efficient iP®

Datasheet

DNS Threat Pulse

Leverage DNS Threat Intelligence For a Proactive Defense

Highlights:

- Comprehensive, accurate, and up-to-date DNS intelligence data feed to increase security on malicious intent
- Unique, massive DNS traffic collection on a global scale for higher data quality and relevance
- Combines multiple trusted, open sources on malicious domains that are analyzed, categorized per threat, curated by leading-edge AI patented technology and pioneering algorithms
- Real-time actionable insights to proactively defend, detect early, and prevent DNS-based cyber attacks globally
- Bundled with DNS Guardian for consolidated and granular security policy management using rich tag capacity for advanced threat protection
- Enables 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 included 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 proactively defend, quickly detect anomalies, and protect against malicious intent globally.

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. The resulting feed is then split into several categories such as phishing and malware among others.

DNS Threat Pulse features two formats: Response Policy Zone (RPZ) and Client Query Filtering (CQF), the latter offering more advanced security along with the EfficientIP DNS Guardian product. The combined solution allows security teams to define, centrally manage, and deploy highly granular and flexible security policies of their choice.

Using Open APIs, it can easily be integrated with the security ecosystem including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR) or Network Access Control (NAC), enabling security events and insights automation for accelerated threat remediation.

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 Generated Algorithmically (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. Generated domain remains the same until the algorithm is changed or updated.
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.
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.
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 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.

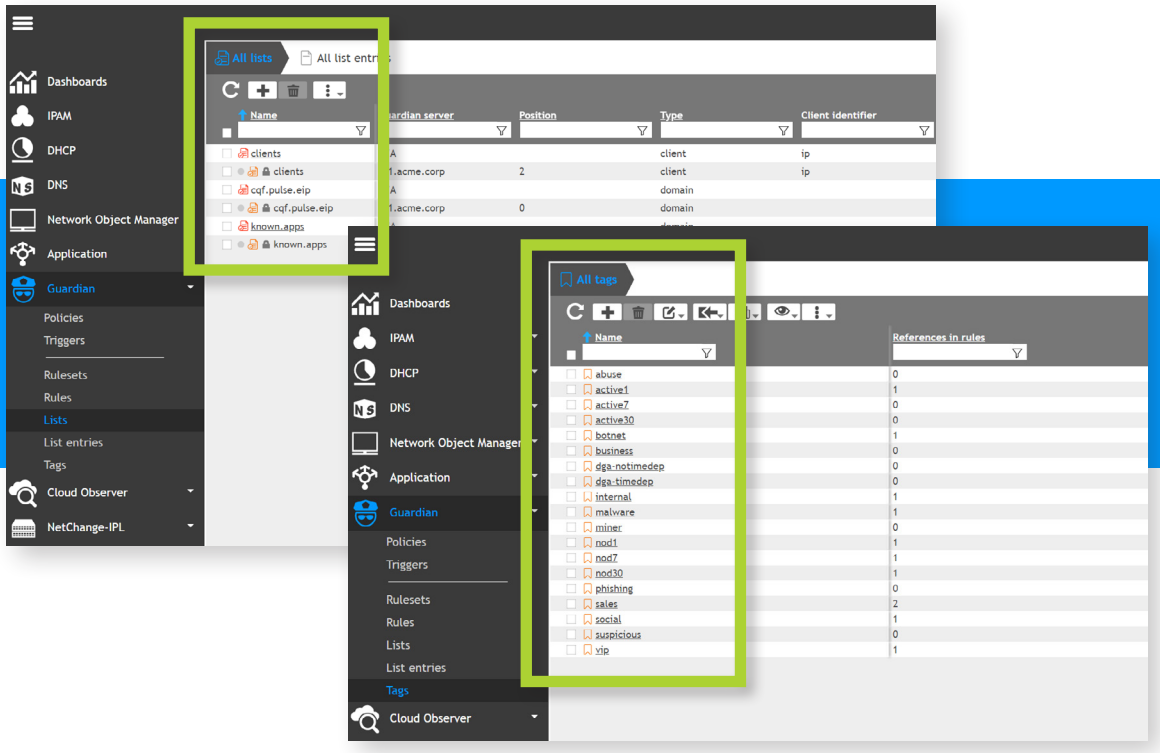
Client Query Filtering Advanced Capability

The DNS Threat Pulse CQF feed brings an additional security barrier with DNS Guardian as categories can be used as tags for defining and customizing application access security policies.

Categories can also be easily combined with other tags such as Client IP or Mac Address, client or client groups identifiers, or identifiers from DHCP or DNS transactions in order to set highly granular and rich policies to be applied to groups of users or even individuals.

All of these can be performed from the central and unified management interface of SOLIDserver. This simplifies and helps consolidate the distribution and enforcement of policies across the network contributing to micro-segmentation, application zoning, and better protection.

Combined with Behavioral Threat Detection and DNS Transaction Inspection brought by DNS Guardian, the solution enables to accurately detect the most sophisticated stealth attacks and threats hidden in the traffic as well as define and implement adaptive countermeasures for maximizing threat protection and increasing detection speed.



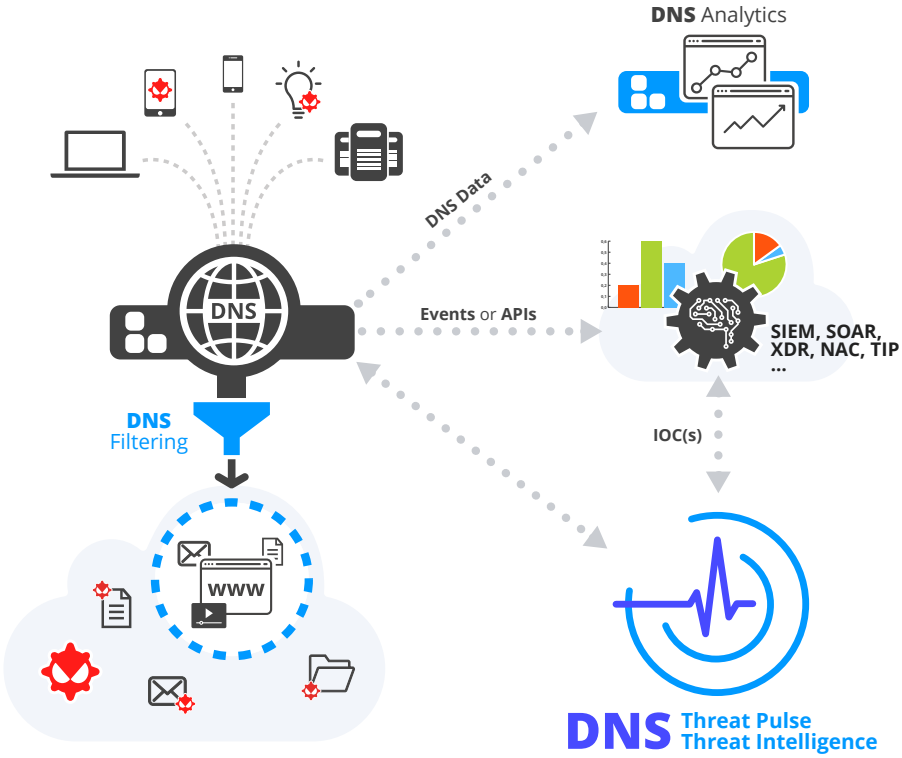
Central and Unified interface for managing Intelligence Feeds and Tags

Integration

Using Open APIs, DNS Threat Pulse CQF feed combined with DNS Guardian can be integrated with the security ecosystem to deliver advanced automated protection capability. DNS threat intelligence insights can fuel any security platforms including SIEM, XDR, SOAR, NAC or Threat Intelligence Platforms (TIP) to deliver valuable use cases such as providing the IP address of an infected device, accelerate threat hunting, remediation, and maximize Security Operation Center (SOC) operational efficiency.

In addition, DNS Threat Pulse can pave the way to new use cases beyond security. It can help classify and categorize any networking behavior and Intent to manage networks according to capacity and performance, resulting in a smooth end-user experience.

With DNS Threat Pulse, enterprises can build a more integrated and holistic end-to-end security infrastructure, reduce complexity, and gain agility.



DNS Threat Intelligence Automation for an integrated security infrastructure

Key Benefits

Improved Visibility

Improve network visibility with comprehensive, insightful, and up-to-date DNS Intelligence data

Proactivity

Gain proactivity with relevant and actionable data in real-time enhancing threat prevention

Speed

Accelerate decisions based on relevant insights and defining the appropriate adaptive countermeasures

Enhanced Security

Strengthen threat protection with CQF as an extra layer of fine-grained access control elevating security with integrated DNS Threat Pulse

efficient iP

REV: C-230515

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