White Paper

iSafer DNS Booster:

Revolutionizing Cybersecurity at the Endpoint DNS Level

In a landscape where most enterprises rely on Next-Generation Firewalls (NGFW) as the cornerstone of their cybersecurity infrastructure, the ever-evolving digital landscape presents new challenges. Malicious actors leverage sophisticated tools, such as AI-generated variations, creating threats that NGFWs alone may not promptly address. Recognizing this, iSafer DNS Booster emerges as the agile solution, fortifying security gateways against blind spots.

DNS, the fundamental protocol for existing online services, faces threats on the front lines of internet connectivity. Traditional DNS architectures lacked automated and intelligent security defenses, leading to a surge in attacks.

iSafer DNS Booster addresses this gap with a tailored solution, actively filtering and blocking threats at the endpoint, surpassing NGFW capabilities. It controls and defends against DNS activities on all connected terminals, offering rapid and cost-effective cybersecurity without the need for endpoint plugins or compatibility processes.

Moreover, iSafer extends its protective capabilities to remote and mobile users in less secure public network environments. Leveraging DNS-based threat detection, it promptly purifies and blocks malicious threats, safeguarding corporate network security.

 | www.urmazi.com | 16F, No. 80, Sec. 1, Zhongxiao W. Rd.,Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.) | SF-WP-31126

Functionality	NGFW	iSafer DNS Booster
Time of Defense	When the connection has been established or a TLS handshake occurs.	Connection has not yet been established.
Filtering Mechanism	URL: Check the HTTP header, the connection has been initiated.FQDN: The corresponding network address must be queried from the DNS server.	Filters domain name at a query stage to prevent users from establishing connections.
Huge Amount Objects Filtering	Creating thousands of addresses or FQDN names or using TLD as a comparison condition will significantly reduce system performance and complicate the setting procedures.	Complete TLD filtering settings in simple steps, and compare tens of thousands of items with ease.
Control Mechanism	Only allow, warning or blocking are supported.	Supports multiple control mechanisms including allow, block, delay, redirect address & host name, Sinkhole, etc.
Whitelist Handling	No relevant reference information as basis.	Able to generate exclusive DNS activity data for individual enterprises and create a whitelist policy that meets their own needs.
Malicious & Phishing Attack Protection	IP is usually used as the protection object, and it is difficult to identify its security based on domain names.	Lock malicious or phishing attack domain names for protection, even if tens of thousands of IP addresses are associated, the identification performance will not be affected.
Encrypted Traffic Detection	It is necessary to reassemble and decrypt the packet through the SSL/TSL program before detection can begin, but this consumes a lot of system resources and affects the firewall processing performance.	It can directly analyze DoT, DoH, and other encrypted traffic and safely block without compromising system performance at all.

Key Benefits of iSafer Solution

Transparent DNS traffic reveals known malicious domains early.

Automated DNS rate limiting safeguards against DNS amplification attacks and reduces DDoS impact.

Blocking and filtering access to harmful content or phishing sites based on DNS activity logs.

Support for advanced security protocols like DNSSEC, DoT, and DoH to ensure secure connections

Threat intelligence services ensure the accuracy and real-time relevance of known protection content.

In conclusion, incorporating DNS records and configurations into your network security strategy actively shields your network from a myriad of threats and vulnerabilities. Regularly reviewing and updating DNS security measures is critical in addressing the ever-evolving threat landscape. iSafer DNS Booster is your dynamic and comprehensive solution for staying ahead in the cybersecurity realm.

About URMAZI Networks Inc.

Specializing in DNS-based cybersecurity, we integrate extensive experience to develop iSafer, our flagship solution addressing enterprise cybersecurity needs. With the USRA research team leveraging AI for early threat detection, we swiftly respond to global challenges, making URMAZI your trusted partner for cutting-edge cybersecurity solutions.

 | www.urmazi.com | 16F, No. 80, Sec. 1, Zhongxiao W. Rd.,Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.) | SF-WP-31126