Service Definition: DomainTools Platform

This service description provides additional information for buyers of the DomainTools Platform.

Bright Cyber is an authorised reseller of the DomainTools Platform. This service is offered through the G-Cloud framework in accordance with the published service listing and associated documentation.

Further information about the platform is available in the brochures provided as part of this service description. Buyers may also contact Bright Cyber using the details below for clarification or support.

Service Roles and Responsibilities

Bright Cyber Responsibilities
Bright Cyber is responsible for the commercial relationship with the buyer and for ensuring service delivery. This includes:

Account Management
- Provision of a named account manager
- Availability Monday to Friday, 9:00am to 5:00pm (excluding public holidays)
- Response to email queries within 4 working hours
- Direct telephone contact details will be provided

Service and Advisory Support
- Advice relating to use of the DomainTools Platform
- Guidance on information security matters relevant to the service

Commercial Management
- Contracting under the G-Cloud agreement
- Billing and invoicing
- Management of service variations, extensions, and additional services where agreed
- All commercial activities managed in accordance with G-Cloud terms and conditions

Bright Cyber will ensure the service is delivered in line with the agreed scope and will support the buyer in using the service effectively.

This may include:
- Coordinating onboarding activities
- Attending service review or progress meetings where required
- Supporting issue escalation and resolution

- Ongoing service coordination and governance

DomainToolsResponsibilities
DomainToolsis responsible for delivery and technical operation of the platform, including:

- Platform provisioning and onboarding
- Delivery of the service in line with the published service description and specifications
- Provision of technical support for the platform

Service Contact Details

Service Contact: Murray Pearce
Email: murray.pearce@bright-cyber.co.uk
Telephone: 0345 257 0071
Website: https://bright-cyber.co.uk

Further information on the DomainTools service follows this page.

Iris Internet Intelligence from DomainTools

DomainTools is the gold-standard Internet intelligence data source.

We provide more data, more frequently, and with more full-Internet risk context than anyone. Access the insights you need to assess risk and make the right decisions through our Iris platform or scale your process with our APIs.

Know now.

Iris Detect

Near real-time Internet infrastructure detection, monitoring, and enforcement.

Capturing key data on new domains and risk-scoring them within minutes of registration, Iris Detect is a game-changer for brand managers, digital risk and fraud prevention teams, and network defenders.

Know more.

Iris Enrich

Robust API including Whois, DNS, SSL certificate, and risk scoring elements to enrich indicators at scale.

Iris Enrich brings critical awareness to analysts, detection engineering teams, threat hunters, and other practitioners.

Know farther.

Iris Investigate

Investigation platform with domain intelligence, risk scoring, and industry leading passive DNS data.

An intuitive web interface and corresponding APIs help security teams quickly and efficiently investigate cyber threats and malicious infrastructure.

“There’s no better way to do this.”

THREAT INTELLIGENCE & HUNTING

Detect relevant indicators earlier in their lifecycle to identify and disrupt incipient attacks.

FORENSICS & INCIDENT RESPONSE

Respond to and triage potential incidents with confidence and speed.

FRAUD PREVENTION

Know if and when malicious domains and infrastructure are spoofing your assets before they cause damage.

LAW ENFORCEMENT

Ensure the safety of critical digital infrastructure with preemptive intelligence to strengthen national security efforts.

OEM

Empower your homegrown or third-party security applications with the world’s best Internet intelligence.

BRAND PROTECTION

Monitor lookalike domain names and protect your brand against cybercriminals.

Key Iris Benefits

- Continuous monitoring of evolving infrastructure
- Investigation workflow management
- Comprehensive data sources
- Insights into emerging threats
- Infrastructure risk assessments

The DomainTools Difference

- Built on over 20 years of engineering experience and threat knowledge
- Reaches into 97% of the full Internet
- Access to billions of open-source data points
- Updated in real-time

DomainTools

DomainTools Threat Feeds

Real-Time Risk for Proactive Security

DomainTools reaches over 97% of the Internet to bring you the best-in-class intelligence on threats in real-time. Powered by this comprehensive view, our feeds grant visibility into potentially malicious domains and hostnames faster than anyone else, allowing you to eliminate threats **before they happen**.

Illuminated Defense

For security teams, playing defense often means constantly reacting to threats. This drains critical time and resources, and leads to analyst burnout.

Introduce a new era of proactive defense with **DomainTools Real-Time Threat Feeds**. Unlike traditional intelligence that reports on already-weaponized infrastructure, our feeds provide instantaneous visibility into risky DNS activity as it appears.

Don't react - **act first**.

"

Through close collaboration this year, we were among the first to adopt DomainTools' Real Time Feeds and API, reducing the time from threat discovery to active prevention to **under one minute**. This level of speed and accuracy effectively closes the window for domain-based attacks. DomainTools has set a new standard for real-time, high-fidelity intelligence - critical to any modern, proactive defense strategy.

"

DAVE AHN, CHIEF ARCHITECT AND VP AT CENTRIPETAL

Risk Feeds

Our predictive risk scoring feeds provide a risk-based view of newly registered or updated domains and infrastructure.

- Identify and act on dangerous domains
- Reduce detection and incident response times
- Integrate accurate, predictive domain risk scoring into your blocking, detection, and incident response workflows

About DomainTools Risk Score

Drawing on data points from more than 390 million current domains, the DomainTools Risk Score predicts how likely a domain is to have been registered with malicious intent, often before it is weaponized. The score comes from two distinct algorithms that evaluate the likelihood of malicious use through a domain's connections and resemblance to other known-bad infrastructure.

DOMAIN RISK

All high-risk domains with scores for phishing, malware, spam, and proximity.

DOMAIN HOTLIST

Highest-risk domains that are also active in passive DNS in the previous 24 hours.

Discovery Feeds

DomainTools discovery feeds surface newly registered, active, and observed domains and hostnames, which are often used for phishing, malware, and spam.

- Gain real-time visibility into young domains or hostnames
- Combat sophisticated cyber attacks
- Strengthen your defenses with intelligence on domain age

NEWLY OBSERVED DOMAINS

Domains never before observed in passive DNS.

NEWLY ACTIVE DOMAINS

Domains not observed in passive DNS in the previous 10 days.

DOMAIN DISCOVERY

Newly discovered domains, including new registrations not necessarily active in passive DNS.

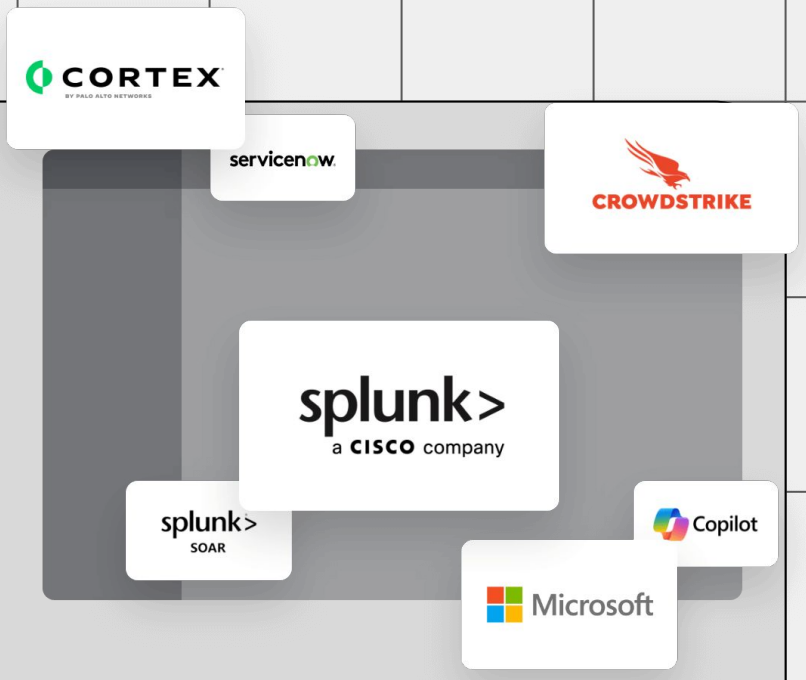
NEWLY OBSERVED HOSTNAMES

Fully qualified domain names (FQDNs) never before observed in passive DNS.

Seamless integrations

for immediate value

Through seamless integrations across leading SIEM, SOAR, TIP, and other security platforms, DomainTools ensures that rich DNS intelligence is available directly within the tools analysts already use. We enable faster visibility into threats, faster judgement on risk levels, and deliver this crucial data wherever it is needed most. These integrations can be incorporated into your environment in as quickly as one day, enabling security teams to unlock instant, actionable intelligence.



ACCESS METHODS

- **Feed API**
- **Download API**
- **Response Policy Zone (RPZ)**

Use Cases

- **Proactive Defense:** Automatically block communication between your devices and potentially harmful domains to protect your network, customers, and employees.
- **Threat Detection:** Accelerate incident response by spotting when your devices are connecting to the newest or highest-risk domains. Use automated processes to investigate and prioritize threats based on their risk level, reducing alert fatigue.
- **Supply Chain & Brand Monitoring:** Identify new domains and subdomains that mimic your supply chain, partners, or brand. Gain full control over detection rules to ensure accurate monitoring and protection.
- **Tracking DGA Domains:** Detect new, algorithmically-generated domains associated with known cyber threats as soon as they appear or become active.

About DomainTools

DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.

DNSDB from DomainTools

Cybercriminals know all about your infrastructure. How much do you know about theirs?

DNSDB is the world's largest passive DNS database, providing a unique, multifaceted view of global Internet infrastructure. With access to this critical intelligence, security teams gain unmatched insight into how threats emerge and evolve over time.

- **2TB** DNS data collected daily
- **100+ billion** DNS records
- **800k+** observations per second
- **1Gb/sec** real-time streaming data

ELIMINATE BLIND SPOTS

View Internet infrastructure to see how adversaries have rolled through domains, IP addresses, and name servers to conceal their activity

STOP PHISHING, MALWARE, AND RANSOMWARE EARLIER

Proactively defend your organization from sophisticated cyber threats.

MINIMIZE RISK

Access real-time and historical passive DNS data to block your infrastructure from being used by bad actors.

Access methods to suit your workflow

DNSDB API

Unlock the power of DNS intelligence across dozens of SIEM, SOAR, and threat intelligence platforms.

Features and Benefits:

- Ability to search RRname, RRdata, and by IPv4 or IPv6 address or address block
- Support for whole-label left-hand-side or right-hand-side domain name wildcards
- Support for IP range or CIDR prefix RRdata searches
- Able to return up to a million results per query
- Flexible Search and support for regular expressions

DNSDB EXPORT

Download an on-premise installation of DNSDB in your own environment or a hosted service.

Features and Benefits:

- Full DNSDB Flexible Search and Standard Search functionality
- Total query privacy for compliance with industry regulations
- Ability to access data in an offline environment
- Unlimited query volume
- Minimal network latency
- Fastest response time

DomainTools

DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.