efficient iP™
DEFINING SMART DDI

Product Documentation

DNS Guardian

Detect - Protect- Remediate

Highlights

- Detection, protection and remediation features for DNS cache and recursive
- Service continuity with 100% DNS cache availability
- Hardened security framework: cache and recursive partition
- Real-time DNS transaction analysis for accurate decision-making
- Identification of DNS attack signatures
- Counter measures specific to each type of attack
- Remediation to root cause
- Advanced DNS statistics for smarter reporting
- Patented Security Solution

Recent years have seen a huge increase in attacks against DNS services: an increase in volume, in size, in diversity and in complexity. DNS servers are key targets for attackers to impact company business. Hackers exploit each time new vulnerabilities, with more and more sophisticated attacks to bypass security measures in place. Among them you will find volumetric attacks (typically DDoS, Amplification and Reflection attacks) and insidious or slow attacks, such as «water torture», Phantom and Sloth attacks.

Each attack targets a specific part of the DNS server, so each attack requires specific counter-measures. Existing DNS security solutions have proved to be insufficient against new attacks and even worst, present high risk of creating false positives. That is mostly because they are not specific enough to the DNS functions and do not analyze the traffic at the DNS transaction level to fire the right counter measures.

Thanks to key technological breakthroughs, EfficientIP has developed DNS Guardian, a unique and innovative DNS security solution for cache servers that provides a case-by-case approach of DNS threats to ensure protection and service continuity.

DNS Guardian: Detect, Protect, Remediate

DNS Guardian offers in-depth analysis of DNS transactions to detect attacks, to protect with adapted counter measures and to remediate attacks by identifying their source. When a DNS cache server is attacked, DNS Guardian ensures service availability to the legitimate traffic, and this regardless of the type of the attack. DNS Guardian's capacity to protect against all kind of DNS threats relies on three key innovations.

Hardened Security Framework: Cache and Recursive Partition to Strengthen the DNS Service
DNS Guardian benefits from an architecture innovation that separates the DNS cache and recursive functions to dramatically strengthen and improve the security framework. When under attack, each function is protected separately, avoiding side effects and continuing to provide service. Counter measures can be adapted to each function and to each attack to be more efficient. It has also allowed us to develop a true DNS transaction analysis.

Full DNS Transaction Analysis to Take the Right Decision

Analyzing DNS transactions offers you unprecedented level of intelligence. DNS Guardian collects in real-time all data related to DNS traffic between the cache and the recursive functions allowing you to understand the transactions from the inside and take the right decision. You can detect the particular signature of an attack such as DNS tunnelling, a Phantom or a sloth domain attack, and activate the right counter measure to protect your DNS services.

Rescue Mode: 100% Cache Availability Whatever the Type of Attack!

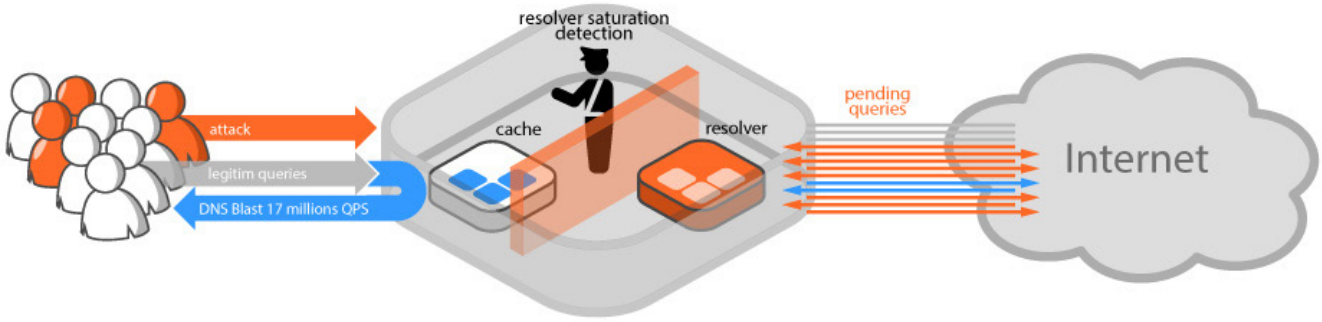
The Rescue Mode is a key innovation and is one of the available counter measures with DNS Guardian.
The Rescue Mode is based on DNS Guardian's intelligence and mitigates volumetric and insidious attacks on recursive and cache functions. Today, a lot of attacks aim at saturating the recursive function, which brings down the cache and makes the service unavailable. Thanks to the separation of the two functions, when the recursive is attacked, the cache keeps working. DNS Guardian detects the attack and activates the Rescue Mode counter measure to ensure that cache data remains 100% available to clients until the end of the attack. The recursive function works on best effort.

Quick Remediation with Source Identification and Advanced DNS Statistics

DNS Guardian monitors DNS activity at the transaction level (queries, responses, fragments, recursions), especially under volumetric attacks to provide unique out of the box statistics. DNS Guardian's DNS data collection and analysis allow you to easily and quickly identify the source of the attack and take action for immediate remediation. For example, cleaning PCs infected with botnets or warning customers that their PCs are infected.

DNS Guardian offers unparalleled diversity for statistics and top lists, at the global and IP address level:
- Global miss cache
- Global hit cache
- Bandwidth consumption
- Top IP address miss cache
- Top IP address NXDOMAIN
- Top IP address SERFAIL
- Top requested domains
- Top IP address latency recursion

No additional appliance is required to collect statistics and make reports.



ABOUT EFFICIENTIP

EfficientIP solutions address organizations' needs to drive business efficiency through the innovative use of IT. Its unified management framework for DNS-DHCP-IPAM, devices and network configurations enhances security, availability and agility of the IT infrastructure. EfficientIP's solutions have been chosen by hundreds of the most demanding organizations across all industries.
www.efficientip.com

EUROPE

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

USA

EfficientIP Inc.
17 Wilmont Mews, Suite 400
West Chester, PA 19382
+1 888-228-4655