Privafy™

Working Securely From Home in an Increasingly Insecure World

A PRIVAFY WHITEPAPER

Working Securely From Home in an Increasingly Insecure World

Recently, pundits were predicting that remote working would displace office life within the next five or ten years, give or take a few years. Well, welcome to the future.

The COVID-19 pandemic has pushed up the timetable for the future, from telemedicine to food delivery services. Perhaps this push is nowhere more evident than in our own homes, where knowledge workers have now set up provisional offices in spare rooms, dining rooms, and finished basements. This time last year, about one in six employees worked from home. Today, that number is a lot closer to five out of six.

Adjusting to life in the post-coronavirus world has been challenging on many levels, particularly for businesses. Entire industries have disappeared overnight, and businesses are struggling to stay productive and connected with a workforce that has migrated from a few regional hubs to thousands of individual homes. The sudden change has left businesses asking themselves the hard questions:

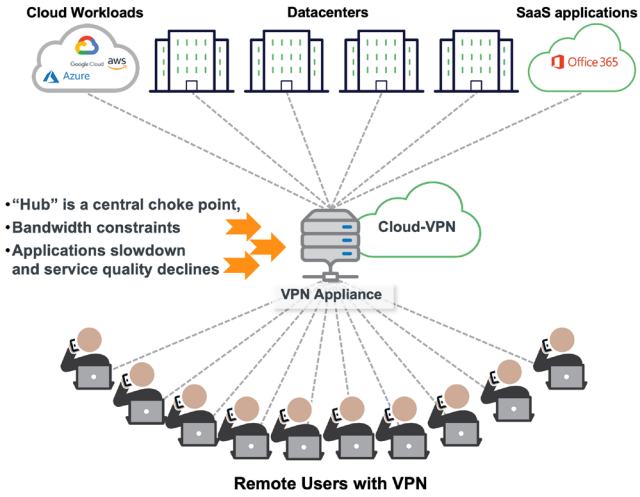
- How do we get business applications and data into the hands of the people who need them?
- How do we scale our remote solutions to serve, not 16% of our employees, but 96%?
- And, most importantly, How do we protect business communications and sensitive business data now that everyone is working outside the safety of our network firewall?

It's a sobering truth that the coronavirus has caught most businesses unprepared for a fully remote workforce. Unsecured access to cloud applications, personal devices with weak passwords, and connectivity across a patchwork of secured and non-secured networks has exacerbated the already serious problem of cyber-attacks on data-in-motion. But perhaps the most pressing security problem for businesses right now is their reliance on their existing virtual private network (VPN) solution to fill in those security gaps. In reality, a fully remote workforce is exactly what will push most VPN solutions past the breaking point.

Why Scaling Your VPN for a Fully Remote Workforce Doesn't Work

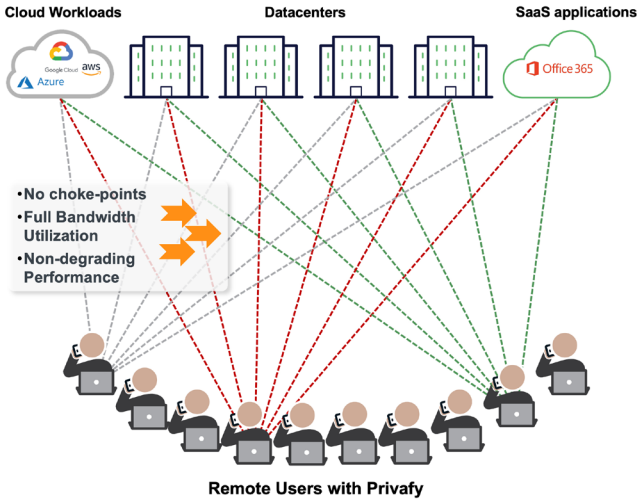
Most VPNs solutions were built for a traditional hub-and-spoke topology. Essentially, the VPN appliance acts as the encryption hub, while the main offices, cloud service providers, and mobile workers form the spokes. This model works well enough when the number of spokes is limited, backhauling traffic through the VPN gateway in a measured manner. But as the number of spokes scales upward, the VPN gateway begins to create bottlenecks that slow network performance and negatively impact worker productivity and add vulnerabilities.

VPN Performance Bottlenecks



In contrast, with Privafy, all rules, policies, and logic are executed in our lightweight CloudEdge and AppEdge endpoints. Our proprietary, hyper-efficient control protocol is coupled with efficient client software to deliver peer-to-peer services with no degradation to network or application performance – eliminating chokepoints and risks.

Peer-to-Peer – Zero Performance Degradation



VPNs Are More Vulnerable to Attack Than You Think

For years, businesses have been told that VPNs create a secure, private tunnel that allows communications and data to traverse safely over public, non-secure networks. This is, in fact, only a partial truth. As cyber criminals have become sophisticated, they have exposed VPN security vulnerabilities, resulting in some very high-visibility data breaches and attacks. VPNs often have outdated encryption protocols because businesses aren't vigilant and consistent about updating their VPN software. VPNs don't inspect and filter incoming and outgoing traffic, which allows some security threats to slip through. And VPNs typically require manual, high-touch administration, which introduces the element of human error into the security equation.

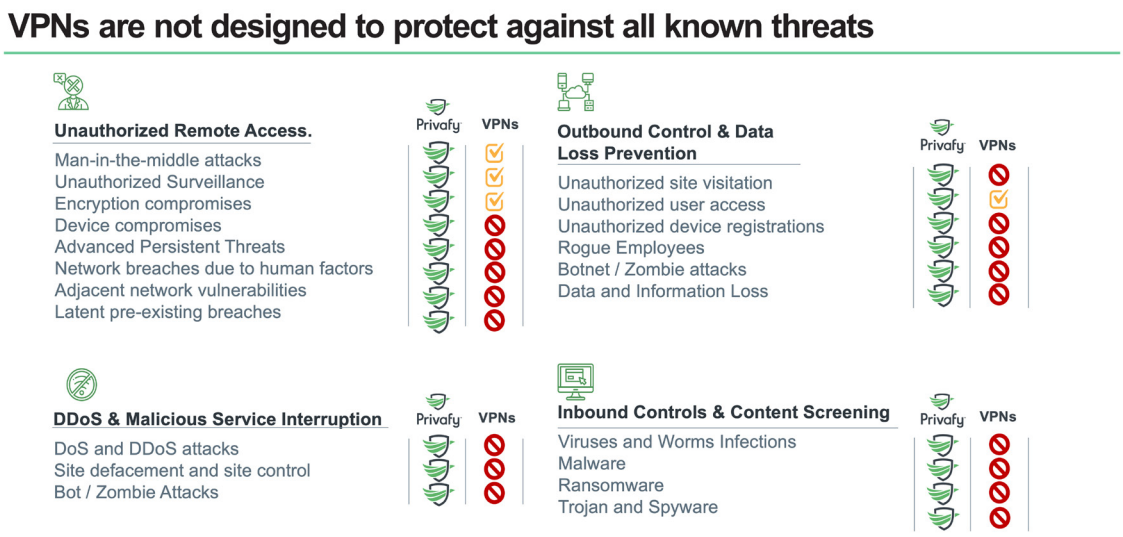
These vulnerabilities open the door to a myriad of cyberattacks, which often go undetected by businesses:

- **Man-in-the-middle attacks** that take advantage of VPNs with Internet Key Encryption (IKE) protocols that use a single static key for tunnel encryption;
- **Unauthorized access** to communications and data by cybercriminals who steal manually generated and stored encryption keys through social engineering or by exploiting human error;
- **Data theft in transit** that occurs as data is decrypted at the VPN gateway and re-encrypted for transit, potentially exposing it to malicious entities during the "switching" process;
- **Network breaches** that take advantage of known vulnerabilities in VPN software that has not been patched or upgraded.

VPNs Don't Deliver the Full-Stack Security Protection You Need

Even the best of class VPN solutions offer only partial protection of data-in-motion. For example, VPNs don't protect you against devices that have been compromised. They won't stop ransomware attacks and block zero-day viruses. They won't protect your network against denial-of-service (DoS) attacks. And they can't protect you against data theft.

Privafy is much more than a VPN: it's an integrated full-stack security solution that protects data-in-motion as well as your network, devices, and cloud applications with the same level of security and protection as if they were working from the office. The chart below illustrates how Privafy "stacks up" to traditional VPN solutions.



Privafy's full-stack protection vs. standard VPN protection

Privafy Works…
From Home, the Office or the Cloud

For the time being, your home office is the new office. Therefore, businesses need to provide the same or better security and productivity tools to employees at home as they have in the office. This is easier said than done. With limited access to IT support, looser enforcement of security policies, and only partial visibility into network traffic, businesses are at a security disadvantage—a fact that cybercriminals are already taking advantageof through increased attacks and new, devious ways to steal access credentials through social engineering (e.g., the rapid increase in fake coronavirus sites).

Privafy provides comprehensives, quick, affordable simple path to distributed workforce security in four important ways:

1. **It's a full-stack security solution.** Privafy delivers comprehensive, enterprise-class security that helps protect against data-in-motion threats, DoS attacks, data theft, and ransomware. More than a VPN, Privafy offers multi-layer security for every endpoint and user, no matter where they are.
2. **It won't slow down your network.** VPN gateways create a single chokepoint as remote traffic is backhauled through the network. Privafy uses a peer-to-peer connectivity model to eliminate this chokepoint, so that network performance remains the same regardless of the number of remote workers, resulting in increased productivity.
3. **It doesn't require on-site IT.** Because Privafy is a cloud-based service, all security management tasks can be performed remotely through a secure Internet connection. Encryption key management, policy updates, and software patches are all done automatically. So, even if your IT staff is working from home, Privafy keeps working for you.
4. **It's simple to set up.** There are no physical installations to perform with Privafy, and no manual configuration is needed. Anyone can set up the Privafy service in minutes; if you can download an app, you can do it yourself.

At a time when nearly every business is trying to cut costs, Privafy has an extra added benefit: it costs significantly less than traditional security solutions. So, you can save money and secure your business from anywhere: at home, in the office, or in the cloud.

Privafy is the future of security. To learn more, visit us at **privafy.com**.

5 Reasons Why Privafy Is Better Than a VPN.

1. VPNs

- Create network bottlenecks by backhauling traffic through a VPN gateway for encryption.

Privafy

- Secure Peer-to-Peer connectivity removes network bottlenecks and supports thousands of remote workers with no degradation in network performance.

2. VPNs

- Are not designed to support a distributed, cloud-based workforce.

Privafy

- It is a cloud-native solution that scales seamlessly as your workforce is increasingly remote.

3. VPNs

- Rely on outdated encryption protocols that are being hacked.

Privafy

- Ensures the best possible encryption through a proprietary, dynamically generated, and fully automated key management system.

4. VPNs

- Only offer a single layer of security, leaving businesses exposed to cyber-attacks.

Privafy

- Provides a full-stack security solution that features full VPN capabilities plus next-gen firewall protection, intrusion detection/prevention, DoS/DDoS protection, malware screening, deep content inspection, and data loss protection.

5. VPNs

- Need to be manually configured and managed, which is expensive, time consuming and prone to human error.

Privafy

- Features zero-touch provisioning and automatic updates to reduce the chance for human errors while reducing maintenance time and costs.

Privafy™
WORK ASSURED

US HEADQUARTERS
2 Burlington Woods Drive
Burlington, MA 01803

SALES
phone: 781.342.1077
email: sales@privafy.com

WEBSITE
Learn more about Privafy
privafy.com

PRIVAFYCENTRAL
Purchase, monitor and manage your Privafy service
https://dashboard.privafy.com/login

PARTNER PORTAL
Access partner training, resources and end-customer materials
privafy.com/partners

About Privafy

Privafy's vision and mission are to harness emerging cloud technologies to bring enterprise-grade data security within reach of businesses of all sizes. The company currently holds 25 technology patents and has offices in Boston, Massachusetts, and Bangalore, India.

The content set forth in this presentation or document is for informational purposes only and does not constitute a binding commitment or obligation on the part of Privafy.
Please visit www.privafy.com for the most current pricing, technical information and features. In the event of a conflict between this content and the information provided on Privafy's website, the website will prevail.