Gartner
Peer Community™

State of Vulnerability Management Programs in 2023

Vulnerability management (VM) programs can help organizations achieve software supply chain security and cyber resilience. Do leaders consider their organization's current VM program up to the task?

One-Minute Insights:

- One-fifth of respondents report their organization's VM program has less funding than required
- About one-third of surveyed leaders say their VM program's metrics and reporting are ineffective
- Many respondent organizations that outsource VM processes do so for network scanning, threat intelligence or application scanning
- The majority of respondent organizations include network access control implementation or penetration testing in their VM strategies
- Splitting responsibilities for vulnerability management and patch management across different teams is a common struggle among surveyed leaders

One-Minute Insights on timely topics are available to Gartner Peer Community members. Sign up for access to over 100 more, and new insights each week.

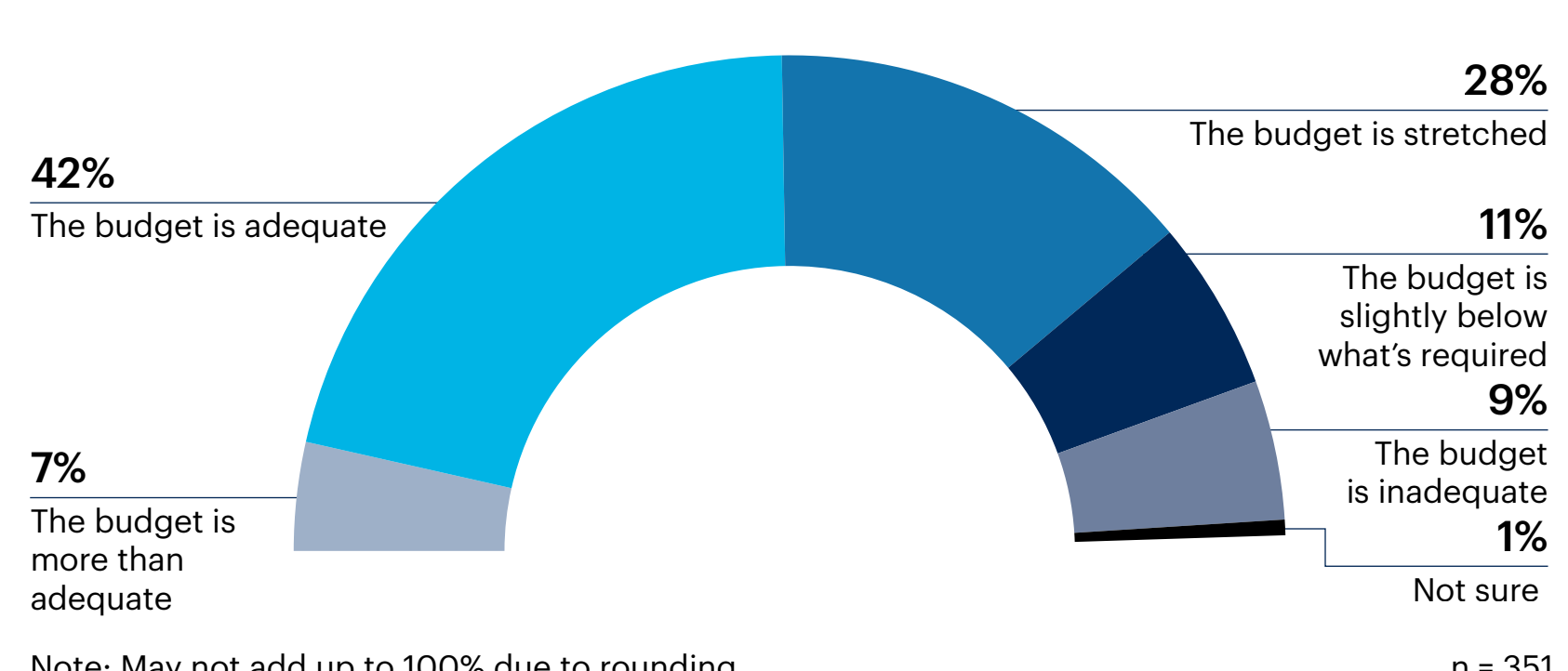
Data collection: May 30 - Jun 27, 2023

Respondents: 351 IT and information security leaders involved in their organization's vulnerability management program

Almost half of surveyed leaders report their organization's VM program has an adequate budget, and many have seen it increase over the last year

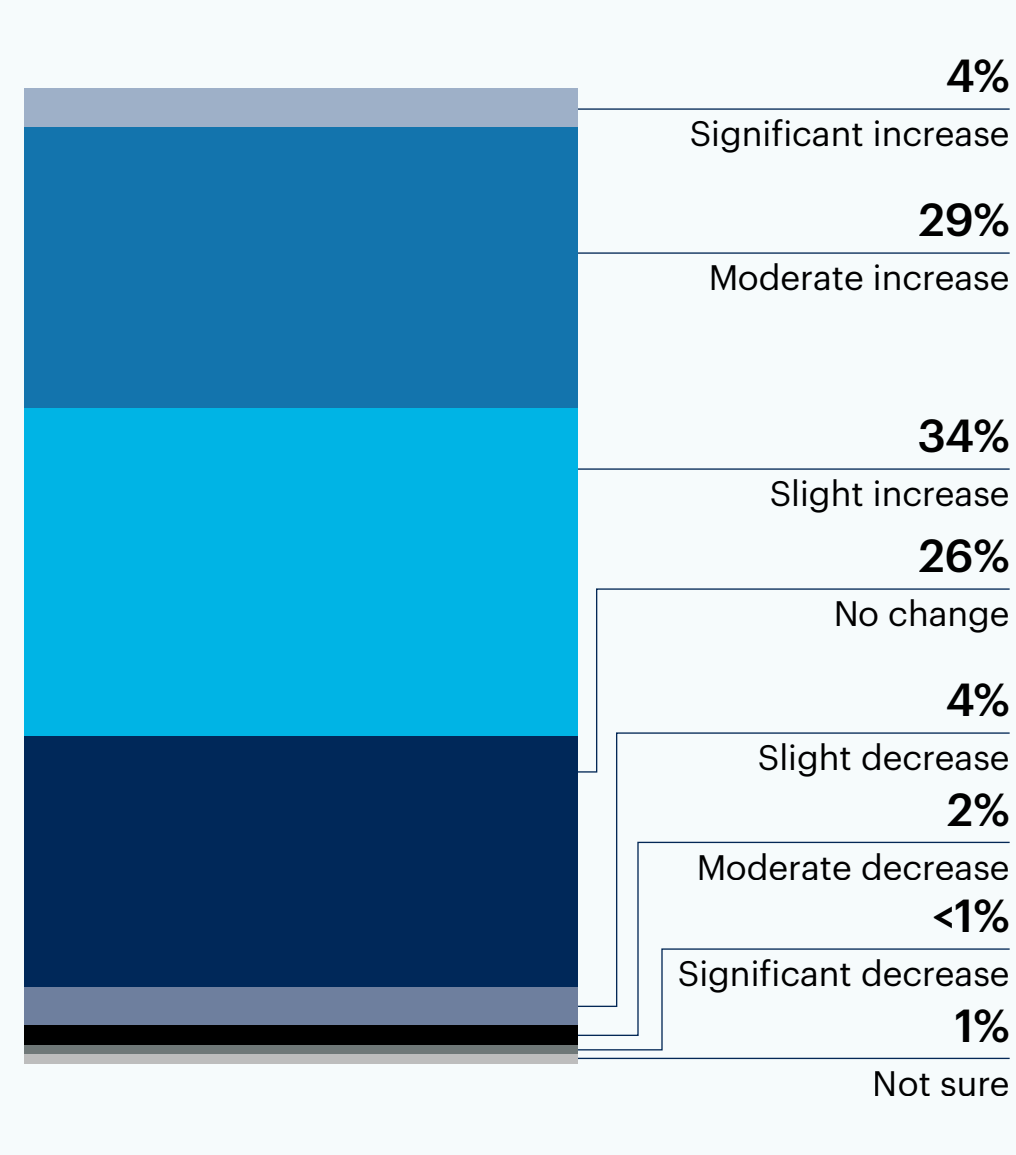
Nearly half **(49%)** of all respondents indicate that **the budget of their organization's VM program is adequate**, while one-fifth (20%) have less funding than they require.

How would you describe the budget for your organization's vulnerability management program?



Note: May not add up to 100% due to rounding

n = 351



About **two-thirds (67%) saw budget increases** for their organization's VM program within the past year.

Has the budget for your organization's vulnerability management program changed in the past year?

n = 351

> "We are being forced by government to put a VM in place for all our business which is a good move on their part, however we are still limited by budget."
>
> - Director, consumer goods industry, 1,000 - 5,000 employees

> "Requires dedicated resources to stay current."
>
> - C-suite, finance industry, 1,000 - 5,000 employees

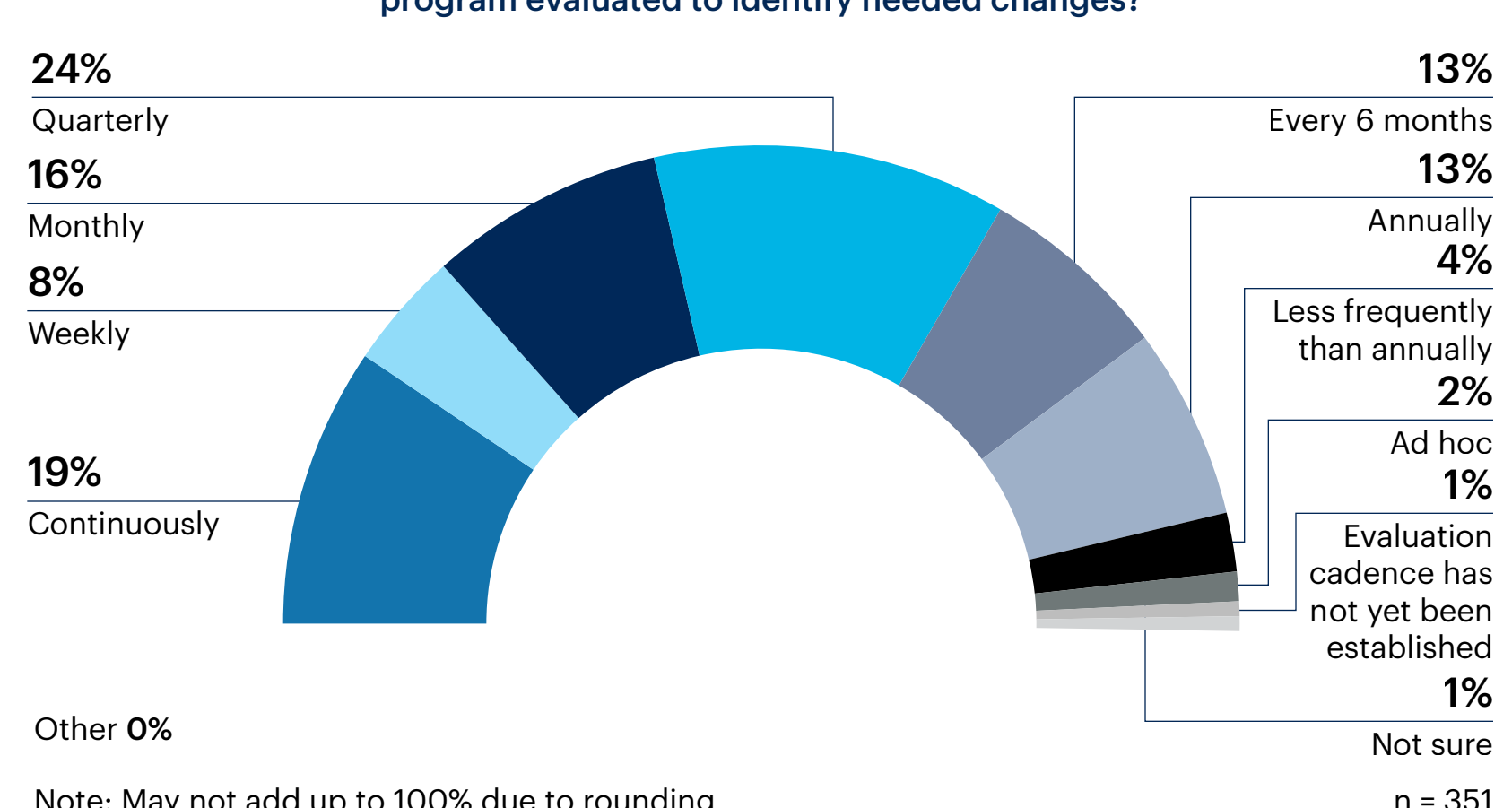
> "VM is currently the most discussed budget topic."
>
> - Director, telecommunications industry, 10,000+ employees

Question: Please share any final thoughts on your organization's vulnerability management program.

Most consider their VM program's vulnerability assessment effective, but over one-third find metrics and reporting to be lacking

67% of surveyed leaders report that their organization's **VM program is evaluated at least quarterly if not more frequently**, with about one-fifth (19%) evaluating the program on a continuous basis.

How often is your organization's vulnerability management program evaluated to identify needed changes?



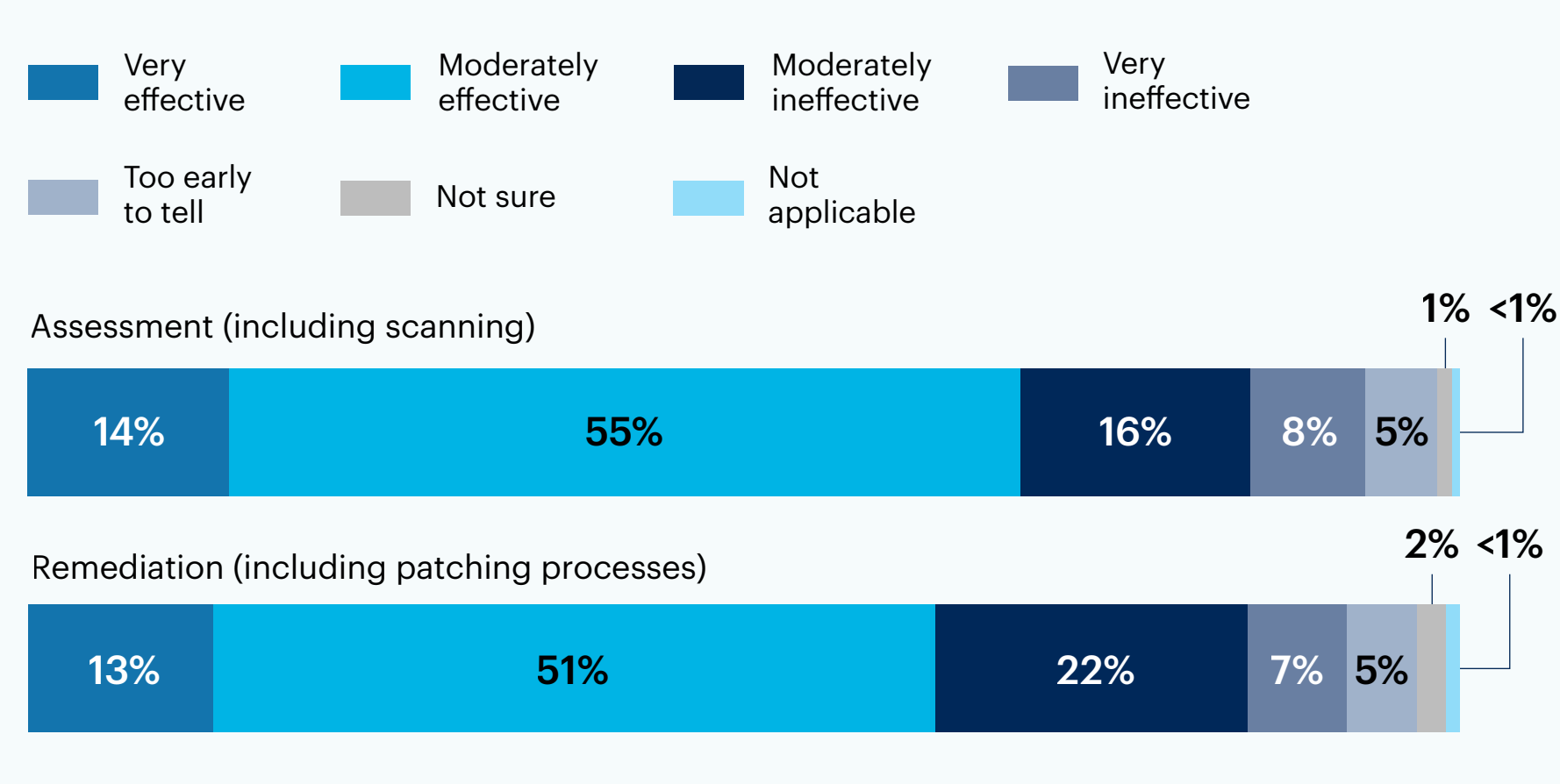
Other **0%**

Note: May not add up to 100% due to rounding

n = 351

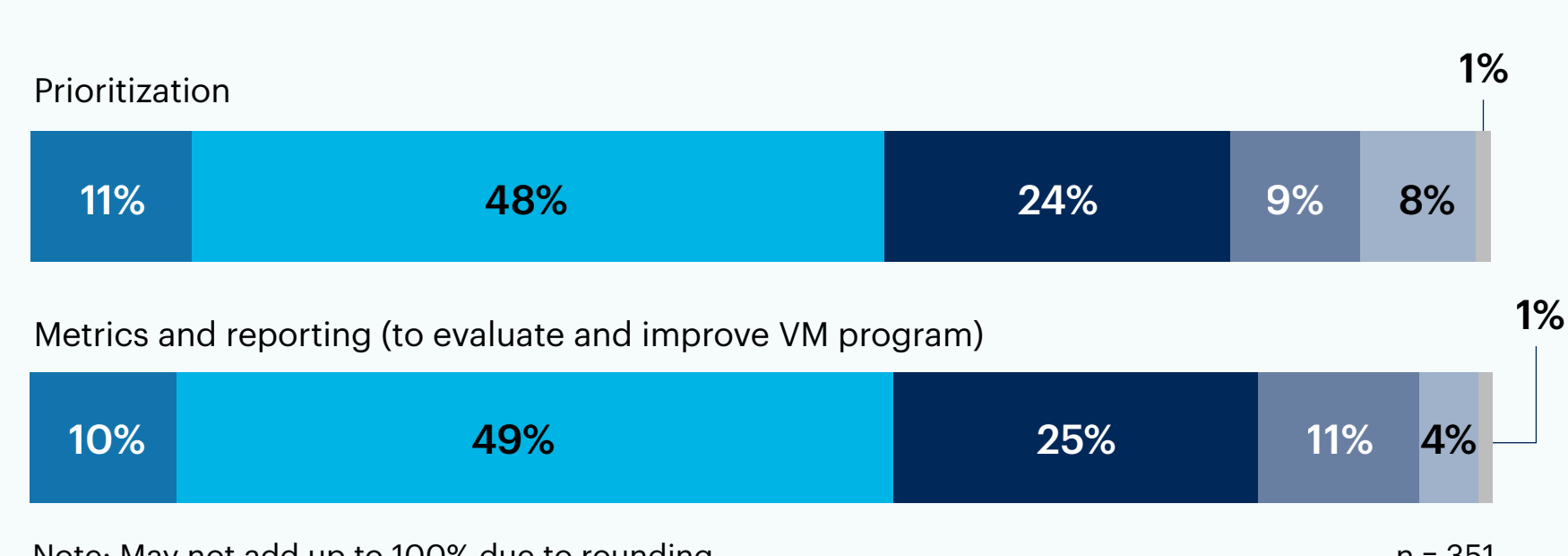
Most respondents note that **vulnerability assessment (69%)** or **remediation (64%)** are effective aspects of their organization's VM program…

From your perspective, how effective are the following aspects of your organization's vulnerability management (VM) program?



…but about one-third of respondents say **metrics and reporting (36%)** or **prioritization (33%)** are ineffective.

From your perspective, how effective are the following aspects of your organization's vulnerability management (VM) program?



Note: May not add up to 100% due to rounding

n = 351

> "Since the pandemic started, our VM was totally recalibrated to accommodate new requirements given the remote environment needs."
>
> - VP, professional services industry, <1,000 employees

> "While we have matched our targets on identifying and assessing our potential vulnerabilities, it is still a long road to improve our continuous monitoring and leverage AI capabilities to automate further the processes and depend less on manual activities."
>
> - C-suite, finance industry, 10,000+ employees

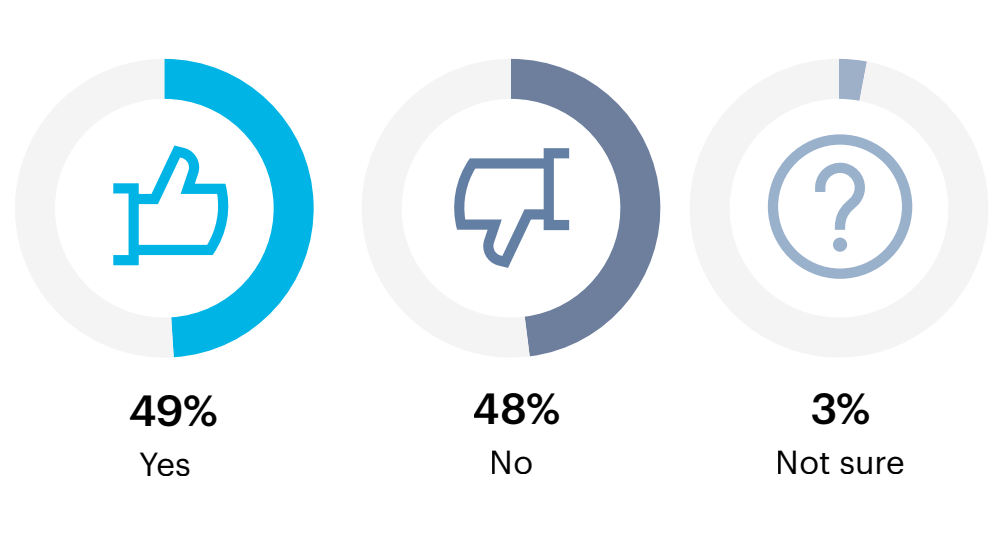
Question: Please share any final thoughts on your organization's vulnerability management program.

Respondent organizations are divided on VM process outsourcing, but most who take this route use it for network scanning

49% of respondent organizations **outsource VM processes** as part of their program, while nearly as many (48%) do not.

Within your organization's vulnerability management (VM) program, are any VM processes outsourced or handled by a managed service provider?

n = 351

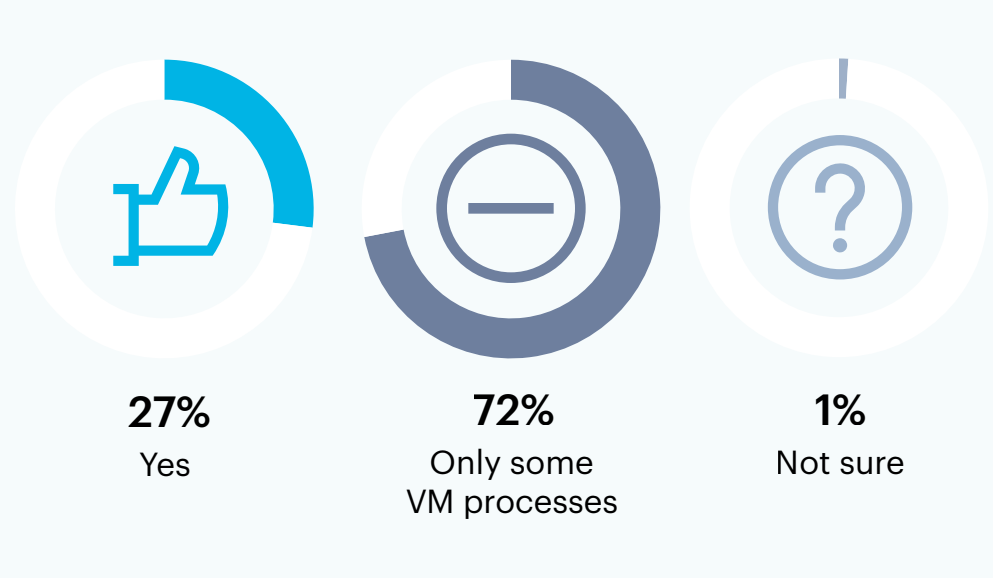


Among respondents whose organizations use outsourcing or a managed service provider for this purpose (n = 171), only 27% do so for all VM processes. The majority **(72%)** note that their organization **only outsources some VM processes**.

n = 171

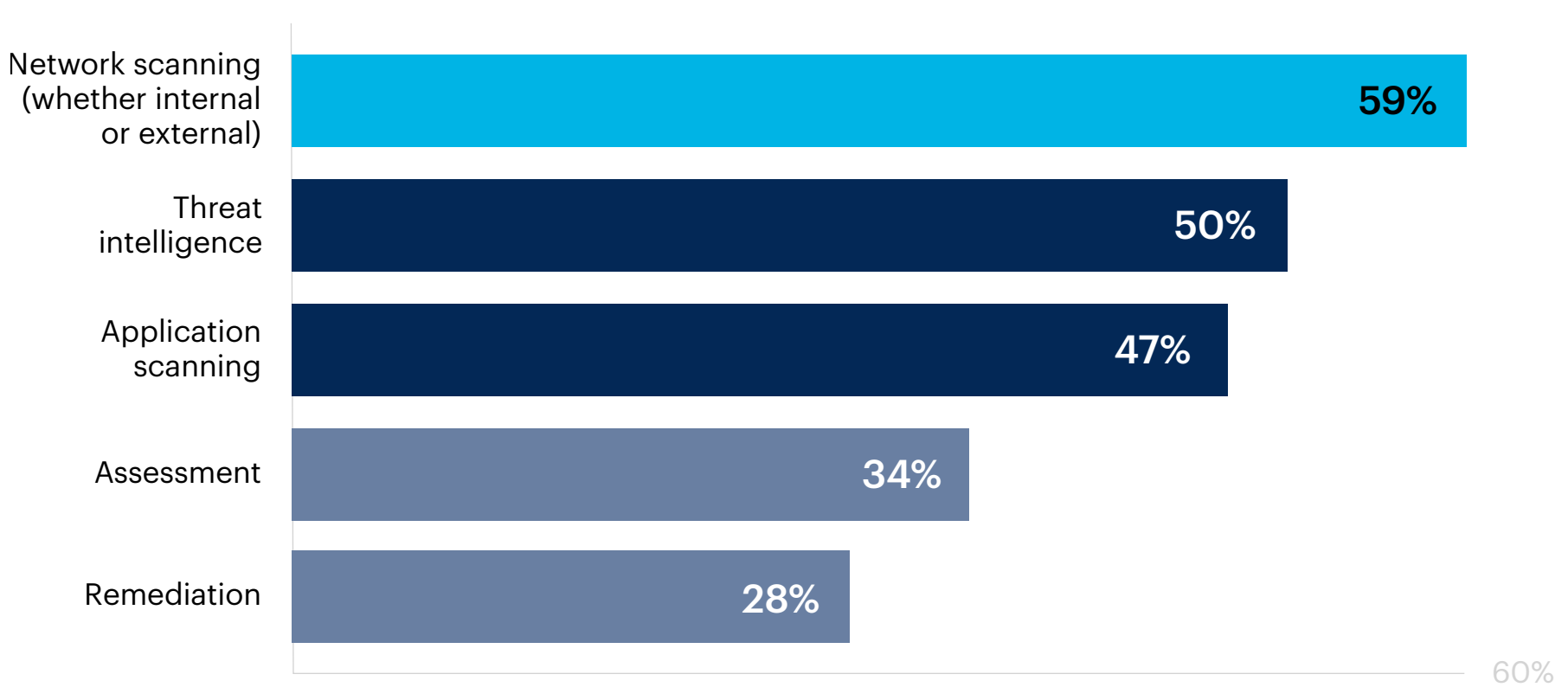
Question shown only to respondents who answered "Yes" to "Within your organization's vulnerability management (VM) program, are any VM processes outsourced or handled by a managed service provider?"

Does your organization outsource or use a managed service provider for all vulnerability management (VM) processes?



Most respondents at organizations that only **outsource select VM processes** (n = 123) indicate that **network scanning (59%)**, **threat intelligence (50%)** or **application scanning (47%)** are handled by external parties.

Within your organization's vulnerability management (VM) program, which VM processes are outsourced or handled by a managed service provider? Select all that apply.



Reporting **24%** | Asset discovery **24%** | Prioritization **11%** | Don't know **2%** | Can not say **3%** | Not applicable **0%** | Other* **1%**

n = 123

Question shown only to respondents who answered "Only some VM processes" to "Does your organization outsource or use a managed service provider for all vulnerability management (VM) processes?"

*Other includes: Off hours work for various duties

> "Distributed responsibility is definitely the biggest issue."
>
> - Director, educational services industry, 10,000+ employees

> "Continuous vulnerability assessment and remediation is important but time consuming. We are leaning towards outsourcing that task to an MSSP."
>
> - Director, transportation industry, <1,000 employees

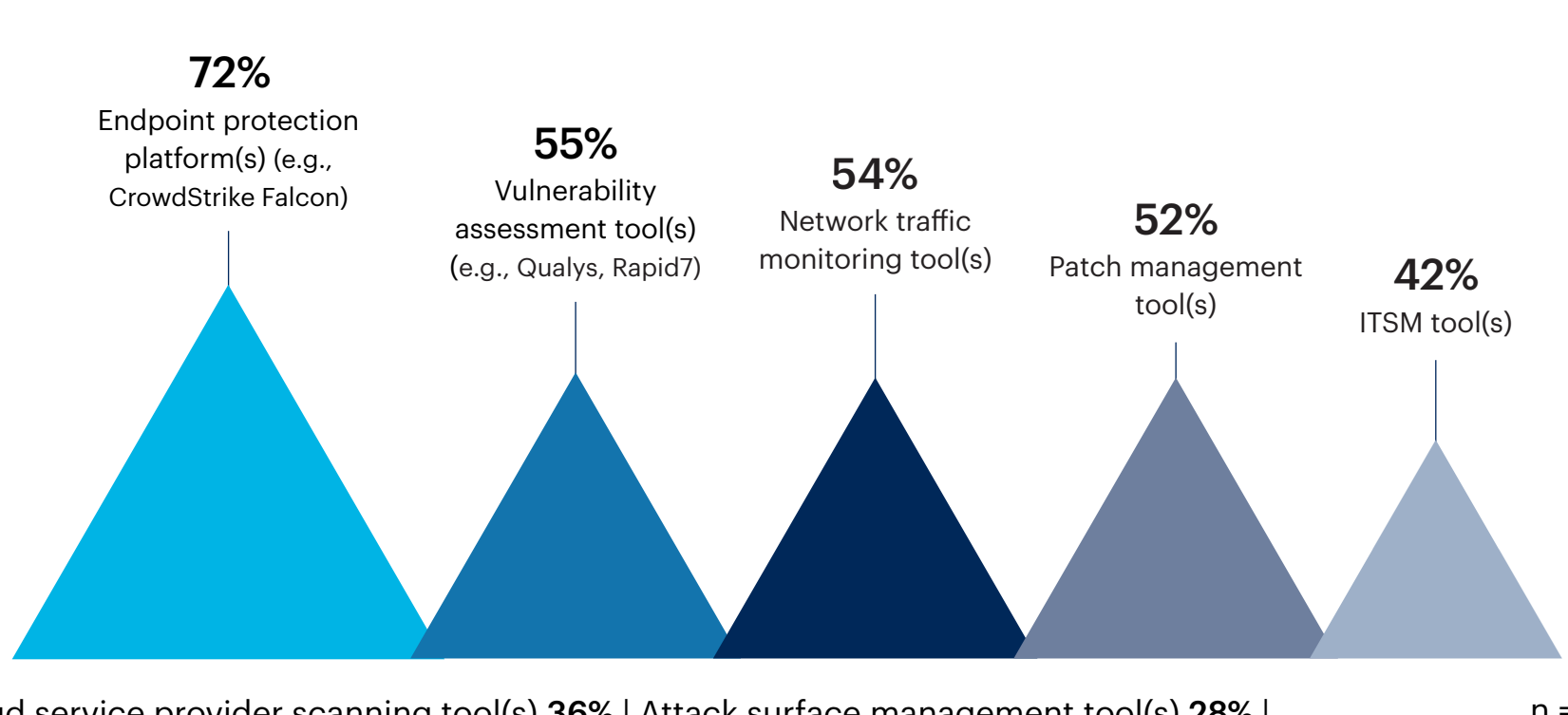
Question: Please share any final thoughts on your organization's vulnerability management program.

Splitting VM and patch management across different teams presents a challenge for many respondent organizations

Almost three-quarters **(72%)** of all surveyed leaders say their organization uses **endpoint protection platforms** for its VM program.

Over half note that their organization's VM program includes tools for vulnerability assessment (55%), network traffic monitoring (54%) or patch management (52%).

Does your organization use any of these purchased solutions as part of its vulnerability management program? Select all that apply.



Cloud service provider scanning tool(s) **36%** | Attack surface management tool(s) **28%** | Risk-based vulnerability management tool(s) **26%** | Breach and attack simulation tool(s) **15%** | Automated workflow tools (e.g., to streamline handoffs for remediation) **14%** | Can not say **1%** | Not applicable **1%** | Other* **1%** | Don't know **0%**

n = 351

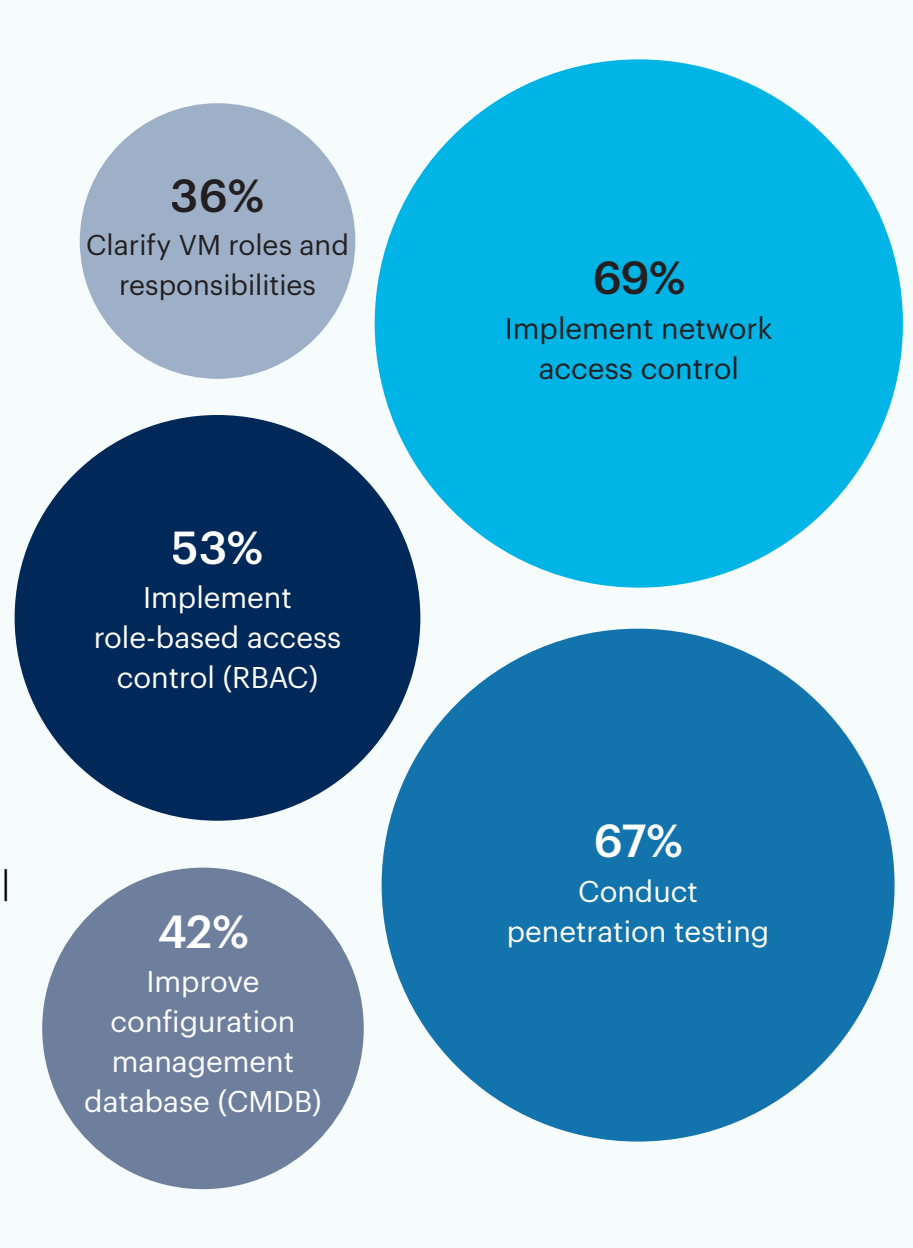
*Other includes: External 3rd party vulnerability scanning, None of the above

The majority of surveyed leaders list implementing **network access control (69%), conducting penetration testing (67%)** or **implementing role-based access control (53%)** among their organization's VM program strategies.

What strategies are part of your organization's vulnerability management (VM) program? Select all that apply.

Automate patching **33%** | Integrate VM tools with IT ticketing or workflow systems **31%** | Improve prioritization **25%** | Incorporate vulnerability assessment tools into CI/CD pipeline **23%** | Consolidate tools for VM and patch management **22%** | Develop custom risk scoring system **13%** | Establish bug bounty program **13%** | Host hackathon events **10%** | Don't know **<1%** | Can not say **<1%** | Not applicable **0%** | Other **0%**

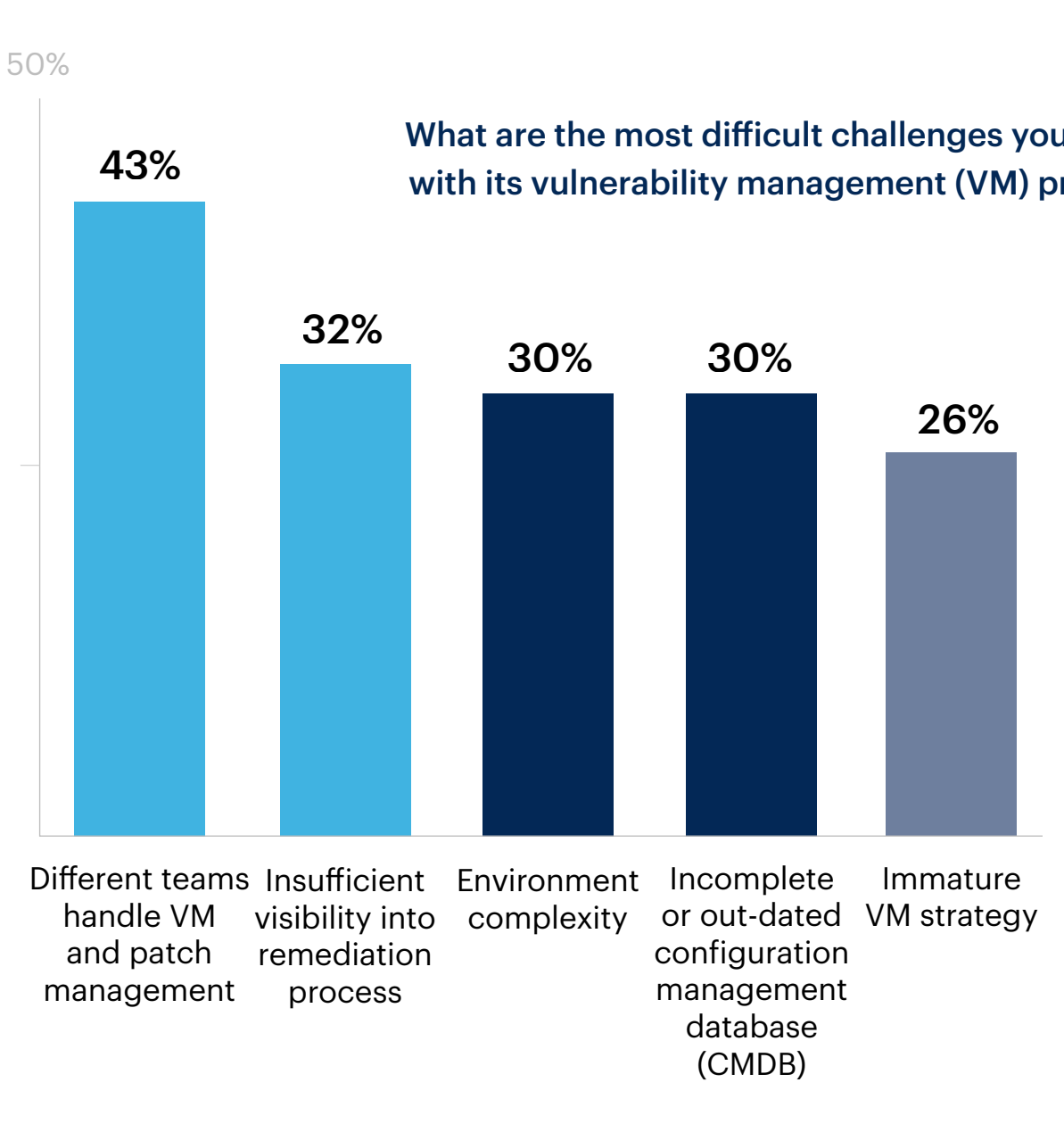
n = 351



Having **different teams assigned to vulnerability management and patch management (43%)** is the **most reported challenge** facing VM programs at respondent organizations.

Other commonly cited hurdles include inadequate visibility into the remediation process (32%), complex environments (30%) and having a configuration management database (CMDB) that is incomplete or out-of-date (30%).

What are the most difficult challenges your organization is facing with its vulnerability management (VM) program? Select up to 3.



Lack of clarity around VM roles and responsibilities **24%** | Regulatory requirements **23%** | Tools/services costs (e.g., subscriptions, maintenance) **23%** | Insufficient staff **23%** | Skills gaps **21%** | Increased number of assets **13%** | Integrations **9%** | Employee BYOD policy **8%** | Insufficient contextual information for prioritization **7%** | Controls not working as expected **4%** | Can not say **1%** | Don't know **0%** | Not applicable **0%** | Other **0%**

n = 351

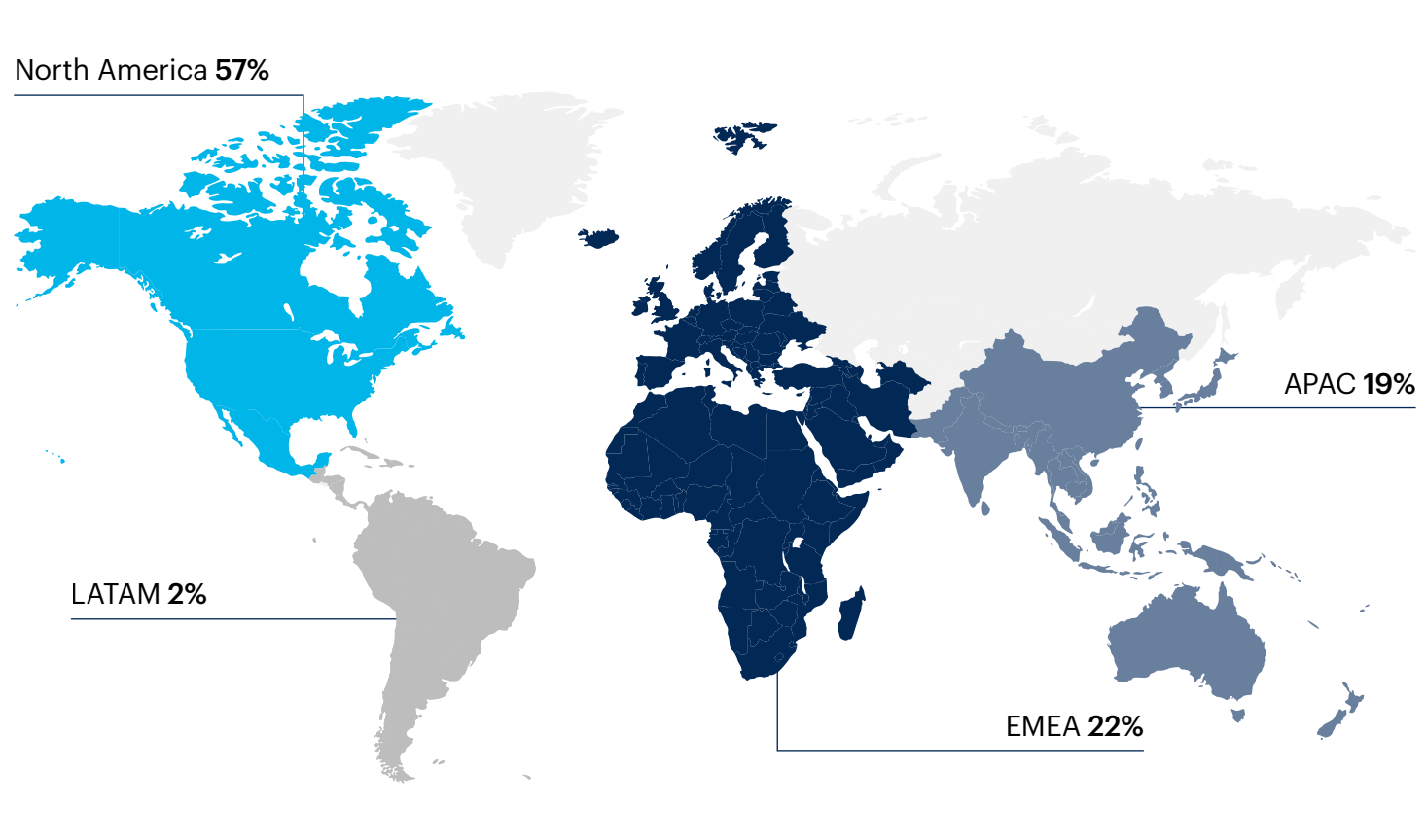
> "A risk register is key as not all vulnerabilities can be remediated and immediately."
>
> - Director, healthcare industry, 10,000+ employees

> "The greatest challenges regarding VM seem to be keeping up with changes in the local and global "technology environment", the changes and additions in legal and policy requirements, and managing the associated budget to provide for adequate control and management."
>
> - C-suite, educational services industry, 5,000 - 10,000 employees

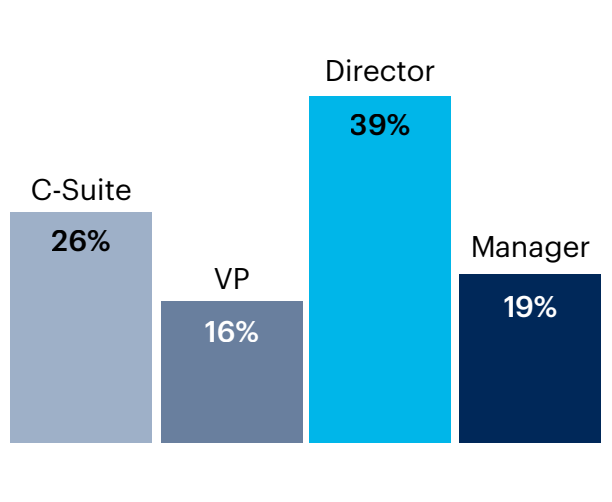
Question: Please share any final thoughts on your organization's vulnerability management program.

Respondent Breakdown

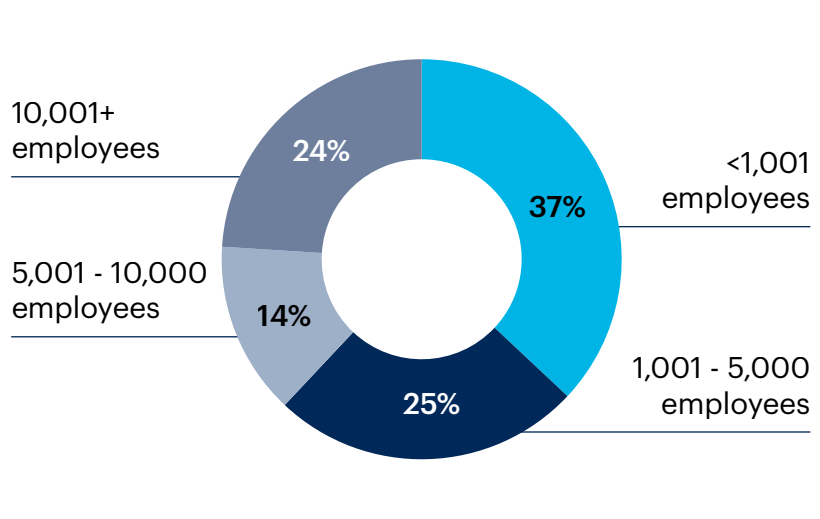
Region



Job Level



Company Size



Note: May not add up to 100% due to rounding

Respondents: 351 IT and information security leaders involved in their organization's vulnerability management program

Gartner

Source: Gartner Peer Community, State of Vulnerability Management Programs in 2023 survey