digital element®

Need for Proxy/VPN Data in Today's Heightened Cybersecurity State

Government enterprises. Healthcare companies. Retail networks. According to a study by Positive Technologies, cybercriminals can breach 93% of company networks. Is anyone surprised by the steady drumbeat of news headlines about cyberattacks across a multitude of industries?

Many security professionals say they're unprepared for the threats they face in the immediate future. Today's enterprise IT professionals are engaged in an intense battle against cybercriminals, often facing losses that span monetary, reputational, productivity and IP theft, to mention only a few. No industry segment has been immune.

There's another threat keeping IT professionals up at night: Virtual Private Network (VPN) usage. There is no shortage of free and paid residential proxy services. Yet some of those services are favored by nefarious actors who use them to masking malicious activities, such as scraping, scanning and testing passwords in order to access your network. The FBI has warned that cyber criminals are exploiting home VPN usage to break into corporate systems.

A deep understanding of the VPN market is essential. Knowing which providers promise criminal-friendly services, such as no logging or paying via cryptocurrency, security teams can gain critical context behind breaches and use that insight to limit the damage, as well as make strategic decisions as to who can access their networks, who requires additional authentication, and who should be blocked altogether.

In today's world, new technologies usher in new tactics used by criminals. They can launch ransom attacks, take over networks, and illegally infiltrate consumer accounts through diverse devices from anywhere in the world. By leveraging camouflage techniques, they can do so anonymously. Tools such as VPNs, proxy servers, queue networks, and SmartDNS allow them to hide their true identities and locations.

The reliance of cyber criminals on these tactics can be key to deciphering crime networks and their activities if businesses take the right approach.

Cybercrime, which includes everything from theft or embezzlement to data hacking and destruction continues to climb. The number of reported breaches jumped 14% in the first quarter of 2022[1]. Ransomware attacks are now demanding payments of $1 million or more.

digital element

Global market intelligence firm IDC expects worldwide security spending to reach $174.7 billion in 2024[2].

A Sharp Increase in VPN Usage

Corporations use VPNs to extend their corporate network to remote locations. VPNs provide an encrypted connection over the internet from a device, say an employee's home laptop, to the corporate network, so that he or she can work remotely. All VPN users in such cases will share a single Internet Protocol (IP) address.

Not surprisingly, remote work and VPN usage shot up 27% during the pandemic[3], but not all of it was due to remote work. A great many consumers subscribed to VPN services for other reasons, such as masking their location in order to ensure privacy, or to circumvent geo-location rules, e.g. pretending to be in the UK in order to watch UK Netflix.

Commercial VPNs Create Multiple Agendas

Consumers have plenty of choice when it comes to subscribing to a VPN service. NordVPN, Strong VPN, ExpressVPN, TunnelBear and Surfshark are just some of the companies that offer VPN at little to no cost. Corporations are not likely to use these to secure their traffic. They're using more reputable and secure VPN providers, such as Apple Private Relay and Cloudflare WARP. Or, they might have their own software that they've developed in-house.

It's wrong to think that all of these services are created equally. Some are free, which can be problematic in that without a credit card or payment information on file, there's no way to trace a nefarious actor to a specific consumer.

Some offer features that are desired by nefarious actors, such as complete anonymity and no-logging of user activity. Criminals are free to do as they please in the knowledge that the VPN service won't record their activities.

Top reasons people use VPNs[5]:

- **General security reasons**, such as avoiding identity theft
- **General privacy reasons**, such as securing their personal data
- **To mitigate risks while on public WiFi service**
- **To meet specific job requirements**
- **To watch streaming video in other countries**

Commercial VPNs rent out servers and IP address space from hosting companies. These aren't your traditional internet service providers (ISPs) such as AT&T and Xfinity that provide internet access at homes. Rather, they are providers that expect significant volumes of traffic from multiple users who are located all over the world.

Some of these commercial VPN providers set up their servers in different geographic locations, enabling end users to change their ISP-assigned IP address to another location for one reason or another, such as accessing content that is geo-restricted. At this point, the intent has moved beyond the privacy-centric person who wants to protect his or her identity online to one who may be interested in skirting rules or policies.

Adding to this complexity, a new crop of "high-end, premium" VPN services emerged during the pandemic that pose a security threat to both consumers and businesses alike.

Free VPN Services and the Rise of Residential IP Hijacking

There is a new kind of provider that touts residential VPN proxy service, which one provider describes as services that allow users to "choose a specific location (country, city, or mobile carrier) and surf the web as a real user in that area." What's key here is that such services don't deal with IP addresses in hosting centers. Rather, they are after IPs that are in use by regular consumers, coming through home residential IP connections.

VPN

Some 68% of U.S. adults use a VPN service for work or personal reasons[4].

Five out of every 10 users of VPN services circumvent region-locked content to stream Netflix, indicating that tens of millions of people use it for that purpose[6].

Users who download free VPN software in order to bypass geographic content restrictions unknowingly have their residential IPs hijacked by these VPN providers. By agreeing to their Terms of Service, the consumers' residential IPs are then sold to other VPN providers that, in turn, sell them as a premium offering.

Consumers who use residential ISPs, such as Charter or Xfinity, can have their IP addresses compromised without their direct knowledge. Their IP addresses are circulated in the proxy space by these commercial VPNs.

This is how it works.

A consumer signs up for a free commercial VPN. They don't have to pay for anything. They download it, install it and turn it on. At that very moment, the commercial VPN provider has now seen their residential IP address. Somewhere in the Terms of Service (that they more than likely didn't read but signed anyway), the consumer has agreed to grant that VPN provider the right to use their residential IP address in the entire proxy pool for routing purposes. That VPN provider then goes to the new crop of residential proxy services, such as Bright Data, Oxylabs, or Smartproxy, and leases that residential IP address.

Once that consumer goes online and their IP address is detected, that residential proxy service can reroute hundreds of thousands of other users from any country outside of the U.S. with a U.S.-based IP address. For this reason, it is essential the corporate security teams understand who the VPN and proxy VPN service providers are, and create a set of rules to protect their network.

Separating the Bad Guys from the Good Guys

Cyber criminals, in particular, have found the use of proxies to be effective. But, it's important to remember that not all proxies have malicious intent. As discussed, VPNs are widely used by legitimate users for diverse purposes and are a popular choice for enhancing security and privacy.

As a result, stopping all VPN users is not practical. It increases the danger that real customers or employees are mistakenly labeled as crooks. Moreover, this method fails to discover the root of cybercrime. In order to mitigate risks and protect real users, companies must find the means to separate the bad guys from the good guys— and one of the tools for accomplishing this is the incorporation of IP-based VPN and proxy data into your platforms and technologies.

As Digital Element explained in Technopedia, “IP address intelligence can shed light on the characteristics of a particular user. Where is the user coming from? Is their identity masked via a VPN? These characteristics -- including geolocation, home or business user, masked or anonymous -- provide important context around the users who attempt to gain access to your network, enabling you to make strategic decisions to protect your company.”

Other IP characteristics can help IT professionals determine how often an IP address has moved, what’s behind it, the number of users to which it has been assigned. Some providers of IP intelligence data can provide the company name, carrier name and whether the traffic is coming from a home, business or data center.

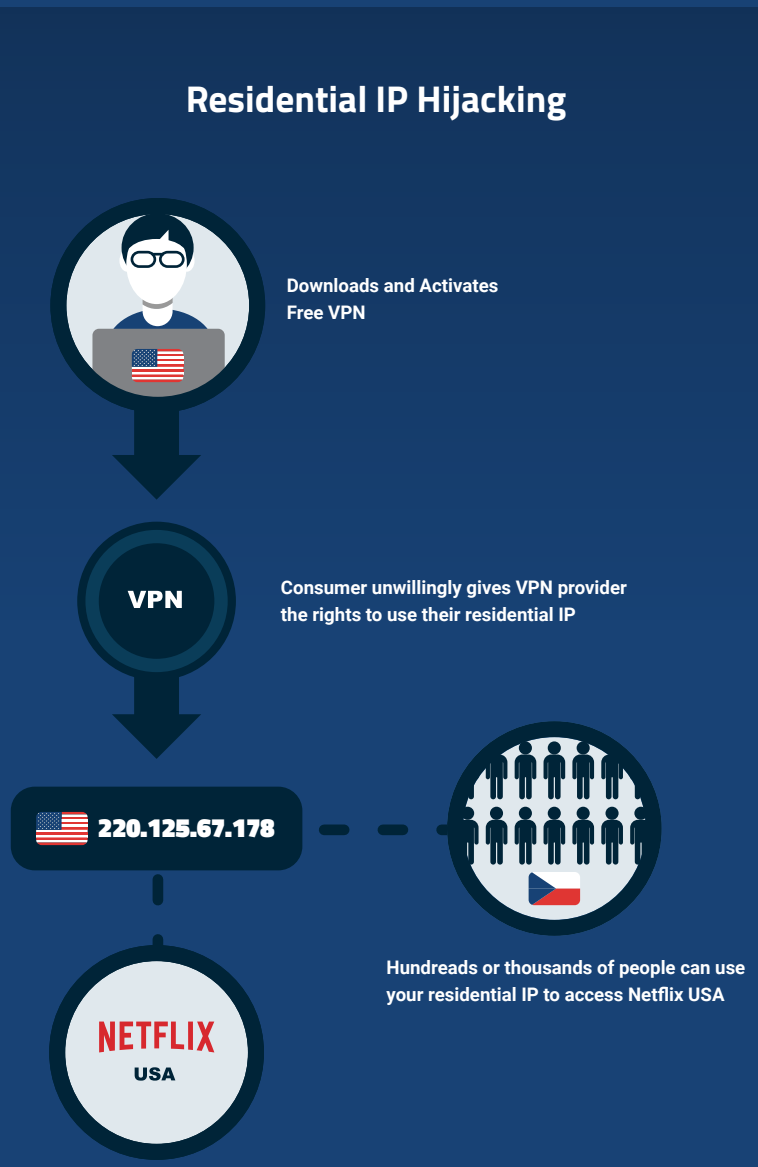
Incorporating IP Intelligence for Corporate Network Protection

IP address intelligence data alone won’t protect a company’s network. Its real value is two-fold. First, it plays a critical role in forensics. If your network is hacked, it can shed light on the characteristics of a particular user. Where is the user coming from? Is the user hiding his or her identity via a VPN, and if so, how?

Going further, IP intelligence data can be used to make smart decisions in terms of who can access, who should be blocked, and who should submit to additional authentication. Some of this data can be used to identify and target low-hanging fruit, such as blocking all traffic that comes via darknets or VPNs known for bad actors.

For instance, the ability to identify if an online user is connected through a proxy and what type of proxy it is enables companies to flag potential criminal activities, set protocols for handling this type of “non-human” traffic differently and then review the post-facto analytics behind these types of connections. By incorporating proxy/VPN data on the front-end of online security measures, companies can automatically flag an IP address as suspicious and reject or block the incoming IP from connecting to their service, website or network.

Additionally, understanding the type of proxy a visitor is connecting to the internet with can trigger fraud alerts. Responses to the type of proxy can vary depending on what type of proxy it is—for example, an anonymous proxy may warrant a higher fraud score than a corporate one. By identifying connections that obscure the end-user location or those that seek to portray a connection from an “acceptable” city or country can now be easily identified and categorized.



digital element

The following types of proxies may warrant a red flag or some level of consideration from the security team:

Geolocation Is the traffic that hits your network coming from an area that makes sense? If your company is exclusive to the Northeast, a spike of traffic from California may be a reason to investigate (or require an additional authentication step). Some countries are known for nefarious behavior, and some security professionals block traffic from those reasons as a matter of course.

Anonymous Actual IP address of the end user is not available which often includes the use of services that change location to circumvent digital rights management, Tor points (free software for enabling anonymous communications), temporary proxies and other masking services.

Transparent Actual IP address of the end user is available via HTTP headers, although the value is not necessarily reliable (i.e. it can be spoofed).

Hosting Addresses belong to a hosting facility, and end users are not typically located in a hosting facility. Some of this traffic is legitimate, however, and some IP intelligence insights can provide the needed context to distinguish between people, bots, and potential business traffic.

Corporate Generally considered harmless, their location can occasionally be a concern. Multiple users proxied through a central location or locations, and thus sharing a single network-apparent IP address, are not reliable.

Public Public traffic requires some consideration, but it doesn't mean it should be blocked automatically. Public traffic means that multiple users are proxied from a location that allows public internet access, such as libraries or airports, and as a result, all users share a single IP address. Some of that traffic may be your own employees accessing your network from the road. Some may be nefarious players attempting to hack into your network using brute force. Again, the context provided by other IP intelligence can help you decide when to require additional authentication.

VPN with No Paper Trail Every VPN and proxy is anonymous by nature, but what happens if the user commits a crime? VPNs that are free, allow for anonymous registration, or accept anonymous payment via a prepaid credit card or crypto may be of concern to some, as there will be no paper trail.

Bullet Proof VPN These are services that don't listen to take-down notices, even if they come from law enforcement. It's probably a good idea to block this traffic.

Of course, success depends on data quality. Reliability of information can vary significantly among data sources. But the most accurate proxy data providers not only ensure that information is constantly updated on a daily basis, but that information also originates from excellent sources.

The Future: Incorporating Other IP Data to Go Beyond Proxies

In order to thrive in the digital world, companies must equip themselves with tools that identify and exploit crooks and cyber criminals to strip them of their anonymity without jeopardizing real users—and this can be accomplished effectively and seamlessly through proxy/VPN data and other IP-intelligence factors.

The analysis of criminal activity can go far beyond proxies. Initially, this may include an assessment of the connection type. For example, a hosting center can be a tool for traffic, not a source. Then traffic originating from it can be examined alongside existing records, such as information stored in a Customer Relationship Management (CRM) database. The same goes for proxy, VPN and queue servers. By evaluating the type of proxy used against the highest quality proxy data, companies can start distinguishing between a reliable VPN and a mechanism that is more suited to suspicious activity.

Beyond connection features, IP geolocation allows companies to run comparisons. For example, in retail, this includes the implementation of smart rules where IP location is automatically checked when there are log-ins from high-risk locations. Alternatively, companies can secure internal networks by tracking speed patterns and identifying suspicious trends, such as people jumping between locations at illogical speeds or in illogical order. It also protects from insider threats or other policy violations by alerting you of outbound VPN or proxy activity.

After analysis, companies can choose their preferred mode of action. Any suspicious activity that poses a low threat can be flagged for additional authentication, such as sending an email or SMS that allows the user to confirm their identity. In the meantime, serious threats can be blocked immediately to prevent damage. Alongside reducing false positives, this approach shows consumers that companies are committed to cybercrime prevention.

Understanding the type of proxy a user is connecting to the internet with has become increasingly important to improving online security for any type of business.

digital element

Some examples of security use cases applying proxy/VPN datasets:

Online Gambling and iGaming

A statewide lottery for Minnesota that allows consumers to participate online, for example, has two options to: 1) Ensure players are "human" (and not bots); or 2) Certify players are from that state—not right across the border in South Dakota. By incorporating IP-based VPN data, the lottery can see if an IP address is associated with a proxy. If yes, then access can automatically be denied. Additionally, a subscriber-level commercial VPN could be used to change a player's actual location to appear to be from Minnesota. In the absence of proxy data, using IP-based geolocation data in the verification process can help the lottery identify down to a state level where that online player is actually originating from—automatically granting or denying access to participate.

Government

An air-service branch of the government can use IP-based VPN data to filter, identify safe VPNs, then develop traffic exemptions for approved vendors, such as Lockheed Martin, in order to automatically grant access to the agency's networks and websites.

Financial Services/E-commerce

Whether an insurance company or an e-tailer conducting business online and accepting digital payments, they can incorporate proxy/VPN data to implement smart rules to automatically verify consumer IP addresses and then determine which transactions to review—and which to approve or decline.

Cybersecurity

Managed security service providers (MSSPs) can use proxy/VPN data as a foundational, front-line layer of fraud-prevention security. They can use these datasets to help prevent unauthorized network and system access attempts. By understanding how online users access and interact with their clients' networks, MSSPs can be better positioned to more quickly respond to potential cyber threats when unusual activities occur.

Streaming and OTT

A sports streaming service that broadcasts regional sporting events around the world can use proxy/VPN databases to determine which IP addresses to geo-block from piracy attempts. The streaming service can also use other IP information parameters to determine when a potential pirate is using a new proxy IP to try and gain access again.

Digital Element is the global IP geolocation and intelligence leader. In business for more than two decades, the company has unrivaled expertise in leveraging IP address insights to deliver new value to companies in a privacy-sensitive, transparent manner. Leveraged by the world's most recognized brands, Digital Element provides clients with innovative solutions designed to optimize engagement across industries and applications, creating unique value at every consumer touchpoint. Many of the world's largest websites, brands, security companies, ad networks, social media platforms and mobile publishers have trusted Digital Element's technology to target advertising, localize content, enhance analytics, and manage content rights as well as detect and prevent online fraud.

US Headquarters:
+1 678.258.6300

www.digitalelement.com

[1] https://www.crn.com/news/security/the-10-biggest-data-breaches-of-2022-so-far-
[2] Columbus, Louis, "The Best Cybersecurity Predictions for 2021 Roundup," Forbes, Dec. 15, 2020.
[3] https://findstack.com/vpn-statistics/
[4] https://findstack.com/vpn-statistics/
[5] iBid
[6] Vojinovic, Ivana, "VPN Statistics for 2021 – Keeping Your Browsing Habits Private," DataProt, Apr. 13, 2021.