VPN for Secure and Private Web Access? Think Again.

How do you prevent web-borne attacks and cyber snooping when users connect to the corporate network from home or on the road? Many believe a Virtual Private Network (VPN) will protect their users against privacy violations and web-borne exploits, but that is not always the case.

How far can you trust VPN? Over the more than 20 years that VPN has been around, its limitations have become obvious. Yes, VPN can make connecting with networks and resources across the web more secure, but it still passes web code to the local web browser, which allows for malware and spyware infiltration as well as data exfiltration and de-anonymization by third parties.

WHAT ARE THE IMPLICATIONS FROM AN IT SECURITY AND PRIVACY PERSPECTIVE?

Executive Summary

VPN creates an encrypted data "tunnel" between the user's computer and a secure server (on the corporate network, for example) that can also serve as a springboard to the web. Still, this secure tunnel is not sufficient, because the inherent security weaknesses of regular browsers leave users exposed to web-borne exploits, localization and de-anonymization. In addition, slow VPN speeds result in productivity losses. The shortcomings of VPN are felt most by organizations that depend on secure web use, consistent access policies and non-attribution when users access apps and websites. By using a disposable cloud browser that prevents any web content from touching the local IT, organizations can achieve the full protection against all related exploits and the complete anonymity that VPN cannot provide.

Encrypted VPN "tunneling" doesn't prevent malware infections. Browser-induced data leaks and unreliable connections allow for de-anonymization. To make things worse, security threats also emanate from rogue VPN service and browser plugin providers.

Using a secure cloud browser not only mitigates all these risks. It also helps organizations avoid other problems commonly associated with VPN, as we will show below. Are the following criteria important for your VPN considerations? If so, think again - think cloud browser:

- **PRIVACY, ANONYMITY AND LOCATION MASKING:** With Silo, the cloud browser delivered as a service by Authentic8, the user's IP address and geolocation remain completely concealed. Only Authentic8's IP address is disclosed to websites.

- **PROTECTION AGAINST MALWARE AND SPYWARE:** The cloud browser creates a perfect isolation layer between the user and the web, while preventing web code from entering the local IT environment or reaching the end device. With Silo, no code from the web can touch the endpoint. Only visual display information (pixels) gets transmitted. This effectively disconnects the user from the web's risk zone.

- **MANAGEABILITY:** By embedding policies in the remote browser - from access controls, to data loss prevention, to compliance auditing - IT regains total command and control over the web with Silo, regardless of device, network, or location of the user.

How VPN Works

To understand what VPN does and what it doesn't, let's look at how it works: A VPN service creates a secure connection between two computers, say between an executive's laptop at home or on the road and a company server.

The "walls" of the VPN tunnel in fact do provide some protection, for example when going online via public WiFi networks or consumer grade home broadband connections. One key advantage: Many services encrypt much of the data transmitted from point to point within the VPN.

VPN, Privacy and Anonymity: Cracks in the Tunnel

Others - and that's the bad news - don't. Their "tunnel walls" are riddled with cracks. With some VPN services, not all data gets encrypted. As if the VPN concept wasn't complex and confusing enough for many, admins and users are shouldered with the burden to verify exactly what a given VPN service is encrypting - and what not.

Another feature of VPN services that is frequently misunderstood is their capability to conceal the user's true identity and location - to a degree. In some cases, not in all, someone accessing the internet can appear to be somewhere entirely different than their actual physical location.

Now You See Me, Now You - Still Do

The latter feature proves useful particularly when conducting sensitive online research on behalf of a law enforcement agency, bank or law firm. Anti-Money Laundering (AML) researchers or fraud investigators, for example, cannot risk to disclose their IP address, corporate network information or location coordinates to a suspicious website as XYZ Bank, New York, NY.

Serving up the information of the machine at the VPN "tunnel exit" instead, VPN allows users to hide such information - but not always. In addition, information leaked from the local browser used with VPN still lets adversaries identify the user via "browser fingerprinting".

In short, most VPN services fail to provide a cloak that would pass professional level muster. Relying on VPN can lead to serious data breaches.

For professional researchers and analysts in security sensitive areas, VPN's shortcomings and inconsistencies pose a big problem. They can put operational security at risk and result in blown covers and incomplete or contaminated research results.

No, VPN Won't Prevent Malware Infections

Another common misconception about VPN is that it provides protection against malware, such as keyloggers, ransomware or phishing attachments that carry an infectious payload.

It does not. Because VPN provides merely an encrypted method to protect data in transit, all it really does is encrypt malware encountered on an infected site or in an email before it gets transmitted for download onto the user's computer and can spread from there.

The list goes on. Think again before relying on VPN for secure and safe web access. In a white paper titled "VPNs Are Not As Secure As You Think," content delivery network Akamai concludes "VPNs are a weak security solution."

"Users Hate the VPN Experience"

VPN is also notoriously slow. Users complain that it puts the brakes on critical workflows and lowers productivity. In their white paper, the Akamai security researchers put it this way: "Users hate the VPN experience."

In comparison, using a secure cloud browser is often faster than using a local browser without VPN. If the last point sounds counterintuitive, there's a simple explanation.

Optimized CPUs and the cloud browser's high bandwidth internet connection are part of the explanation. What's more, while the actual web page may be huge, the amount of display data that Silo sends back to the user tends to be significantly smaller.

The reason is simple. Lengthy scripts, hidden thumbnail images and humongous CSS sheets remain contained on the Authentic8 server. For the user, the page looks just the same. A 30-50% reduction in bandwidth usage is not uncommon with Silo, and less bandwidth means faster speeds.

Most VPN services fail to provide a cloak that would pass professional level muster. Relying on VPN can lead to serious data breaches.

Cashing in on Confusion: Rogue VPN Apps

Granted - given the inherent security weaknesses of the internet, without VPN many organizations and individual users would be even worse off. Yet the confusion about VPN has also attracted shady operators.

Criminals and unscrupulous marketers are looking to cash in on users' legitimate security and privacy concerns. Instead of increasing user privacy, low-cost or free VPN apps and browser plugins offered by scammers are adding new threats.

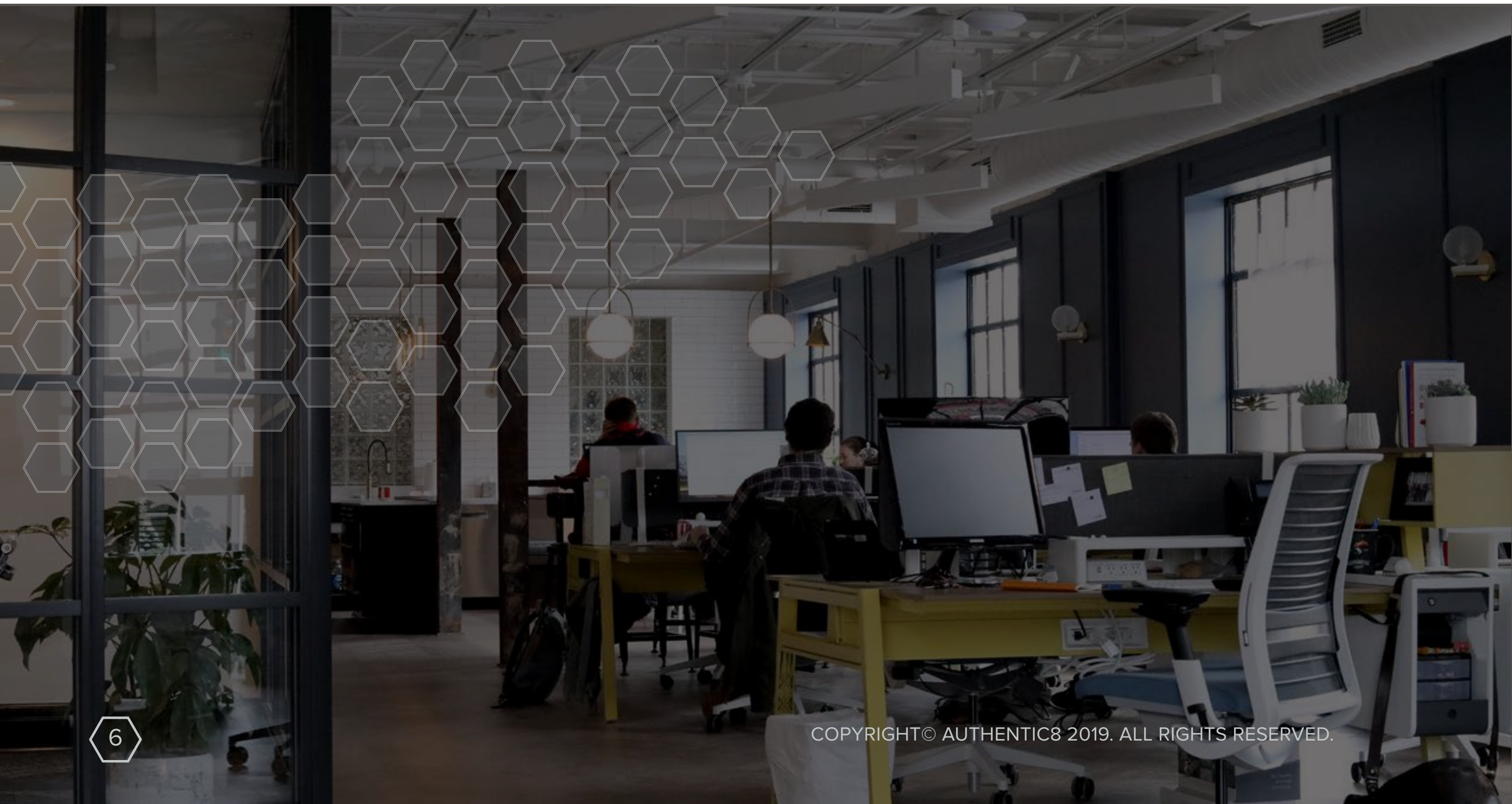
Phony VPN services have been found to spy on unsuspecting users or to expose their computers to malicious code, for example via injection of ad spam ("malvertising") into the browser.

VPN Manageability: Complexity Adds New Risks

On the enterprise level, even legitimate VPN offers 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 current shortage of IT security professionals compounds the challenge. If policies are not applied consistently across all gateways, security suffers. As the Akamai researchers warn in their white paper:

> "VPNs result in fragmented security policies for distributed enterprises."



Fed Up With VPN?
Take Back Control.

If VPN doesn't offer the all-encompassing protection against privacy violations and data breaches that many - including more than a few IT professionals - still believe it does, what's the alternative?

Major banks and investment houses, leading law firms, and more than 100 government agencies think they know the answer. Increasingly, especially in areas with higher security and regulatory requirements, they are relying on a new approach: browser isolation in the cloud.

What is driving this change? "With global critical infrastructure systems under constant attack, organizations need flexible access to the most advanced technology possible to ensure resiliency," said John DeSimone, VP of Cybersecurity and Special Missions at Raytheon. The defense and cybersecurity giant chose Silo, the secure cloud browser delivered by Authentic8, to protect its global mission partners.

Cloud Browser Delivers Security, Privacy - and Speed

Here's how Silo works: 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).

Using a secure cloud browser ensures that users remain safe, compliant, and anonymous online. In a statement, Raytheon explained its choice of Silo this way: "Silo eliminates risk on the web, allowing users to utilize internet resources and applications for critical workflows while protecting their digital environment."

With Silo, Authentic8 delivers a secure cloud browser as a service centrally managed by a team of dedicated IT security professionals. Authentic8 does not monetize Silo user data, which are 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.

silo

VPN vs. Cloud Browser: At-a-Glance Comparison

WANTED	VPN	SILO CLOUD BROWSER
DATA ENCRYPTION	Generally, data is encrypted with a VPN. Not always. Check with the provider.	Silo delivers web content as visual display data (benign pixels instead of potentially malicious web code) and protects all transmitted data with strong encryption.
ANONYMITY	VPN allows for limited (and not always reliable) anonymization, for example by hiding the user's IP address. For VPN users accessing the web through a local browser, this may create a false sense of security. Because of the regular browser's inherent security weaknesses, users can be "de-anonymized" and targeted based on residual code and cookies from past browser sessions and site visits.	Silo provides complete anonymity. Because only Authentic8's IP addresses are used, attribution to individual users, networks or organizations becomes impossible. Attempts to "browser fingerprint" a site visitor will fail.
LOCATION MASKING	Many VPN services offer to change the IP address and geolocation presented to websites a user visits. But the reliability of this feature (too) often depends on factors like connection stability and code quality of the VPN client. Most VPN providers also won't prevent disclosure of the user's location to websites that use HTML Geolocation API. This risk affects for example shared computers where a prior user has given an app or site permission to access the browser location.	With Silo, no location information about the user's machine, network or organization is disclosed on the web. Only the location information of the disposable browser instance on Authentic8's server is shared. With the Silo Toolbox web app, users can set the location and language configuration for their web session ("managed attribution").
PROTECTION AGAINST MALWARE AND SPYWARE	None.	With Silo, no code from the web can touch the local computer or network, which physically precludes web-borne exploits like ransomware, keylogging programs or tracking code from affecting the local IT. All content is processed in a secure container in the Authentic8 cloud, centrally managed by a team of dedicated IT security professionals.

WANTED	VPN	SILO CLOUD BROWSER
MANAGEABILITY	In organizations with complex IT landscapes, policies are often applied manually and inconsistently to different VPN gateways. This can lead to vulnerabilities.	Because each Silo session is built with embedded policies pre-defined by IT, oversight and control are ensured each time users access the web. Centralized browser management and control minimize risk and facilitate compliance reviews.
TRUSTWORTHINESS	Caution is advised. Too many shady players offer “free” VPN for nefarious purposes. A big name behind the VPN offer doesn’t mean users get what they expect. A Facebook VPN app, Onavo, was pulled from the Apple apps store because it apparently violated Apple’s data gathering rules.	The right to privacy on the web is an integral part of the foundation Silo was built on. Authentic8 will not monetize user data. This is why we don’t deliver a free service. Silo is a security service that stands on its own and has proved, from its inception, unmatched value in keeping user data secure and private. Silo meets and supports the compliance requirements of the European Union’s General Data Protection Regulation (GDPR).
SPEED	VPN’s chronically slow speed is one of the most common user complaints. VPN is often combined with a patchwork of other security solutions and has been known for slowing down business in many organizations.	Organizations who suffered productivity losses due to slow VPN overcame this bottleneck by protecting teams with Silo instead. Customers and industry reviewers frequently report speeds faster than with a regular browser.

To find out more about Silo, the cloud browser,
connect with our team: www.authentic8.com

silo