Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Know Who You're Talking To (KWYTT) with WHOIS, IP, and DNS Intelligence

Identities on the Internet are difficult to establish and easy to masquerade. Complementary to setting up sophisticated security solutions to keep the bad guys out, it can be constructive to learn everything possible about who companies are dealing with.

Know Who You're Talking To (KWYTT) is a complementary policy of the zero-trust approach to network security, where organizations do not trust anything inside or outside the network by default. It is an extension of the Know-Your-Customer (KYC) policy that financial institutions are required to comply with. The model improves cyber risk protection, fraud detection, and regulatory compliance by expanding continuous identification and verification of customers, users, partners, merchants, vendors, employees, C-suites, or really anyone in the world.

Here are three KWYTT processes that WHOIS, IP, and Domain Name System (DNS) intelligence can help with.

Are Your Customers Who They Say They Are?

KYC has contributed to the fight against money laundering and financial crime for years. Building on KYC's key attributes such as customer identification and validation mechanisms, KWYTT calls for additional measures to verify customers' digital footprints. Here is how WhoisXML API's cyber intelligence sources can help with this undertaking:

Notable Use Cases	Connected Data Points
KYC policy compliance through primary customer identification and validation	• Is the customer's IP address located in a cybercrime hotspot? Is the customer's domain name registered in a high-risk location? • Does your customer's website information match those documented in DNS and WHOIS records? • Does the website fall under dubious categories?
Enhanced due diligence and fraud detection	• Are any of your customer's domains and IP addresses flagged as malicious? • Do your customer's details appear as part of other suspicious and malicious domain registrations? • Which other domains share the customer's IP address? Are they part of a dedicated or shared infrastructure? Are they malicious?
Financial transaction verification and identity access management	• Are the customer's recorded IP address, Internet service provider (ISP), and connection type the same at the moment of the transaction? • Is the customer's IP address found to be malicious or located in a cybercrime hotspot at the time of the transaction? • Are any financial transactions made from/to out of region or from/to offshore?
Ongoing customer monitoring	• Are transactions or activities suddenly happening from out-of-the-area locations? • Are there new suspicious subdomain additions to the customer's site infrastructure? • Are any of the customer's newly added domains or subdomains flagged as malicious?

2

Can You Trust Your Third-Party Partners?

Third-party risk management (TPRM) entails identifying and mitigating risks associated with merchants, vendors, suppliers, partners, and other third parties a company does business with. In support of TPRM, KWYTT makes digital supply chains more transparent, enabling organizations to have more visibility and control over risk exposure, who they share data with, and access controls. WhoisXML API's WHOIS, IP, and DNS data sources provide additional intelligence that makes KWYTT more comprehensive.

Notable Use Cases	Connected Data Points
Primary supplier and merchant profile risk assessment	• What are the domain's registration details and are they redacted? Do they match the details the third party provided? • How is the merchant's or supplier's website categorized? • Is the domain or IP address classified as malicious?
Enhanced supplier profile assessment	• Are ownership details connected or associated with any malicious domain(s) • Is the supplier's domain registered in a high-risk location? • Are the supplier's nameserver, ports, and Secure Sockets Layer (SSL) certificates configured correctly?
Supplier's connections	• Does the supplier's domain resolve to a shared or dedicated IP address? What other domains share the host? • Is the vendor hosted alongside malicious digital assets? • How many domains resemble the vendor that are not actually owned by the vendor?
Supplier monitoring	• Do any of the supplier's newly added domains and subdomains contain suspicious details (other brands are mentioned, etc.)? • Are there any newly added typosquatting domains and subdomains targeting the supplier? • Are there suspicious changes to the supplier's SSL and DNS server configurations?

3

Who Else Are You or Your Business Partners Talking To?

Zero-trust policy requires constant identification and validation of everyone else that connects to your or your business partners' network. While some of these entities can be potential customers or partners researching the company's products and services, some of them could also be suspicious. They could be trademark infringers, brand impersonators, typosquatters, phishers, and other cybercriminals. KWYTT policy covers traffic from and to these people, too. What details can WhoisXML API's DNS, IP, and domain intelligence provide about these entities as part of KWYTT activities?

Notable Use Cases	Connected Data Points
Cybercrime and fraud protection and prevention	• What is the source IP address of the traffic? Is it located in a cybercrime hotspot? • Is the source IP address malicious? Does it belong to a malicious IP range? Is it connected to malicious domains? • Is the email domain malicious? Does it imitate legitimate brands? Is it connected to other malicious domains based on its current or historical WHOIS records?
Prevent trademark infringement and support Uniform Domain-Name Dispute-Resolution Policy (UDRP) complaints	• Are there existing and newly added domains and subdomains that seem to be imitating yours? • What content do these domains and subdomains host? Does the content indicate that the cyber resources were added in bad faith? • When were these typosquatting domains and subdomains added?
Takedown of dangerous web properties	• Which registrar manages the malicious domain? • Which IP netblock does the malicious IP address belong to? Who administers the netblock? • What ISP has control over the malicious IP address?
Avoid being impersonated in phishing, business email compromise (BEC), and other malicious scams	• Are there new or existing domains and subdomains that appear to be imitating yours? Have any of them been reported as malicious? • Are there new domain and subdomain additions that use your C-level executives' names? • Are the contents of these domains and subdomains suspicious?

About Us

It's crucial to verify the identity and credibility of anyone and everyone communicating with your network, including employees, company executives, customers, third-party suppliers, competitors, or potential malicious actors.

WhoisXML API provides well-parsed, normalized, and comprehensive WHOIS, IP, and DNS intelligence to enrich KWYTT processes and related initiatives. For over a decade, we have gathered and aggregated 11.5+ billion historical WHOIS records, 2.3+ billion hostnames, 11.5+ million IP netblocks, and 99.68% of active IPv4 and IPv6 addresses.

Contact us to know more about how our DNS, IP, and WHOIS data sources can contribute to KWYTT policies.

WhoisXMLAPI

The Who Behind Domain, IP & Cyber Threat Intelligence