efficient iP®

Datasheet

DNS Intelligence Center

DNS-centric Intelligence for Proactive Threat Detection and Investigation

Highlights:

- Insightful, actionable, and reliable DNS analytics and intelligence to proactively detect and effortlessly investigate potential threats
- Single-pane-of-glass visibility of malicious and suspicious domains matched in DNS enterprise traffic across the entire DNS architecture
- User-friendly interactive dashboards to easily search domain names and navigate historical data to instantly spot suspicious behavior and threat matches
- Cutting-edge, global data collection infrastructure for higher quality and relevance to build efficient DNS-centric Intelligence
- Highly-scalable, cloud-based, enterprise-grade infrastructure, offering a cost-effective analytics solution
- Comprehensive end-to-end solution in combination with DNS Guardian and DNS Threat Pulse for efficient threat prevention and accelerated remediation

Ever-growing and increasingly-sophisticated cyber threats, proliferation of devices, and today's diverse infrastructures are increasing the overall complexity of networks, making them difficult to protect. Threat intelligence has emerged as a pivotal aspect of cybersecurity defense, with 60% of organizations considering it vital to company strategy and defense against cyberattacks.

According to the 2023 IDC Threat Report, 90% of enterprises have experienced one or more DNS-based attacks and 85% of malware actors are using DNS to develop their attack. While DNS is actively abused by cybercriminals, DNS traffic includes rich DNS insights to help defend against threats upstream.

This is why organizations need to develop DNS-centric Intelligence. More specifically, they need to be able to detect and investigate malicious intent and suspicious behavior as early as possible, before it has an impact on their business. Addressing this need, DNS Intelligence Center (DNS IC) offers SOCs and security teams insightful, actionable, and reliable DNS analytics and intelligence accessible from a unified cloud-based visualization portal, helping organizations to proactively detect and investigate threats across multi-faceted networks.

DNS Intelligence Center at a Glance

The DNS IC portal allows organizations to view comprehensive, analyzed, and categorized data on domain names, including insights into suspicious domain behavior, so they can easily detect potential threats and efficiently investigate suspicious activity to take appropriate security measures. By matching the EfficientIP DNS Threat Intelligence database with enterprise DNS traffic and by analyzing suspicious domain behavior in the DNS data history, security teams can immediately identify potential threats and take proactive actions. With detailed domain name intelligence and analytics such as risk scoring and Indicators of Compromise (IoC), and domain behavior insights such as suspicious domain query rates and service failures, they can effortlessly investigate a domain name, quickly assess whether it is malicious or not, and rapidly decide on the course of action.

Leveraging a highly scalable cloud-based enterprise-grade infrastructure makes DNS IC reliable and sustainable over the long term. Its modern architecture is designed for continuous and large-scale collection and storage of DNS statistics across multiple servers, geographies, and networks. This massive amount of data is processed and classified using pioneering AI-based and mathematical algorithms to generate near real-time insights and analytics that users can access at their fingertips, from any device.

DNS IC can be used in combination with EfficientIP's DNS Guardian and DNS Threat Pulse, offering a comprehensive end-to-end solution for a proactive stance against cyber threats that includes prevention, detection, investigation, and remediation. Integration with the security ecosystem enables you to automate the security response and move towards a more holistic security infrastructure for greater agility.

DNS analytics and intelligence dashboards, available from a unified visualization portal

Key Features

Comprehensive DNS analytics and intelligence

DNS IC provides rich and insightful DNS analytics and detailed intelligence on domain names enabling security teams to view and assess what's inside DNS traffic. Information viewable includes:

Domain Reputation Analytics

- Number of malicious hits against the EfficientIP DNS Threat Intelligence database, total and per DNS server
- Threat Category
- Risk score ranging from A (low risk) to F (high risk)
- Host server IP address and country for a given Domain Name
- First and last seen date
- Presence in Threat Intelligence sources
- Top domains by category and subcategory
- Presence in major domain names lists
- Whois
- SSL certificate information
- Other DNS and web information (history of DNS records associated with a FQDN, other FQDNs associated with the same IP address, word map, website screenshot...)

DNS IC also provides comprehensive insights and analytics about domain and subdomain behavior based on historical DNS data, focusing on destination domains

Global Domains Behavior Statistics

- Number of public domains, newly locally observed domains, and detected suspicious domains
- List of suspicious and newly locally observed domains
- Domain distribution based on average query rate and observed sub-domains registration
- Top domains generating queries, sub-domains, ServFails and NxDomains, and high recursion time

Suspicious Domain Behavior Insights

- Details of recent queries
- Suspicious queries samples and rates
- Number of observed sub-domains over time
- Domain's behavior compared to global threshold
- Suspicious activity indicators such as ServFail, NXDomain and recursion time

Single-pane-of-glass visibility

From a centralized, unified portal available from any device, your security team has granular visibility down to individual DNS servers or across the entire DNS infrastructure. This visibility on intent and behavior accelerates your decision-making process i.e. do nothing, investigate, or report.

Interactive dashboards

From user-friendly, predefined dashboards including widgets, you can easily search, filter, and browse historical domain name information. It is also possible to zoom in and out with a visual timeline to spot trends and peaks, eliminate noise, and go deeper to find where the problem lies. Widgets can be embedded into third-party business applications for broader accessibility and monitoring.

Threat Detection

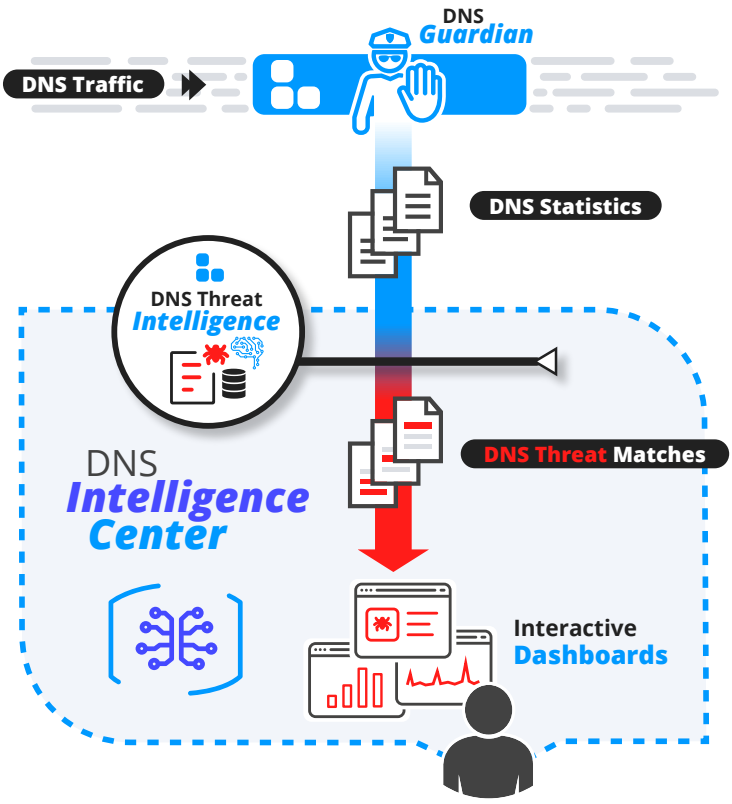
With DNS Intelligence Center, you can instantly point and identify malicious intent earlier. This is made possible thanks to two innovative cloud-based detection technologies:

1. **AI-Driven Reputation-Based Detection**

   Enterprise DNS traffic is matched with our unique DNS AI-Generated Threat Intelligence containing comprehensive, categorized, and active threats. This intelligence includes advanced ML-driven algorithms that utilize image recognition and Natural Language Processing (NLP) for phishing detection, along with tuple clustering for Domain Generation Algorithm (DGA) threat detection. DNS IC classifies matched occurrences into defined categories such as malware, phishing, or DGA. Through the interactive dashboard, you can obtain a more detailed breakdown for each detected threat, including the associated domain, category and other relevant information.

2. **DNS Suspicious Domain Behavior Detection**

   DNS traffic historical data is deeply processed with heuristic and mathematical algorithms over time to identify suspicious domain behavior that may indicate suspicious activities related to complex, active threats such as data exfiltration, DNS tunneling, or C2C. You can instantly view the list of detected suspicious domain names in the interactive dashboard, which is updated in near real-time to reflect the results of this continuous processing.



DNS IC Threat Detection for malicious intent identification

Threat Investigation

1. **Based on domain intelligence analysis**

   By browsing detailed metrics including whois and certificate, category, Indicators of Compromise (IoCs), location and Risk Scoring among other DNS, web, and site information, your SOC and security teams can efficiently investigate, complete root cause analysis, and assess the level of risk associated with a domain name.

2. **Based on domain behavior analysis**

   Accessing deep, fact-based insights into domain behavior enables SOC teams to investigate the domain's level of suspicion and confirm whether or not it is malicious and associated with a threat.

By correlating both domain intelligence and behavior insights, SOC and security teams can further accelerate investigations, enhancing response time and operational efficiency.

Simple deployment and access

As a cloud-based service, DNS IC is easy to set up, deploy, activate, and access once subscribed to. It can scale quickly by adding new DNS servers according to business needs. Relevant DNS statistics are instantly analyzed, aggregated, and displayed in dashboards.

High qualitative data processing

Comprehensive, volumetric DNS data and statistics are collected continuously across any devices, applications, and networks (on-premise, cloud or multi-cloud) at internet scale. They are combined with contextual information from the organization's DNS traffic to increase data relevance and quality. History and details on past as well as current behavior and intent are included. All of this forms a cutting-edge DNS Threat Intelligence database that is always up-to-date, relevant, and accurate. The data is then analyzed, curated, and processed leveraging AI-ML technology together with heuristic and mathematical algorithms to generate reliable DNS analytics.

Enterprise-grade platform

As it leverages a highly scalable enterprise-grade platform that uses modern cloud technologies, long-term reliability and sustainability of DNS IC is ensured. Its microservice architecture caters to any volume of DNS statistics whatever the customer's profile and distributed architecture. In addition, optimized data flow and storage make it a flexible and cost-effective alternative to dedicated hardware-based analytics solutions.

Complete End-to-End Solution

For advanced, global protection, DNS IC can be used in combination with DNS Threat Pulse, DNS Guardian and Client Query Filtering, allowing security teams to define, centrally manage, and deploy highly granular and flexible security policies by mapping domains, tags, client groups or even individuals. This comprehensive end-to-end solution enables behavioral threat protection and accelerated remediation using adaptive countermeasures, to protect against cyber threats, preventing infection and malicious activity.

Moving one step further, by integrating DNS intelligence with existing security tools, organizations can quickly correlate DNS domain names intelligence and analytics across various systems (SIEM, SOAR, NAC, TIP…), automate incident handling for a more adapted response, and reduce MTTR for greater business resilience. This brings you closer to a more integrated security infrastructure, gaining agility and overall efficiency.

By adding DNS IC to your security ecosystem, you take a proactive stance against any anomalies on network utilization, behavior, and intent that can impact security, compliance, and service continuity.

Key Benefits

Improved Visibility

Increase network visibility with insightful, actionable, and reliable DNS analytics and intelligence data

Efficient Threat Investigation

Efficiently Investigate suspicious behavior using consolidated DNS analytics and intelligence to speed up appropriate remediation

Active Threat Detection

Actively detect suspicious and malicious intent in corporate DNS traffic by pinpointing classified threats and identifying suspicious behavior in domains

Enhanced Security Posture

Fuel DNS-centric Intelligence, strengthen threat prevention and protection, and build a more integrated security infrastructure

efficient iP®

REV: C-241023

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