efficient iP™
DEFINING SMART DDI

Solution Paper

Secure Your Business, Secure Your DNS

Key Takeaways

- Ensure business continuity through adaptive security with DNS Guardian
- Block zero-day vulnerabilities with Hybrid DNS Engine
- Mitigate amplification and reflection threats with DNS RRL
- Protect against malware and phishing with DNS Firewall (RPZ)
- Mitigate internet DNS DDoS attacks and maintain resiliency with DNS Cloud
- Ensure authenticity and integrity of DNS services with DNSSEC Automation
- Absorb extreme DDoS cache attacks with DNS Blast

Why Traditional Security Solutions Are Not Good Enough To Protect DNS Services

As a consequence of their fundamental role in the IT infrastructure, DNS servers must be accessible to everyone- making them a prime target for hackers who make use of their dual role in the "kill-chain" as either a threat vector (protocol) or a direct objective (servers). Surprisingly, while the entire internet and its overall services such as browsing, emailing, ToIP, or even printing rely on DNS, its infrastructure remains poorly secured.

A 2016 EfficientIP global DNS security survey highlights that 74% of the respondents have been targeted by a DNS attack at least once in the last 12 months.

As a result, their businesses have been impacted the following ways: 40% were impacted by downtime, 15% suffered intellectual property theft, and 21% reported loss of business.

IDC, in a recent security survey, concluded that "very little is being done about DNS security and companies feel that the basic protection offered by a firewall is enough. This is a real case of the wrong answer to a real problem. Firewalls are not the right technology to fight zero day vulnerabilities on DNS servers or when they are under DNS DDoS attack, as they will have no effect". A brand new and comprehensive approach must be integrated into the network security plan to efficiently protect DNS services and users from attacks and threats hidden within the DNS traffic. This is even more of an issue considering the evidence found by Forrester, who states the biggest threat to digital security comes from the inside of the network, with almost 40% of breaches perpetrated from inside a company.

Taking A Holistic Approach To DNS Threats With A 360° Security Solution

Hackers aim to target public and private DNS servers or abuse the way the DNS protocol works to infiltrate the network, disrupt business or steal confidential data.

DNS threats have become more and more sophisticated, combining multiple vectors in a single attack, in a continuously evolving landscape. However, DNS attacks can still be classified in three main categories:

- Volumetric attacks, typically DDoS, amplification and reflection attacks
- Insidious or slow attacks, such as slow-drip «water torture», NX domain and sloth domain attacks
- Attacks using bugs and/or flaws in DNS services, such as zero-day vulnerabilities and DNS tunneling

EfficientIP innovations offer a purpose-built layer of in-depth-defense to fill the gap left by traditional security solutions to tackle theses DNS security threats. The unique EfficientIP 360° security protects your public and private DNS from both internal and externals threats, regardless of attack type.

This innovative solution includes the following components: SOLIDserver™ Hybrid DNS, DNS Guardian, DNS Cloud, DNS Firewall, and DNS Blast.

DNS Guardian: Adaptive Security To Ensure Business Continuity

DNS Guardian offers adaptive security to DNS cache services by detecting attacks, and activating adapted countermeasures to ensure DNS services continuity and attack mitigation. DNS Guardian's unmatched security capacities rely on three key innovations:

Cache and Recursive Partition

DNS Guardian benefits from an innovative architecture 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 negative side effects to ensure service continuity.

Advanced DNS Transaction Analysis

Analysis of DNS transactions answered directly from the cache or going through the recursive function offers you unprecedented level of intelligence. This ensures an unmatched ability to detect advanced attack patterns such as DNS tunneling, phantom or a sloth domain attacks. This offers you the opportunity to activate the right countermeasure at the right time to protect your DNS services.

Adaptive Countermeasures For 100% Availability

The greater sophistication of attacks requires countermeasures more intelligent than merely blocking DNS traffic from supposed malicious IP sources. What will happen when the attack source is unidentifiable? How important is the risk of blocking legitimate clients? A modern DNS security system must be agile enough to adapt its protection mechanisms to mitigate the risk of false positive, while ensuring the service continuity to legitimate clients.

DNS Guardian offers graduated, adaptive countermeasures with three distinct automated modes of protection:

- Block Mode: Every query coming from the IP source of the attack is blocked.
- Quarantine Mode: For the IP source of the attack, only queries that are already in the DNS cache will be answered.
- Rescue Mode: When the source of the attack is not identifiable, patented Rescue Mode is activated on the cache function to ensure that cache data remains 100% available to clients until the end of the attack.

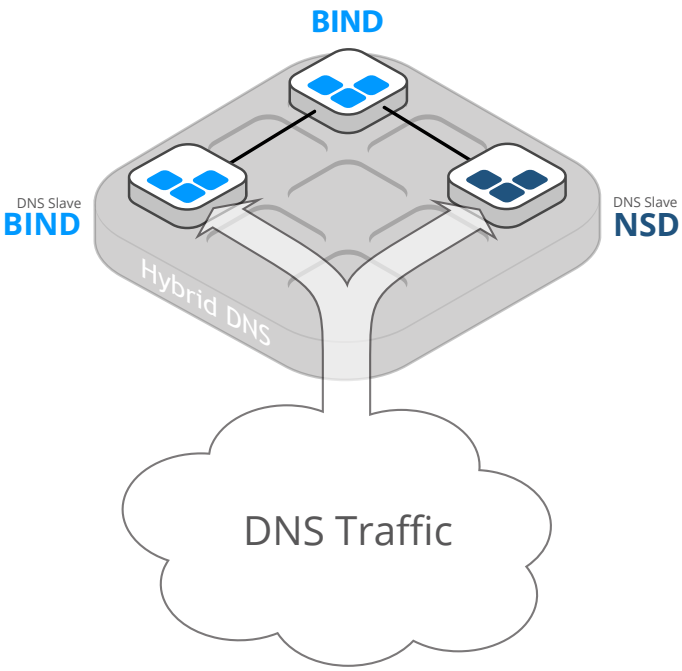
Thanks to DNS Guardian innovations, the entire family of slow-drip flooding attacks is detected, mitigated and remediated- from those that already exist to unknown or future threats. DNS Guardian's patented security mechanisms ensure a unique level of service continuity, even while under attack from an unidentifiable source.

Hybrid DNS Engine, The Ultimate Answer Against DNS Zero-Day Vulnerabilities

In 2015, more than 11 major security vulnerabilities have been published on the most popular DNS engine, BIND. Since the first quarter of 2016, 4 new major security alerts were published, including one that could kill a BIND DNS server with a simple query. These threats make using several DNS technologies a "must have" as a security best practice for sound network infrastructures.

The Hybrid DNS Engine provides the highest level of security against zero-day vulnerabilities. SOLIDserver Hybrid DNS offers two different technologies in one appliance, easily and transparently managed as a single entity (BIND & NSD/Unbound). This simplifies the deployment of hybrid DNS architectures, and ensures the compliance to fundamental security best practices, eliminating single point of failure.

When a security alert affects name server software, Hybrid DNS Engine provides an alternative name server software- one that is not exposed to the threat- to which you can switch with a single click. Your DNS service continues normally, and you revert to using the original name server software only after its vulnerability has been patched, tested and verified. For administrators, this means increased agility and smarter risk management for security threats.



Secure Your Internet Visibility With Hybrid Cloud DNS

A customer's online experience with a company's brand is highly dependent on the performance, resiliency and availability of its public DNS infrastructures. First impression is everything- make sure it will be a good experience.

The EfficientIP hybrid Cloud DNS offers a unique solution to extend your DNS services on the global Amazon Route 53 network. In a few easy steps, your DNS services are distributed across a series of worldwide locations. The SOLIDserver DDI appliance centrally manages your in-house DNS servers and your Domain Name in the cloud from a single pane-of-glass.

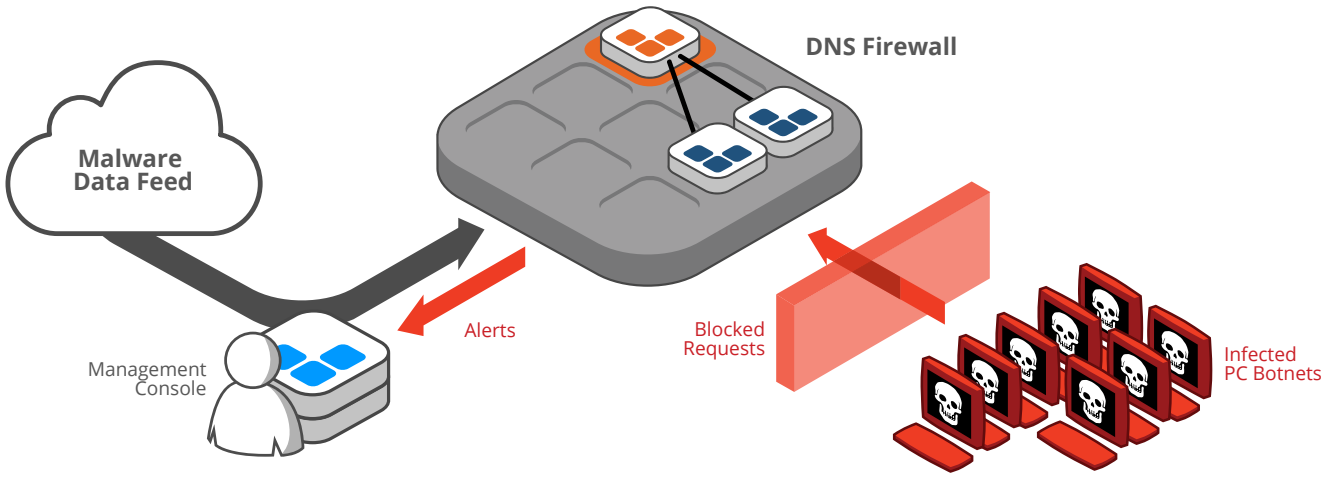
The DNS Cloud solution offers you the best performance and resilience that you can expect with a service level agreement of 100%[1]. Thanks to a unique anycast IP address and worldwide DNS spots, Amazon's DNS infrastructure ensures unmatched service availability and scalability, and a greater user experience for your customers, even during a DDoS attack.

DNS Firewall (RPZ): Protect Against Malware and Phishing

More than 91% of malware uses DNS services to build attacks[2]. The DNS protocol plays multiple key roles in this kill-chain, from enabling the initial infection and exfiltration of confidential data, to communication with the C&C (Command and Control) server for DoS attack synchronization. The velocity and low volume of involved traffic, deeply hidden into DNS layer as legitimate flow, make it almost impossible for a firewall, antivirus program or other non-specialized solution to quickly detect the attacks.

The EfficientIP DNS Firewall solution offers a dedicated layer of defense to monitor and analyze DNS traffic, protecting users and infrastructures against DNS-based malware. The SOLIDserver appliance offers advanced management of response policy zone (DNS RPZ) based upon dynamic reputation data feed and manual configuration, to ensure an up-to-date list of malicious or forbidden IP addresses, domains, URLs, or name servers.

DNS Firewall prevents users from the initial infection by blocking requests to malicious domain names. It identifies malware activity, blocking C&C callbacks or data exfiltration, and locates compromised devices on the network.



DNS Firewall policies are deployed from a single management platform on multivendor DNS environment, SOLIDserver appliances and Linux-based DNS infrastructures.

DNS Blast: Absorb Extreme DDoS Attacks On Cache DNS

The World's Fastest DNS Cache Server

During a DoS attack, the hacker attempts to kill the DNS server so that legitimate queries cannot be answered. Your DNS service must be powerful enough to receive and carefully analyze all the requests it is sent, in order to make sure that legitimate requests are answered- even when mixed in with huge numbers of attack queries. DNS performance acts as a strong layer of defense.

DNS Blast is a cache appliance that can support up to 17 millions queries per second. It can most likely handle more bandwidth than the actual network itself, therefore ensuring cache service capacity to reply will never be saturated.

With the SOLIDserver DNS Blast appliance from EfficientIP, you can confidently provide the DNS service your business deserves. By eliminating dozens of DNS clusters and load balancers, you can dramatically decrease the total cost of ownership, simplify your DNS infrastructure, and achieve a higher level of security.

Eliminate The Risk Of Data Corruption With DNSSEC

DNSSEC is a standard protocol (IETF) allowing customers to solve DNS protocol security problems. It eliminates all risk of DNS cache poisoning. With SOLIDserver, EfficientIP automates and simplifies DNSSEC implementation by providing a centralized and unified approach to DNS service management.

EfficientIP partners with Thales to provide a highly secure DNSSEC solution. Thales' HSM appliances integrate with SOLIDserver™ appliances to secure the cryptographic mechanisms used for DNSSEC signatures.

Apply DNS Best Practices Through SmartArchitecture™

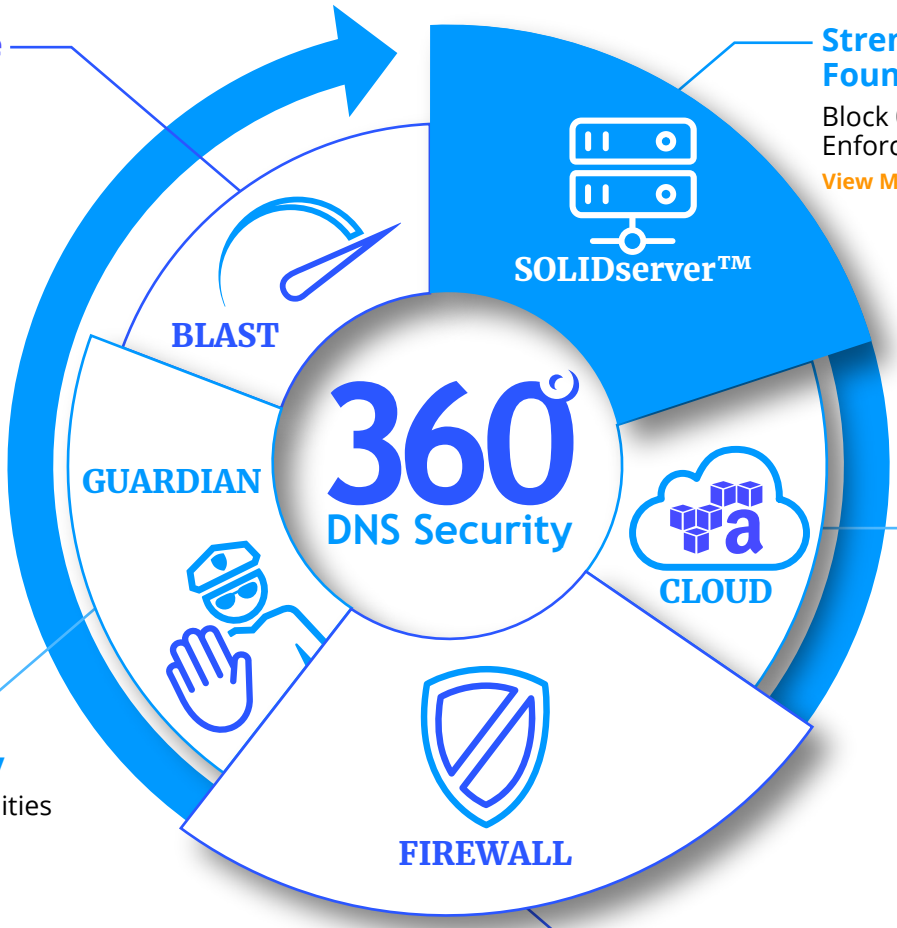
SmartArchitecture™ is a library of state-of-the-art templates of DNS-DHCP architectures, applied on a group of servers (Microsoft®, Open source, Amazon Route 53, SOLIDserver) to easily and automatically design, deploy and manage your architectures with security best practices enforcement.

The SOLIDserver centralized management platform will automatically configure all DNS servers according to their individual role within the selected architecture template. It is no longer necessary to manually configure each server in order to build the architecture; the entire process is now carried out automatically. For example, you can easily deploy stealth architecture, hiding the primary server to limit the risk of being attacked.

[1] See Amazon Route 53 Service Level Agreement

[2] Cisco 2016 Security Report

Secure Your Business
Secure Your DNS



Absorb Extreme DoS Attacks on Cache Servers
Cache Security & Performance
View More >

Strengthen Security Foundation
Block 0-Day Vulnerabilities
Enforce Best Practices
View More >

Secure Internet Visibility
Resiliency & Robustness
View More >

Ensure DNS Continuity with Adaptive Security
Block 0-Day Vulnerabilities
Enforce Best Practices
View More >

Protect Users & Block DNS-Based Malware Activity
Prevent, Detect & Mitigate
View More >

About EfficientIP:
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 world-wide 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.
17 Wilmont Mews, Suite 400
West Chester, PA 19382
+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
16 Raffles Quay #38-03
Hong Leong Building
Singapore 048581