SECURELINK
VENDOR PRIVILEGED ACCESS

Is your VPN worth the risk?:

ASSESS YOUR THIRD-PARTY ACCESS LIMITATIONS

When you're considering a new process or solution for your business, there are many factors that come into play. But generally, the decision comes down to whether the value of a process change outweighs the cost of adoption. Plainly, "how broken is our existing system and should a shift be a priority for my team?"

In the world of third-party remote access, virtual private networks, or more commonly known as VPNs, have slipped through this filter for far too many years. To use VPNs as the sole security tool to manage third-party access has introduced risks for enterprises around the world. Even with this fact being well-known and widely accepted, network managers still don't always find a better method.

LET'S LOOK INTO WHY.

First, VPNs have long been the primary enterprise remote access solution. They were designed to be used for employees, so the extended use for vendors seemed to make sense. Second, what other choice is there? As more and more core business productivity tasks are being outsourced to external talent and teams, managers need a solution to easily and quickly facilitate remote access to vendors. Teams are familiar with VPNs and view the implementation of a new tool as low priority. **That platforms may not be perfect for third-party access, but is a process change critical right now?**

The answer is: yes. More than critical, it's urgent. **59% of data breaches are tied to third-party vendors**. VPNs are not a hidden or obscure vulnerability. **According to a recent study by Clearsky, hacking groups are focusing on VPNs as a way to establish a foothold in a network in the first stage of their attacks.** VPNs give bad actors a path to their preferred target for entry, privileged access to user accounts. Once inside, the scope of their access is sweeping and threatens the health of your entire organization. The status quo is unacceptable and relying on outdated solutions, as comfortable as they may be, only serves your organization into the "slowest gazelle" for the hacker packs who are always innovating their attacks.

If you want to protect your network and reputation, be aware of the productivity and security limitations of your VPN in relation to third parties and remote access.

The checklist below will outline the symptoms of a broken and exposed third-party remote access system. Measure your VPN platform against these standards to determine how effective it is for your network protection and overall productivity. You'll find that switching to a solution that's specifically designed for managing the privileged access your vendors' have is essential for network security and will also save your team time, money, and resources.

DO YOU **REALLY** KNOW WHO'S ON YOUR NETWORK?

Network security begins with ensuring only authorized users are able to gain access. Since VPNs were designed to handle internal employee access, they often leave security and productivity gaps when managing third-party remote access.

Evaluate how your VPN solution addresses the risks associated with onboarding and offboarding users from multiple vendor partners.

Assessment:

Vendor partners employ individual technicians that deliver support on your network. Compare your VPN capabilities with these registration, identification, and authentication limitations.

- Is only good for protecting data in motion.
- Secures the connection but not the endpoint or its data.
- Provides limited registration and onboarding capabilities specific to vendor's rather than employees.
- Provides limited visibility to activity occurring over an external connection.

Credential protection is critical to network security. If bad actors acquire privileged keys, they can cause havoc. Compromised credentials have been at the heart of the biggest data breaches of the last decade.

Assess your exposure.

- You have no insight into how your vendor partners handle credential security.
- You're unable to prevent vendor technicians from sharing credentials to your network.

Best Practice:

In order to truly understand who is on your network and what they are doing, access must be linked to individual users. VPN alternatives should be vendor access management solutions that:

- Allow self-registration in order to reduce enterprise-side onboarding resources.
- Use multi-factor authentication to ensure users are who they claim to be.
- Have a credential vault for privileged access so vendors never see app-level credentials.
- Have employment status verification to ensure vendors' technicians that no longer work for the company have their access immediately restricted.

THE PRINCIPLE OF LEAST PRIVILEGE

Network managers need secure methods to allow users and applications to perform critical functions on their network. However, when third parties require this kind of privileged access, it's important that security protocols focus on restricting user and program privileges to only those necessary for the required job.

Data protection has two primary goals. Reducing the risk of a data breach, and in the event of a breach, limiting the scope of damage an unauthorized connection can inflict. The success of both depend on the strength of your access controls for privileged accounts.

It's the difference between having a master key to the building, and one that only opens certain rooms.

Be sure your enterprise VPN solution offers granular controls.

Assessment:

These are characteristics of an unsecured system with broad access controls

- Your VPN requires extra steps to grant system access.
- It's unclear how many vendors are accessing your network and systems at any time.
- You don't know which individuals within a third-party organization are connecting.
- Vendors have the same privileges no matter what their task is or access required.
- Changing vendor privileges is a challenge to implement.
- You're unable to restrict access for vendor users according to pre-established permissions.
- You cannot restrict network access to only the information required. You can only grant access to all of your systems, or you can't be as granular as you need to be.
- Attended access is required to provide remote collaboration and desktop sharing.

Best Practice:

Granular vendor access controls are critical to network security and required to meet most regulatory compliance standards. When considering a VPN replacement, review solutions that can:

- Set up access schedules or require access approval before a session starts.
- Restrict vendor technicians to only the network privileges set by your managers at the machine and port level.
- Provide technicians with controlled unattended access to their resources and knowledge base.
- Address industry-specific third-party access regulations to ensure compliance.
- Ad-hoc and audited attended support sessions.

THE MORE SECURE YOUR VPN, THE LESS PRODUCTIVE YOUR WORKFORCE

VPNs force network managers to choose between security and productivity when they're utilized as a third-party remote access solution. When the security of VPN use is increased, system performance goes down and manager implementation demand goes up.

With higher levels of data encryption, application access can be slowed or completely disrupted leading to workflow problems and reduced customer service quality.

When it comes to remote access, VPNs are built to deliver increased security for internal user connections. However, implementing strong security protocols for internal employees is much easier than it is with external users. Without the same leverage to ensure vendor technicians follow best practices, VPNs force network managers to set up separate protections to fill the security gaps.

With no centralized third-party access management system, VPNs can require lots of customized support to set up and maintain security and compliance standards.

Do you prioritize network protections and drain your resources, or gamble with vulnerable systems to streamline workflows?

Assessment:

See what compromises your VPN has pushed you to make.

- Your network managers spend time designing custom vendor access procedures or processes to maintain network security.
- Your application access is impacted by higher encryption levels.
- Your VPN lacks unattended collaboration functionality, such as RDP and desktop sharing.
- No built-in chat feature to provide increased remote support efficiency.
- Network activity audits are time consuming and often incomplete.

Best Practice:

Trying to force a square peg into a round hole will cost your team time and money. Instead, use a vendor privileged access management solution that was designed for the unique needs of third-party users. It should seamlessly deliver these core built-in features:

- Least privileged access.
- Individual user authentication.
- Detailed activity audits for every session.
- Centralized access management.

THIRD-PARTY VENDOR ACCOUNTABILITY

Audit and compliance are our final points on the checklist, but by this point you should know the efficacy of your reporting. The security of your network is only as good as your ability to control and track the users on it.

VPNs create privileged accounts with broad network access and weak protections against credential sharing. This lack of granular authentication and control makes individual accountability impossible.

Third-party connections are one of the easiest and most common ways a hacker enters an enterprise network. With only basic auditing capabilities, you can't spot suspicious activity or track a breach back to the vendor that opened the door.

Assessment:

Determine your level of network visibility. Which of these apply to your systems?

- You cannot limit access to specific network resources.
- Your third-party audit feature offers the same level of details as basic employee access tracking.
- You have limited visibility into the exact systems accessed, when, and by what user.
- You do not receive network access notifications.
- It would be challenging to link a breach to a specific vendor.
- You cannot monitor user activity in real-time.
- Your VPN isn't designed to comply with federal regulations.
- In the event an audit, your compliance would be difficult to prove.

Best Practice:

High-definition audit trails begin with identification, authentication, and least privileged access. When access is linked to the individual, granular tracking is possible. VPNs are an attractive target for hackers. You need the ability to monitor activity to confirm only the right technicians have the correct level of access at the right time. Here are features of a high-definition audit you should have:

- Record of every movement inside the network.
- High-level session information, like technician name, reason for access, session start and end time, and services accessed.
- Video recordings for RDP and desktop sharing sessions, files transferred, commands entered, and keystroke logs.
- Easily generated audit reports that clearly illustrate compliance with regulations and support fast and thorough incident investigations.

VPNs have been at the root of some of the biggest data breaches in history. If this assessment has made clear vulnerabilities in your VPN use, there is a solution that can better protect your network. SecureLink is a vendor privileged access management platform designed for security, efficiency, and ease-of-use. Each best practice outlined above is a feature of SecureLink's purpose-built solution.