# SECURE YOUR BUSINESS SECURE YOUR DNS

## Enhanced DNS infrastructure Security

## 360° DNS Security

- Adaptive Security to Ensure Business Continuity with DNS Guardian
- Block Zero-Day Vulnerabilities with Hybrid DNS Engine
- Mitigate Amplification & Reflection Threats wiht DNS RRL
- Protect Against Malware and Phishing with DNS Firewall (RPZ)
- Internet DNS DDoS Attack Mitigation & Resiliency with DNS Cloud
- Authenticity & Integrity of DNS Services: DNSSEC Automation
- Absorb Extreme DDoS Cache Attacks with DNS Blast

DNS servers deliver critical services to your company, such as internet accessibility for your customers, partners and employees as well as access to network applications and other indispensable services such as email, CRM, VoIP, services in the Cloud...

As a consequence of their fundamental role in the Information Technology infrastructure, DNS servers are visible and vulnerable to everyone. They are playing a dual role in the "kill-chain", as a threat vector and as a favorite target.

DNS attacks are more and more sophisticated, combining multiple attack vectors at the same time and the DNS landscape security is continuously moving. There are different types of DNS attacks:

- Volumetric attacks, typically DDoS, Amplification and Reflection attacks.
- Insidious or slow attacks, such as «water torture», Phantom and Sloth Domain attacks .
- Attacks using bugs and/or flaws in DNS services or on operating system running DNS services.

An IDC DNS Security survey conducted in June 2014 shows that 72 % of respondents said they had been targeted by a DNS attack in the last 12 months. As a result, their businesses reflected the following: 45% were impacted by downtime, 36% reported loss of business, and 40% had intellectual property stolen.

IDC 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".

## Detect, Protect & Remediate DNS Attacks with 360° Security Solution

EfficientIP offers a specialized layer of in-depth-defense to fill the gap left by traditional security solutions to tackle DNS security threats.

EfficientIP's unique 360° security solution protects against any type of attacks for both public and private DNS infrastructures. The 360° security solution includes the following solutions: DNS Guardian, DNS Blast, SOLIDserver Hybrid DNS Engine, DNS Cloud and DNS Firewall.

## DNS Guardian: Adaptive Security to Ensure Business Continuity

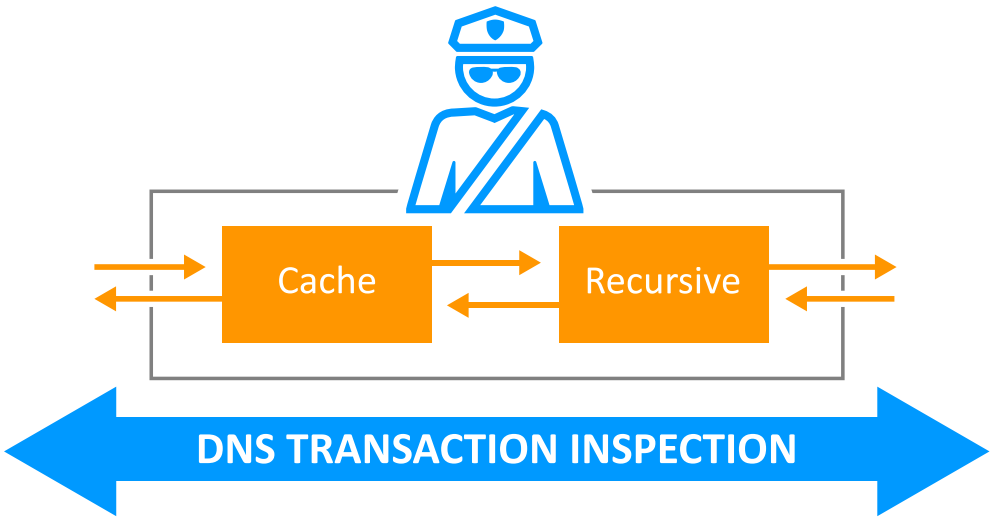
DNS Guardian offers adaptive security to DNS cache services by detecting attacks, identifying them and activating adapted counter measures. DNS Guardian's unmatched security capacities rely on three key innovations.

### Cache and Recursive Partition

DNS Guardian benefits from an architecture innovation that separates the DNS cache and recursive functions to dramatically strengthen and improve the security fra- mework. When under attack, each function is protected separately, avoiding side effects and continuing to provide service.

### Advanced Transaction Analysis

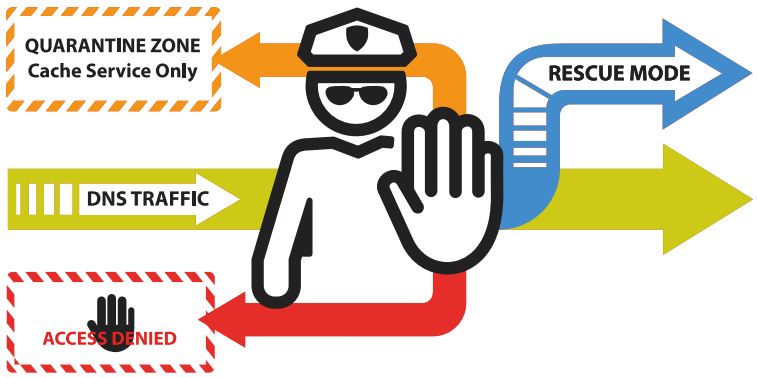
Analyzing DNS transactions offers you unprecedented level of intelligence. You can detect the particular signature of an attack such as DNS tunnelling, a Phantom or a sloth domain attack, and activate the right counter measure to protect your DNS services.



### Adaptive Counter-Measures for 100% Availability

DNS Guardian embeds three types of counter-measures:

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




## Hybrid DNS Engine, the Ultimate Answer Against DNS Zero-Day Vulnerabilities

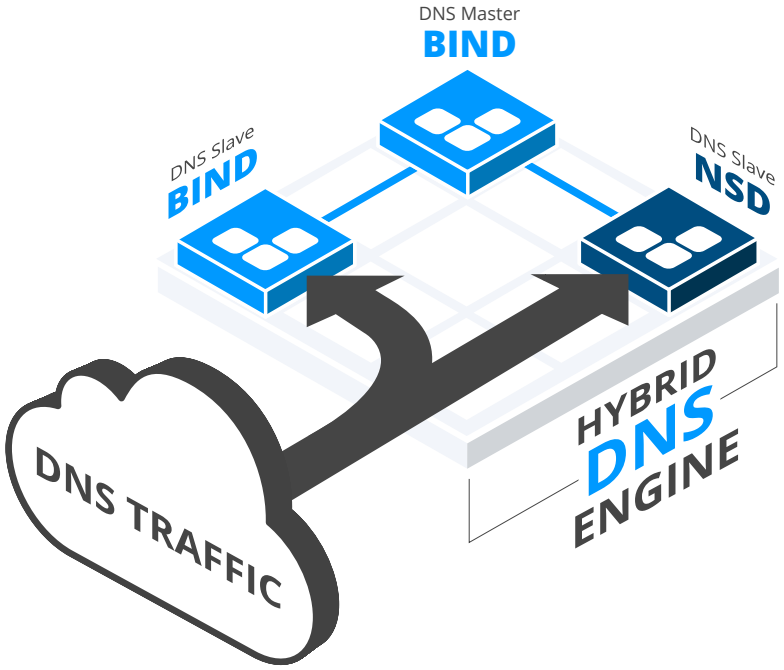
Using several technologies for the same objective is a common security best practice for network infrastructures. Hybrid DNS Engine provides the highest-level of security against Zero-Day vulnerabilities.

When a security alert or actual cyber attack affects your currently running name server software, Hybrid DNS Engine gives you an alternative name server software that you can switch to 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, it means better agility & risk management to security threats. Hybrid DNS Engine provides greater security, less risk, better performance, and easier administration.

## Secure Internet DNS Infrastructure with Hybrid Cloud Deployment

If you need more security and the best performance for your Internet DNS infrastructure, you can choose to deploy a Hybrid Cloud DNS Infrastructure. You will centrally manage your in-house DNS server and your Domain Name in the Cloud. EfficientIP's DNS Cloud is the only solution that integrates the Route 53 offering from Amazon Web Services, providing you with the ability to manage local and cloud DNS infrastructures from a single management console.

DNS Cloud includes all standard route 53 features. Cloud DNS deployment offers you the best performance and resilience that you can expect with a service level agreement of 100%. Thanks to a unique IP address anycast and 52 DNS spots distributed across the world, Amazon's DNS infrastructure ensures service availability to your end users, even during a DDoS attack. DNS Cloud is scalable, simple to deploy, cost effective, flexible and very secure.




## DNS Firewall (RPZ): Protect Against Malware and Phishing

DNS-based malwares are particularly dangerous as they're used to steal critical data, from you and from your customers.

EfficientIP's DNS Firewall proactively protects users by detecting and blocking malware activity, identifying infected devices and preventing new attacks. EfficientIP's DNS Firewall protects 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 DDoS attack, the hacker tries to kill the DNS server so that legitimate queries can't be answered. Your DNS server must be powerful enough to receive and to carefully analyze all requests sent to it, in order that legitimate requests are answered even when mixed in with huge numbers of attack queries.

DNS Blast is a cache appliance that can support up to 17 millions queries per second. It can handle more bandwidth than the network itself; therefore, the cache will never be saturated.

With EfficientIP's SOLIDserver™ DNS Blast appliance, you can confidently provide the DNS service your business deserves. By eliminating dozens of DNS clusters and load balancers, you will dramatically decrease the total cost of ownership, simplify your DNS infrastructure, and increase a higher level of security. The DNS cache can also be synchronized between several EfficientIP DNS servers to increase performance and efficiency.

## Eliminate the risk of data corruption with DNSSEC

DNSSEC is a standard protocol (IETF) allowing customer to solve security problems of the DNS protocol. 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.

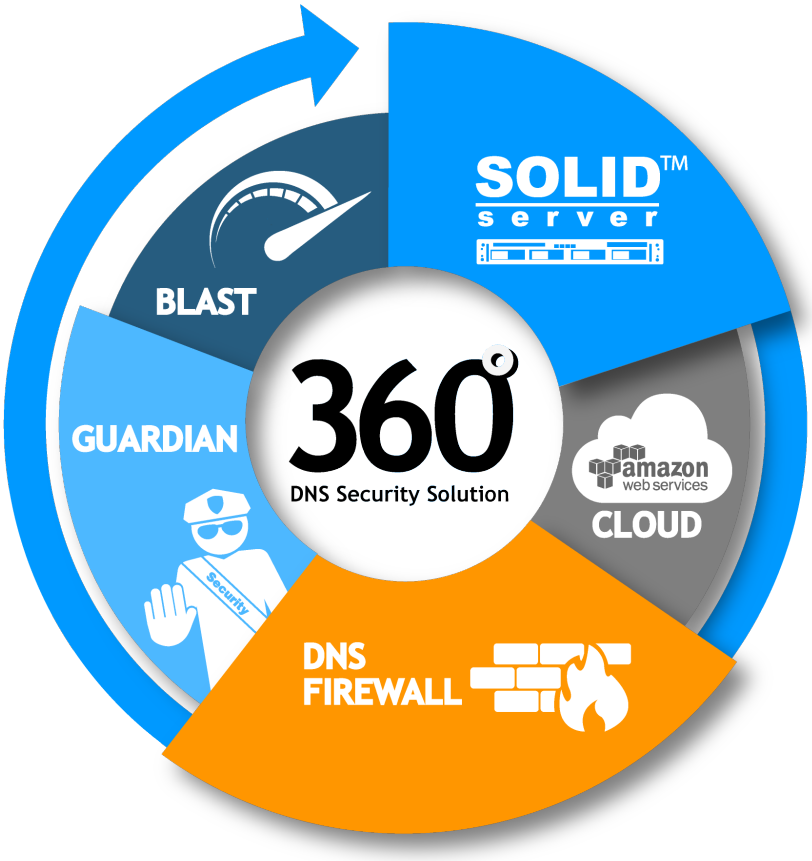
EfficientIP partners with Thales to provide a highly secure DNSSEC solution. Thales' HSM appliances integrate with SOLIDserver™ appliances to secure the cryptographic mechanisms used for DNSSEC signatures.

## Apply DNS Best Practices through Smart Architecture™

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.

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 a stealth architecture hiding the primary server to limit the risk of being attacked.

It is also strongly recommended to update BIND as often as possible to limit vulnerability exposure. EfficientIP releases security patches within 24 hours following the official publication of the vulnerability fix in order to ensure the highest level of security by running the latest version of BIND. These patches are available on EfficientIP's web site and customers are also notified via EfficientIP's customer mailing list.




efficient iP™

REV: B-1609

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.
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
101C Telok Ayer Street #04-00
SINGAPORE 068574
+65 6678 7752