Anonymous Web Browsing With Light Point Web

In addition to advanced malware and ransomware protection, the Light Point Web Full Isolation Platform™ provides enterprise-grade nonattributable or misattributable web browsing. Learn how Light Point Web compares to traditional anonymous web browsing solutions.
INTRODUCTION

Anonymous online research is a need many organizations have for a broad range of reasons. There are several different tools and approaches used by these organizations to accomplish this goal, and some are better than others.

The Light Point Web Full Isolation Platform, developed by Light Point Security, is a uniquely strong solution for this need. Not only does it mask the user’s identity, location, history, and more, but it also offers full protection from online malware and ransomware.

WHAT IS LIGHT POINT WEB?

Light Point Web is a fully isolated web browsing solution designed by former National Security Agency (NSA) cybersecurity experts. It was created to leverage the power of isolation to allow users to safely browse to any website, without depending on unreliable detection algorithms.

Light Point Web transparently moves the user’s web browser off of their computer entirely, allowing them to browse the web from a one-time-use virtual environment on a hardened remote server that can be located anywhere. Light Point Web is not a proxy or a VPN. Proxy and VPN solutions attempt to make the web browsing the user is doing on their local computer appear to be coming from another location. Light Point Web, on the other hand, actually does perform the web browsing on a remote system, not on the user’s local computer.

Unlike with proxies and VPNs, with Light Point Web no web content ever reaches the user’s computer – that means no JavaScript, no Flash, no Java, not even any HTML or CSS. Instead, all web content is fetched, executed and rendered on the remote server, and only a visual stream in the form of pixels is sent to the user’s computer. At the end of the user’s browsing session, the entire virtual environment is completely destroyed and rebuilt from a pristine image. This automatically eliminates any potential malware, tracking cookies and browsing history.

ANONYMOUS BROWSING WITH LIGHT POINT WEB

Light Point Web is perfectly suited to enable organizations to perform secure, anonymous browsing, without leaking details about their identity, or potentially infecting their network. Light Point Web hides a user’s identity online in the following ways:

- **IP Address Masking**: Websites you visit cannot determine your IP address. Instead they only see the IP address of Light Point Security’s cloud server from which you are browsing.

- **Browser Agent and Operating System Masking**: Websites you visit do not see the user agent (UA) string from your real browser. Instead they only see the UA string of the Light Point Web custom browser running on the cloud server, so they cannot use this information to identify or track you. Similarly, websites only see the operating system of the Light Point Web cloud server, not your real operating system.
- **Masking of Entire Browsing Environment:** In addition to your operating system and browser’s user agent string, Light Point Web masks your entire browsing environment. This includes your time zone, language preference, fonts, browser plug-ins installed, and more.

- **Automatically Rotating IP Addresses:** Light Point Web leverages our expansive cloud network to automatically move from server to server. This means that you are constantly being assigned different IP addresses - making it that much harder for websites to track you over time.

- **Automatically Deleted Cookies and History:** At the end of every browsing session, the Light Point Web virtual environment is completely destroyed and rebuilt. This means no cookies, history, or anything else persist between sessions that can be used to track you over time.

- **Tracking Cookie Prevention:** Light Point Web has a built-in ad blocker, which further increases your online anonymity by preventing trackers from following you within the same browsing session.

- **Managed Misattribution:** Light Point Web offers the ability to let users misattribute their browser traffic to a geographic location of the user’s choice.

- **Not a Proxy:** Light Point Web is a fully isolated remote web browser. It is not a proxy. As such, it is not identified as a proxy by proxy detection technology. This means that you won’t be blocked by websites that block proxy users, or flagged as a proxy user, which can be enough to raise suspicions.

- **Doesn’t Leak Information:** The biggest benefit of Light Point Web not being a proxy is that it doesn’t leak your information because it is not susceptible to typical proxy vulnerabilities like DNS leaks and WebRTC leaks.

- **Protection from Web-Based Malware:** If a target website infects your computer with malware, you have completely lost your anonymity, even if you are using tools to hide your identity, because that malware has access to everything on that computer. Light Point Web’s unique isolation-based security design means users do not have to worry about malware infections revealing their identity to their targets, or even worse, giving their targets access to their data.

- **Tor Integration:** Light Point Web’s Tor mode provides an alternative method of anonymity, and access to the dark web.

**WEAKNESSES OF OTHER SOLUTIONS**

Organizations that need anonymous browsing use a few different methods to accomplish this task. Below are two of the most common methods, and the pitfalls of each.

**PROXY SERVERS AND PROXY SITES**

One of the most common methods to achieve anonymous web browsing is the use of proxies. This can be either with traditional proxy servers, or by using a proxy site. However, they have security vulnerabilities that could lead to the user’s true identity being exposed.

- **Leaked IP Address Through HTTP Headers:** Most proxy software wasn’t designed with anonymity as a goal. Users of proxy software may be surprised to learn that many proxies include an extra HTTP header to websites that contains the user’s true IP address. Just one example is the “X-Forwarded-For” header, but others may be used as well.
• **Plugins Can Ignore Proxy Settings:** Even if you configure your browser to use a proxy, browser plugins do not have to honor those settings. Knowledgeable adversaries can use a custom built Flash object to reveal the use of anonymizing proxies and the true identity of visitors to their websites.

• **DNS Leaks:** A DNS leak allows the websites you visit to discover your locally configured DNS server even if you are using a proxy. Depending on your DNS configuration, this vulnerability can reveal your location and identity.

• **WebRTC Leaks:** WebRTC is a technology that enables peer-to-peer video conferencing, desktop sharing and similar capabilities to happen through your browser without the use of a plugin. WebRTC has an inherent flaw that allows an attacker to obtain your true IP address even if you are using a proxy.

• **Injection of Malicious Ads:** Many anonymizing proxies on the web are not run by the most reputable people, and in some cases you may not even know who is behind the software you are using. From time to time, they have been known to inject dangerous content, like malicious ads, into the sites they serve. These malicious ads will be delivered to the user’s computer, where they can lead to a full network infection, putting your organization's private data at risk, and exposing your identity.

• **Collection of Browsing Data:** When you route your browsing through a proxy, you are implicitly trusting that proxy with all of your browsing activity. Owners of the proxy will have access to your true IP address, as well as a complete log of what sites you visit, and what information you enter into forms, which could include passwords. They could also potentially share this information with your targets.

Beyond these security pitfalls, are usability issues. For proxy sites especially, the user must remember to always go to a proxy site before they navigate to their target site. It is inevitable that a user will at some point forget this step, or type the target URL into the wrong address bar and press enter before realizing their mistake.

### SEPARATE NON-ATTRIBUTED NETWORKS

Some organizations set up a second covert network that is not attributed to the organization’s identity in any way. When users need to do anonymous browsing, they use a different computer which is attached to this network.

The downside to this approach is that users require extensive training because they must be very careful to not perform any action which could link this network to the organization. Once that happens, you can no longer rely on this network to actually conceal your identity.

It is also costly to purchase and maintain a second network of computers. From a usability aspect, this is also burdensome to the employees that must constantly switch back and forth between systems. This constant switching increases the likelihood that they make a mistake and enter information into a site that could attribute the covert network to the organization.
USE CASES

Below are a few example use cases illustrating how Light Point Web is used to anonymize a user’s online identity.

INTELLIGENCE COMMUNITY

• **Open Source Intelligence**: Intelligence analysts collect publicly available information, known as “Open Source Intelligence,” from the web to augment the information they obtain through other channels. Although this information is obtained through publicly available sources, the fact that a particular organization is interested in specific information may be sensitive in nature. These intelligence analysts use Light Point Web to easily gather Open Source Intelligence without the fear that it will be traced back to their organization.

• **Clandestine Web Access**: Clandestine operatives sometimes find themselves in unfriendly territory, and needing to report back to home base from an untrusted computer network where there is a high likelihood that all web traffic on that network is being monitored. If the clandestine operative visits a website that can be traced to a government agency on such a network, he would be exposed. Because all communication is encrypted with Light Point Web, clandestine operatives can use it to protect their identities while browsing from networks where it is believed that all of their web activity is being monitored by hostile individuals, even if they browse to incriminating websites.

LAW ENFORCEMENT

• **Criminal Investigations**: Local, state and federal law enforcement, use the web to gather information during criminal investigations. This includes investigations in highly sensitive areas, like terrorist activities, gang violence, drug cartels, human trafficking, child pornography, and financial fraud. Law enforcement officers use Light Point Web to collect evidence without tipping off the suspect of the ongoing investigation.

COMMERCIAL ENTERPRISES

• **Anti-piracy Investigations**: The Motion Picture Association of America (MPAA) and the major motion picture studios aggressively pursue those involved in the piracy of their intellectual property. With Light Point Web, their anti-piracy teams can covertly investigate those involved in the illegal distribution of pirated content without it being traced back to the studios and alerting the individuals under investigation.

• **Financial Fraud Investigations**: Financial institutions use Light Point Web to investigate financial crimes, like money laundering, without it tracing back to their organization and tipping off the subject of the investigation.
CONCLUSION

Light Point Web’s anonymous web browsing solution provides protection from malware, while delivering more reliable anonymity and a better user experience than traditional solutions. To learn more about how Light Point Web’s isolation technology works, see our white paper “Why Web-Based Malware Is the Most Serious Threat to Your Business.”

To learn more about how Light Point Web can protect your identity online, contact Light Point Security:

Web: http://lightpointsecurity.com
Email: sales@lightpointsecurity.com
Phone: +1-443-459-1590

About Light Point Security
Light Point Security was founded by former NSA cybersecurity experts with decades of experience in national security. The award-winning company pioneered the concept of using a remote browser to protect organizations from web-based malware, and is the leading provider of browser isolation solutions. The Light Point Web Full Isolation Platform also provides anonymous browsing and data analytics into user behavior. Customers include Fortune 500 companies, financial institutions, healthcare organizations, and the federal government, among others.