Enterprise Strategy Group by TechTarget

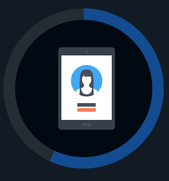
MANAGING THE ENDPOINT VULNERABILITY GAP

Requirements from widespread work-from-anywhere policies have escalated the need for endpoint management and security convergence. IT and security teams require new mechanisms capable of providing common visibility, assessment, mitigation of software and configuration vulnerabilities, threat prevention, and support for threat investigation and response activities. TechTarget's Enterprise Strategy Group recently surveyed IT and cybersecurity decision makers in order to gain insights into these trends.

Notable findings from this study include:

55%
of organizations **have converged endpoint management and security functions.**

48%
of organizations are consolidating endpoint management and security solution vendors.



57%
of organizations have had a bring-your-own-device (BYOD) policy for at least four years.

47%
of organizations believe that consolidating endpoint management and security functions will improve their ability to deliver new applications to users.

68%
of organizations use more than 10 tools for endpoint management and security.

ONLY 43%
of organizations actively monitor more than three-quarters of their endpoint devices.

77%
of organizations have experienced some type of cyber-attack started through the exploit of an unknown, unmanaged, or poorly managed endpoint.

34%
of organizations say that aligning IT and cybersecurity priorities for patching is one of the **top challenges with endpoint vulnerability management.**

For more from this Enterprise Strategy Group study, read the full research report, *Managing the Endpoint Vulnerability Gap.*

LEARN MORE

Source: Enterprise Strategy Group Research Report, *Managing the Endpoint Vulnerability Gap,* May 2023.
© 2023 TechTarget, Inc. All Rights Reserved.