Lookout

Top 5 Disadvantages of VPN

Enter Zero Trust Network Access (ZTNA), the modern approach to remote access and network security

For more than 25 years, VPNs have been central to providing remote users with access to applications residing on the corporate network.The worldwide surge in remote work due to the COVID-19 pandemic has led to a dramatic increase in the use of VPNs, thus expanding the enterprises' attack surface. In fact, threat actors are increasingly targeting VPNs, as evidenced by the countless news articles about VPN exploits and known VPN vulnerabilities.

Virtually every enterprise in the world has deployed a traditional VPN solution, which has lost its effectiveness as organizations went remote and turned to cloud services. Moreover, the pandemic-led shift to remote work has overloaded these traditional gateways and, in some cases, forced enterprises to increase spending on outdated and inadequate VPN technology and hardware just to keep things running.

As we settle into the new normal, many enterprises are also learning about the disadvantages of VPN in the areas of scalability, security and performance.

Of course, VPN isn't without its upside. Remote access VPNs provide enterprises with a means to enable remote work. A virtual or physical appliance within the WAN, the public Internet and client software on employee devices can be effective for certain IT and network administrators who need to set up a network and log into a database.

While it is true that remote access VPN saved the day for some businesses, itis also true that increased usage has further magnified some of its disadvantages.

1

VPNs Were Never Designed for Continuous Use

When VPNs originally came to light, the use case was never to connect the entire workforce to the WAN. Traditionally, enterprises purchased VPN solutions to connect a small percentage of the workforce for short periods of time. With a shift to large-scale workforce from home, existing VPN structure is forced to support a continuous workload it wasn't intended for. This creates an environment where VPN servers are subject to excessive loads that can negatively affect performance and user experience.

2

VPN Are Complex to Manage and Scale

Enterprises may attempt to address VPN overload issues with additional VPN appliances or concentrators, but this adds cost and complexity to the network. Similarly, configuring VPN appliances requires a more complex configuration. Further, because VPNs provide remote access, but not enterprise-grade security and monitoring, they must be complemented by management solutions and security tools. These additional appliances and applications lead to even more configuration and maintenance, thus more challenging to scale.

3

VPNs Introduce Cyber Risk

Once a user connects via VPN, they have effectively unrestricted access to the rest of the subnet. For some enterprises, this means non-admin users have network access to critical infrastructure and data when they shouldn't. Further, this approach increases the risk of malware spread and data breaches. For ransomware operators for example, this makes it easy for them to gain access and find the data they need to hijack. Meanwhile, VPNs are totally blind to content level attacks and would not know if ransomware was uploaded or if sensitive data was downloaded.

4

VPNs Provide a Poor User Experience

User experience is now tied to the cloud, which means we expect seamless access to what we need. As a result, it makes very little sense to redirect all your traffic via VPN back through your corporate network in order to go to the cloud. This adds unnecessary latency, which can be frustrating for the end user.

5

VPNs only provide Access to Managed Devices Without Addressing Users' Privacy

In a BYOD world, VPNs only allow access to managed devices which requires the installation of an agent on the device – this is more intrusive and the last thing anyone wants on their device is another agent. What's more, since VPNs provide network access, this can expose risk to users' private data.

Enter ZTNA: A software defined approach to remote access and network security

Lookout ZTNA directly addresses VPN's disadvantages and provides enterprises with a secure, scalable and simpler means to manage a remote access solution. Lookout ZTNA is a modern approach to secure and scalable remote application access that can enhance existing VPNs.

1. Built for continuous access/simpler to manage. Lookout's globally distributed platform is purpose built for continuous access. Enterprises don't have to worry about overloading a single VPN appliance with cloud-native infrastructure.
2. Delivers hyper-scalability. Enterprises don't need to add more appliances to scale as the workforce expands and contracts.
3. Provides granular access control. Lookout ZTNA gives enterprises design access controls at the application level and based on user profiles. This leads to a significant reduction in risk compared to VPN's network level approach.
4. Proactively protects against threats and protects privacy. With Lookout ZTNA, network traffic goes through end-to-end packet inspection using a robust cloud-based security stack designed to detect and prevent malicious behavior. Users securely authenticate via MFA and encrypted network protocols. Access rights are assigned based on profiles and specific applications. Finally, risk assessment occurs continuously during each user session.
5. Connect anywhere from any device. The workforce is remote and they need to access cloud applications such as Microsoft O365 and Google Workspace from wherever they are working – there are no agents to deploy, manage and update.

For more details, please refer to the Lookout ZTNA Brochure.

Lookout