5 key reasons why VPN alone won't protect you or your research

VPN: promises vs. reality for digital investigators

Since it first entered the scene some twenty years ago, the concept of a virtual private network (VPN) has been promising internet users a solution for protecting their online privacy and anonymity. It offered to turn a public unsecured connection into a private encrypted "tunnel" and to mask their IP address, making them virtually untraceable to websites and online adversaries.

But as organizations began relying on their VPNs to conduct private transactions and perform sensitive research, they quickly found out that the secure connection network has some sizable cracks in it; and that with some VPN services, not all data gets encrypted, leaving users vulnerable to web-borne malware and data leaks.

Let's look at some of the common misconceptions about privacy and security offered by a VPN, and what it means for security-conscious organizations and online researchers.

1 VPN doesn't fully conceal the user's identity and location

For web users conducting sensitive research such as analysts, security researchers, fraud investigators or law enforcement, the ability to remain completely hidden and anonymous online is essential for the success of their missions. Anti-Money Laundering (AML) researchers in a bank, for example, cannot risk disclosing their IP address, corporate network information or location coordinates to a suspicious website, because that could alert adversaries and allow them to cover their tracks.

The problem is that many browser extensions leak crucial information, such as users' DNS, allowing sites that you visit to potentially find out about the real connection details behind your VPN extension.

Also, despite claims of complete privacy, many VPN service providers (both free and paid) have been known to leak their users' traffic information and retain logs of their users' web activities to monetize connection data. None of this is good news for researchers who are trying to stay anonymous while investigating fraud or criminal activity on the internet.

2 VPN won't prevent malware infections

Another common misconception about VPNs is that it protects against malware, such as keyloggers, ransomware or phishing attempts that carry an infectious payload. In reality though, all that VPN does is provide an encrypted method to protect data in transit. So it essentially encrypts malware encountered on an infected site or in an email before it gets transmitted for download onto the user's computer.

Even with a VPN, malware can still successfully reach the user's endpoint and freely infect a user's device.

3 Rogue VPN apps are adding threats, not reducing them

As VPNs continue to gain popularity among security-conscious users, there are a growing number of shady operators who are profiting from the organizations' trust in VPN security and privacy promise. VPN apps and browser plugins offered by scammers are adding new threats, preying on users looking for increased privacy on a small budget or for free. Sham VPN services have been found to spy on unsuspecting users or to expose their computers to malicious code, for example via injection of ad spam ("malvertising") into the browser.

4 VPN manageability: added complexity compounds risks

On the enterprise level, even legitimate VPNs can introduce new vulnerabilities. When enterprise apps are deployed in different locations, on-site or in the public cloud, each of them may require a separate VPN gateway that needs to be configured manually. The ongoing shortage of IT security professionals is compounding the challenge. If policies are not applied consistently across all gateways, security suffers.

5 There are many scenarios where a VPN can leak your IP

Even legitimate VPN providers are prone to domain name system (DNS) leaks. Using a VPN through a browser extension is particularly vulnerable to leaks, with up to 70 percent of VPN Chrome extensions studied being responsible for leaking a user's DNS.

Outside of extensions, there are many scenarios where a VPN may leak data:

- Not all providers cover both IPv4 and IPv6, which may result in an IP leak if a VPN provider does not route both types of traffic to their servers. If, for example, your computer tries to connect to an IPv6-only site, and your VPN covers only IPv4, you can encounter a leak.
- In a scenario where your VPN connection suddenly drops, it's important to understand what happens to ongoing traffic. Many VPNs don't come with a kill switch that stops all traffic — instead, they allow it to continue to go through your original network, leaving your traffic unprotected.
- Certain common standards, such as WebRTC, are particularly prone to DNS leaks through VPN. WebRTC utilizes P2P, voice calling, video chat, etc., — all through the browser. In browsers such as Firefox, Chrome and Opera, WebRTC is enabled by default. The only way to stop the VPN leaks is to disable WebRTC completely.

To add to the problem, even the most security-conscious users often resist using the VPN, citing its cumbersome experience and slow speeds. So, is there a solution where researchers could remain safe and anonymous online, without hindering productivity and at speeds faster than with a locally installed browser without the VPN?

Silo, the cloud browser delivered as-a-service by Authentic8, offers security, privacy and speed. Silo processes all web content remotely, isolated in a cloud container. Instead of web code, it transmits an encrypted display of the remote browser session back to the user. The remote browser instance is built fresh at session start and destroyed at session end. It leaves no trace of the user's web activities behind (such as cookies or residual code).

Beyond just isolated browsing, Silo for Research gives users complete control of their digital fingerprint and leverages a global network of non-attributable IP addresses to provide in-region access. All evidence can be safely collected, stored, translated and shared through one solution. And with Silo, logs can only be accessed and managed by customer admins, providing added protections for users to keep their research secure and compliant.

Authentic8 does not monetize Silo user data, which is stored and processed only to the minimum required to provide the service. Silo is used by some of the world's most security-sensitive organizations in various fields and industries.

For more information on how tools like Silo can help you safely utilize the dark web in your investigation, **visit our website** or **request a demo**.

silo
BY AUTHENTIC8

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com