



Secure Remote Access in 2026

Based on Aberdeen's primary research, this project provides insights into how organizations are managing the complex transition from legacy remote access (e.g., traditional VPNs) to modern, identity-centric frameworks (e.g., ZTNA, SSE, SASE). The survey captures insights from enterprise buyers and prospects on:



Drivers & Inhibitors: What is pushing organizations to invest (e.g., remote/hybrid work, ransomware mitigation, cloud adoption) and what is holding them back (cost, integration complexity, skills gaps).



Strategic Shifts: How buyers are navigating device management (managed vs. BYOD) and technology transitions (phasing out VPNs for cloud-native / Zero Trust solutions; passwords to ?).



Expectations vs. Reality: The extent to which organizations are actually achieving expected outcomes like reduced IT costs, improved user experience, and mitigation of security- and compliance-related risks.



Real-World Risks: The frequency and impact of specific security- and compliance-incidents over the last 12 months, including data breaches, ransomware, phishing, unplanned downtime, and insider threats.



Budgets & Roadblocks: Current IT spending allocations for secure remote access, and the biggest implementation challenges (such as user inertia or vendor-related issues).

Derek E. Brink, CISSP

Vice President and Research Fellow, Aberdeen Strategy & Research
(a division of Spiceworks Ziff Davis)

Adjunct Faculty, Harvard University and Brandeis University

✉ derek.brink@aberdeen.com <http://www.linkedin.com/in/derekbrink>

ABERDEEN
RESEARCH

The remote access market is still very much in transition (see the article “**Secure remote access: Tech, trends, and timing**”). Enterprise buyers are often running both traditional VPNs and MFA, along with modern ZTNA/SASE and Identity solutions. SWZD and Aberdeen can apply this research to help solution providers and their enterprise buyers benchmark their progress against peers, identify and address key risks or roadblocks, and build a data-driven business case for modernizing and consolidating their technology stack.

Which Buyers (Enterprises) and Sellers (Solution Providers) Would Be Interested in These Findings?

This research can support and enable engagement with both **Tech Professionals (IT, Cybersecurity) and Tech Leaders** who evaluate and deploy secure remote access technologies, as well as **Business Leaders** concerned with compliance, budget justification, business continuity, regulatory compliance, and risk. The findings apply broadly across company sizes and industries, particularly targeting organizations struggling with technology sprawl, high support costs, or the ongoing need to secure and manage a remote/hybrid workforce.

Solution Provider Landscape (illustrative)



Traditional VPN

Cisco, Palo Alto Networks, Fortinet, Check Point, SonicWall, Juniper, F5, Barracuda



Zero Trust Network Access (ZTNA)

Zscaler, Palo Alto Networks, Cisco, Cloudflare, Netskope, Okta, Akamai, Ivanti, Appgate



SSE and SASE

Zscaler, Palo Alto Networks, Cisco, Netskope, Cloudflare, Fortinet, Versa, Cato Networks



Remote Desktop (RDP) & SSH

Microsoft, Citrix, VMware, CyberArk, BeyondTrust, Delinea, Teleport



VDI & Cloud Desktop

Microsoft, AWS, Google Cloud, Citrix, VMware, Nutanix, Parallels, Workspot

For More Information: <https://www.aberdeen.com/contact-us/>