For Healthcare

Modern Healthcare Service

The healthcare industry has seen a significant shift towards digitalization in recent years. Technology has transformed the way healthcare services are delivered and managed, making them more efficient and effective. The use of electronic medical records (EMRs), telemedicine, and mobile health (mHealth) applications has enabled healthcare providers to offer more personalized and convenient services to their patients.

The Challenges

With this digital transformation, the healthcare industry is facing new challenges in securing patient data and maintaining network security. The healthcare industry has become a prime target for cybercriminals due to the high value of patient data. This has resulted in a growing need for robust security measures to protect patient data and ensure the confidentiality, integrity, and availability of healthcare services.

Meanwhile, the modern healthcare system relies heavily on Information Technology (IT) and network connectivity to provide efficient and effective healthcare services. With the increasing use of technology in healthcare, network security has become more critical than ever.

How DNS Service & Security Matter

The domain name system (DNS) is a vital component of the IT infrastructure that underpins modern healthcare services. Healthcare services such as EMRs, telemedicine, and mHealth applications rely on DNS for proper operation.

From different perspectives, here are why reliable and secured DNS services are important:

- For Administration Authority: Healthcare organizations rely on DNS to manage their IT infrastructure and ensure that healthcare services are available to patients and the organization, avoid cyber threats by malicious attacks causing sensitive data breaches or system downtime.

- For Patients: Patients rely on healthcare services to receive timely and quality medical care. A reliable and secure DNS service ensures that patients can access healthcare services without interruption. It also helps to protect their personal and medical data from cyber threats.

DNS security is important because it protects against a variety of DNS attacks. DNS security solutions can help prevent attackers from redirecting users to malicious websites, stealing login credentials, or causing other types of harm. They can also help prevent DNS-based data exfiltration, where attackers use DNS queries to exfiltrate sensitive data from an organization's network. Furthermore, it can provide real-time monitoring and threat intelligence to identify and mitigate DNS-based attacks.

Why hacker would like targeting on DNS service and resulting

DNS is a critical component of the Internet infrastructure, and as such, it is an attractive and easy-reach target for hackers. By compromising DNS services, hackers can achieve several malicious goals, such as Phishing, Malware Distribution, DDoS Attacks, DNS Cache Poisoning and may causing service interruptions for huge money.

The effects of compromising DNS services can be severe for healthcare organizations. It can result in the loss of sensitive patient data, disruption of healthcare services, damage to the reputation of the healthcare organization, and financial losses. Additionally, healthcare organizations that fail to protect their DNS services can face legal and regulatory consequences, such as fines and penalties for non-compliance with HIPAA or ISO regulations.

What iSafer DNS Booster can do for your organization

Preventing Malware Infections

DNS can be used to block access to known malicious websites that may contain malware or phishing schemes. By strengthening DNS security capabilities, healthcare organizations can prevent malware infections, which can compromise sensitive patient data and disrupt healthcare services.

Improving Network Performance

DNS caching is used to speed up network performance by reducing the time it takes to resolve domain names. However, if the DNS cache is poisoned, it can lead to network downtime and degraded performance. Strengthening DNS security can improve network performance by preventing DNS cache poisoning attacks and ensuring that DNS requests are resolved quickly and accurately.

Reducing Security Incidents and Data Breaches

DNS attacks, such as DNS spoofing and cache poisoning, can lead to security incidents and data breaches. These incidents can result in the loss of sensitive patient data, damage to the reputation of the healthcare organization, and financial losses. By strengthening DNS security, healthcare organizations can reduce the risk of security incidents and data breaches.

Simplifying Compliance with Regulations

Compliance with regulations such as HIPAA and ISO requires healthcare organizations to ensure the confidentiality, integrity, and availability of patient data. DNS security is a critical component of compliance with these regulations.

Enhancing Business Continuity

DNS is a critical component of business continuity. A DNS outage can result in network downtime, which can disrupt healthcare services and cause financial losses.

IDC 2022 DNS Security Report

51%
were victim to a phishing attack

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

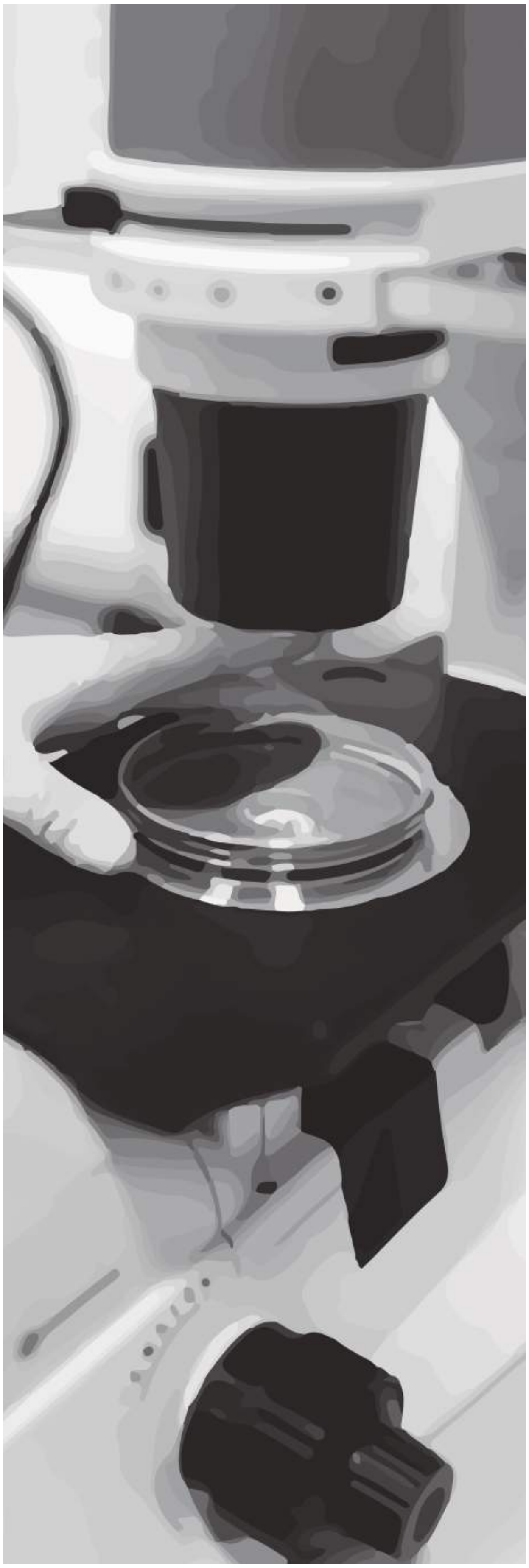
7
attack on average per organization in the past 12 months

$942k
average cost of attack

73%

Awareness of DNS security is very strong

say it is critical



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

Good domain security is the foundation for various innovated healthcare services. However, statistics from the past 12 months show that most cyber threats faced are related to external attacks such as malicious websites, spyware, phishing, DDoS, and ransomware, all of which can be effectively identified and blocked during the domain name query process.

The design of iSafer DNS Booster is to provide your organization with the most competent helper in optimizing DNS services and integrating threat intelligence into security services. Under the limited resources of enterprise manpower and operating budget, iSafer DNS Booster takes the initiative to stand on the front line, blocking malicious threats from the outside, protecting internal user connection behavior, and safeguarding important assets and business operations as well.