BlackBerry | Cybersecurity

PULSE

Only 8% of IT Security Executives Feel Very Confident in Their Legacy AV Solutions

Industry leaders understand that an in-depth security strategy is required to combat attackers. Organizations are still using legacy antivirus (AV) tools that may be inefficient for IT staff and ineffective at stopping today's threats.

Pulse and BlackBerry surveyed 100 IT security executives to understand how they handle unknown malware threats and how they plan to improve preventative security tools.

Data collected Jan. 18 - Feb. 5, 2022

Respondents: 100 IT Security Executives

Legacy AV solutions are insufficient to protect against unknown malware threats.

The majority (99%) of IT security executives agree that a prevention strategy that is effective against unknown malware must be able to identify and prevent threats before they execute.

To what extent do you agree that a pre-execution prevention strategy is needed to stop modern forms of unknown malware that might not be included in current signature files?

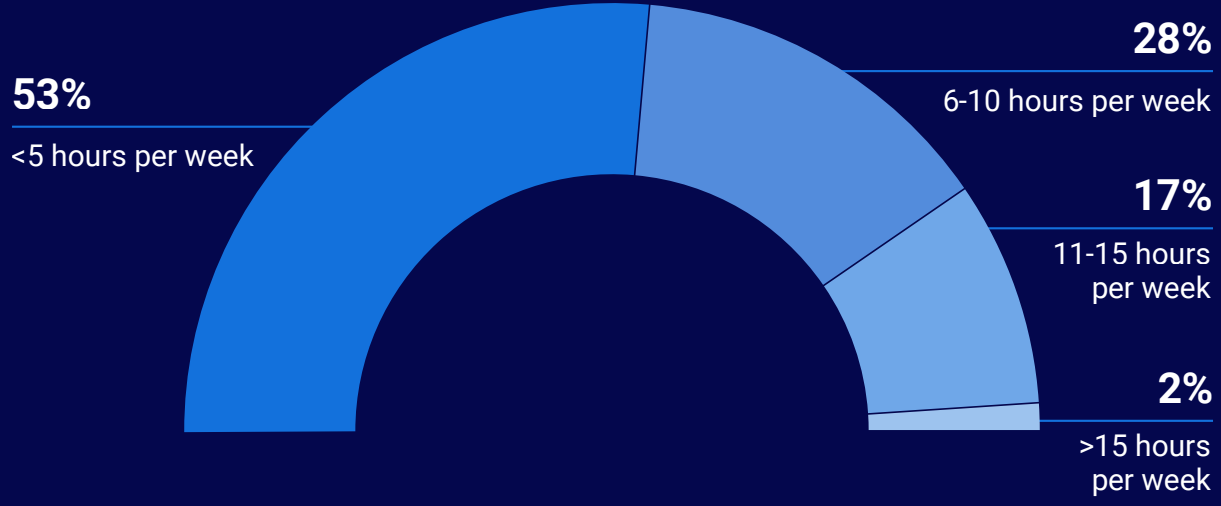
Understand the benefits of implementing AI-Driven EDR protection.

Learn More

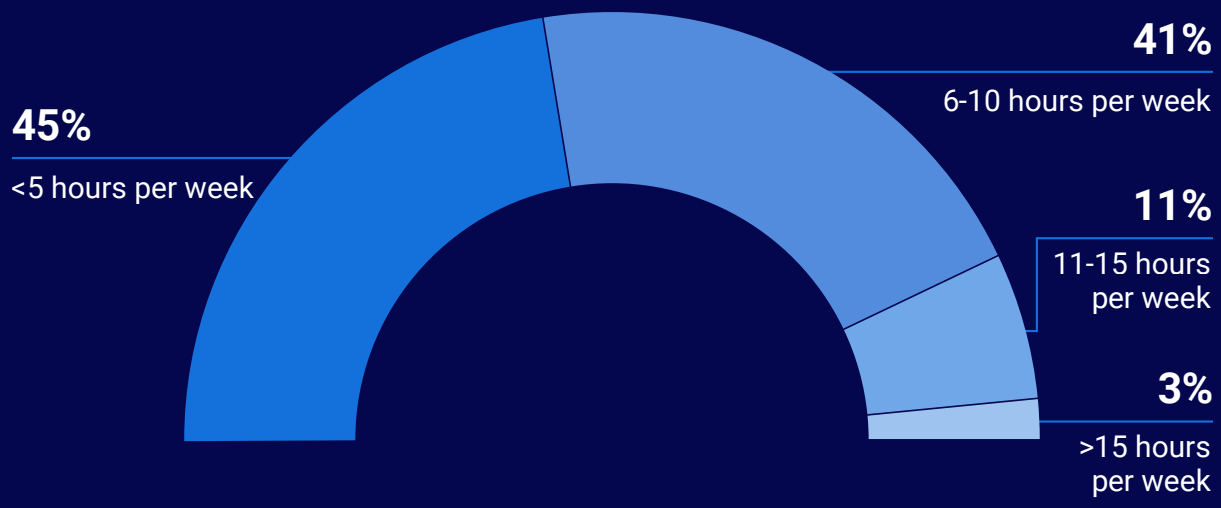
More than half (55%) of respondents say their IT staff are spending more than 5 hours per week administering and updating signature-based AV solutions. By comparison, only 47% of respondents indicated this was the case a year ago. Specifically, the number of respondents who say their IT teams spend 6-10 hours on updates and administration jumped from 28% to 41%.

How much time is your IT staff spending administering and updating older signature-based AV solutions?

2021



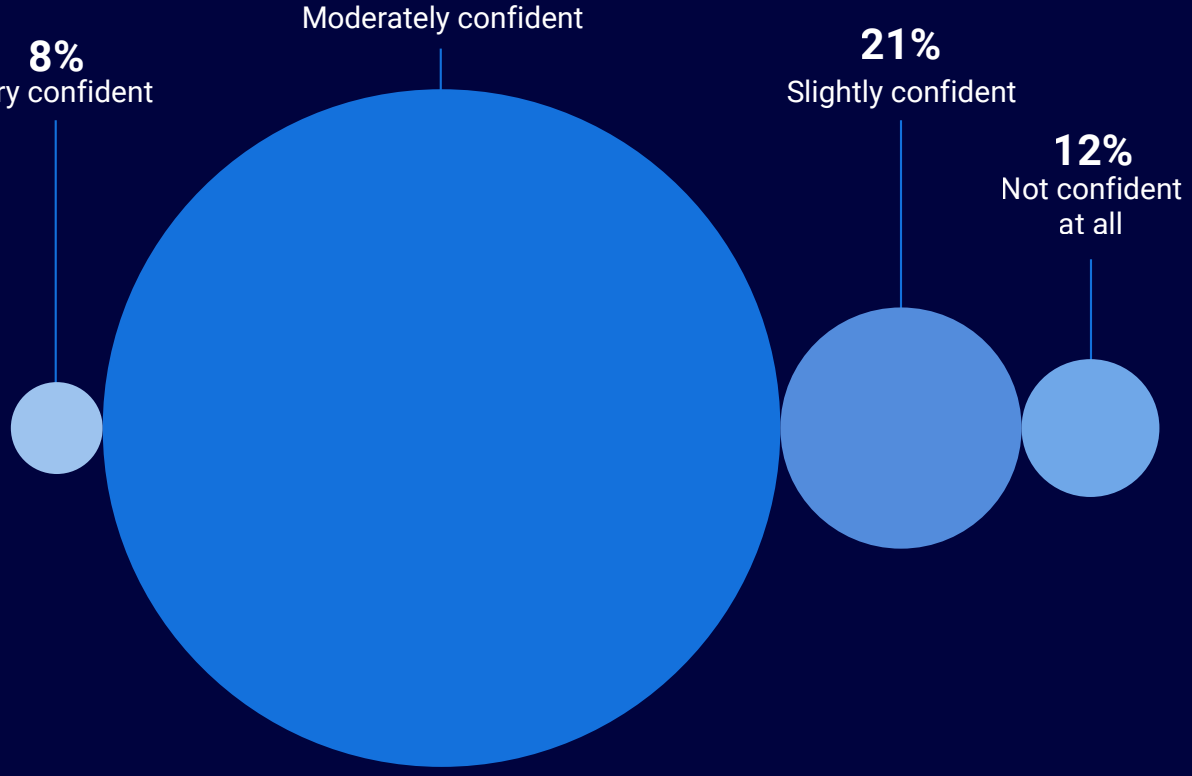
2022



Only 8% of IT security executives are very confident that their legacy AV solutions can detect and prevent modern malware threats. Since last year, the percentage of leaders who are not confident in their legacy AV solution has increased from 8% to 12%.

How confident are you in your legacy AV solution at detecting and preventing modern malware threats?

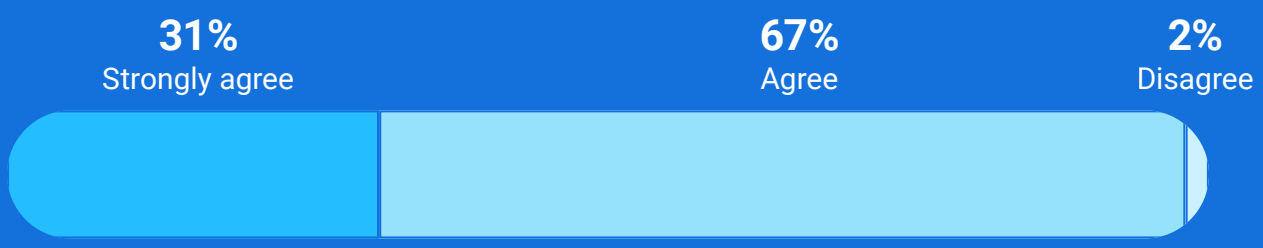
59%



Modern cybersecurity tools need to keep up with modern threats, and artificial intelligence and machine learning (AI/ML) make that possible.

The vast majority (98%) of professionals surveyed believe that AI/ML-based cybersecurity tools are important to stopping malware execution and zero-day threats.

To what extent do you agree that artificial intelligence (AI) and machine learning (ML)-based cybersecurity tools are important to stopping threats?



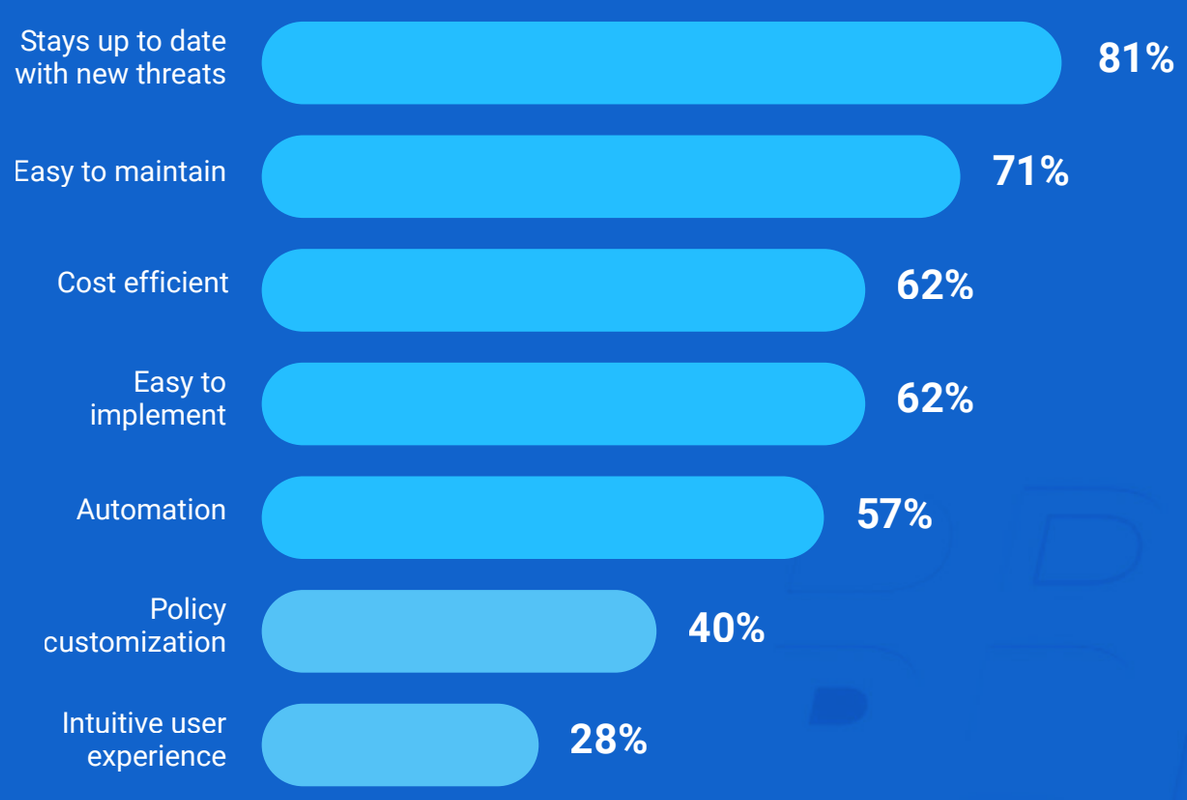
Learn how to mitigate cyber incidents in milliseconds by combining sophisticated AI and ML technologies with best-in-breed EDR strategy.

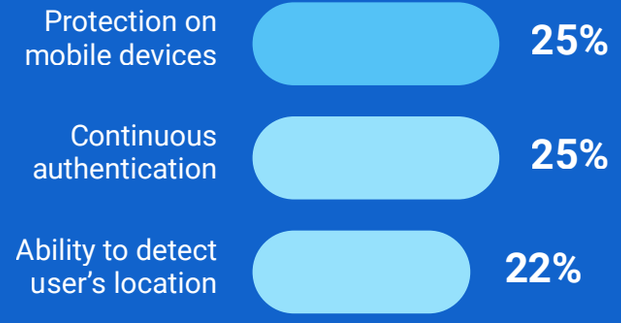
Get The Brief

IT security executives evaluate new security tools based on many criteria, the most important being ease of maintenance (73%), which overtook staying up to date with new threats as the key decision driver for 2022. This makes sense given the increase in the amount of time IT staff are spending on administration of legacy tools this year.

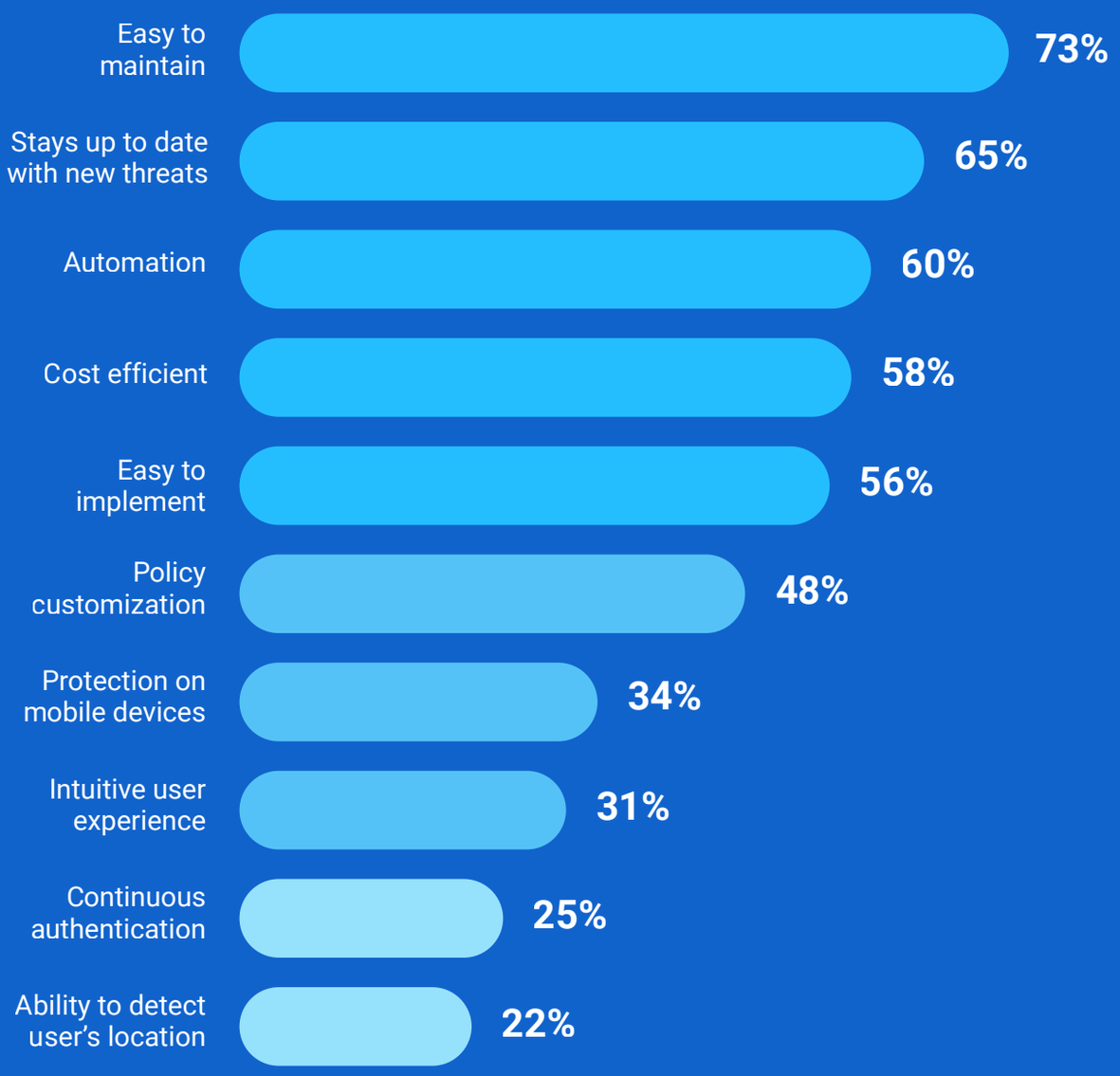
When evaluating security tools, what are the five most important criteria?

2021





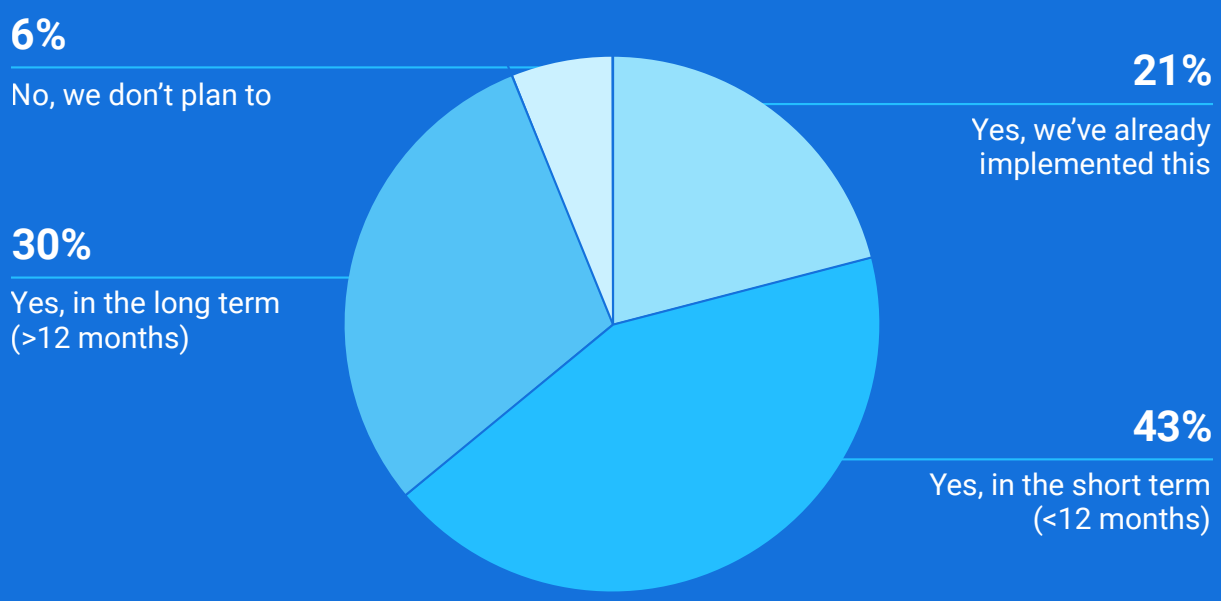
2022



The proportion of security executives who have implemented AI/ML has increased from 17% to 21% since last year. Meanwhile, 43% of IT security executives are planning to implement AI/ML-based endpoint protection solutions within the next 12 months.

Is your organization currently implementing or planning to

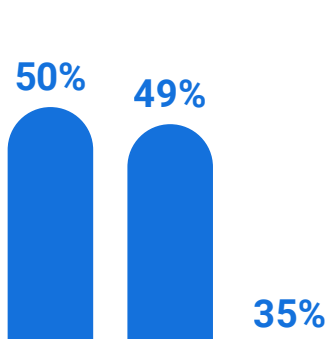
implement AI and ML-based endpoint protection solutions?

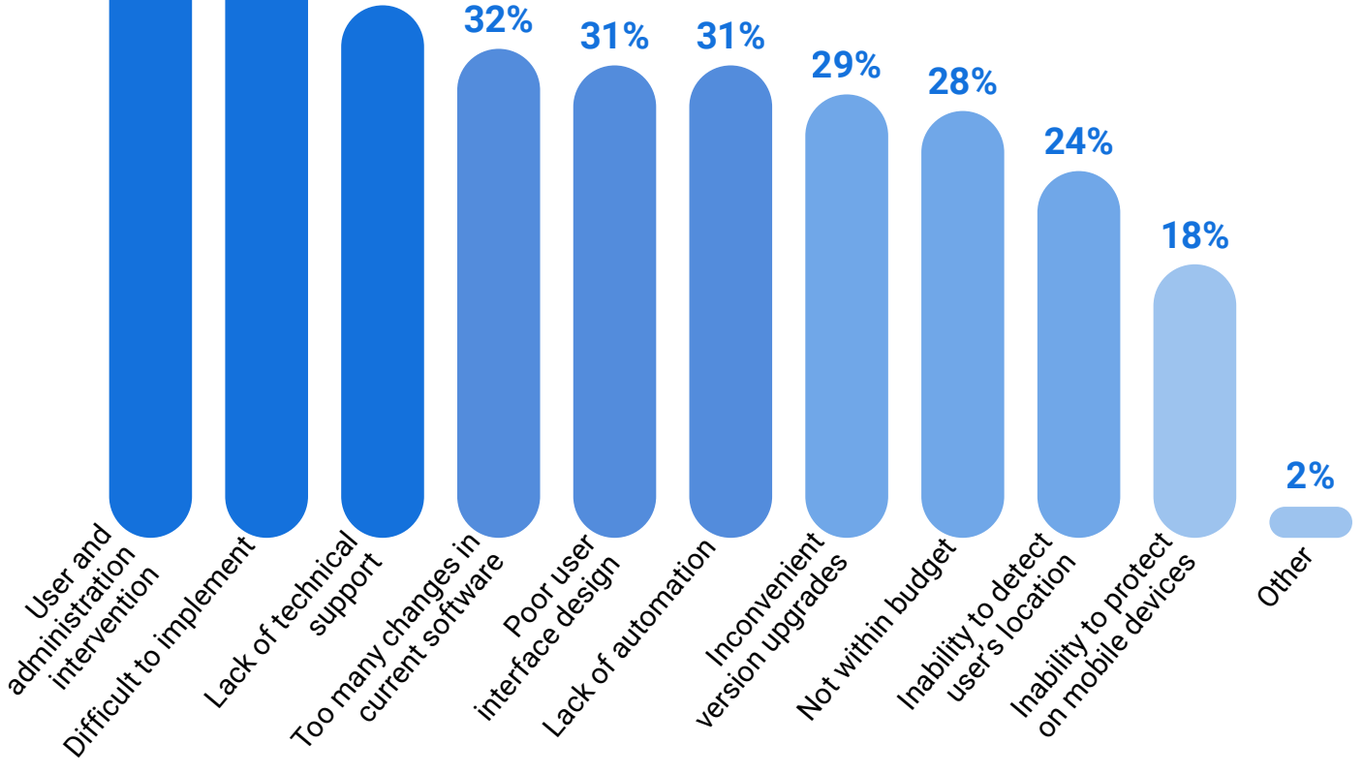


Endpoint protection tools are also crucial for protection against modern security threats.

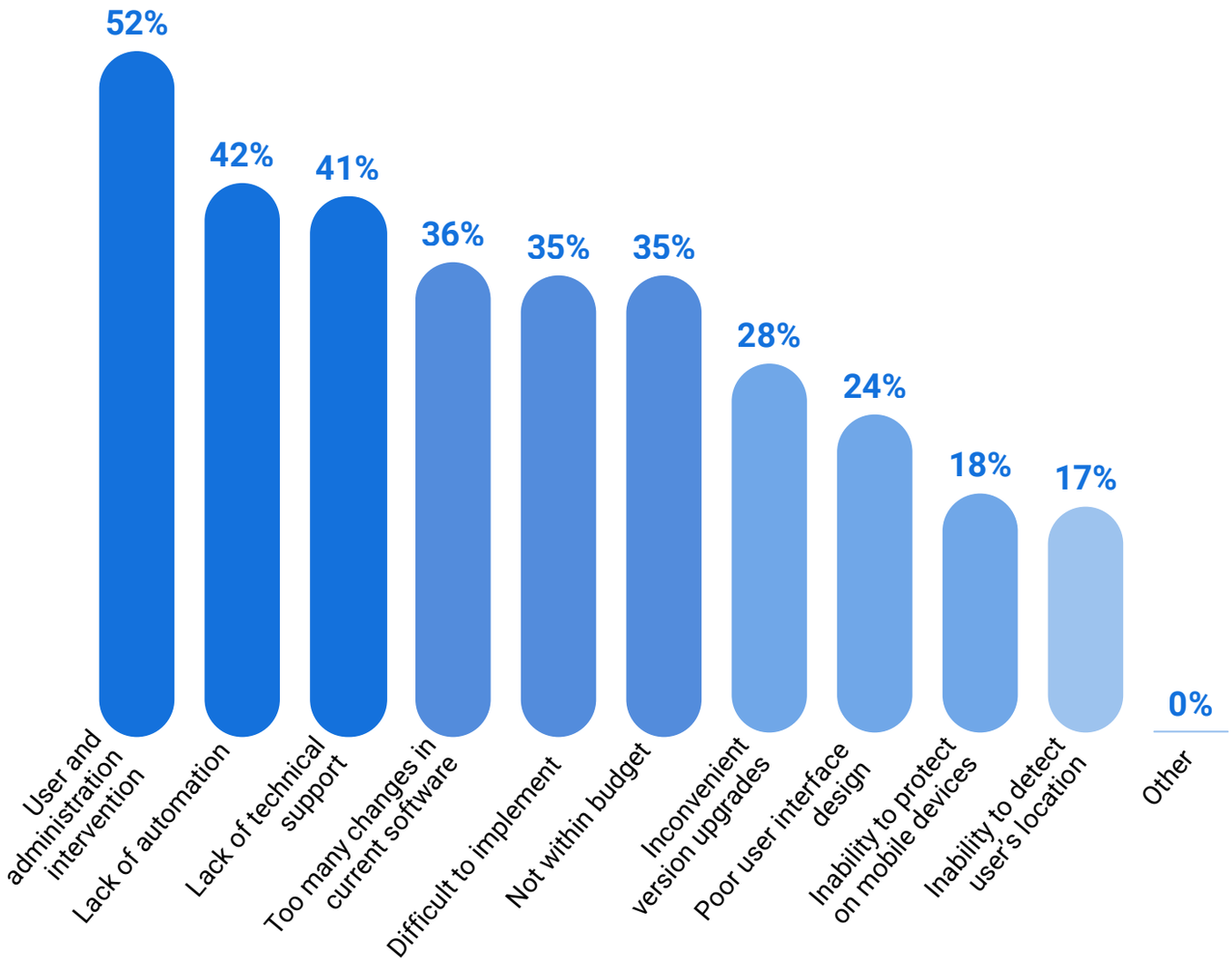
The biggest challenges of endpoint protection tools in 2021 were user and admin intervention (50%), difficulty in implementation (49%), and a lack of tech support (35%). In 2022, lack of automation (42%) replaced difficult implementation as the #2 challenge of endpoint protection tools.

What are the biggest challenges of endpoint protection tools?





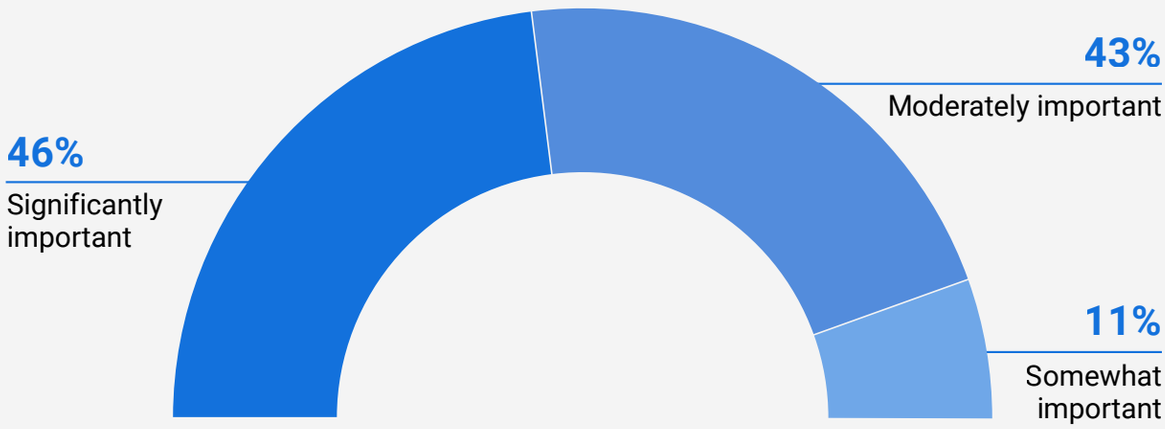
2022



89% of IT security executives feel it's moderately to significantly important to have an endpoint

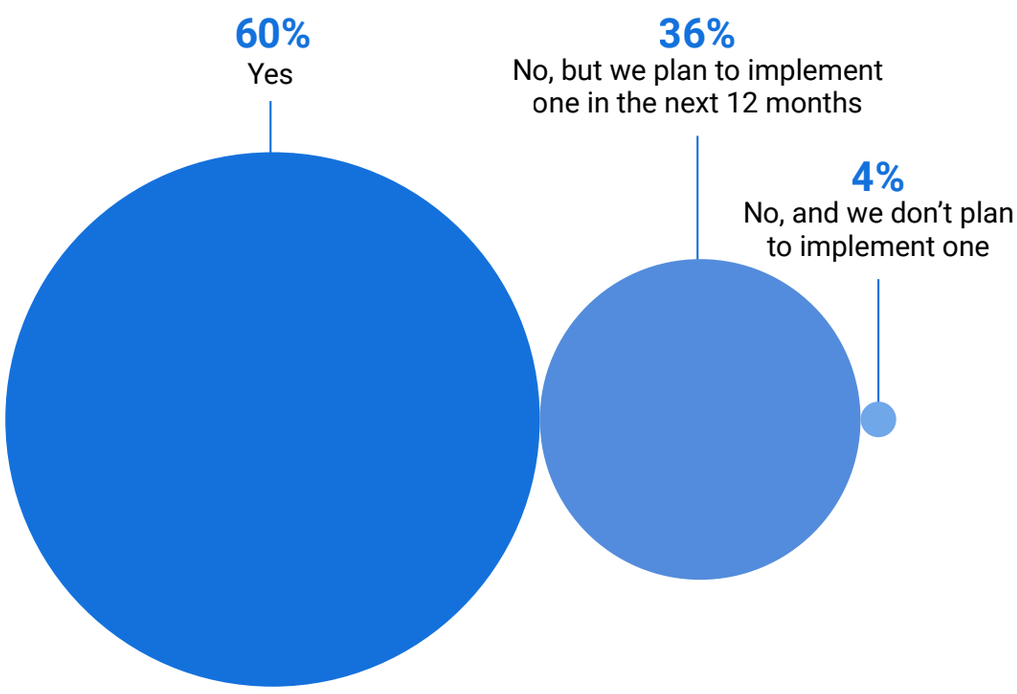
security tool that protects against both known and unknown threats.

How important is it to you to have an endpoint security tool that protects against known and unknown threats, versus a signature-based AV solution that only focuses on known threats?



More than half (60%) of IT security executives have implemented an endpoint detection and response tool as part of their security stack, while another 36% plan to implement one in the next 12 months.

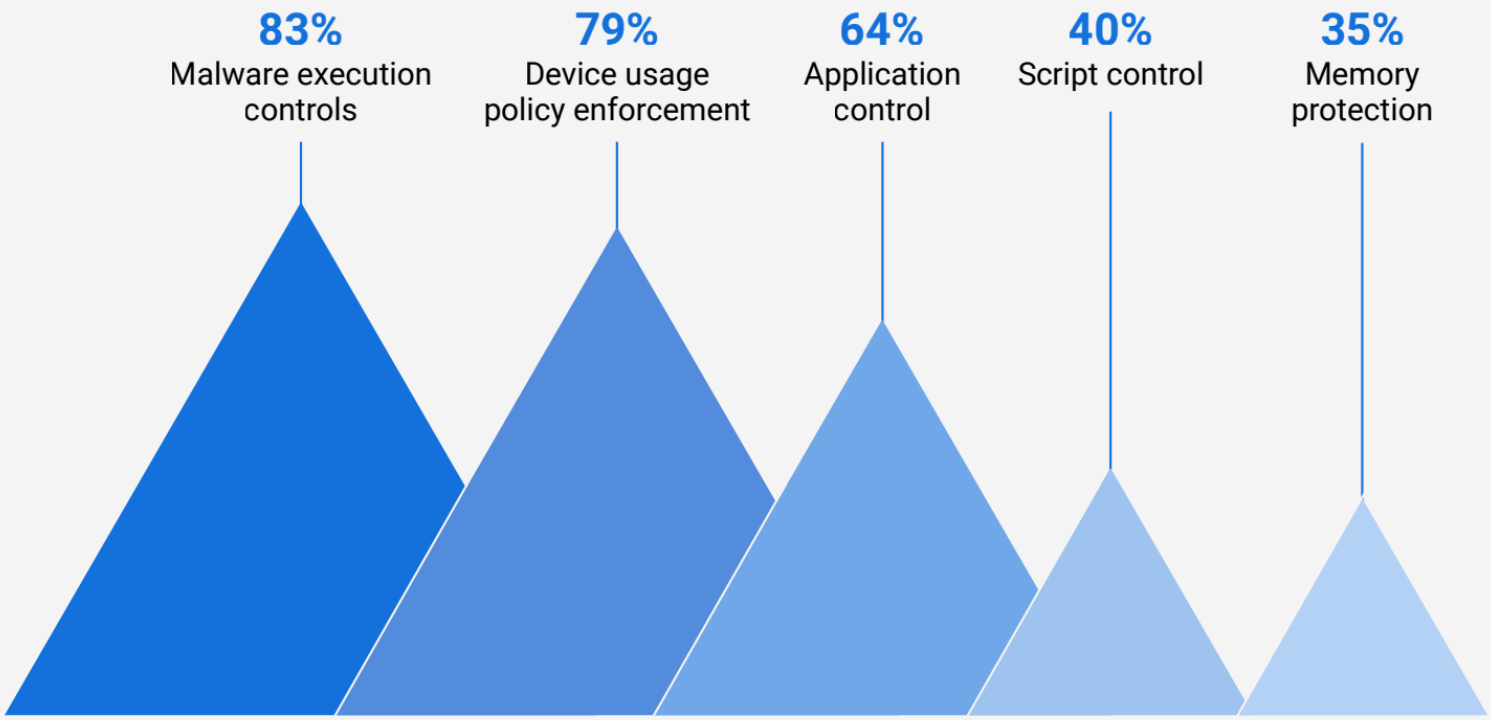
Does your organization use an endpoint detection and response tool as part of your security stack?



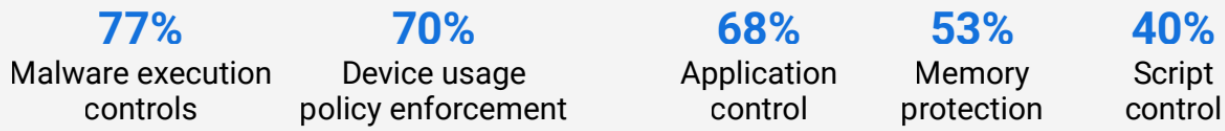
The biggest benefits to implementing endpoint protection tools are malware execution controls (77%), and device usage policy enforcement (70%). However, memory protection had the most significant jump in interest; in 2021 only 35% of respondents listed it as a benefit, but in 2022 this rose to 53%.

What are the benefits of implementing endpoint protection tools?

2021

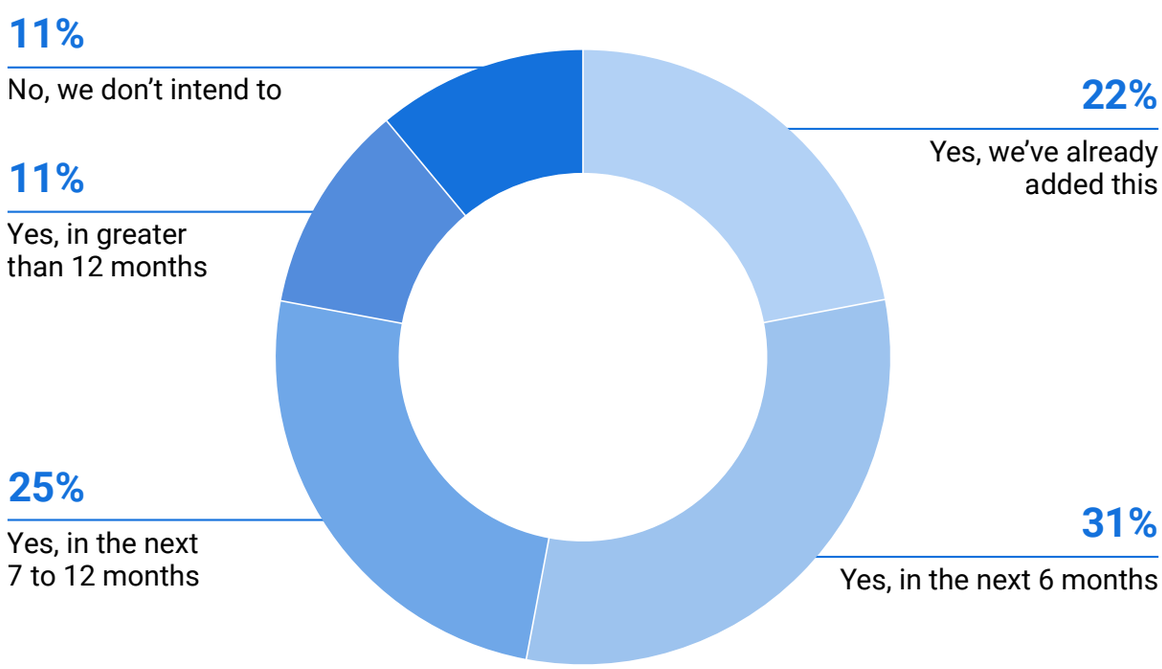


2022



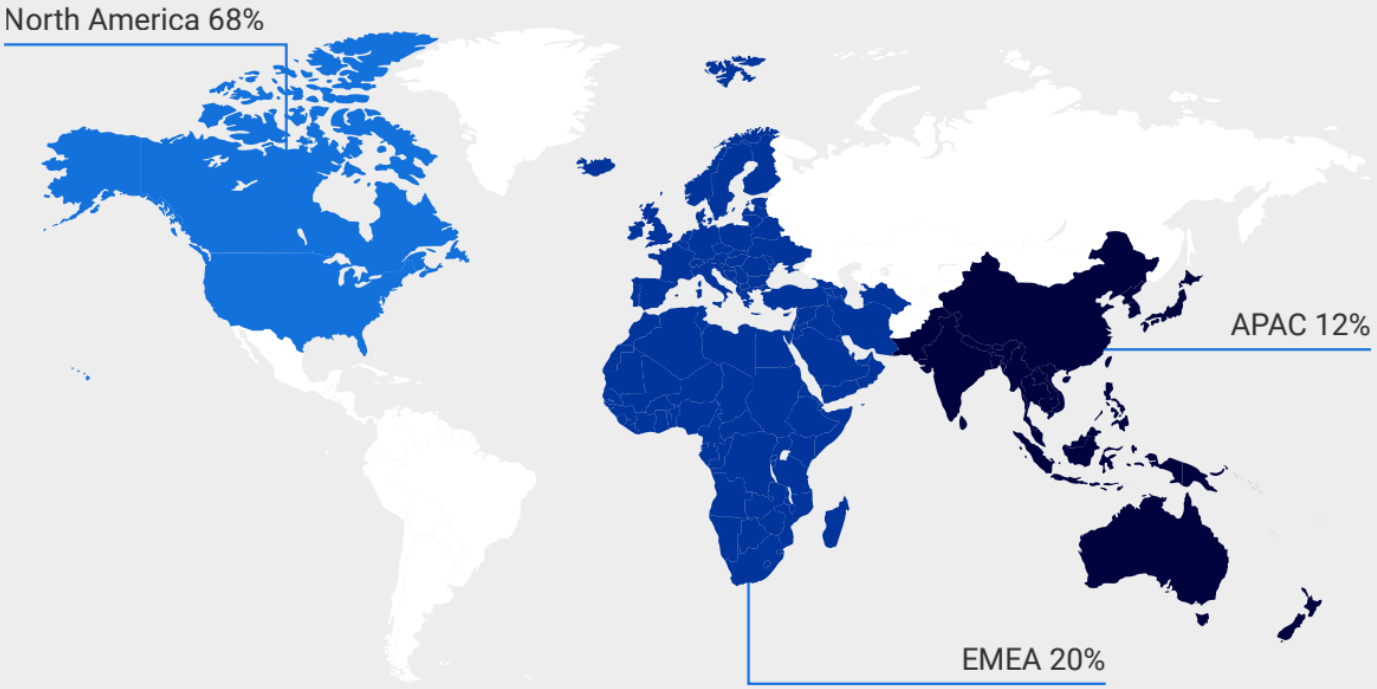
67% of IT security executives intend to add a continuous authentication tool to their cybersecurity stack, and 56% will do so by 2023.

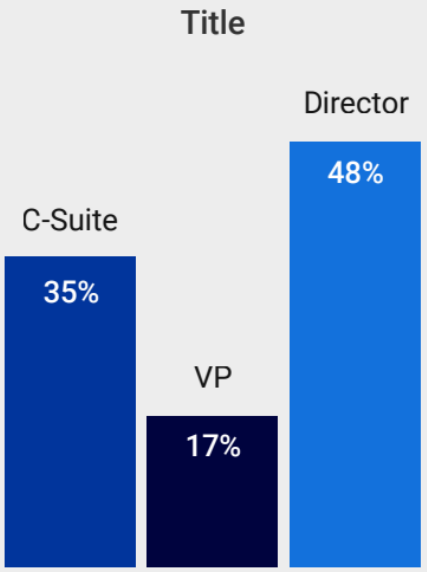
Has your organization added or do you plan to add a continuous authentication tool to your cybersecurity stack?

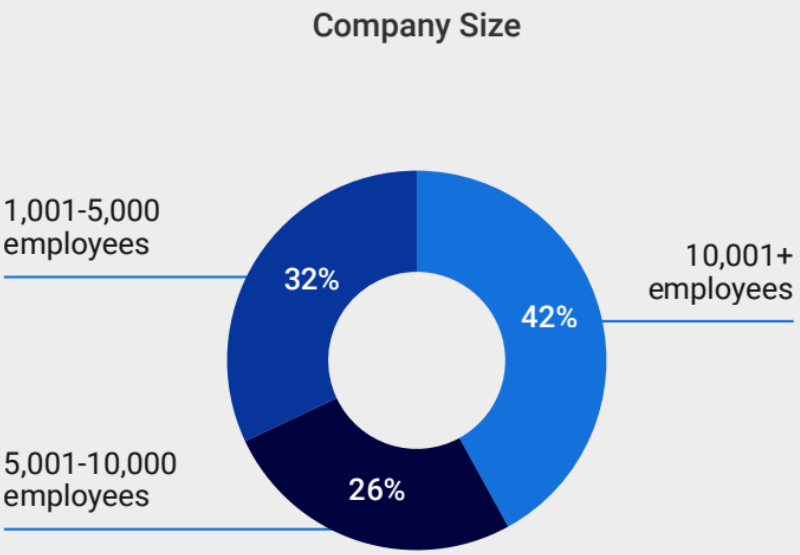


Respondent Breakdown

Region







Insights powered by PULSE