TeamViewer

Mitigate risk and enhance security with an effective IT strategy

TeamViewer Tensor's enterprise-ready security features help organizations operate uninterrupted despite rising cyber-threats and growing concerns. Maintaining uptime is an ongoing challenge for the largest businesses. As companies grow, so do their attack vectors and their exposure to bad actors.

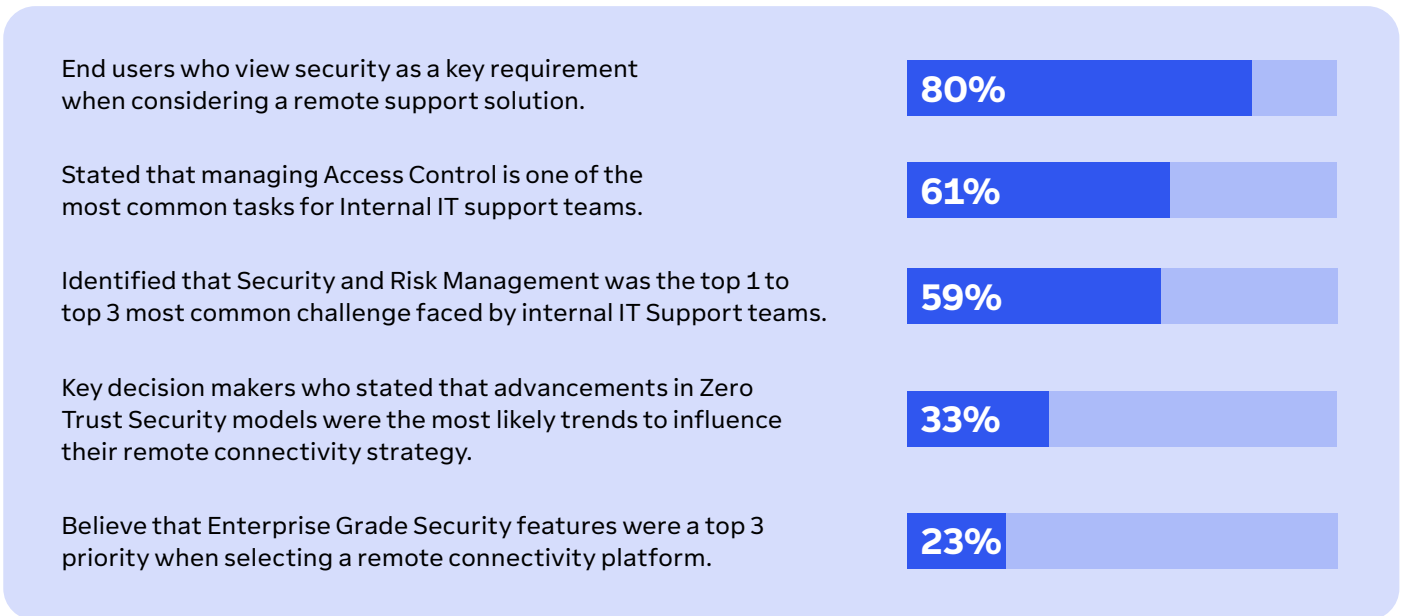
A remote support solution is meant to keep businesses agile, productivity high, and operations running as intended and uninterrupted, not the opposite. Choosing the right solution means choosing with a zero-trust mind frame, that is what's needed to stay ahead in today's environment.

As the new year continues to move forward, all eyes will be on how the public sector, private organizations, and IT leadership teams reinforce their security posture to prepare for complex and growing cyber threats. In contrast, they will be doing so while navigating an aging infrastructure, stricter compliance requirements, and an expanding remote workforce.

2024 saw nearly 7 billion known records breached across 2,741 publicly disclosed incidents. These cyber-attacks were spread across different verticals including healthcare, telecom, supply chain systems, and culminating in the federal space with the US Treasury data breach in December.

Concerns around cybersecurity are on the rise

TeamViewer's enterprise market research highlights a growing trend around security concerns and how it influences the way customers select a remote connectivity solution.



Public organizations facing this kind of downtime and losing the public's trust due to exposure means that the process of selecting third party software vendors needs to move beyond the vulnerable practices we have in place today.

Distributed offices across the US and hybrid/remote work models add another layer of complexity. This makes it more critical for organizations to ensure that their end point management and support software doesn't leave them compromising on security or struggling with multiple, disjointed systems. IT leaders need to be looking much closer into high performance solutions with unified enterprise-grade security.

For that reason, conditional access, single sign-On, and auditability are no longer optional but are now table stakes. Organizations benefit from comprehensive connection logging and AI-driven insights helping them stay aligned with compliance and regulatory standards.

Companies with the strongest security posture are positioning themselves to tackle complex challenges and selecting best-in-class solutions to fortify their datacenters. Implementing automated remediation for security gaps and interactive remote connectivity would obviously give them a clear advantage.

Conditional Access
Prevent unauthorized access to people and devices through conditional access.

Single Sign-On (SSO)
Simplify credential management, lock out shadow IT, and stay aligned with organizational requirements.

Auditability
Stay compliant with company policies by using AI-powered connection logging and reporting.

Bring Your Own Certificate (BYOC)
Enables you to use your own certificates to authenticate the devices involved in a TeamViewer connection.

Take the next step to learn more about the latest security features in TeamViewer Tensor and find out what we can do for you

Contact us now to book a meeting

Stay connected