Use Case Sheet

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Fueling the Latter Stages of the Attack Surface Management Cycle with High-Fidelity DNS Data

Business Problem

Attack surface management (ASM) is a never-ending process that goes beyond asset discovery and enumeration. While these initial stages help platform users gain attack surface visibility, the view would remain opaque without in-depth asset attribution and real-time monitoring. Additionally, attack surface reduction would be unattainable without the ability to execute vulnerability prioritization and remediation. For ASM to be effective in the long run, users must also perpetually go through the whole cycle while ensuring a fast, efficient, and reliable feedback loop supported by data.

Data-Driven Solution

Attack surfaces are constantly evolving—the picture is never static, as organizations always ramp up business activity. At the same time, the bad guys continue to find ingenious ways to exploit vulnerabilities and weaponize seemingly innocent cyber resources. Offering the capabilities to go through the entire ASM cycle requires continuous access to relevant, up-to-date, and high-fidelity data relevant to the connected world's Domain Name System (DNS). An unhampered view of Internet-wide data can provide much-needed asset attribution, fuel vulnerability scoring algorithms, and improve security team efficiency through remediation prioritization, among other critical ASM missions.

Notable Use Cases	Connected Data Points
Provide attribution to discovered assets	• What domain names were registered using the attack surface owner's organization email address? What registrars are responsible for the domains? • When were the company's subdomains added, when were they last updated, and how are they used? • To which IP ranges do the organization's IP addresses belong? Who manages or owns the IP block?
Check the ownership details of rogue assets for mitigation and takedown	• Who are behind rogue assets, including typosquatting domains? • Who is the administering organization of abused IP addresses targeting the attack surface owner? • What are the registration details of root domains with typosquatting subdomains? When were the subdomains added, and when were they last updated?
Assess risks and vulnerabilities for prioritization and remediation	• Given the status codes of the organization's domains, how vulnerable are they to hijacking? • What misconfigurations are there in the organization's domain and website infrastructure? For example, are there incorrect hostnames, deprecated Secure Sockets Layer (SSL) protocols, or suboptimal cipher suites? Are there single points of failure (SPoFs) related to the organization's DNS records, IP block, and Autonomous System number (ASN)? • With the organization's DNS configuration, how vulnerable is it to DNS-based attacks, such as DNS hijacking? Are DNS records overly descriptive and leaving too many breadcrumbs for threat actors?
Continuously monitor discovered assets and the DNS round-the-clock	• Are there suspicious changes in the organization's IP block and A, MX, NS, and other DNS records? • Are there recent registrations or additions of rogue assets? Have any of these been flagged as malicious? • What are the IP block administration or ownership details of rogue devices connecting to the organization's network?

> *We have this great responsibility to effectively and efficiently manage our clients' attack surfaces, and we can't do that with blurred vision. We have to see everything that's going on, and WhoisXML API has been helping us see what's happening in the DNS without going through painstaking data aggregation and normalization.*

Solutions Engineer
Attack Surface Management (ASM) Company

> *The Proofpoint Digital Risk Team uses WHOIS data as an input to heuristic detection of suspicious and/or malicious domains. At Proofpoint, we're in the business of protecting our customers from threats across web, mobile, email, and social. WhoisXML API's domain intelligence allows us to quickly integrate WHOIS lookups into our security heuristics and algorithms without having to worry about hosting services, staging, and merging data, and the complicated task of normalization.*

Rich Sutton, VP of Engineering
Proofpoint

Finding Your Own DNS Data (FYODD) Doesn't Let You Scale

Delivering a real-time and uninterrupted satellite view of the world's DNS is our core business. The WhoisXML API data engine is built and frequently upgraded to offer you the most complete, updated, and unique Internet intelligence footprints. We aim to contribute to our clients' competitive edge at every step and give back months or years of development cycle time to your most pressing and mission-critical projects and deployments.

How the WXA Data Engine Is Ready to Add to Your Success Today

1. Collection	2. Unification	3. Maintenance	4. Delivery	5. Innovation
• Internet-wide data sensing and crawling since 2010 • Legal agreements with major data aggregators • Large and growing network of data exchange partners	• Consistent data parsing of multiple data points across formats • Resolving incomplete, conflicting, and inaccurate records	• Addition of new and historical domains, subdomains, and IP and DNS records • Daily updating of millions of WHOIS, DNS, IP, and other records	• Batch feeds and APIs with complete documentation • Different support and customer success tiers • Enterprise-grade IT infrastructure	• Ongoing improvement of data coverage, freshness, and accessibility • New features, products iterations, and solutions driven by market demand

Our Enterprise Value Proposition

Our intelligence is available through customized enterprise packages and product suites with multi-year contracts, flexible licensing models, nonrestrictive data access, and dedicated account and customer success teams. Contact us for more information.

Diamond: Includes all products listed below with Premium SLA
Gold: Pick 2 of each Tier, includes Gold SLA
Silver: Pick 1 of each Tier, includes Silver SLA
Starter: Pick 1 Tier-1 product, 1 Tier-2 product

Tier	Product	Update Frequency
P	Real-time & Historic Whois Streaming	Real-time Stream, Daily & Quarterly Feed, Real-time API Lookups
P	Real-time & Historic Passive DNS Coverage	Daily + Weekly Feed, Real-time API Lookups
P	Enterprise & Threat Intelligence APIs	Enterprise APIs T5 & Threat Intelligence APIs (1M CPM)
1	Real-time WHOIS Data Coverage	Daily & Quarterly Feed, Real-time API
1	Real-time DNS Coverage	Weekly Feeds, Real-time API
1	IP Geolocation & Netblocks Data Coverage	Daily Feeds
1	Website Contacts & Categorization Feed	Daily Feed
2	Subdomains Database Feed	Daily Feed
2	IP Netblocks (IPv4 + IPv6)	Daily Feed
2	IP Geolocation Database	Daily Feed
2	Typosquatting Data Feed (Enriched)	Daily Feed
2	Disposable Email Domains Feed	Daily Feed
2	MAC Address Database Feed	Daily Feed

About Us

WhoisXML API aggregates and delivers comprehensive domain, IP, DNS, and subdomain data repositories. WhoisXML API has more than 52,000 satisfied customers from various sectors and industries, such as cybersecurity, marketing, law enforcement, e-commerce, financial services, and more. Visit whoisxmlapi.com or contact us for more information about our products and capabilities.

WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence