BlackBerry. Cybersecurity

Gartner Peer Insights.

ZTNA for Hybrid Work Environments

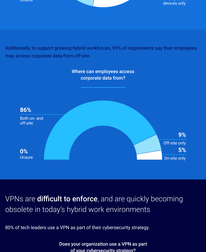
Legacy technologies such as VPNs and virtual desktops were never designed for a world where most people work outside the office at least part of the time. Not only do these legacy technologies not scale, but they also introduce additional security risks. A shift to Zero Trust security models is critical, and well overdue.

BlackBerry used the Gartner Peer Insights platform to survey 200 IT and InfoSec leaders supporting hybrid workforces to understand how they're approaching BYOD security.

Data collection: September 6 - December 7, 2022
Respondents: 300 IT & InfoSec leaders

Hybrid work environments mean **less control** over how and where corporate data is accessed

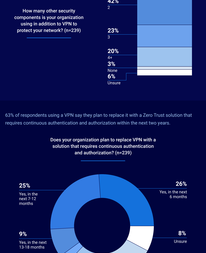
Over three-quarters of respondents (76%) say their employees may access corporate data from privately owned devices.



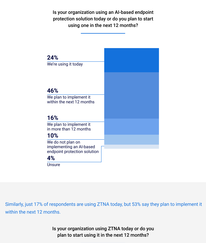
Additionally, to support growing hybrid workforces, 95% of respondents say their employees may access corporate data from off-site.

VPNs are **difficult to enforce**, and are quickly becoming obsolete in today's hybrid work environments

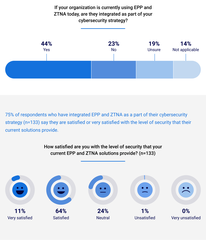
80% of tech leaders use a VPN as part of their cybersecurity strategy.



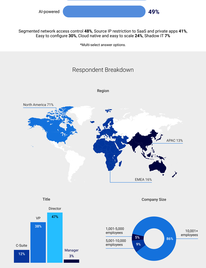
Among those who have access to a VPN, nearly half (47%) say employees and contractors are authorized to access private corporate data and apps without it.



Additionally, 74% of respondents who use a VPN say they are not confident or don't know if a VPN is sufficient to protect their organization from cyberattacks.



85% of surveyed leaders who use a VPN (n=239) say that they use two or more other security components in addition to VPN.



63% of respondents using a VPN say they plan to replace it with a Zero Trust solution that requires continuous authentication and authorization within the next two years.

Security teams are rapidly moving towards **Endpoint Protection Platform** (EPP) and **Zero Trust Network Access** (ZTNA) for their next-gen security needs

While less than a quarter of respondents (24%) are using an AI-based endpoint protection solution today, 46% say they plan to implement one within the next year.

Similarly, just 17% of respondents are using ZTNA today, but 53% say they plan to implement it within the next 12 months.

Less than half of the surveyed leaders say EPP and ZTNA are currently integrated as part of their cybersecurity strategy.

75% of respondents who have integrated EPP and ZTNA as part of their cybersecurity strategy (n=133) say they are satisfied or very satisfied with the level of security that their current solutions provide.

Adaptive access control (71%), the ability to separate managed and unmanaged devices (65%) and continuous authentication and authorization (62%) top the list of features ZTNA users look for in a solution.

Segmented network access control **48%**, Source IP restriction to SaaS and private apps **41%**, Easy to configure **38%**, Cloud native and easy to scale **24%**, Shadow IT **7%**

*Multi-select answer options.

Respondent Breakdown

Gartner

Source: Gartner Peer Insights, ZTNA for Hybrid Work Environments survey