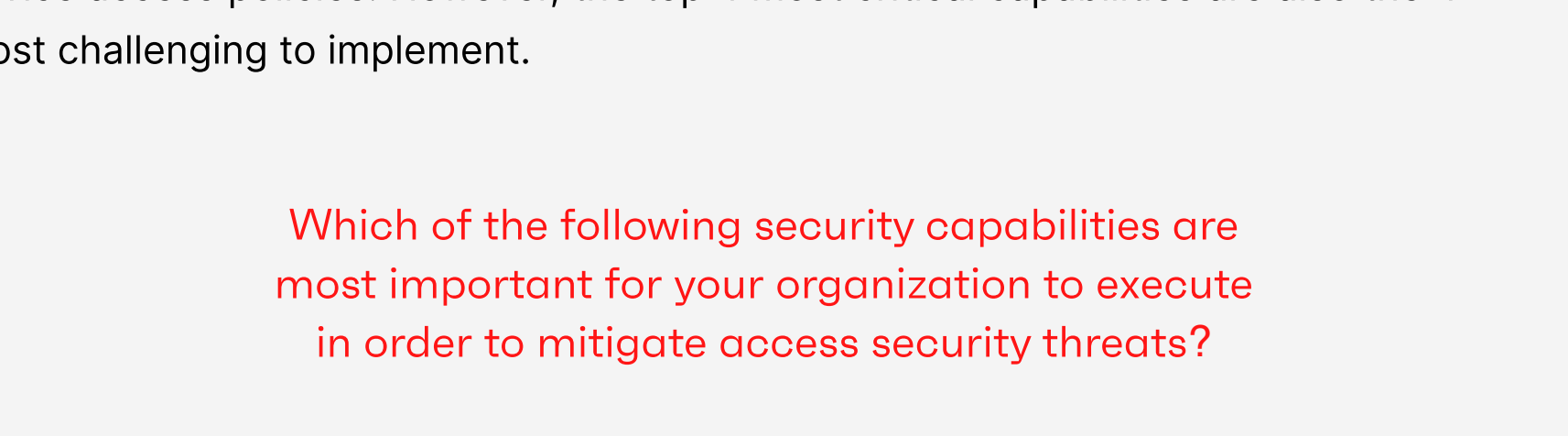
Companies need to define access policies to combat security threats

Over the last year, many companies in North America have suffered security attacks. Most commonly, IT and security leaders' organizations have been impacted by malware attacks (51%), account fraud and identity theft (46%), and application unavailability and outages (44%).

Which 5 of the following security threats have most impacted your organization in the past 12 months?



Most impactful security threats by industry:

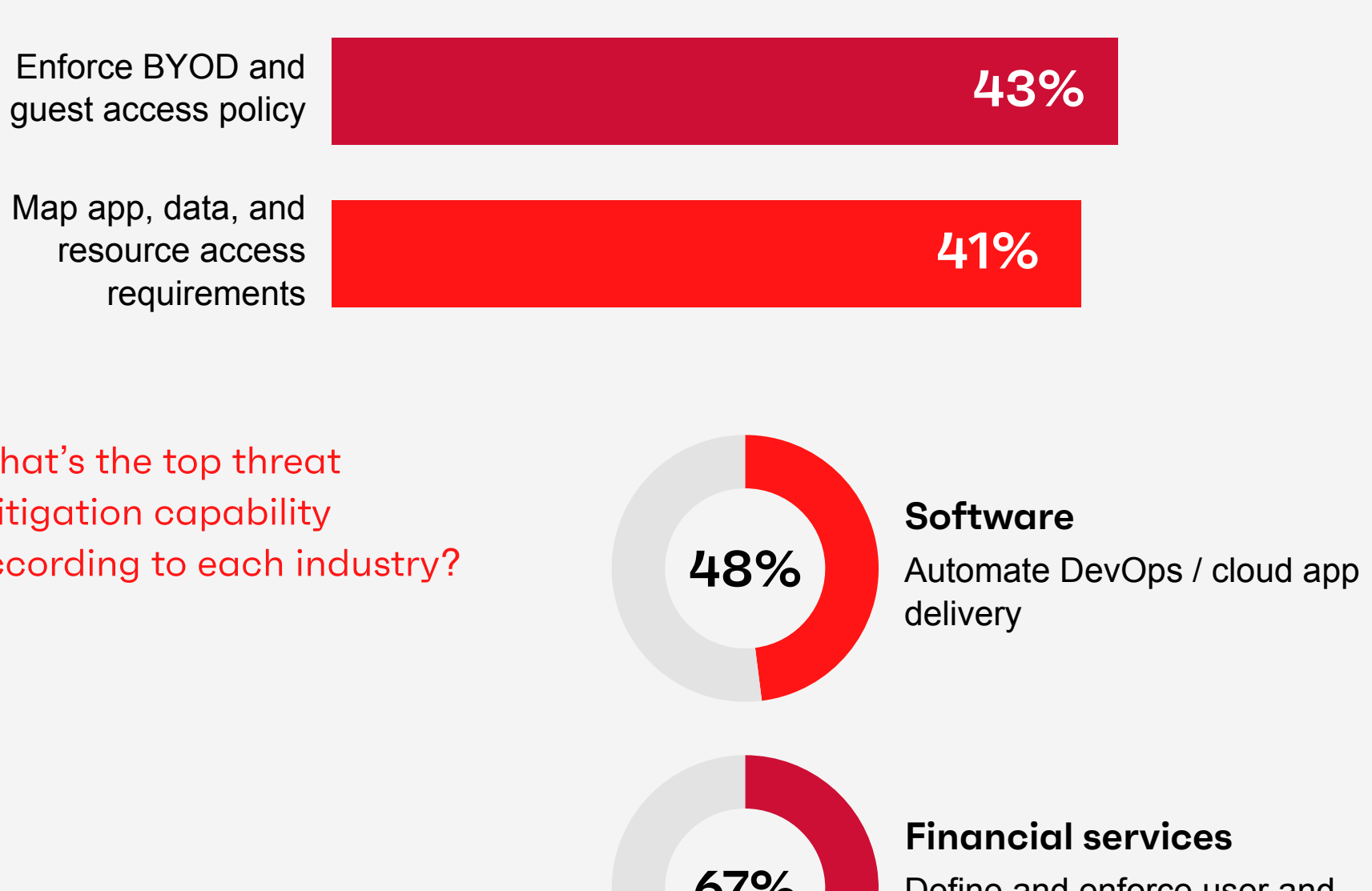


To reduce the impact of these mounting security threats, 62% of IT and security leaders say it is most important for their organization to define and enforce user and device access policies. However, the top 4 most critical capabilities are also the 4 most challenging to implement.

Which of the following security capabilities are most important for your organization to execute in order to mitigate access security threats?



Which 5 of the following security capabilities are most challenging for your organization to execute in order to mitigate access security threats/risks?



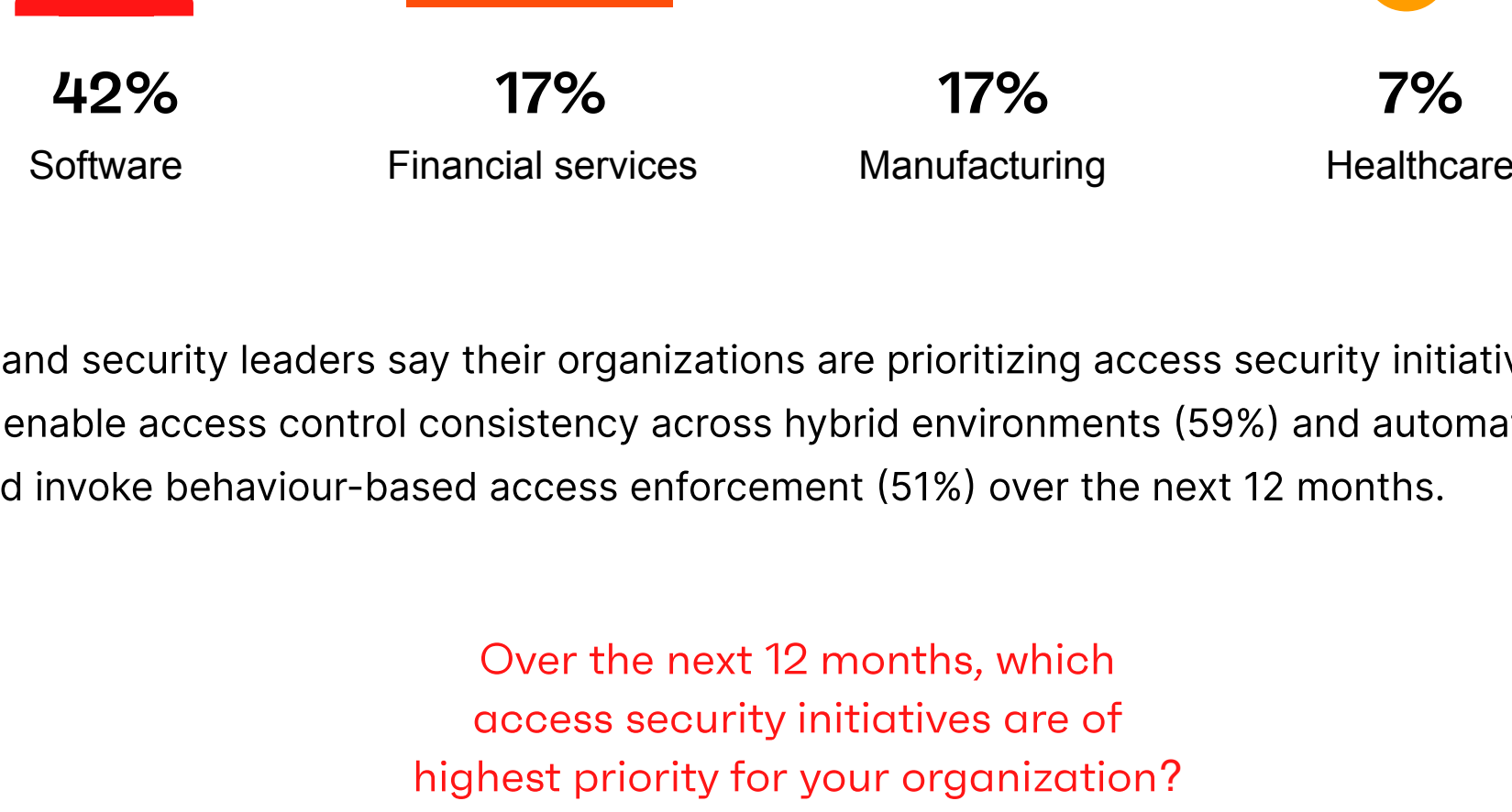
What's the top threat mitigation capability according to each industry?



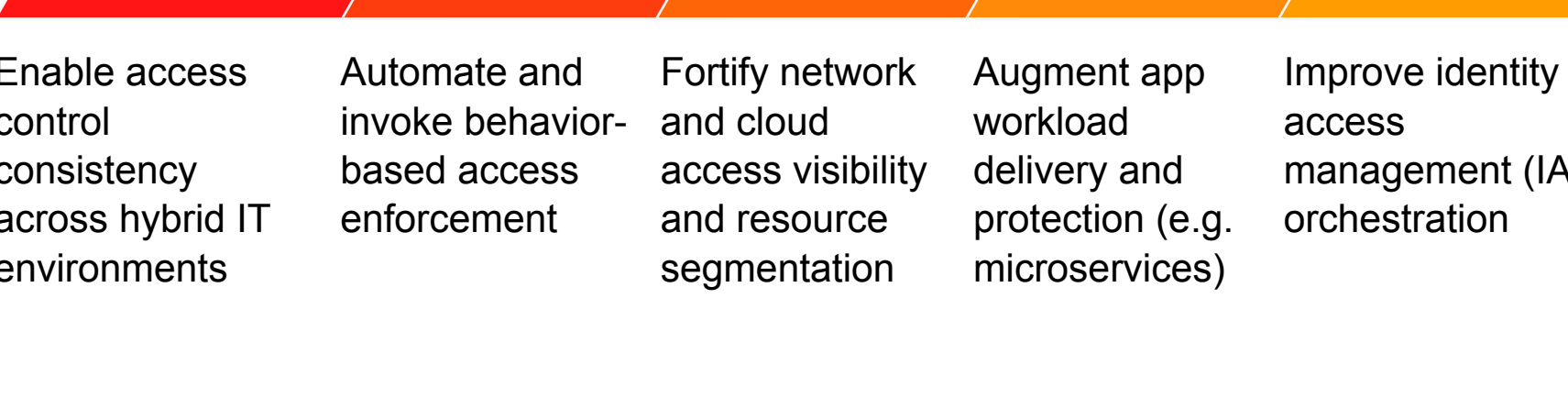
To further prevent security threats, tech leaders are prioritizing Zero Trust and securing hybrid IT

98% of IT and security practitioners in North America say their security practices will become more aligned with a Zero Trust strategy over the next 12 months, including 21% who say they'll become significantly or completely aligned.

In the next 12 months, to what extent will your organization's existing security controls become more aligned with Zero Trust?

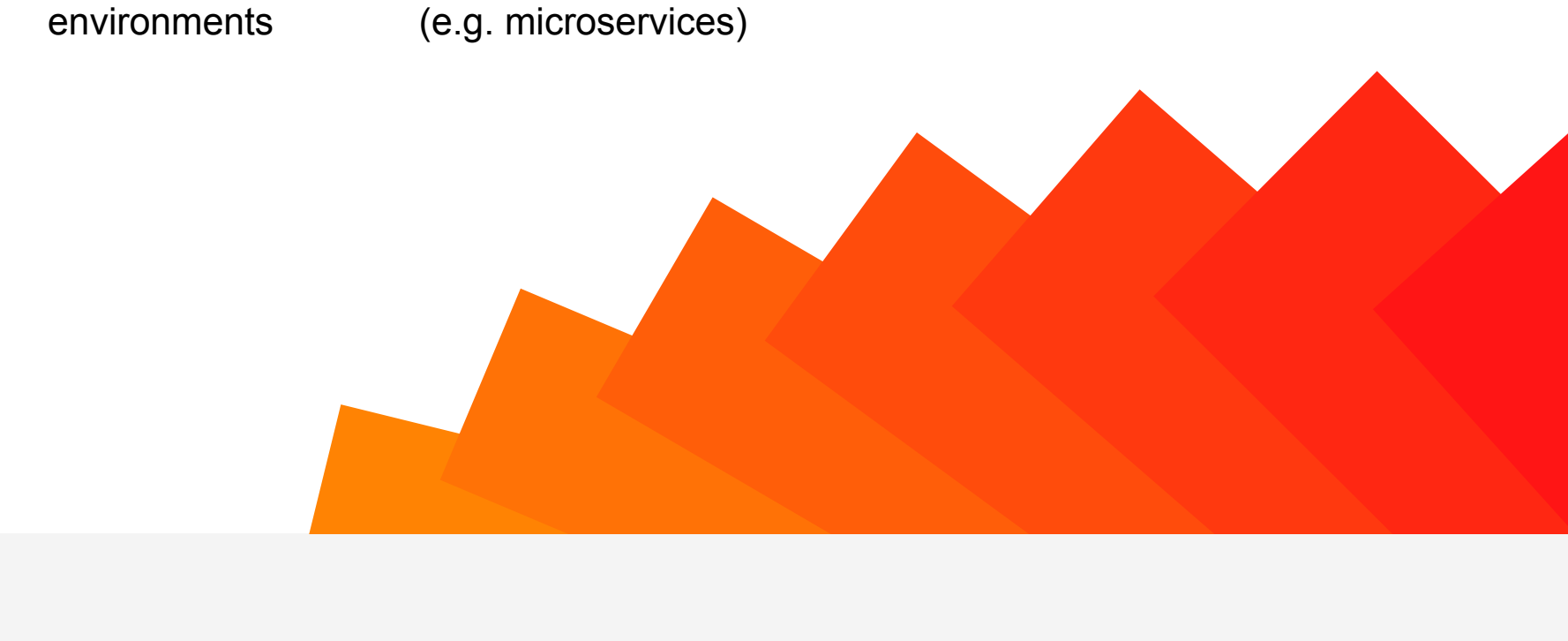


Industry by industry, who's going to be significantly or completely aligned with Zero Trust?

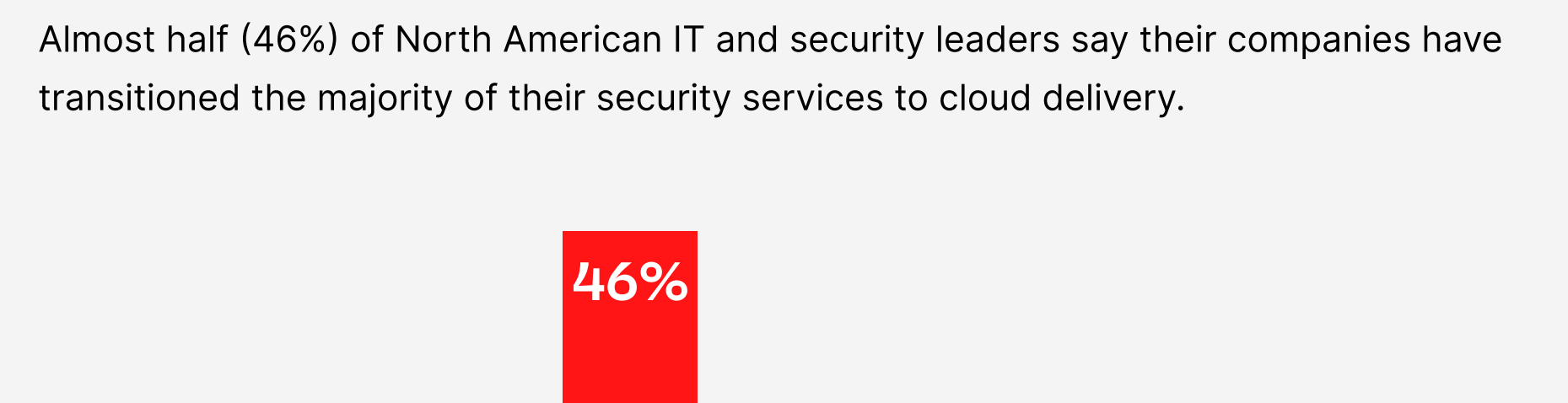


IT and security leaders say their organizations are prioritizing access security initiatives to enable access control consistency across hybrid environments (59%) and automate and invoke behavior-based access enforcement (51%) over the next 12 months.

Over the next 12 months, which access security initiatives are of highest priority for your organization?

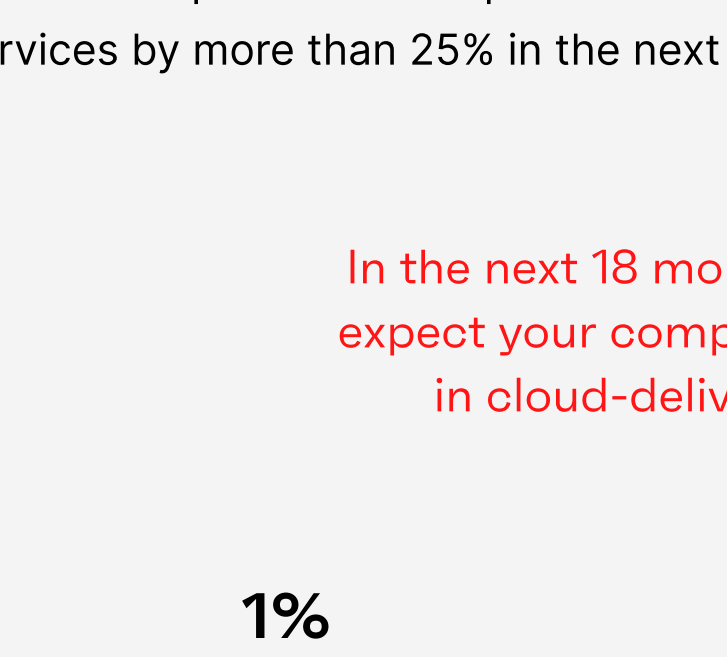


Top security initiative priorities by industry:



IT and security leaders are transitioning to cloud-delivered security services, and plan to consolidate vendors

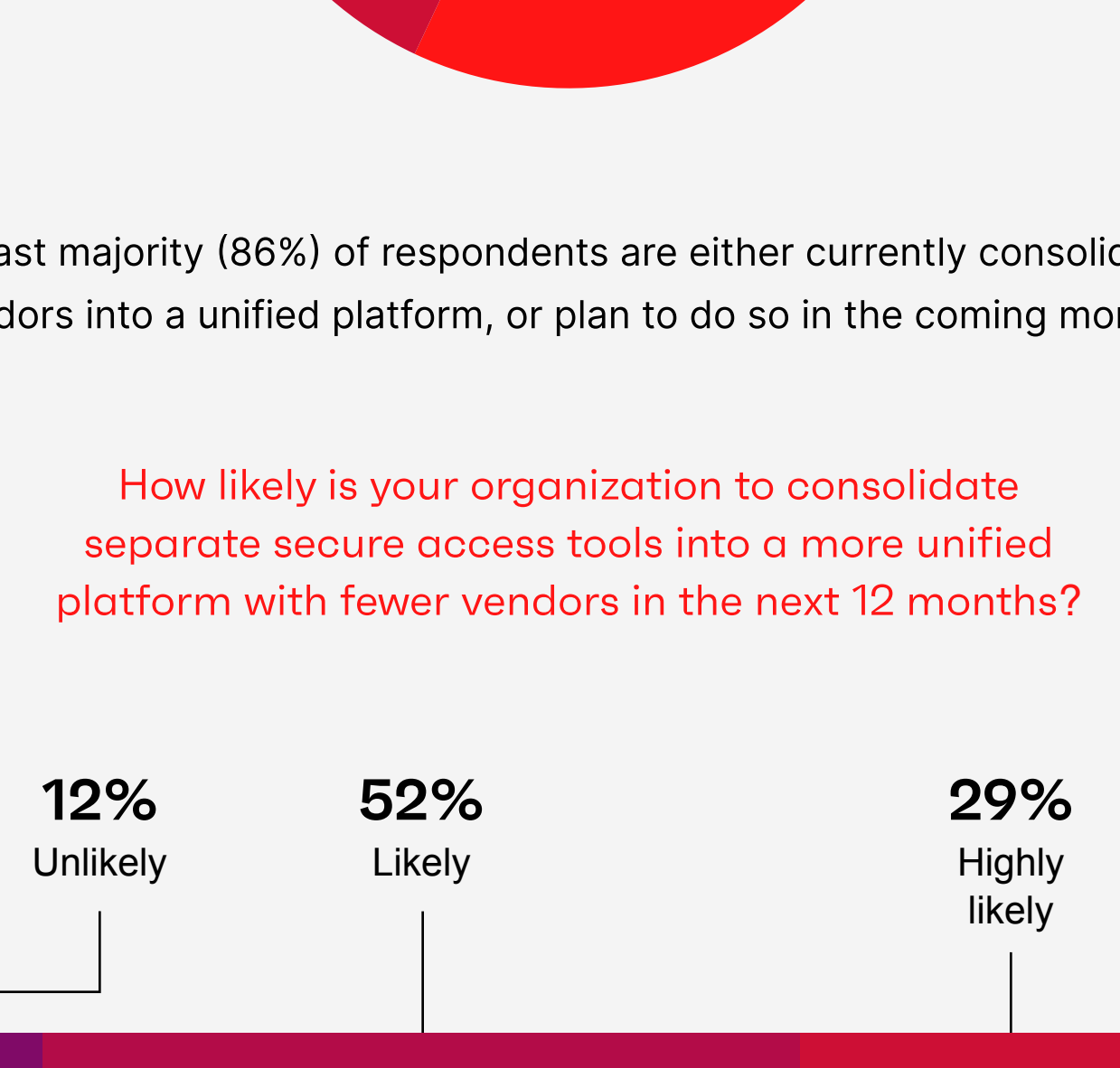
Almost half (46%) of North American IT and security leaders say their companies have transitioned the majority of their security services to cloud delivery.



How many security services has your company transitioned to cloud delivery from traditional on-premises security tools?

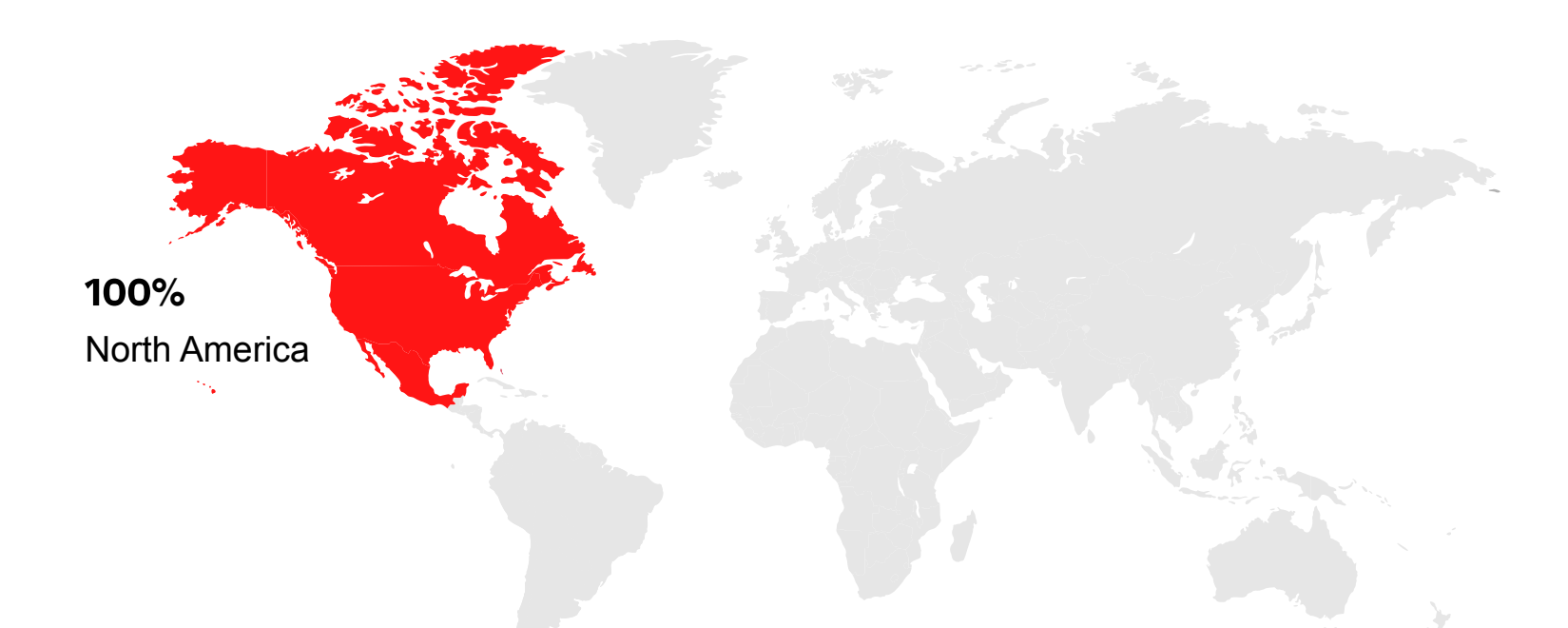
And 43% expect their companies to increase their spend on cloud-delivered security services by more than 25% in the next year.

In the next 18 months, to what extent do you expect your company to increase investment in cloud-delivered security services?



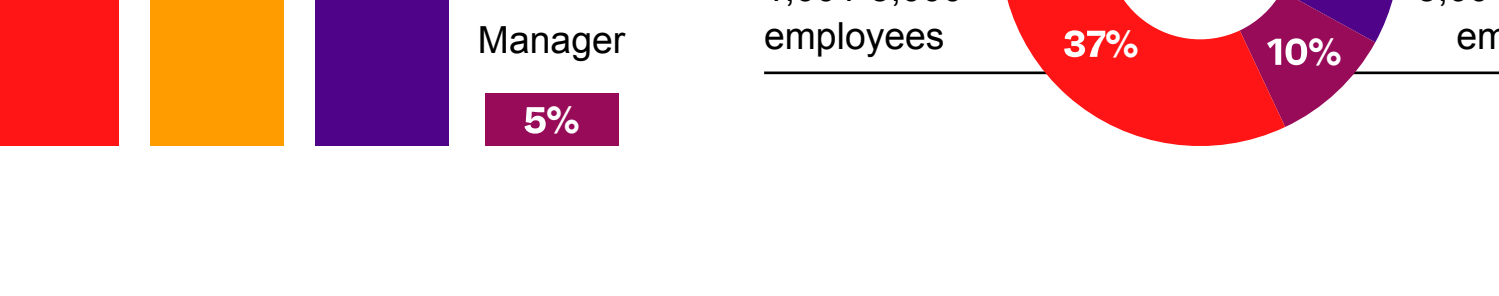
Lastly, the vast majority (86%) of respondents are either currently consolidating security vendors into a unified platform, or plan to do so in the coming months.

How likely is your organization to consolidate separate secure access tools into a more unified platform with fewer vendors in the next 12 months?



Respondent Breakdown

Region



Title

Company size

