



# Strengthen Cybersecurity – Knowing Your DNS Activities

All online services rely on the most important network infrastructure component - Domain Name System (DNS) - which is the communication protocol that translates easily memorable enterprise domain names or service URLs into system host IP addresses. Mobile internet-connected devices have improved the applications and services, no longer confined to a specific location or time to meet the actual needs of users, such as online information search, shopping, v-conferencing, e-learning, online banking, gaming, cloud storage, telemedicine, IoT control, online reading or applying personal certificates, and countless digital applications. Obviously, the domain name system is an indispensable core role for enterprise or institutional service networking; internet services also depend on the normal operation of the domain name system to achieve their goals. Properly utilizing the features of the domain name system can not only optimize the quality and efficiency of various services but also enhance competitiveness and create higher value.

iSafer is URMAZI's specialized solution designed for advanced management and security threat defense of domain name systems, which is a software platform that can be installed in virtualized environments. Considering that many enterprise IT resources are limited and use general open-source software architecture for their domain name systems, the management functions are rudimentary, and security defense mechanisms are lacking, which not only makes it difficult to match the flexible applications of modern broadband networks but also maintain relevant activity tracking records. Hackers are also aware of the wide-ranging impact of attacking the domain name system on application services.

Therefore, a domain name system without security enhancement is unable to cope with the ever-changing malicious network attack behavior. It is extremely easy to actively introduce attack threats due to the lack of security recognition capabilities of user terminals, resulting in significant losses of corporate assets and reputation. iSafer starts with endpoint DNS management and is the best targeted tool to solve the above-mentioned difficulties for your enterprise.

## IDC 2022 DNS Security Report

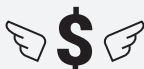


Awareness of DNS security is very strong

say it is critical



**7** attack on average per organization in the past 12 months



**\$942k** average cost of attack



**51%** were victim to a phishing attack



**70%** suffered application downtime (cloud or in-house)

The registered domain names worldwide in the 4Q of 2022 reached 350.4 million, representing an 8.7% YoY increase from 2021.

↑ **8.7%**

**Domain name growth is beyond imagination, and security threats are hidden within!**

### iSafer Play Multiple Roles



#### Observer

Support you in monitoring all DNS-related activities.



#### Optimizer

Improve access quality thru DNS service optimization.



#### Protector

Block threats at the edge of your network border.



#### AI Learner

Self-acquire unknown info and enhance recognition ability.



#### Analyzer

Automation making categorized and statistics reports for management.


In advanced management, iSafer accurately records and preserves the query and response activities of the domain name system. This not only serves as evidence for service incidents, but also enables IT administrators to establish unique management rules based on the needs of business operations. By filtering unnecessary query services or delaying the processing or response of specific information, external persistent attacks by bots can be greatly reduced. This ensures that enterprise employees can focus on service content related to production efficiency.

Additionally, iSafer has domain service health checks and load balancing capabilities, as well as support for domain multiple redirection mechanisms. This assists enterprises in establishing stable application service backup plans and ensuring service continuity. The built-in SafeSearch function can be applied to mainstream search engines (such as Bing, Google, YouTube, etc.) to block and filter inappropriate search results without the need to configure rules on each device within the organization.

Unlike other network security devices such as NGFW or IPS, iSafer is natively designed with domain security as its foundation, filling in the gaps that other network security devices may have, and allowing enterprises to strengthen their cybersecurity defense capabilities through domain-based technology. Taking domain DDoS attacks as an example, iSafer allows IT administrators to implement security rule actions such as blocking, delaying, or redirecting based on composite conditions of query sources and query frequency. The role of iSafer Sinkhole is to guide malicious domain name queries into specific trap, while generating alert information for defense purposes. Leveraging domain activity characteristics to enhance network security is iSafer's unique advantage, and it is the best solution to directly address the problem of NGFW and IPS devices' insufficient processing loads.

In addition, iSafer combines with URMAZI's exclusive Security Research Academy (USRA) for threat intelligence content, which is based on deep learning and artificial intelligence technology to explore connection behavior data based on domain content, analyze, classify, and predict it as value-added services. It actively blocks and protects against strongly threatening attacks such as Botnet, Phishing, and Scam, as well as a database of resolved data for 55 other behavior domain categories, effectively strengthening the security of endpoint users' internet connections and providing more accurate behavior information, helping IT administrators and business decision-makers build more advanced, secure, and competitive network services for their organizations, protect assets, and create higher productivity and revenue.





The iSafer DNS Booster not only improves enterprise DNS service efficiency, but also includes other advanced management mechanisms and security protection features :



### Activity logs

iSafer automatically archives and retains domain name query and response logs for the past seven days and the last five minutes, and distinguishes new activity lists for observation or response. This provides network administrators with the ability to quickly locate and narrow down issues as needed.



### Service multihoming

In the face of global competition, service stability and non-interruption are the most important aspects of enterprise services. iSafer has a health check mechanism that monitors the connection quality status of service hosts around the clock and uses algorithm technology to appropriately distribute traffic entering service hosts. This not only significantly reduces the risk of being unable to connect to various services due to a single DNS server failure, but also enhances the operational efficiency of web services by its load balancing function, protecting service server resources from being exhausted.



### Blacklist policy

Custom formats or RPZ format files can be imported to restrict malicious domain names or IP addresses inside and outside the country as the first line of defense for information security protection. With more and more malicious programs and zombie devices using DNS queries to connect to C&C servers, the blacklist policy allows managers to customize blocked domain names and query response addresses to prevent users from accessing malicious or inappropriate domain names or IP addresses.



### Log forwarding

For large organizations that require long-term monitoring of connection behavior records, iSafer supports managers in establishing automatic log forwarding functions for easy integration into other third-party SIEM management platforms.

## Summary

iSafer DNS Booster is the industry's first DNS management solution that combines global threat intelligence with advanced protection mechanisms for end-user domain connections. It ensures secure access to information and services for end-users, significantly reducing the risk of network threats and improving productivity and security in the workplace. Additionally, it improves and optimizes the traditional domain name system's management and operation, addressing numerous blind spots and efficiency issues to meet the challenges of future application services' connectivity quality and user experience.

**iSafer is an essential and reliable helper for your enterprise network security.**