Manufacturing and Retail IT Security Challenges

Modern manufacturing industries, whether traditional or high-tech, have greatly increased production efficiency and emphasized automation and intelligence with the improvement of high-speed internet infrastructure. This has led the retail industry to create many services that are more precise and closer to the market, generating revenue. Global operations require services to be digitized and networked, and to be quickly and accurately disseminated to different locations and end-users. Whether it's production data, user information, or user experience, they are all useful tools that support business decision-making by management, allowing businesses to expand their services and profits.

Office Automation (OA) is commonly used in manufacturing and retail industries for tools such as email, ordering systems, inventory management, personnel databases, financial systems, customer service systems, etc. Operational Technology (OT) commonly refers to POS sales systems, inventory management systems, etc. These application services all contain a large amount of enterprise operational secrets, so it is necessary to strengthen personnel security awareness and establish automated IT security defense capabilities to keep threats out. Hackers often invade systems to control production machinery, which not only affects production capacity or causes interruptions but may also lead to personnel injury or death. These incidents can significantly affect customer business reputation and experience and are ultimately the goal of hackers' ransomware attacks.

When application services are operated on the Internet, the domain name system is an essential foundational technology responsible for translating website names into IP addresses. However, it is also a weakness that attackers can frequently exploit. DNS attacks or interference can occur through DNS Spoofing, Phishing, Cache Pollution, DDoS attacks, etc. The result can redirect users to malicious websites, steal login credentials, or implant Trojan horses, causing severe and unpredictable damages to the enterprise.

What are the security threats?

Information security threats are diverse and include both internal and external threats. Therefore, IT management authorities need to use a combination of methods to strengthen their defense capabilities and protect the internal security environment. NGFWs, Web Filters, Sandboxes, and other IT security products all have specific protective expertise, making it difficult to have a comprehensive IT threat defense capability with a single product.

If IT security threats become a reality, they can cause irreversible impacts and disasters to all connected devices. The types of threats include computer viruses, phishing attacks, data breaches, ransomware attacks, etc.

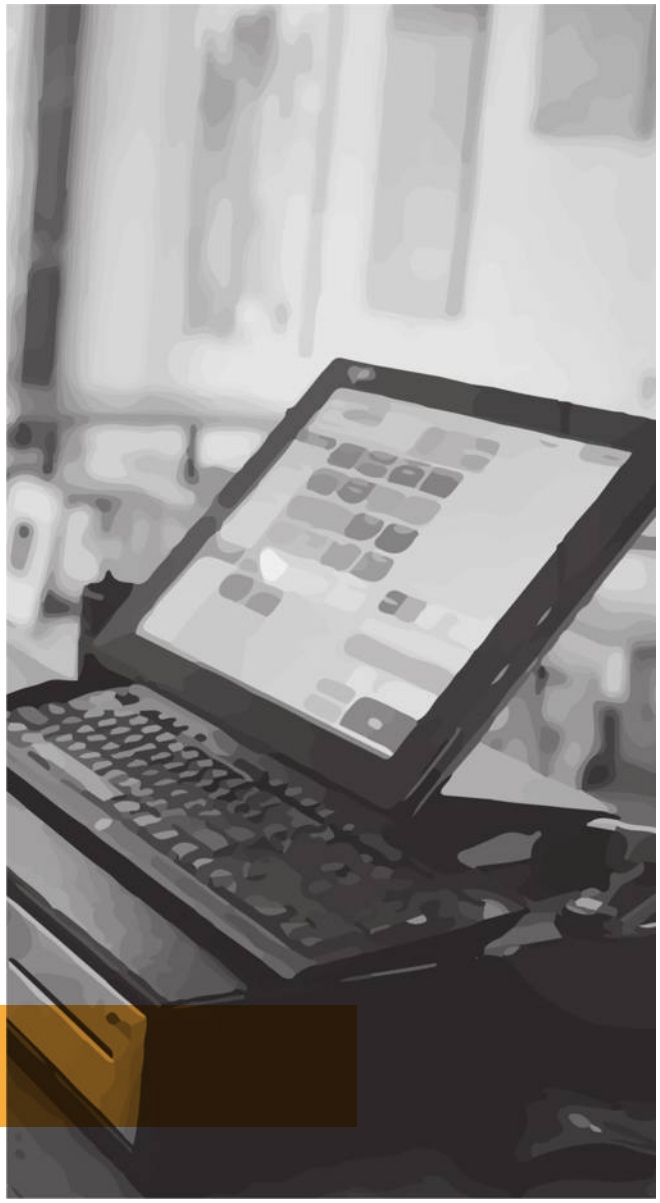
Key to Strengthen Cybersceurity – The DNS

Given that all Internet services rely on DNS resolution to function properly, both users and malicious hackers need to achieve their respective goals through the DNS service process. Users need stable and secure service connections, while malicious hackers try to break down security mechanisms to gain illegal benefits. Doesn’t like NGFW or web filtering products match and block attack features and content after the connection is established.In contrast, iSafer DNS Booster intervenes in security checks during the first critical process of service initiation – DNS resolution queries. Any threats will trigger the synchronous blocking of malicious domain connections to proactively protect end-users and reduce exposure to threats before causing harm, safeguarding enterprise information and property security. We need to strengthen external network intrusion detection and regional joint defense, and enhance the resistance of the Domain Name System (DNS) to attacks to ensure the "confidentiality" and "integrity" of DNS data, as well as the continuous "availability" of DNS.

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.

Integrity

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.

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 of enterprise development for various innovative network services. However, statistics from the past 12 months show that most cyber threats faced by enterprises 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 enterprise 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 for the enterprise.

