DATASHEET

# iSafer – Protective DNS Solution

Visibility | Security | Service for Enterprise

## Risks of DNS Attacks

Near 85% of malicious actors exploit DNS services to develop attacks such as ransomware, phishing, botnets, etc. This is due to the proliferation of online services, making DNS security threats highly destructive to services. Most cybersecurity practices in enterprises focus on multiple pattern protections in NGFW (Next-Generation Firewall). However, dealing with lurking C2 (Command and Control) and security vulnerabilities in old network devices is particularly challenging, leading to disasters such as data breaches or system hijacking. Network services would be safeguarded and reliable if we could block malicious activities during domain name queries.

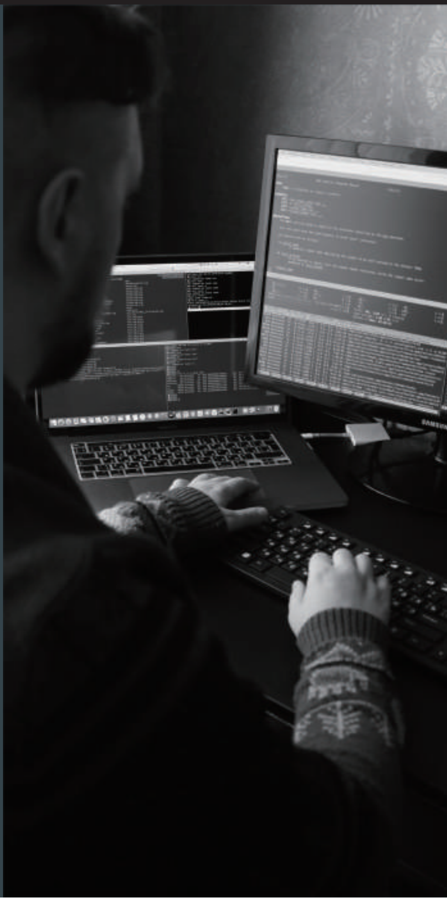
- Easy Management
- Seamless Adoption
- Efficient Protection
- Cost Effective

## iSafer - Protective DNS Solution

The essential components of the Protective DNS (PDNS) solution include "known threat intelligence" and "domain query behavior control." Threat intelligence is the foundation for filtering and blocking malicious connections, safeguarding network endpoints, and isolating contact with known cybersecurity risk sources. Domain query behavior control enables automatic monitoring of abnormal traffic or query behavior patterns, retaining relevant logs to enhance incident traceability and analysis capabilities significantly. iSafer DNS Booster, as a leading indicator in the PDNS industry, not only integrates security defense capabilities and provides dynamic DNS risk indicators for security teams to stay updated with the latest security information to comply with global cybersecurity regulatory requirements. iSafer also features advanced network services such as DNS server and load balancing, supporting enterprises in constructing more stable and efficient online services and applications, addressing the dual needs of challenging security defense and basic service optimization at once.

## iSafer Advanced Features

- DNS Firewall
- DNS Proxy
- Global Threat Intelligence
- DNS Server
- DNS Risk Assessment
- DNS Traffic Insight & Reporting
- Load Balancing
- Inbound Multihoming



## System Specification

| Feature & Version | Essential | Advanced | Superior |
|---|---|---|---|
| System Model | SF10 / 20E | SF10 / 20A | SF50S |
| Query per second (QPS) | 10k / 20k[a] | 10k / 20k[a] | 50k |
| **System Main Services** | | | |
| DNS Proxy[b] & Request Route | ✓ | ✓ | ✓ |
| DNS Server Load Balance | ✓ | ✓ | ✓ |
| DNS Server [b] | N/A | ✓ | ✓ |
| DNS Multihoming[c] | N/A | ✓ | ✓ |
| Black & White List Import by IP or Subnet Based | ✓ | ✓ | ✓ |
| RRL[d] Control for IP or Subnet or Domain Based | ✓ | ✓ | ✓ |
| SafeSearch Content Filtering | ✓ | ✓ | ✓ |
| DNS Sinkhole Protection | N/A | ✓ | ✓ |
| **DDoS Dynamic Block Protect** | | | |
| Set blocking time by query number or query rate | ✓ | ✓ | ✓ |
| Set blocking time by RCode respond number or ratio | ✓ | ✓ | ✓ |
| Set blocking time by QType query number or query rate | ✓ | ✓ | ✓ |
| **DDoS Protect Policy** | | | |
| Set Query Threshold Limitation | ✓ | ✓ | ✓ |
| Allow, Block, Delay, Translate IP or DomainName | ✓ | ✓ | ✓ |
| **Global Threat Intelligence Service** | | | |
| Go-start Category Pack(Botnet, Phishing, Scam) | Subscription | | |
| Plus Category Pack(Ransomware, Crypto, URL Shortening, NRD, etc)[e] | Subscription | | |
| **Min. system requirements: 4 vCore, 16 GB RAM, 512 GB Storage, VMware ESXi v6.5 or higher.** | | | |

[a] Factory default with 10k QPS, it's able to upgrade to 20k by order individual license. [b] Service supports UDP, TCP, DoT, DoH, and DNSCrypt. [c] Product comes with license of 2 domains. If more domains are needed, extra license is required. [d] RRL stands for Response Rate Limit. [e] Total of 58 categories which includes Go-start, no need to pay extra license fee within valid subscription period if number of category increases.
Remark. URMAZI keeps the right for adjusting system features or performance without notice.