



SOLVING FOR RANSOMWARE THREATS: INSIGHTS INTO CURRENT LEADERSHIP ACTIONS

Data collection: February 20, 2022 - March 15, 2022

Respondents: 100 IT decision-makers



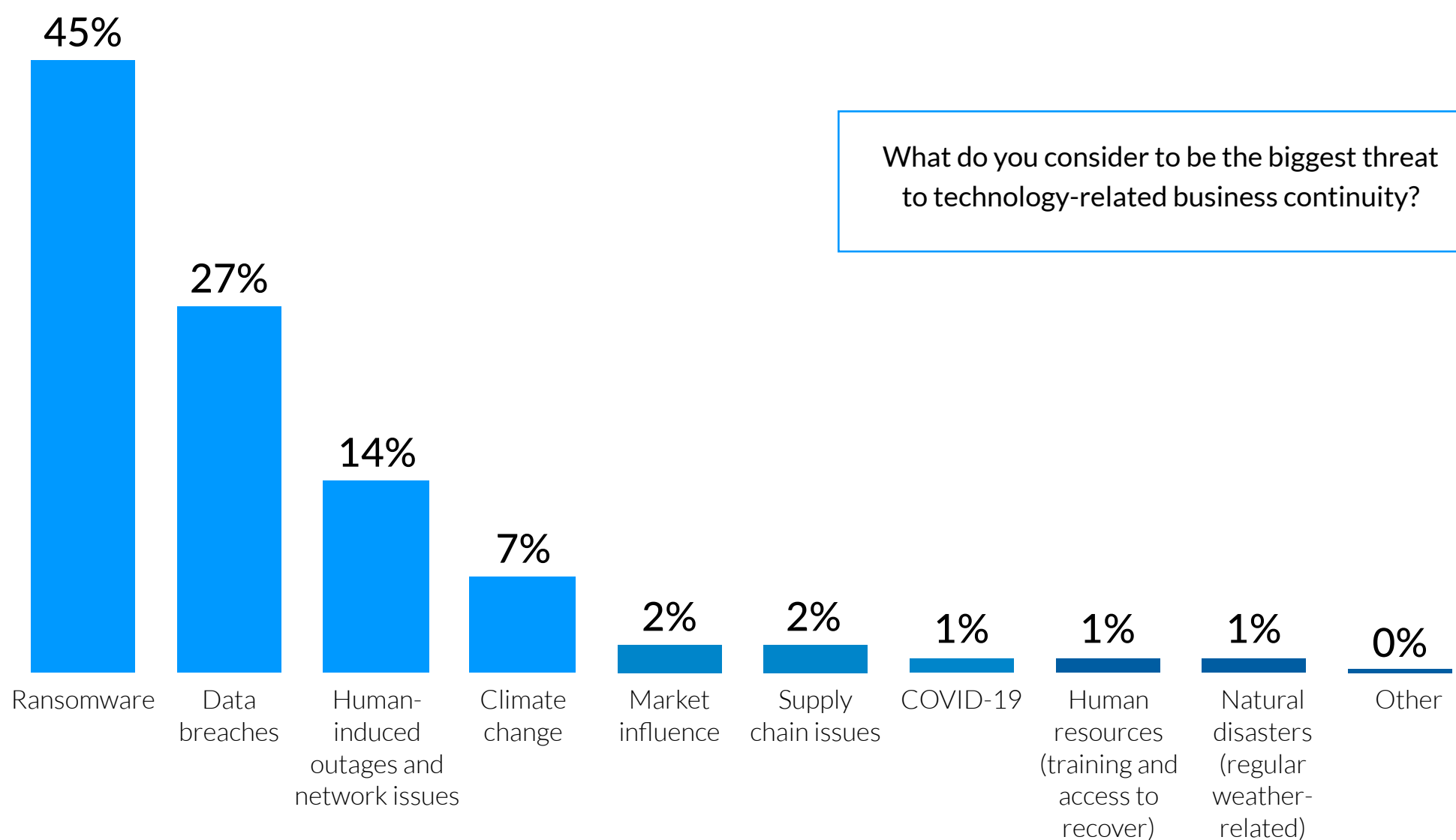
SOLVING FOR RANSOMWARE THREATS: INSIGHTS INTO CURRENT LEADERSHIP ACTIONS

Solving ransomware threats is a top concern among many company leadership teams, not just those in IT departments. To properly prepare for such a threat, businesses must begin taking a much more comprehensive approach, emphasizing the recovery aspects that too often get less attention.

To delve into the perspectives surrounding ransomware threats and what organizations are currently doing to shore up weaknesses and prepare for potential attacks, Pulse and InterVision surveyed 100 IT leaders.

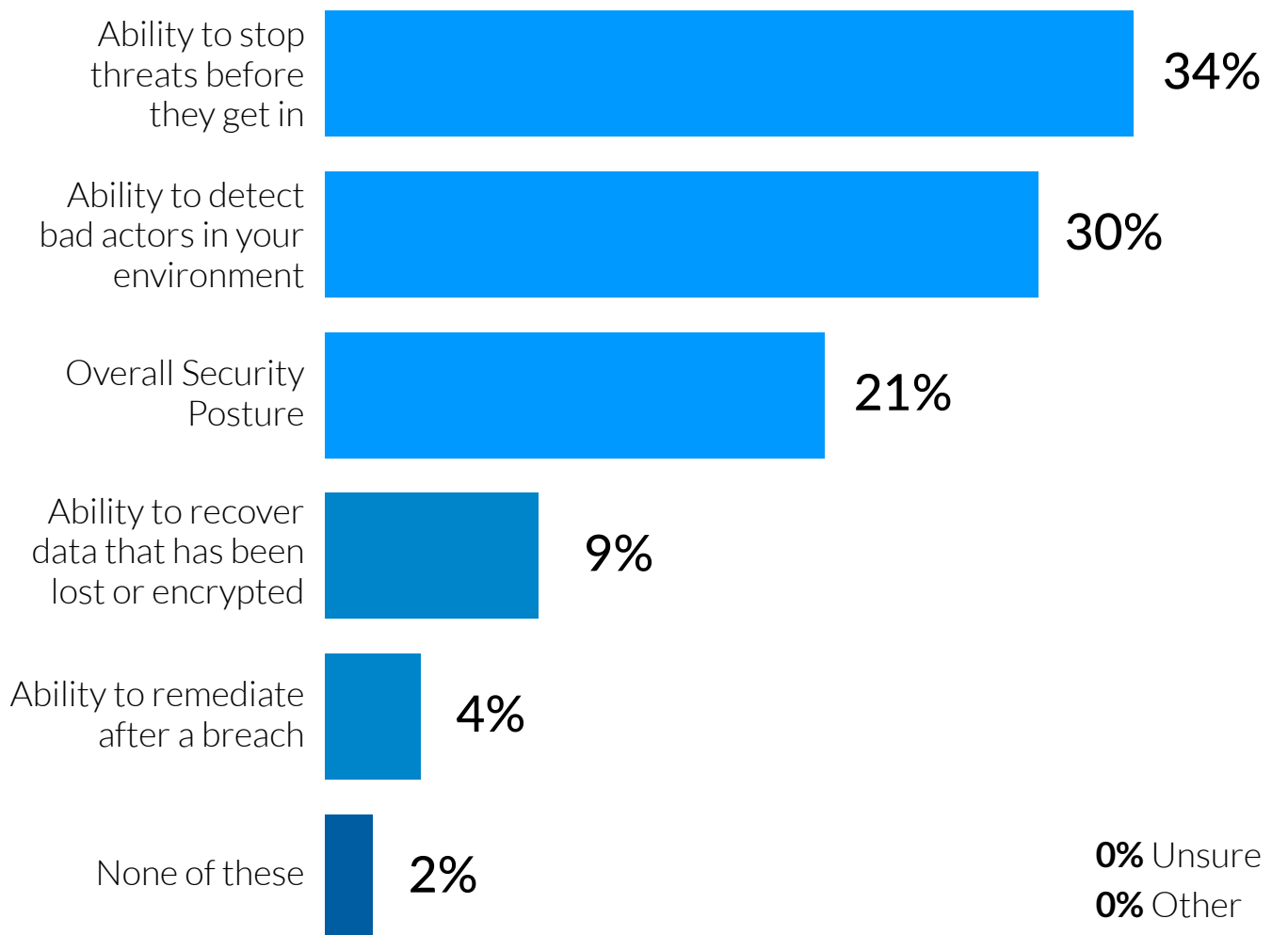
Decision-makers consider ransomware to be the top threat to their business and struggle to stop threats early

Ransomware was the top threat for 45% of respondents, while data breaches were the top threat for just over one-quarter (27%).



When responding to a cybersecurity breach, 34% of respondents say their biggest gap is their ability to stop threats before they get in. For 30%, it is the ability to detect bad actors in their environment.

What is the biggest gap in your business' ability to respond to a cybersecurity breach?

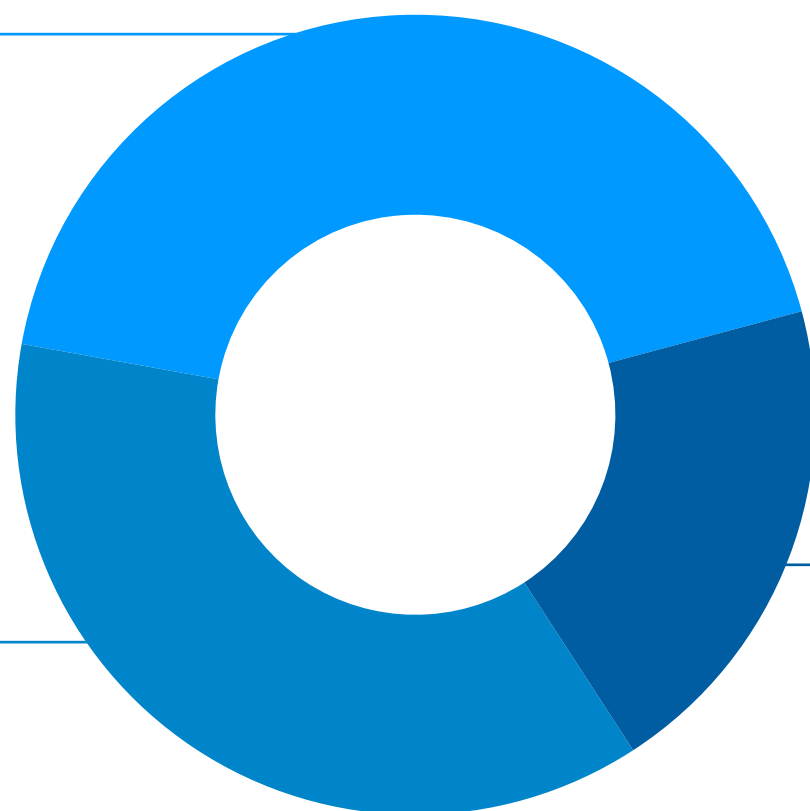


Technology and process were the top-cited areas for improvement when it comes to ransomware threats. People – the most expensive resource – was the least common choice.

When it comes to ransomware threats, in what area do you see the biggest room for improvement at your business?

43%

Process



0% None of these
0% Unsure

37%

Technology

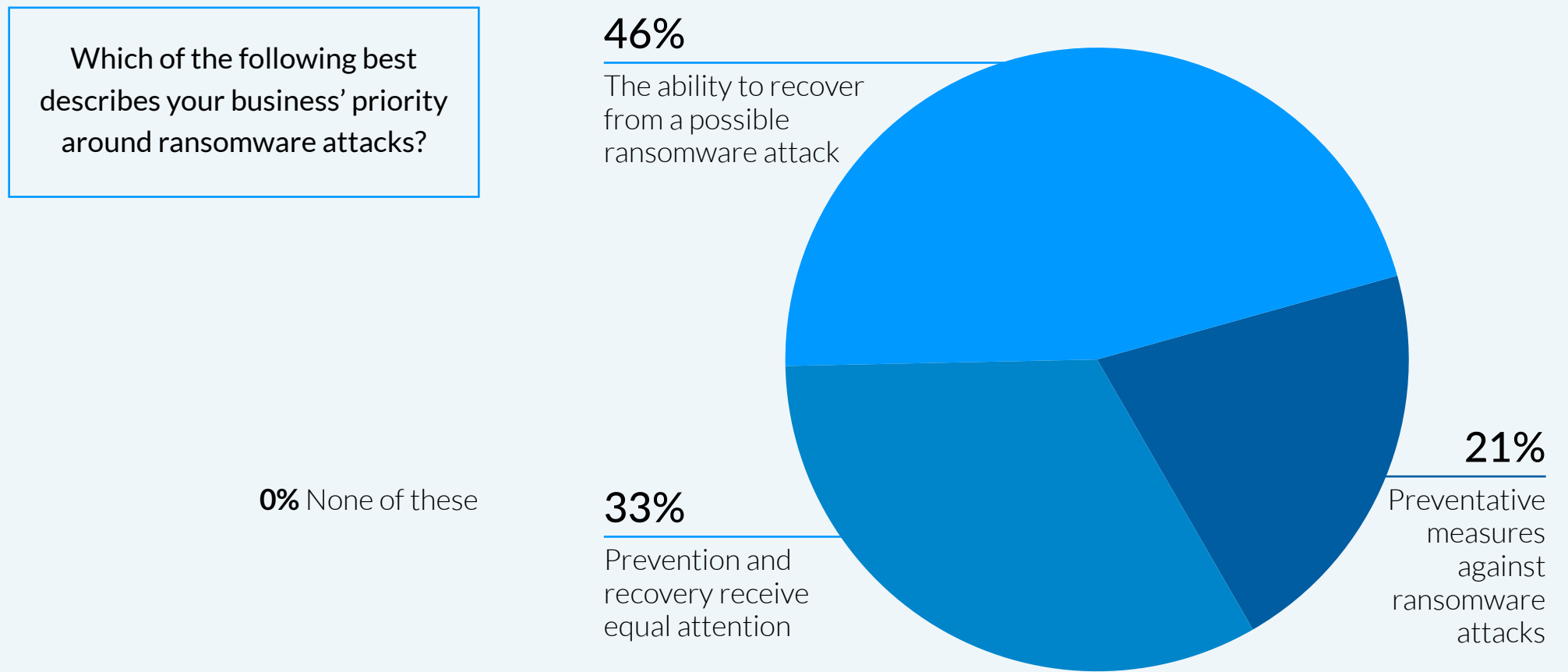
20%

People

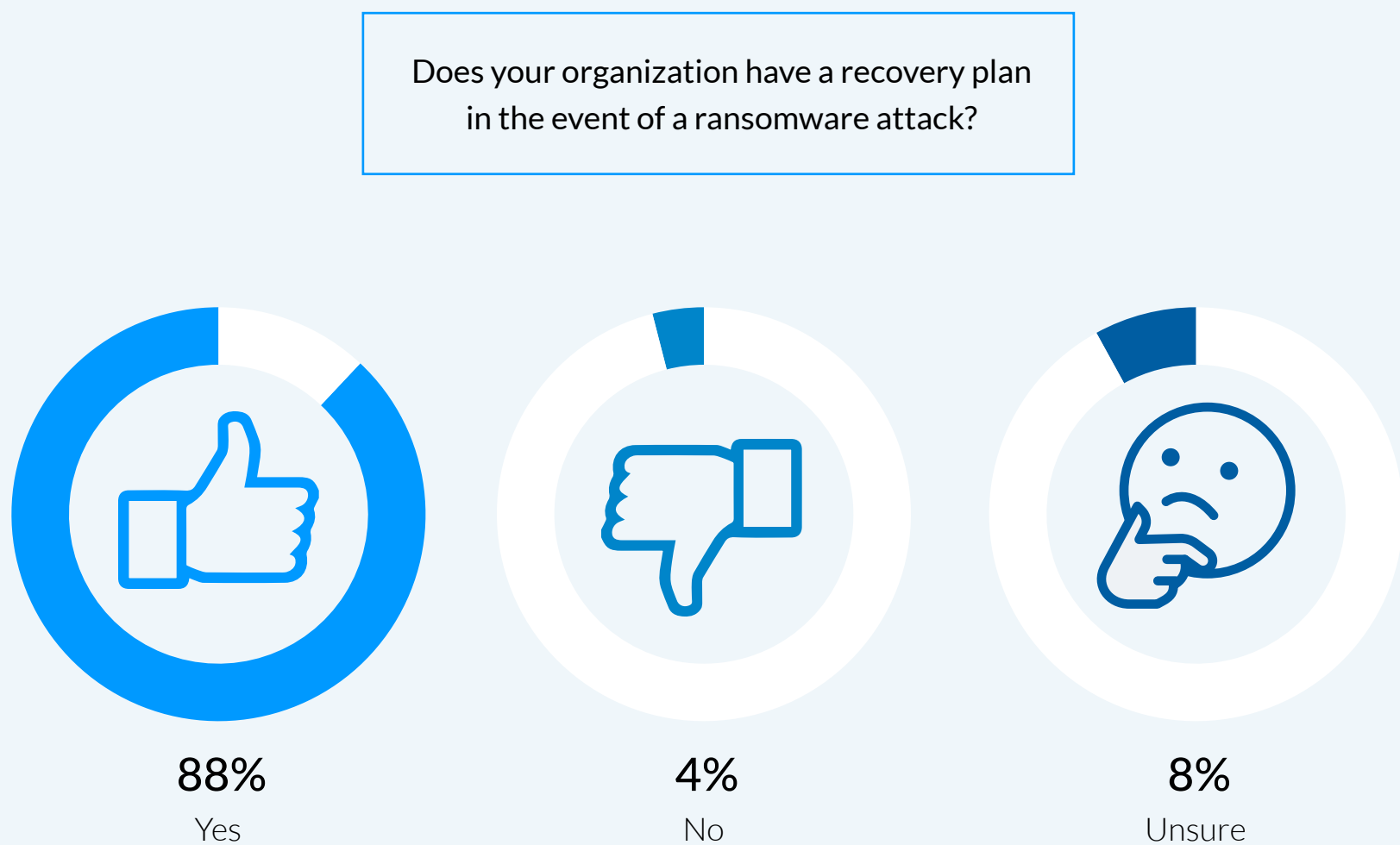


Businesses focus primarily on ransomware attack recovery, not prevention

More than double the number of respondents say their business' priority is around the ability to recover from a ransomware attack (46%) versus setting preventative measures (21%).



Nearly 90% of respondents say their organization has a recovery plan in place.



Over three-quarters of respondents say their business conducts tests on their ability to recover from a ransomware attack.

Does your organization test its ability to recover from a ransomware attack?



76%
Yes



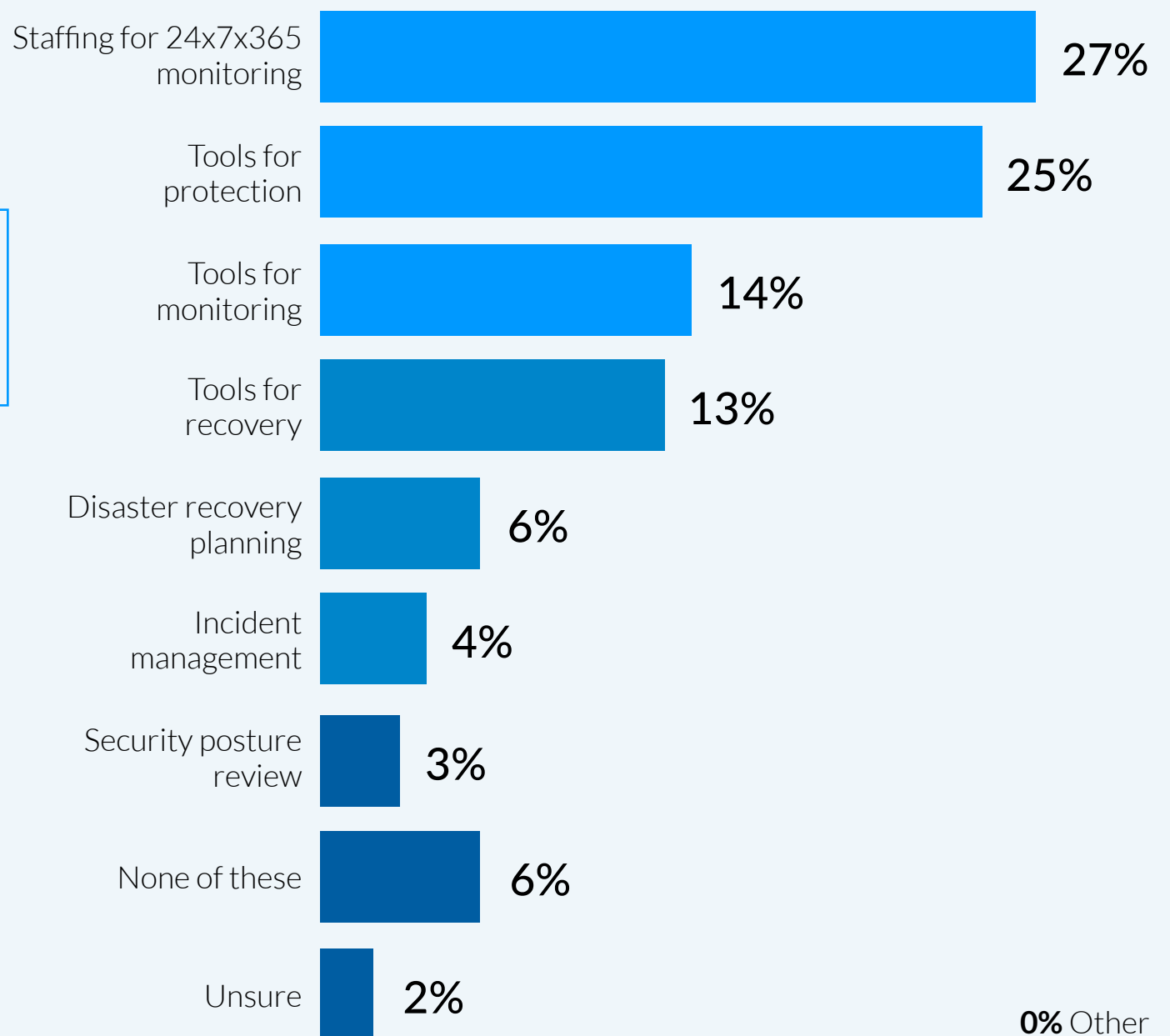
14%
No



10%
Unsure

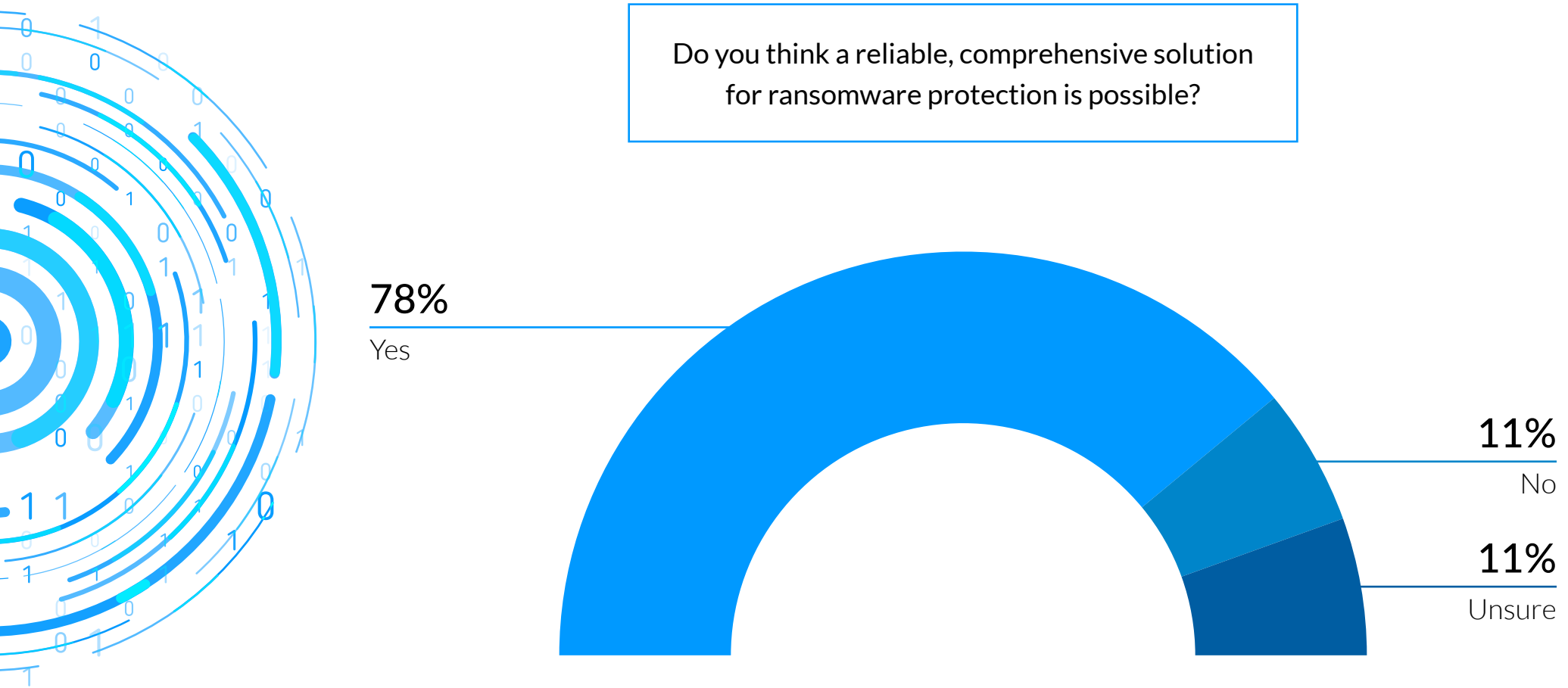
Most respondents feel their organization is least prepared with either staffing to monitor (27%) or tools to protect (25%) against ransomware.

When it comes to ransomware, in what area is your organization LEAST prepared?

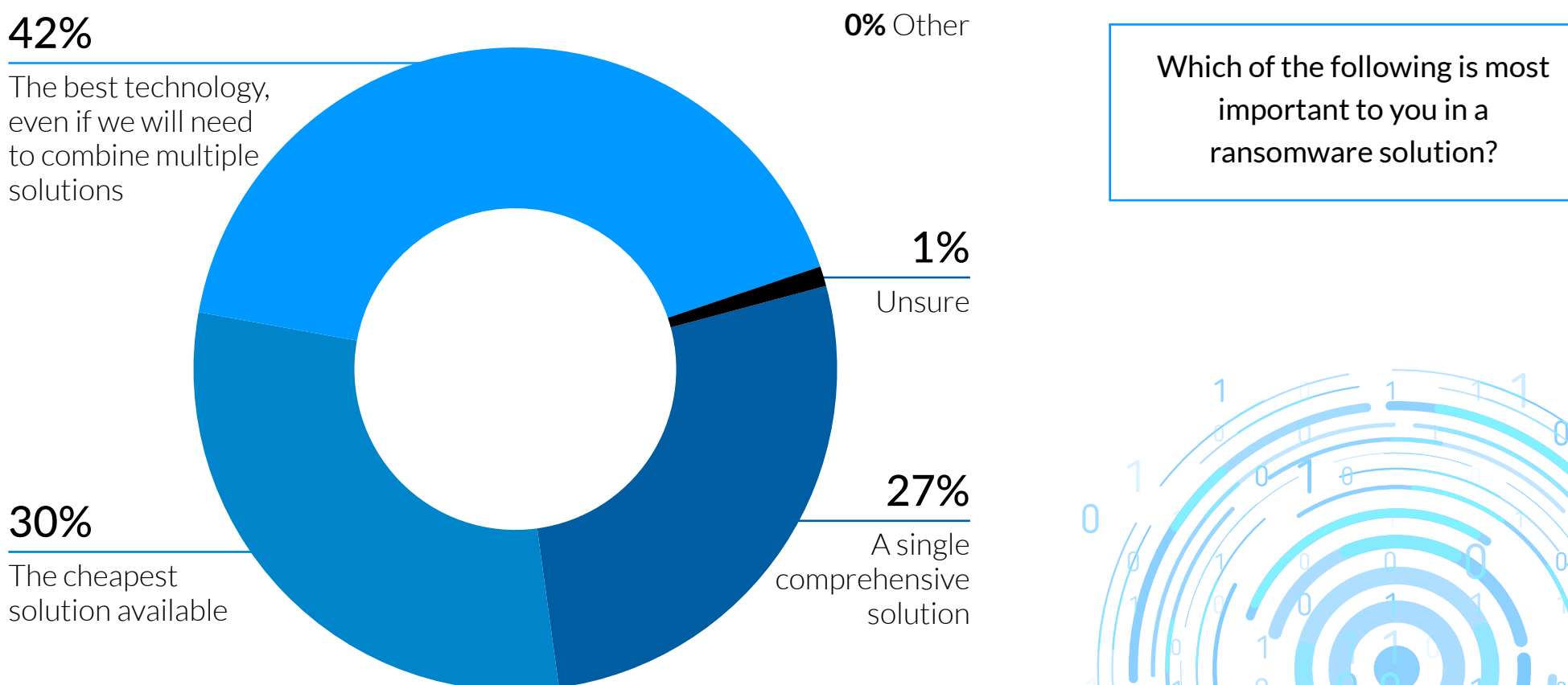


Decision-makers want the best technology for ransomware protection and most start by consulting peers or research analysts

78% of respondents believe that a reliable and comprehensive ransomware solution is possible.

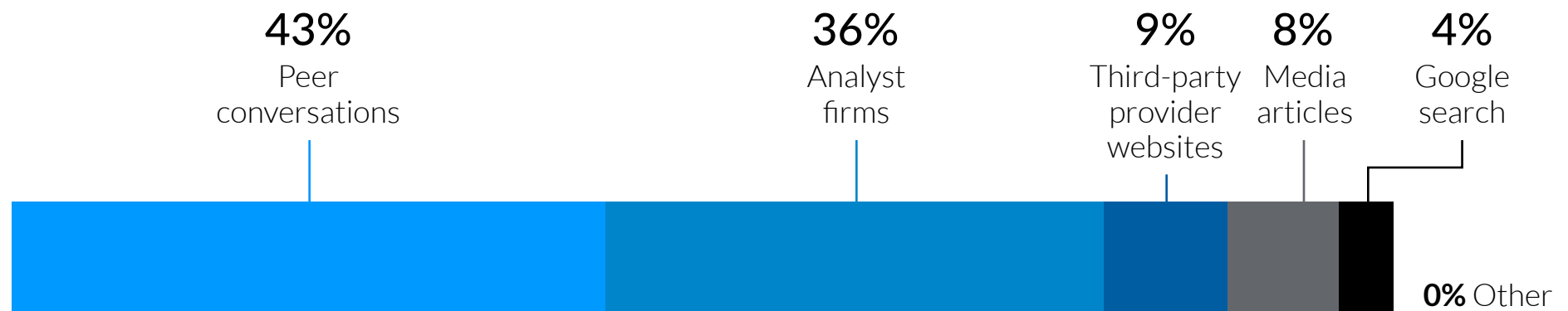


But for most (42%), having the best technology is more important than having a single comprehensive solution.



When deciding how to protect against ransomware, 43% of leaders first seek the guidance of a peer, while 36% turn to analyst firms to start.

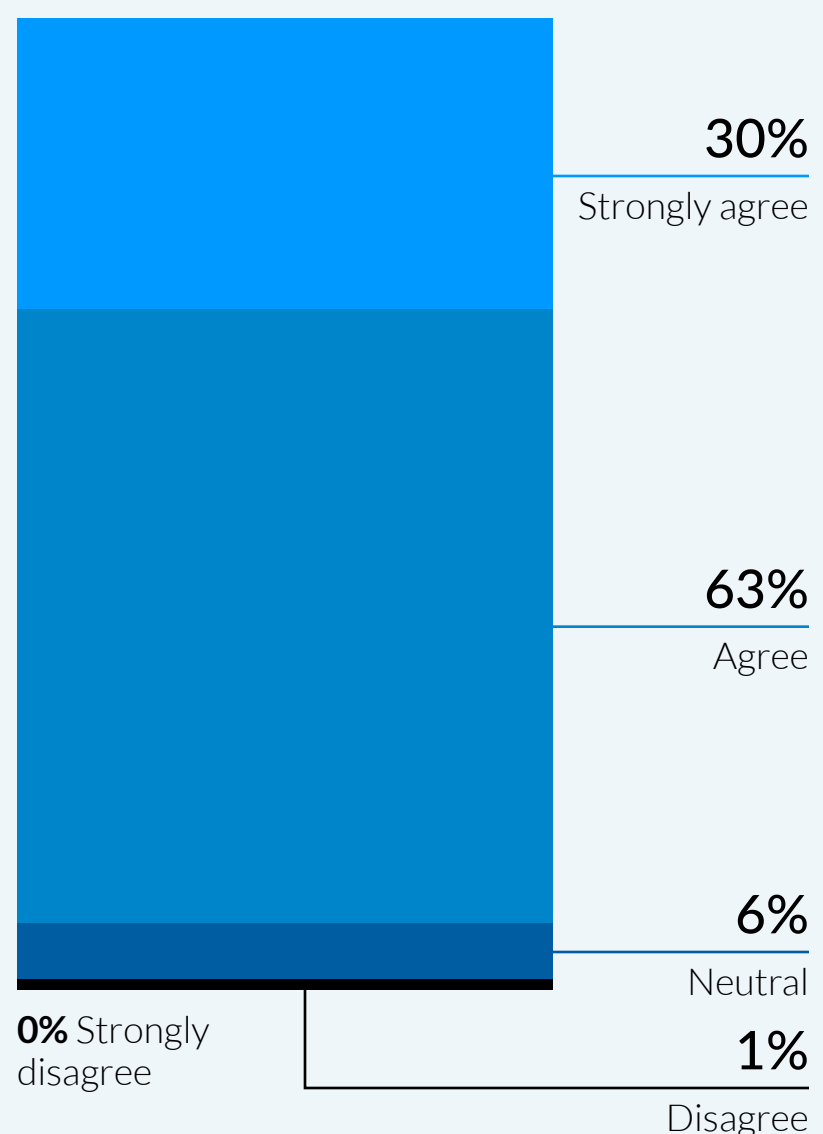
When beginning your research to protect the organization from ransomware, what source do you typically start with?



Effective ransomware protection demands a comprehensive and holistic approach from organizations

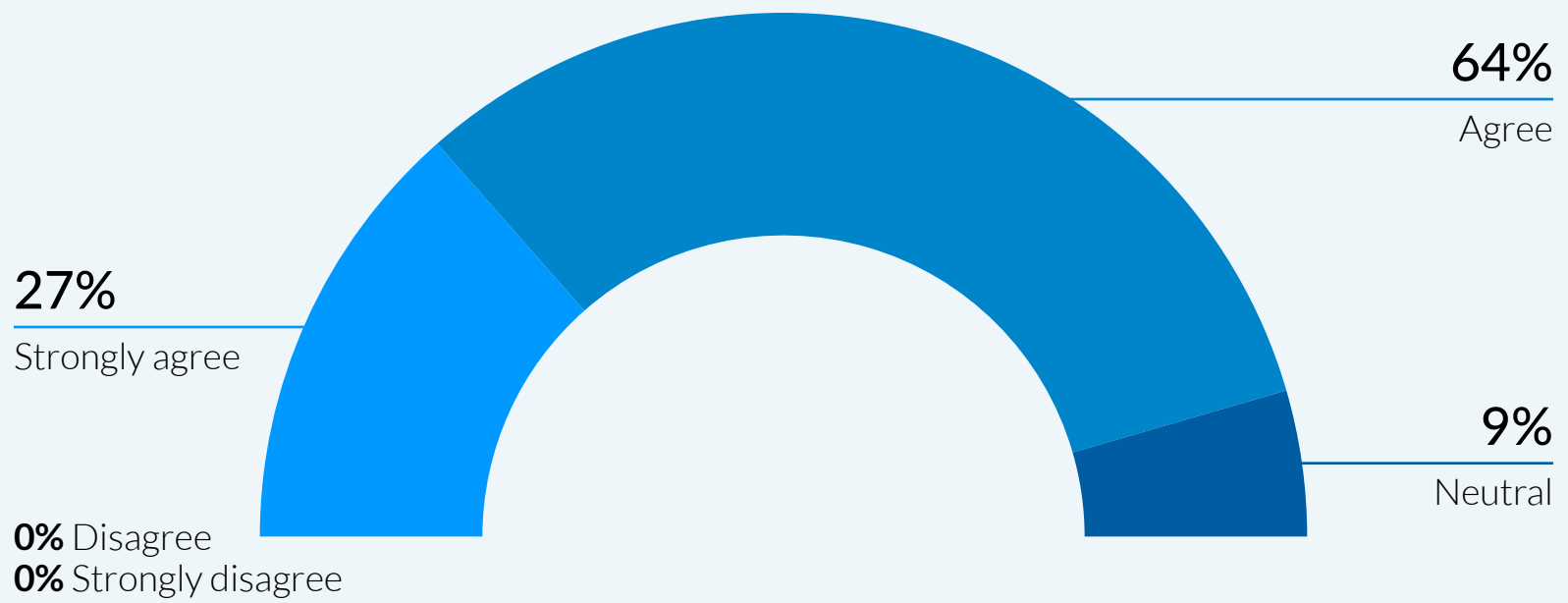
93% of leaders agree that organizations need a comprehensive approach to ransomware.

To what extent do you agree or disagree with the following statement: "Organizations need a comprehensive approach to ransomware that will protect, detect, and restore both critical information and business operations."



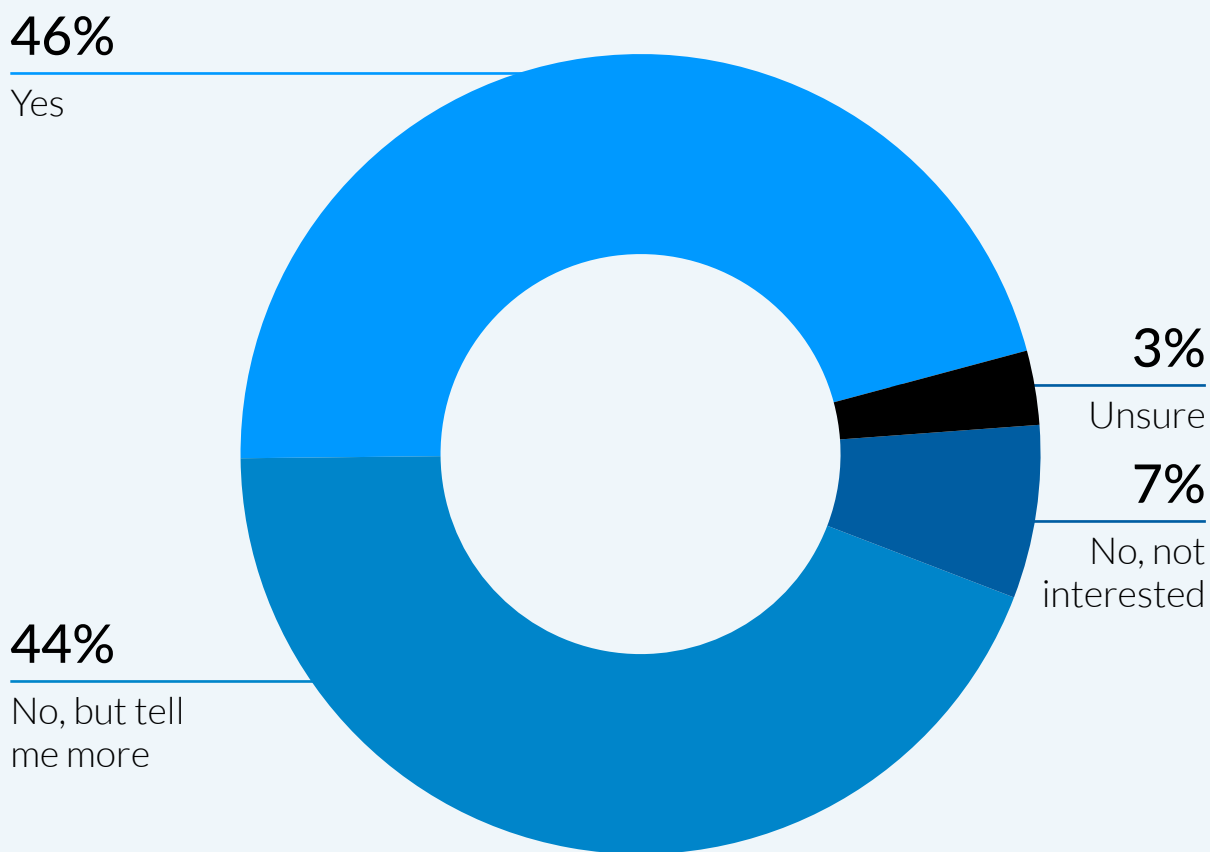
Not a single respondent disagreed that cybersecurity and disaster recovery teams must work together to solve ransomware challenges.

To what extent do you agree or disagree with the following statement: "Organizations need to pair cybersecurity and disaster recovery teams together to solve ransomware challenges from a holistic perspective."



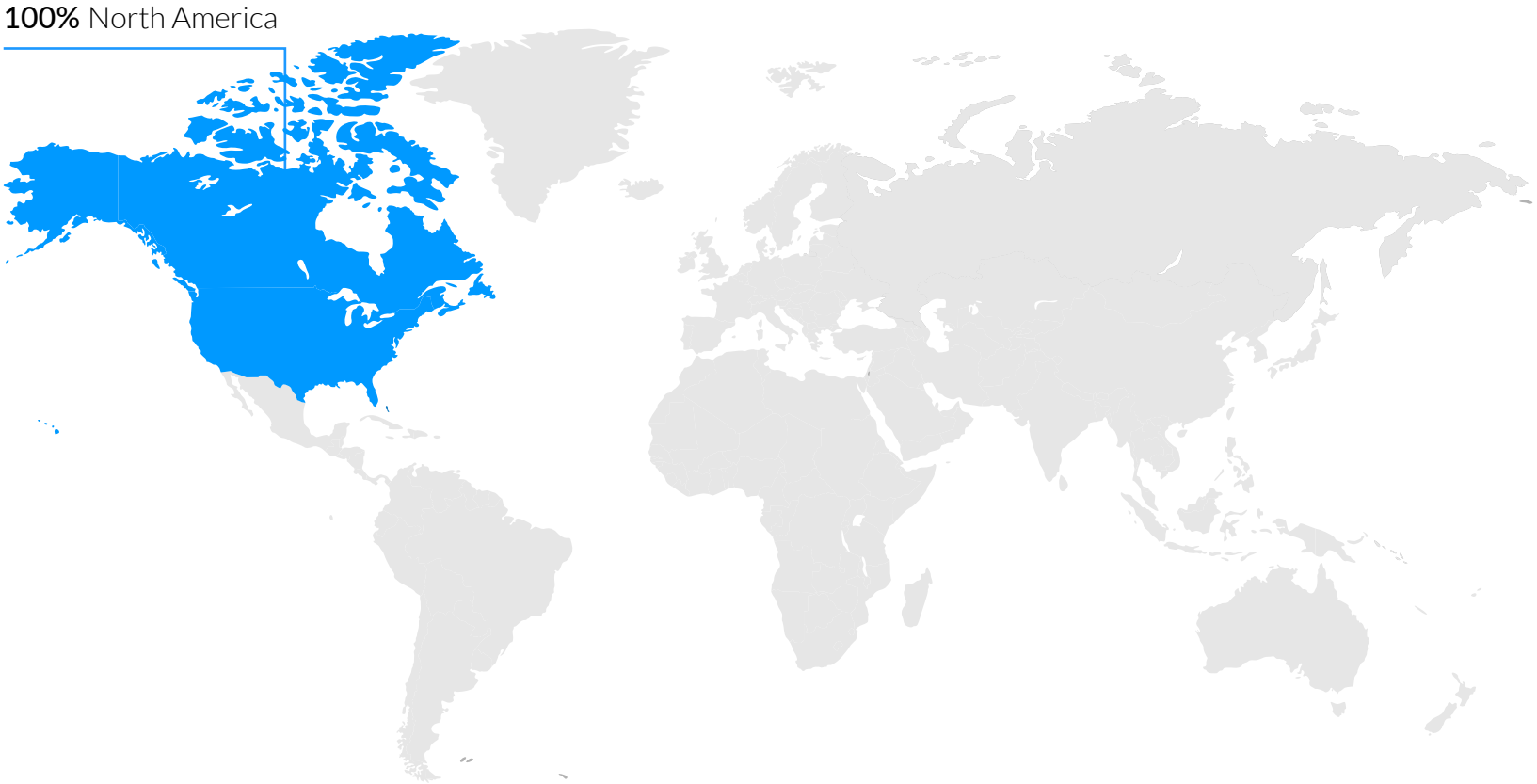
There is an appetite for a solution as almost all (90%) respondents have heard of or are interested in learning more about RPaaS.

Have you heard of ransomware protection as a service (RPaaS)?

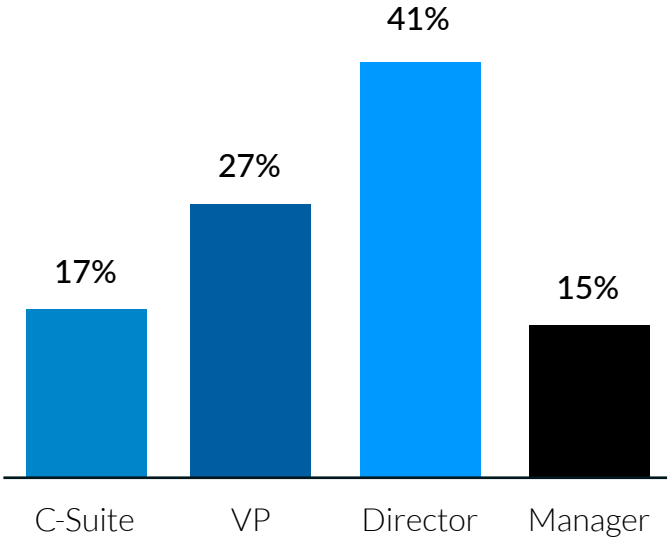


Respondent Breakdown

Region



Title



Company Size

