efficient iP®

Solution Brochure

360° DNS Security:
Your First Line of Defense

Proactively Protect, Detect Early, and Effectively Respond to DNS Threats

- Deep DNS expertise and breakthrough threat detection with patented, innovative, and AI-driven algorithms.
- Comprehensive DNS-centric threat intelligence processing traffic on a global scale
- Advanced User-Based Application Access Control with Protective DNS Security offering innovative, highly granular DNS Filtering
- World's fastest DNS cache handling 17M queries/second with ultra-low latency
- Adaptive and Automated Response & Recovery minimizing risks, ensuring uninterrupted service
- Comprehensive Zero-Trust DNS Security integrating advanced filtering, observability, and continuous real-time DNS traffic analysis

The Need for 360° DNS Security

DNS servers are the backbone of modern network infrastructure, enabling essential services like email, internet, and cloud application access, which are crucial for business connectivity. However, as cyber threats grow more sophisticated, DNS servers have become prime targets and vectors for attacks.

Malware actors exploit DNS in 85% of cyber assaults, utilizing it as a conduit for malevolent activities spanning DDoS attacks, phishing, data exfiltration, and more. In 2023, 90% of organizations faced DNS attacks, averaging $1.1 million per attack. Traditional security solutions, such as Next-Generation Firewalls (NGFWs), often fall short in providing adequate protection against these specialized threats.

Furthermore, organizations grapple with escalating compliance pressures from regulations like GDPR, NIS 2 and DORA, requiring stringent DNS security measures. At the same time, increasing network complexity, driven by cloud migration and fragmented tools, creates visibility gaps and weakens security enforcement. Additionally, the underutilization of DNS data leaves organizations vulnerable to undetected threats.

A comprehensive 360° DNS Security strategy is essential to address these challenges, ensuring data protection, service continuity, and operational efficiency.

Protective DNS Security: Protect, Detect, Respond, and Recover

EfficientIP's 360° DNS Security is your DNS-centric first line of defense, empowering security and network teams to protect, detect, and respond to a wide range of DNS-based threats. This comprehensive, flexible, and robust solution enables security teams, SecOps, and SOCs to proactively secure their public and private DNS infrastructures across diverse networks and manage DNS attacks throughout their lifecycle, ensuring data protection, service continuity, and operational efficiency.

Proactively Protect

At the core of EfficientIP's DNS Security solution lies a hardened security foundation with built-in security mechanisms such as **Hybrid DNS Engine** switch or DNSSEC and the **world's fastest DNS cache**, to prevent the most severe DNS attacks like volumetric DDoS. As a **Protective DNS (PDNS)** solution, it provides standard and **advanced DNS filtering** capabilities with highly granular, data-rich, and client-based policy design to block malicious domains before they are ever resolved and accessed. Centralized management of these security policies simplifies deployment and enforcement, and ensures consistency across the enterprise for effective application access control. Combined with our comprehensive, up-to-date **DNS-centric threat intelligence** feed, this provides an additional layer of defense against malicious domains.

Early Detect

The DNS Security solution combines unique **DNS Traffic Inspection** (DTI) with **User Behavioral Analysis** and pioneering, **patented AI-driven algorithms** such as Tuple Clustering, Natural Language Processing (NLP), and image recognition, to detect attacks early, including the most sophisticated ones such as zero-day threats, DGAs, phishing, data exfiltration, DNS tunneling, command and control, and phantom or sloth attacks. This comprehensive approach empowers security teams to detect threats early, preventing even the most sophisticated attacks before they impact business operations.

Effectively Respond & Recover

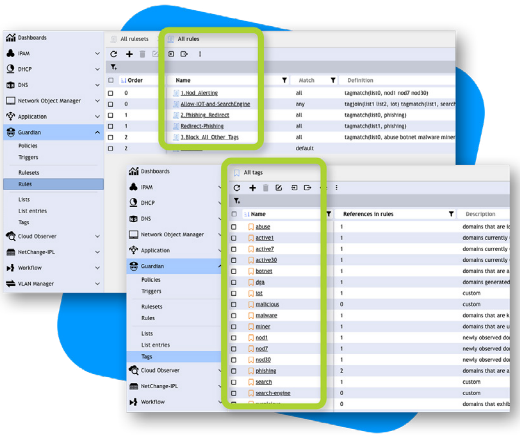
Based on threat analysis and pre-defined policies, the EfficientIP DNS Security solution effectively and dynamically responds to threats by providing graduated and **adaptive countermeasures**, such as quarantining suspicious IP addresses or protecting the cache service, to properly mitigate and thwart threats and ensure service uptime while virtually eliminating the risk of false positives. SOCs and SecOps can quickly investigate threats with **near real-time DNS analytics and intelligence**. By sharing **actionable DNS insights** via APIs or security events, the solution can seamlessly integrate with the security ecosystem tools such as SOAR, SIEM, or NAC to automate threat remediation, streamline security operations and workflows, and improve both response time and operational efficiency.

Use Cases for EfficientIP's 360° DNS Security Solution

EfficientIP's DNS Security solution provides comprehensive protection for organizations across various industries. Below are three key use cases that highlight the solution's effectiveness in addressing critical security challenges:

Enforce Zero Trust Access Control and Prevent Security Breaches

EfficientIP's DNS Security solution allows organizations to implement an advanced access control technology using DNS-centric threat intelligence feed and user roles, and prevent attacks at the frontline of the network, aligning with Zero Trust security framework principles.

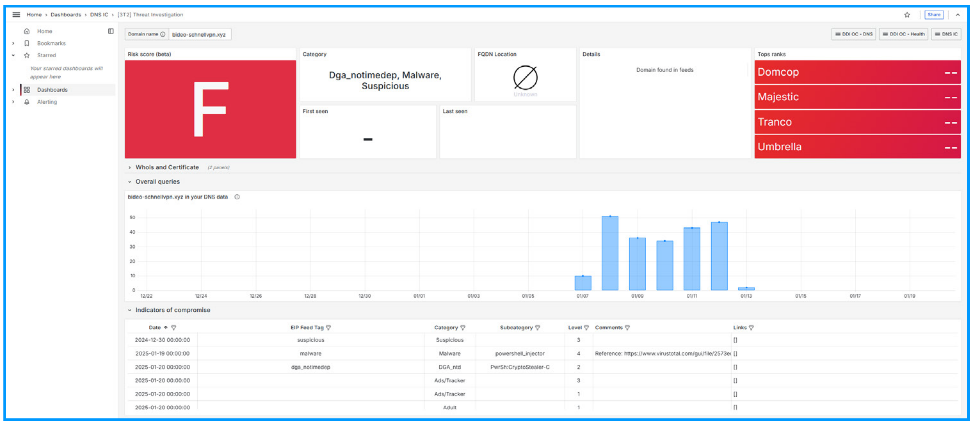


Order	Name	Match	Definition
0	1.Nod_Alerting	all	tagmatch(list0, nod1 nod7 nod30)
0	Allow-IOT-and-SearchEngine	any	tagjoin(list1 list2, iot) tagmatch(list1, search
1	2.Phishing_Redirect	all	tagmatch(list0, phishing)
1	Redirect-Phishing	all	tagmatch(list1, phishing)
2	3.Block_All_Other_Tags	all	tagmatch(list0, abuse botnet malware miner
2		default	

Name	References in rules	Description
abuse	1	domains that are i
active1	1	domains currently
active7	1	domains currently
active30	1	domains currently
botnet	1	domains that are a
dga	1	domains generated
iot	1	custom
malicious	0	custom
malware	1	domains that are k
miner	1	domains that are u
nod1	1	newly observed do
nod7	1	newly observed do
nod30	1	newly observed do
phishing	2	domains that are a
search	1	custom
search-engine	0	custom
suspicious	0	domains that exhib

Stop Threats Earlier, No Matter How Sophisticated

AI-driven engines combined with real-time deep DNS Transaction Inspection and User Behavioral Analysis early detect and block anomalies and malicious activities, including DNS tunneling, phishing, and zero-day attacks.



Domain name: bideo-schnellvpn.xyz

Risk score (beta): F

Category: Dga_notimedep, Malware, Suspicious

FQDN Location: Unknown

Details: Domain found in feeds

Tops ranks

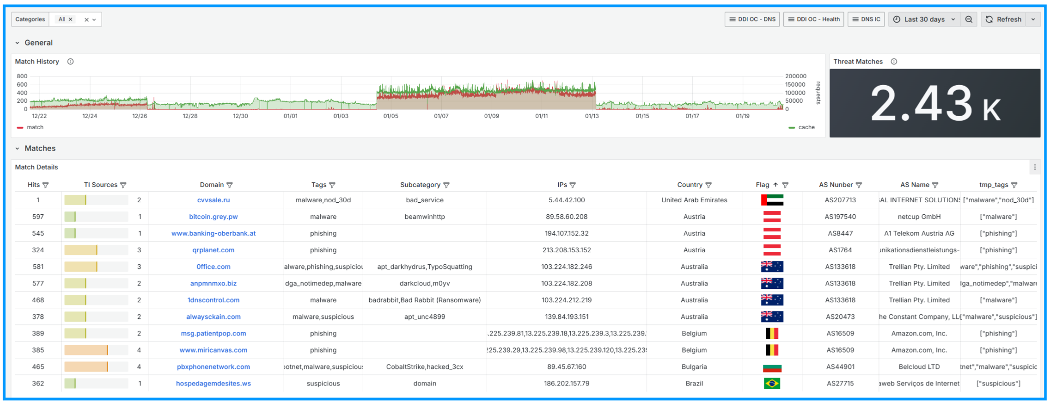
First seen: -

Last seen

Date	EIP Feed Tag	Category	Subcategory	Level	Comments	Links
2024-12-30 00:00:00	suspicious	Suspicious		3		[]
2025-01-19 00:00:00	malware	Malware	powershell_injector	4	Reference: https://www.virustotal.com/gui/file/2573e	[]
2025-01-20 00:00:00	dga_notimedep	DGA_ntd	PwrSh:CryptoStealer-C	2		[]
2025-01-20 00:00:00		Ads/Tracker		3		[]
2025-01-20 00:00:00		Ads/Tracker		1		[]
2025-01-20 00:00:00		Adult		1		[]

Accelerate Incident Response and Remediate Threats Faster

Patented Adaptive countermeasures, such as IP blocking and Rescue Mode, enables the activation of the right defense at the right time according to the attack type. DNS intelligence and analytics streamline threat investigation, and seamless integration with security systems such as SOAR and SIEM enables automatic threat remediation.



Threat Matches: 2.43 K

Hits	TI Sources	Domain	Tags	Subcategory	IPs	Country	Flag	AS Nunber	AS Name	tmp_tags
1	2	cvvsale.ru	malware,nod_30d	bad_service	5.44.42.100	United Arab Emirates	🇦🇪	AS207713	AL INTERNET SOLUTIONS	["malware","nod_30d"]
597	1	bitcoin.grey.pw	malware	beamwinhttp	89.58.60.208	Austria	🇦🇹	AS197540	netcup GmbH	["malware"]
545	1	www.banking-oberbank.at	phishing		194.107.152.32	Austria	🇦🇹	AS8447	A1 Telekom Austria AG	["phishing"]
324	3	qrplanet.com	phishing		213.208.153.152	Austria	🇦🇹	AS1764	unikationsdienstleistungs-	["phishing"]
581	3	0ffice.com	alware,phishing,suspiciou	apt_darkhydrus,TypoSquatting	103.224.182.246	Australia	🇦🇺	AS133618	Trellian Pty. Limited	ware","phishing","suspici
577	2	anpmnmxo.biz	dga_notimedep,malware	darkcloud,m0yv	103.224.182.208	Australia	🇦🇺	AS133618	Trellian Pty. Limited	lga_notimedep","malware
468	2	1dnscontrol.com	malware	badrabbit,Bad Rabbit (Ransomware)	103.224.212.219	Australia	🇦🇺	AS133618	Trellian Pty. Limited	["malware"]
378	2	alwaysckain.com	malware,suspicious	apt_unc4899	139.84.193.151	Australia	🇦🇺	AS20473	he Constant Company, LL	["malware","suspicious"]
389	2	msg.patientpop.com	phishing		.225.239.81,13.225.239.18,13.225.239.3,13.225.239.	Belgium	🇧🇪	AS16509	Amazon.com, Inc.	["phishing"]
385	4	www.miricanvas.com	phishing		225.239.29,13.225.239.98,13.225.239.120,13.225.23	Belgium	🇧🇪	AS16509	Amazon.com, Inc.	["phishing"]
465	4	pbxphonenetwork.com	otnet,malware,suspiciou	CobaltStrike,hacked_3cx	89.45.67.160	Bulgaria	🇧🇬	AS44901	Belcloud LTD	tnet","malware","suspicic
362	1	hospedagemdesites.ws	suspicious	domain	186.202.157.79	Brazil	🇧🇷	AS27715	aweb Serviços de Internet	["suspicious"]

Benefits of EfficientIP’s Protective DNS Security Solution

Faster and Deeper Threat Detection:

Quickly and comprehensively identify increasingly sophisticated cyber threats such as malware, phishing, cache poisoning, DDoS attacks, data exfiltration through zero-day malicious domains, DNS tunneling, command and control exchanges, phantom or sloth attacks, or DNS hijacking, with breakthrough technologies and lay the foundation for predictive security.

More Effective Threat Response:

Respond to threats more effectively with patented adaptive countermeasures defined by threat analysis like blocking IP addresses, quarantining suspicious devices, or activating specific measures such as Rescue Mode, protecting cache service continuity. Seamless integration with the security ecosystem (e.g., SOAR, SIEM, NAC) enables automated threat remediation.

Elevated Security Posture:

Safeguard networks, apps, data, and users from internal and external DNS-based threats Comprehensive and protective DNS Security goes beyond traditional signature-based security systems to ensure that organizations are shielded against even the most sophisticated and evolving threats, contributing to Zero Trust architectures and a more holistic and integrated security infrastructure for increased resilience.

Enhanced Service Continuity:

Ensure service continuity through global, intelligent, and scalable DNS-layer protection, including hardened security framework by design, high-performant DNS with fastest cache and cache service protection, and effective threat response leveraging adaptive countermeasures and integration with the ecosystem. This helps mitigate threats, minimize business disruption, and restore operations in disaster cases.

Increased Operational Efficiency:

Automated threat detection, response, and recovery, including with the security ecosystem thanks to rich plug-in library, APIs, and security events sharing, streamlines security operations and workflows, reduces manual intervention, and saves time. This lowers the burden on security teams and enhances incident response times. It empowers security and network teams to collaborate, breaking down silos and increasing efficiency.

Improved Risk Management and Compliance:

Improve risk management and ensure compliance with regulations such as NIS 2, NIST 2.0, DORA, GDPR, HIPAA, and PCI-DSS with robust DNS threat prevention and detection, continuous monitoring for in-depth visibility, incident handling, and detailed reporting to better manage and minimize cyber risks, strengthen defenses, and enhance cyber resilience.

360° DNS Security: An Advanced Product Suite

EfficientIP's 360° DNS Security solution comprises a suite of advanced products:

SOLIDserver DNS Service

The SOLIDserver DNS Service lays the foundation for robust DNS services with built-in advanced security mechanisms that ensure availability and security including hybrid DNS technology, DNSSEC, and DNS firewall leveraging RPZ.

DNS Guardian

As EfficientIP's flagship security product, it delivers advanced DNS security with patented DNS Transaction Inspection (DTI), User Behavioral Analysis (UBA), patented countermeasures, and seamless integration with security ecosystems for comprehensive protection and service continuity.

DNS Threat Pulse (DTP)

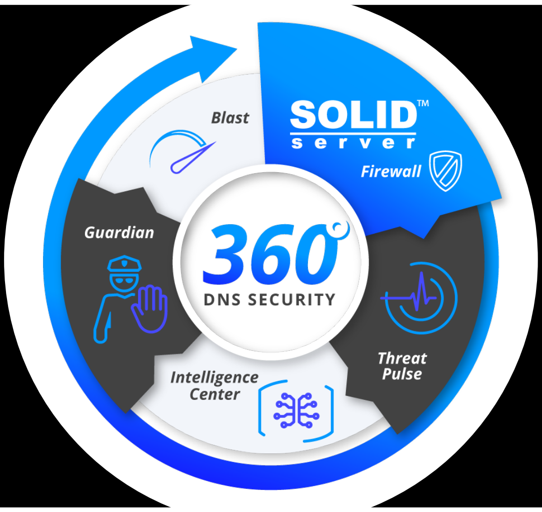
DNS Threat Pulse offers comprehensive, accurate, up-to-date DNS threat intelligence powered by AI. When paired with DNS Guardian, it enhances access control using RPZ or CQF formats, ensuring streamlined risk management and proactive defense against DNS cyber threats globally.

DNS Intelligence Center (DNS IC)

DNS IC provides insightful, actionable, and reliable DNS analytics and detailed domain information from a unified cloud-based visualization portal to address the need of DNS-centric intelligence, helping security teams to quickly detect and investigate threats across networks.

DNS Blast

DNS Blast offers carrier-grade, high-performance DNS Security combining the world's fastest DNS cache appliance with the most advanced built-in security features to protect against the largest spectrum of DNS attacks including extreme volumetric DDoS attacks, ensuring service availability and improving user experience with ultra-low latency.



Together, these products provide a comprehensive DNS security solution that ensures robust, end-to-end DNS security, empowering multiple teams to collaborate effectively in threat mitigation and incident response, enforcing Zero Trust principles.

With market-leading DNS expertise and innovative technology, EfficientIP's 360° DNS Security comes fully integrated as part of SOLIDserver™ DDI. Highly scalable and flexible, it meets all customer requirements and architectures, spanning on-premises, cloud, and hybrid. Thanks to its enterprise-grade cloud platform, the solution leverages AI-based data collection, processing, and analysis at Internet scale. Recognized by analysts, 360° DNS Security is a strong weapon in cybersecurity defense and an essential component of modern networks.

efficient iP®

REV: C-240521

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