The Challenges

The education sector is increasingly relying on technology for teaching, learning, and administration purposes. However, with this increased reliance on technology comes the risk of cyber threats that can negatively impact educational institutions.

DNS Threats

A properly functioning DNS is essential to ensure that users are directed to the correct websites and specific services. DNS service plays a critical role in securing educational institutions against cyber threats. By securing the DNS infrastructure, schools can prevent DNS-based attacks, such as DNS hijacking and cache poisoning. DNS security also enhances the overall security posture of an institution by providing visibility and control over DNS traffic.

IDC 2022 DNS Security Report

51%
were victim to a phishing attack

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

7
attack on average per organization in the past 12 months

$942k
average cost of attack

73%

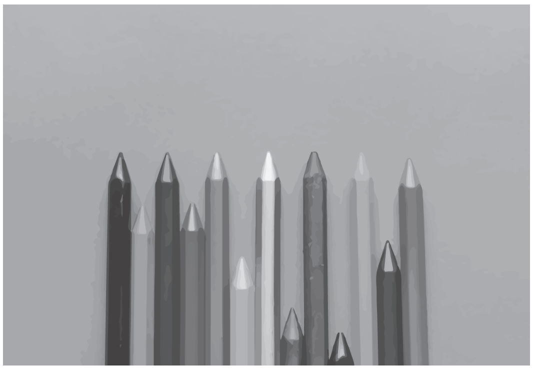
Awareness of DNS security is very strong

say it is critical

Services on cloud, still a need to strengthen DNS security?

From a cybersecurity perspective, the answer is yes.

- DNS is still a core component of the network service infrastructure. Although application services are hosted in the cloud, DNS still allows users to access them, and DNS attacks can cause services to be unavailable or redirect users to malicious websites.
- Although third-party hosting services such as Amazon or Cloudflare may provide some level of DNS security, they cannot guarantee comprehensive protection against all types of attacks.
- Cloud-based services are still vulnerable to DNS attacks, such as DNS spoofing, cache poisoning, and DNS reflection attacks. Therefore, implementing additional DNS security measures to protect your services and users is a necessary management practice.



What is iSafer?
And what benefits to gain for your organization?

URMAZI iSafer DNS Booster is a software-based solution specifically design for DNS service optimization and security enforcement, effectively providing organizations the power to discover, block, and mitigate cyberthreats.

Confidentiality

iSafer supports advanced DNS communication encryption protocols (DoT/DoH/DNSCrypt) to prevent malicious interception or tampering of domain queries during application service, ensuring the security and confidentiality of query responses.

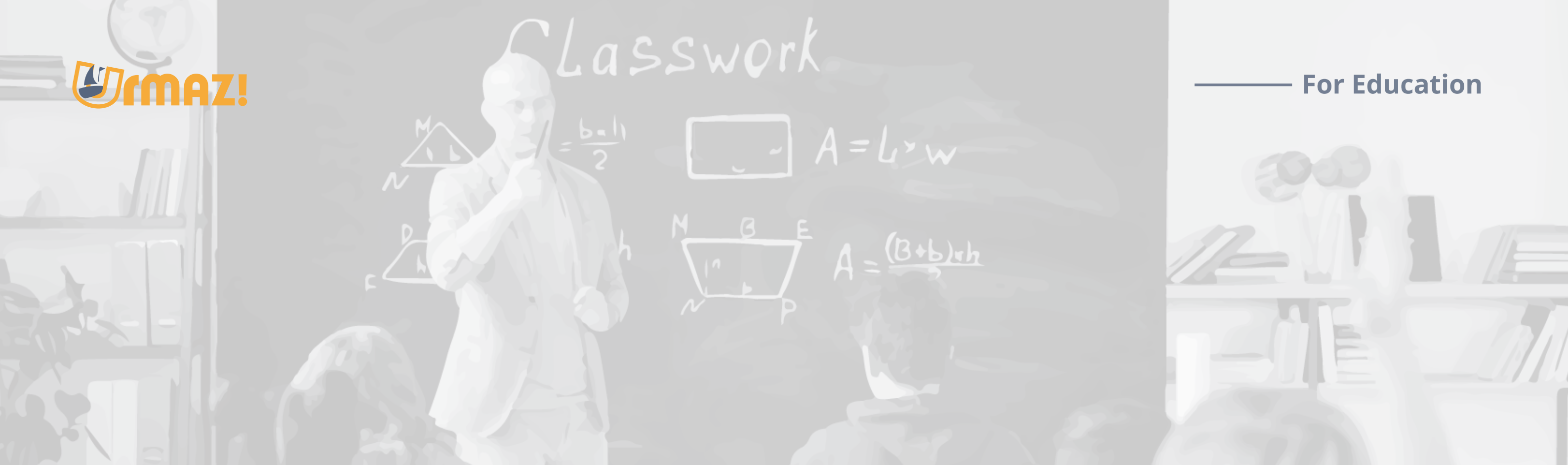
ntegrity

The iSafer processing core executes continuous recording and monitoring of DNS system activities, providing network administrators with insights into the query and response processes, and transforming these records into relevant statistical charts. This enables flexible adjustment and optimization of information security management policies.

Availability

External attackers often launch Distributed Denial of Service (DDoS) attacks on DNS systems, causing system resource exhaustion and interrupting all Internet-dependent services, resulting in significant losses. In addition, schools may face high-traffic scenarios during large-scale services such as course selection, online video teaching, and departmental services, making stable service availability crucial. iSafer provides corresponding mechanisms, such as:

- Limiting the critical number of queries from network sources and taking advanced protection measures such as blocking/delaying/redirecting/overwriting in response to matching queries, to avoid DDoS attacks.
- DNS system service load balancing to effectively reduce the load on backend service hosts and ensure stable service quality.
- Automatic caching and learning capabilities for unfamiliar queries or response variations, establishing faster response times for improved availability.



For Education

Advanced iSafer Features :

SafeSearch

Network administrators no longer need to exhaust themselves by setting inappropriate search engine content security rules for each connected device. Enabling SafeSearch forces connected devices to apply filtering policies.

Multihoming

iSafer has a health check mechanism that can significantly reduce the risk of being unable to connect to various services due to a single point DNS server failure. At the same time, its traffic load balancing function can enhance the operational efficiency of web services, protecting service server resources from being exhausted.

Sinkhole

A security protection feature that lures suspicious sources and responds to a default specific IP to prevent the suspicious source from infiltrating the internal network. It also alerts users of abnormal activities and helps network administrators to trace the source and behavior patterns.

Blacklist

This allows for the restriction of malicious domain names or IP addresses within and outside the network, serving as the first line of defense for cybersecurity. With the increasing number of malicious programs and zombie devices using DNS queries for Command and Control (C&C) servers, Blacklist enables administrators to customize the domains and query response addresses to be blocked, preventing users from accessing malicious or inappropriate domain names or IP addresses.

iSafer MULTIPLE ROLES

- Observer
- Optimizer
- Protector
- AI Learner
- Analyzer

Conclusion |

A properly operational DNS is critical for the security and reliability of Internet services. No matter K-12 or higher education campus, administration authority should ensure that your DNS infrastructure is properly configured, secured, and maintained to minimize the risk of cyberattacks and other disruptions. With iSafer to keep cyber threats away for your students and associates as well.