The Remote Access Challenge

Are you using VPN technology to grant access to your remote employees & third-party vendors?

Remote working is at an all-time high. Enabling remote access for employees and vendors is critical to maintaining productivity.

Does your team have the appropriate secure tools in place to handle a large volume of users connecting remotely into your network?

1 Can you enable granular access?

YES / NO

"All or nothing" VPNs enable greater levels of access than employees or vendors need for their job functions.

Enforcing a policy of least privilege gives users just the right level of access needed for their roles, with individual accountability for shared accounts.

2 Do you know exactly who is accessing your network, what they are doing when connected, and for how long?

YES / NO

"Always-on" VPNs provide no visibility or control over individual user activity, especially on a shared device.

Restricting unapproved protocols and directing approved sessions to a predefined route reduces the attack surface.

3 Are you able to capture detailed session data for all remote access sessions, for review in real time or later on?

YES / NO

The inability to review or track activity when users are remotely connected to your network is problematic from a security and compliance standpoint.

Capturing detailed session logs creates an audit trail that enables accountability and compliance.

4 Do you protect credentials used for privileged remote access by employees and vendors?

YES / NO

Credentials are often stored insecurely, either written down or saved to a spreadsheet or other insecure manner.

Securing privileged accounts in a password vault not only protects them but also enables a smoother user experience by automatically injecting them into the session.

5 Do you have one single path for approvals?

YES / NO

Inefficient workflows slow down IT teams and frustrate end users.

Consolidating the tracking, approval, and auditing of privileged accounts in one place reduces the administrative burden and speeds the overall process.

Did you answer "no" to any of the questions?

Your organization is at risk!

How can organizations who leverage VPNs provide a more secure & scalable access solution for their remote workers and third-party vendors?

BeyondTrust Privileged Remote Access

BeyondTrust enables secure remote access in a single, flexible solution that simplifies deployments and ensures maximum scalability—while empowering remote workers to be productive.

Using **BeyondTrust Privileged Remote Access** as a replacement to your corporate VPN for privileged remote workers and third-party vendors eliminates remote access blind spots, reduces the attack surface, creates an audit trail and drives productivity.

VPN vs. BeyondTrust Privileged Remote Access

CAPABILITY	VPN	BeyondTrust
Remote Access	✓	✓
Secure Connectivity	✓	✓
Network Layer Access (Protocol Tunneling)	✓	✓
Encrypted Traffic	✓	✓
Application Layer Virtualization		✓
Remote Desktop		✓
Proxied RDP Access		✓
Proxied VNC Access		✓
Proxied SSH Access		✓
Application Session Monitoring		✓
Application Session Recording		✓
Just-in-Time Access		✓
Zero Trust Architecture		✓
Privileged Access Management (PAM) Integration		✓
ITSM Integration		✓
Password Management & Credential Storage		✓
Cloud or On-Premises Deployment (Physical or Virtual Appliance)		✓
Agentless Access		✓
Extensive Operating System & Platform Support		✓
Prevention of Lateral Movement		✓
Audit Trail & Session Reporting		✓

Enforce a policy of least privilege by giving specific users precisely the right level of access to applications, sessions, and protocols, while removing the administrative burden of configuring and installing VPNs for vendors, privileged users, and remote workers using unmanaged "Bring Your Own Devices" (BYOD).

Learn More or Schedule a Demo

beyondtrust.com/remote-access

BeyondTrust