nodify

Digital Element's Threat Intelligence Solution

Nodify Product Data Sheet

With the rise in data breaches, cyber threats, and growing concerns about internet privacy, the widespread adoption of VPNs and Proxy networks has surged in recent years. This uptick is primarily fueled by an increased awareness of online privacy and security. While VPNs play a crucial role in enhancing online privacy and security by encrypting internet traffic and concealing users' IP addresses, they can also be leveraged by malicious actors. Cybercriminals often employ VPNs to obscure their locations, making it more challenging for businesses and cybersecurity professionals to trace the origins of online activities.

To navigate this evolving landscape, Nodify is specifically designed to provide powerful contextual IP address metadata. It offers extensive insights into the origins of web traffic, including VPNs, proxies, and darknets, enabling cybersecurity professionals to gain a comprehensive understanding of the potential threats posed by such traffic. This comprehensive information equips companies with the data and insights needed to determine the relative security risk associated with an IP address and respond appropriately.

Unlike other fraud detection solutions, Nodify provides additional context around the VPN/proxy/darknet tied to an IP address. The IP addresses that are seen correspond to device behaviors.

Understand if a given IP address is associated with a benign VPN provider or one that is frequently used by malicious actors.

If ingress (inbound) traffic is seen coming from one of these IP addresses, you will know if someone is trying to access services from a VPN, proxy or darknet as well as the implications resulting from that access.

If egress (outbound) traffic is seen going to one of these IP addresses, you would be able to know if someone is using a VPN, proxy, or darknet and additional information behind it.

nodify

Nodify Product Data Sheet

Additional contextual knowledge provided such as:

- VPN classification (masked, public, or private)
- Does not log the user's activity
- Provider's name/URL
- IP addresses related to a provider
- Allows anonymity for the user
- Languages of the target market of the VPN provider

The most comprehensive anonymous traffic contextualization solution in the market, Nodify can:

- Differentiate between an extremely risky VPN connection or a "good" VPN connection to avoid blocking safe connections.Provider's name/URL
- Protect revenue streams by deriving additional context behind a connection to know which transactions pose a risk.
- Prevent bad actors from infiltrating and hijacking your systems by identifying anonymized connections.Does not log the user's activity
- Prevent corporate espionage by ensuring inbound connections to your system are not from a VPN, proxy or darknet.

Nodify is leveraged though an API, giving customers access to a daily feed of all active provider nodes. This data, coupled with contextual data around each provider, gives cybersecurity professionals the ability to assess the level of threat such traffic poses.