The Top 5 Remote Access Problems

With the growing number of connected devices and vulnerabilities surrounding remote access tools and passwords, IT departments are faced with managing the security risks while keeping employees productive. The rapid expansion of remote working is expected to continue, and the security requirements related to secure remote access are more critical than ever.

Does your team have the appropriate secure tools in place to handle the most pressing issues related to a large volume of third-party vendors, internal privileged users and remote workers connecting remotely into your network?

I have third-party vendors in my network, but I don't really know what they are doing.

1 MANAGING VENDOR ACCESS

On average, IT professionals report that nearly 182 third-party vendors access their internal network on a weekly basis[1]. These third-parties range from hardware vendors to software manufacturers or IT outsourcers. They often have Active Directory or other privileged credentials, and most likely a VPN – enabling them to log in to your network at any time and stay connected as long as they like.

[1] BeyondTrust, "Privileged Access Threat Report", 2019

I want to adopt a least privileged policy in my organization.

2 "ALL OR NOTHING" PRIVILEGED ACCESS

Most of your employees or vendors only need access to very specific systems. Using a VPN allows access at the network layer, commonly providing more access than is needed, often resulting in too much access and "leftover" access when users are removed or replaced. This is especially true when a large number of internal users and vendors are dependent on remote access for critical job functions. Tools like VPNs lack granular controls and can only enable only "all or nothing" access at the network layer and lack functionality to manage applications or sessions.

My organization is being held to strict compliance mandates that we must meet.

3 MEETING COMPLIANCE GUIDELINES

Many organizations are held to strict compliance standards such as PCI, GDPR and HIPAA. Auditing procedures are in place to ensure that compliance requirements are being met, and it is the organization's job to provide evidence that they are following standards. Many legacy access tools, like RDP or VNC, are unable to be adequately track or audit activity during remote sessions.

I need to keep remote workers productive and able to access the IT assets they need to do their jobs.

4 REMOTE WORKING ENABLEMENT

VPNs simply weren't built for application layer security, end user visibility, shared desktops, and modern web applications. In addition to the security risk, VPN performance can deteriorate when many remote employees are connected. Companies are seeking alternate ways for employees to be able to work without disruption, while providing a better remote access experience.

I need to lock down shared admin account passwords & enforce corporate password policies.

5 PASSWORDS ARE STORED MANUALLY & INSECURELY

Privileged user accounts are a common network entry point for hackers. Since many IT professionals use multiple privileged accounts to access endpoints in the network, the volume of credentials to manage and secure is high. These credentials are often stored and shared insecurely using spreadsheets or sticky notes. They are often forgotten, noncompliant, repeated, and rarely or never changed.

Legacy Tools Lack Adequate Security & Productivity Features

Legacy access management technologies, like VPNs or RDP, only address a limited number of use cases, which can result in using a patchwork of tools based on the task. The lack of automated workflows can slow IT teams even more.

They also have significant security gaps, as a result of the lack of granular levels of access or the inability to create logs for compliance audits.

Control, Manage, & Audit Remote Access With BeyondTrust

Privileged Remote Access

Enables organizations to give your remote employees and third-party vendors access to your network without a VPN connection. Users are granted granular access to different network segments or specific systems using privileges. This capability not only mitigates the risks of a broad approach to network layered privilege assignment, but also helps organizations achieve compliance mandates or frameworks that specify access controls.

Using Beyond Trust Privileged Remote Access - either in conjunction with or as a replacement to your corporate VPN - enables your organization to eliminate remote access blind spots, reduce the attack surface, and drive productivity in the following ways:

- Enforce a policy of least privilege by giving specific users precisely the right level of access to applications, sessions, and protocols
- Enable individual accountability for shared accounts by providing an audit trail for access
- Define what endpoints users can access, when the users can access them, and what applications or actions they can use during those sessions
- Remove the administrative burden of configuring and installing VPNs for vendors, privileged users, and remote workers using unmanaged devices (Bring Your Own Device, or "BYOD")
- Control and monitor sessions via a secure agent or using standard protocols for RDP, VNC, Web, and SSH connections

Additionally, Privileged Remote Access includes a password vault that ensures managed accounts have their passwords rotated on a regular schedule. For the most sensitive accounts, you can implement one-time-passwords, meaning each time a password is used, it is changed to a new password or rotated.

Enable security professionals to control, monitor, and manage access to critical systems by all privileged users, both internal and external, with BeyondTrust.

Learn more and view a demo of Privileged Remote Access

beyondtrust.com/remote-access

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering companies to secure and manage their entire universe of privileges. The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance.

beyondtrust.com