BlackBerry. PULSE

Only 7% 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.

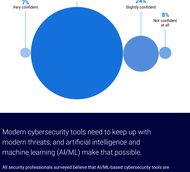
Pulse and BlackBerry surveyed 105 IT security executives to understand how they handle unknown malware threats and how they plan to improve preventative security tools.

Data collected Jan. 18 - Feb. 9, 2021 | Respondents: 105 IT Security Executives

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

The majority (96%) 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.

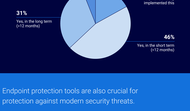
Almost half (47%) of respondents say their IT staff are spending more than 5 hours per week administering and updating signature-based AV solutions.



Only 7% of IT security executives are very confident that their legacy AV solutions can detect and prevent modern malware threats.

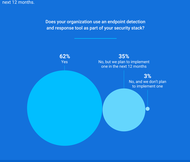
Modern cybersecurity tools need to keep up with modern threats, and artificial intelligence and machine learning (AI/ML) make that possible.

All security professionals surveyed believe that AI/ML-based cybersecurity tools are important to stopping malware execution and zero-day threats.



IT security executives evaluate new security tools based on many criteria, the most important being that the tool stays up to date with new threats (81%).

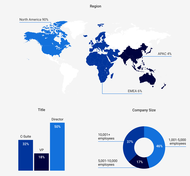
46% of IT security executives are planning to implement AI/ML-based endpoint protection solutions within the next 12 months.



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

The biggest challenges of endpoint protection tools are user and admin intervention (32%), difficulty in implementation (49%), and a lack of tech support (35%).

80% of IT security executives feel it's moderately to significantly important to have an endpoint security tool that protects against known and unknown threats.



More than half (52%) of IT security executives have implemented an endpoint detection and response tool as part of their security stack, while another 35% plan to implement one in the next 12 months.

The biggest benefits to implementing endpoint protection tools are malware execution controls (83%), and device usage policy enforcement (79%).

66% of IT security executives intend to add a continuous authentication tool to their cybersecurity stack, and almost half (48%) will do so by 2022.

Visit the BlackBerry website for more information on how and why you should replace legacy AV products.

Respondent Breakdown