efficient iP®

Datasheet

DNS Threat Pulse

Leverage DNS Threat Intelligence For Proactive Protection

Highlights:

- Leverage unique, massive DNS traffic collection on a global scale for higher data quality and relevance
- Combine multiple reputable DNS data sources, that are analyzed, categorized, and curated by leading-edge AI patented technology and pioneering algorithms for increased accuracy
- Generate comprehensive, accurate, and up-to-date DNS intelligence data feed to proactively protect against malicious intent and increase security
- Bundle with DNS Intelligence Center to early detect and efficiently investigate threats by correlating Threat Intelligence with your DNS traffic and by analyzing global DNS traffic to enrich domain info with contextual insights.
- Bundle with DNS Guardian for consolidated and granular security policy management using rich tag capacity for advanced threat protection
- Enable holistic end-to-end network security by automated sharing of security events with ecosystem for accelerated threat remediation

The ever-growing diversity of networks and connected devices (SD-WAN, IoT, hybrid and multi-cloud,...) drive the usage and generation of data in general. This diversity adds complexity to IT infrastructure manageability and operations creating security holes. Enterprise sensitive data is more exposed to increasing and sophisticated cyber threats and needs to be protected.

Because DNS is actively used for any network transaction, including those in cyberattacks, it contains large amounts of information about network usage, behavior, and intent, hence valuable information that remains underestimated.

The EfficientIP DNS Threat Pulse product offers security and NetSecOps teams a comprehensive, accurate, and up-to-date DNS threat intelligence data feed to help organizations protect their network proactively.

DNS Threat Pulse at a Glance

DNS Threat Pulse aggregates multiple open and trusted sources containing malicious domain information. With market-recognized DNS expertise and innovation, EfficientIP leverages unique massive DNS traffic collection and analysis on a global scale used to fuel Artificial Intelligence (AI) leading-edge patented technology and pioneering algorithms. These algorithms are used in a curation process to consolidate, classify, and categorize the data feed and deliver insightful and actionable data in real-time. This includes identifying Domain Generation Algorithm (DGA) domains using EfficientIP's patented tuple clustering model, and detecting phishing domains using Natural Language Processing (NLP) and image recognition techniques. The resulting feed then categorizes domains into malware, phishing, DGA, DoH, and additional threat categories.

DNS Threat Pulse can be enforced by DNS Firewall and DNS Guardian in two formats: Response Policy Zone (RPZ) for standard DNS filtering and Client Query Filtering (CQF) for more granular, user or device-based enforcement, enabling security teams to apply differentiated policies based on user groups, locations, or endpoints. The combined solution allows security teams to centrally define and enforce granular, flexible security policies.

DNS Threat Pulse seamlessly integrates into existing security ecosystems, using open APIs and available plug-ins to enrich detection and response workflows with DNS intelligence.

Key Features

Extensive Threat Categories

Category	Description
Abuse	Domains that are identified as being used for abusive behavior, such as spamming, scanning or brute forcing.
Botnet	Domains that are associated with botnets, which are networks of compromised devices controlled by a malicious actor to perform various activities, such as DDoS attacks, spamming, or data theft. The host in this category may use Command And Control type of communication leveraging DNS as transport protocol.
Domain Generation Algorithm (DGA)	Domains that are generated by malware to evade detection and contact Command and Control servers. These domains frequently change, with new ones often being generated, which makes them difficult to block with traditional methods. **DGA Time Dependent:** A DGA domain is considered «time-dependent» if it is generated using a mathematical algorithm that uses a seed that changes with time of day. Generated domain changes periodically based on the current time. **DGA Time Independent:** a DGA domain is considered «non-time-dependent» if it is generated using a fixed algorithm that does not rely on the current time. The generated domain remains the same until the algorithm is changed or updated. EfficientIP addresses both types of DGAs using patented tuple clustering algorithms that detect DGA activity based on behavior, rather than known signatures, helping uncover domains that static feeds often miss.
Malware	Domains that are known to host or distribute malicious software, including viruses, Trojans, ransomware, and other types of malware.
Miner	Domains that are used for cryptojacking, which is the use of a device's computing resources without the owner's consent to mine cryptocurrency.
DNS over HTTPS (DoH)	Domains actively providing DNS over HTTPS, identified through cross-correlated public and proprietary data and validated via live testing, ensuring accuracy and relevance.[1]
Newly Observed Domains (NOD)	Domains that have been recently seen, and have little or no history. They may be used for malicious purposes and can be marked suspicious. Sub-categorized by period of time.
Phishing	Domains that are associated with phishing attacks, which are attempts to trick users into revealing sensitive information, such as login credentials or financial information. EfficientIP categorizes phishing domains using AI-driven algorithms such as Natural Language Processing (NLP) and image similarity analysis to detect brand impersonation and look-alike domain patterns that traditional URL-based approaches may miss.

1. The DoH category is included only in the CQF format

Category	Description
Suspicious	Domains that exhibit suspicious behavior but don't fit into any of the other categories yet, such as those that are newly registered or observed or those that exhibit anomalous traffic patterns.
Active	Domains that are used by current active threats and for which DNS traffic has been observed over the Internet during the previous days. Provide additional insights to efficiently and quickly detect threats upstream.

Artificial Intelligence Assisted

AI patented technology and pioneering algorithms are used in a curation process to consolidate malicious domain names and their metadata in categories to ensure utmost relevance anytime. Applied more specifically to DGA and phishing, they permit increase of coverage and efficiency on generated malicious domains. They also predict and accelerate the finding of new or modified algorithms, suspicious websites, and help identify malicious activity from contextual client traffic.

Available Formats

The feed is supplied in two formats:

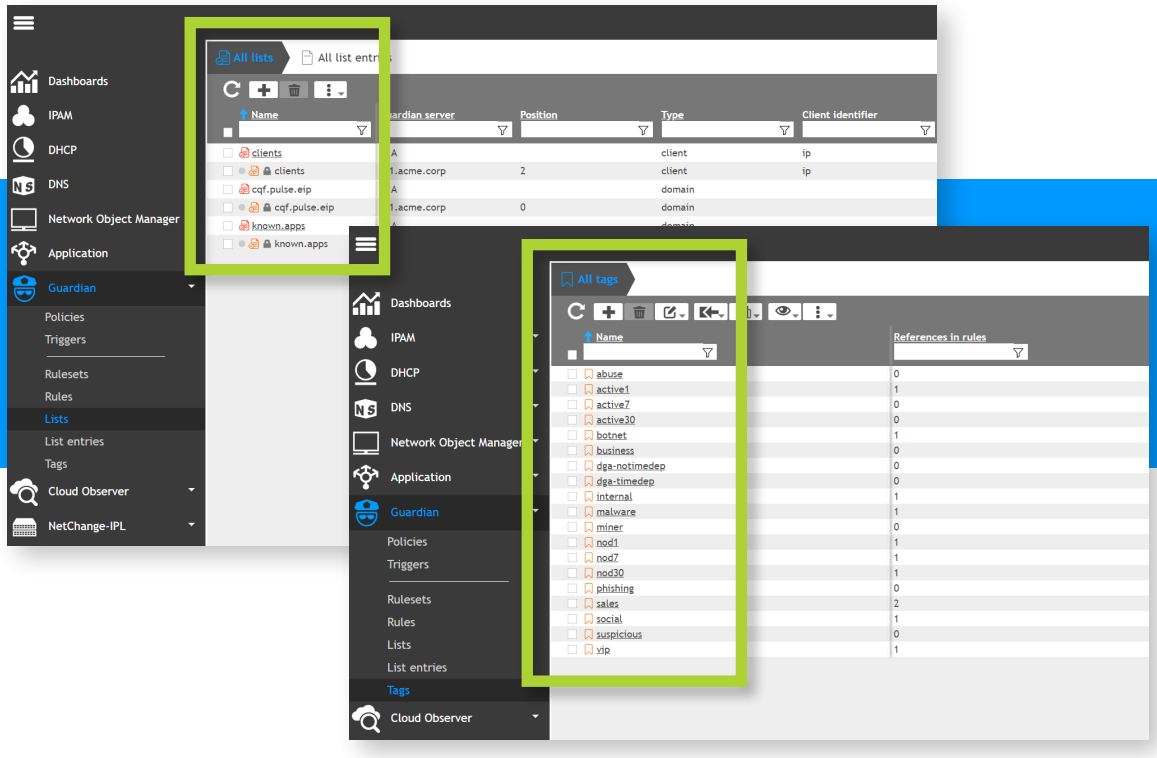
1. The **Response Policy Zone (RPZ)** format is a standard for filtering lists and feeds, compatible with any generic DNS firewall, and providing one zone per category, or one consolidated uncategorized flat one.
2. The **Client Query Filtering (CQF)** format provides an advanced capability compared to RPZ as all categories can be combined in one feed making distribution and management simple. It provides more entries than RPZ for a better coverage, and a finer grain control with rich tagging capability per category. In addition, the CQF format can be combined with the EfficientIP DNS Guardian to augment Client Application Access Control.

Advanced Client Query Filtering (CQF) for Granular Feed Enforcement

Client Query Filtering (CQF) enables granular, identity-aware DNS policy enforcement by combining DNS Threat Pulse (DTP) domain categories, such as malware, phishing, DGA, or DoH, with client or device identifiers such as IP address, MAC address, user group, or network segment. Instead of applying a single, global filtering rule, CQF allows security teams to tailor actions such as allow, block, redirect, or quarantine based on who is making the request and which domain category is being accessed.

By enforcing DTP categories at the client level, CQF prevents access to malicious or unauthorized destinations before any data is exchanged. This approach supports advanced security strategies, including micro-segmentation, application zoning, and Zero Trust, by ensuring only authorized users and devices can resolve specific applications or services. DNS resolution becomes an additional control point to validate identity and enforce least-privilege access across the network.

Policies are centrally managed and distributed through the SOLIDserver unified management interface, simplifying operational workflows, ensuring consistency across distributed environments, and improving security posture without adding complexity or latency.



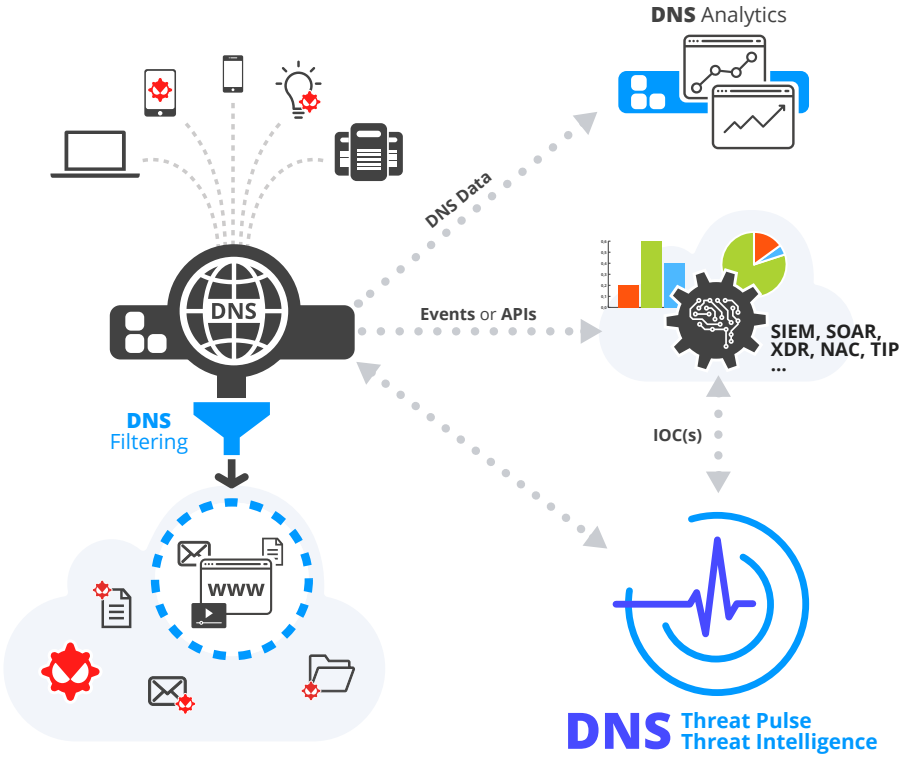
Central and Unified interface for managing Intelligence Feeds and Tags

Enhance SOC Efficiency with DNS Threat Intelligence Integration

Using a library of plug-ins and open APIs, the DNS Threat Pulse feed, combined with DNS Guardian, can be integrated with the security ecosystem to deliver coordinated and automated protection. DNS threat intelligence can be shared with platforms such as SIEM, XDR, SOAR, NAC, or Threat Intelligence Platforms (TIP) to strengthen detection, investigation, and remediation workflows within existing security processes.

DNS Threat Pulse categorization also helps teams understand which types of domains are being accessed across the network, supporting more informed policy decisions.

By integrating DNS Threat Pulse into the security stack, enterprises can build a more cohesive and efficient end-to-end security infrastructure and simplify ongoing security management.



DNS Threat Intelligence Automation for an integrated security infrastructure

Key Benefits

Richer Intelligence

Gain comprehensive, insightful, and up-to-date DNS intelligence data feed with curated, multi-source categorization.

Fine-Grained Enforcement

Apply high-granular identity-based DNS policies with DTP in CQF format and DNS Guardian for precise protection.

Proactive Protection

Leverage dynamic DNS threat intelligence feed and adaptive countermeasures to define DNS filtering policies and block threats earlier.

High Accuracy

Multi-source validation and patented AI-driven categorization techniques reduce false positives and increase confidence in enforcement decisions.

efficient iP®

REV: C-251110

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752