SENTRY

The Ultimate Sentinel Against Unknown Cybersecurity Threats

Mainstream security gateway products typically defend against known attack methods from the past. However, the present and future are rife with new AI-driven attack techniques, lacking historical reference data. How can we predict and defend against these unknown cybersecurity threats before they manifest into recognizable patterns?

DNS services are fundamental components for the online digital operations of enterprises. Consequently, sensitive data within an organization can be easily discerned from DNS service content. Firewalls often lack the capability to secure DNS activities, making them a frequent target for hackers. Organizations need DNS-based solutions to address this vulnerability.

Our SENTRY® series software products are designed as cybersecurity solutions in the realm of "Protective Domain Name Service."

Intelligence Governance

Risk-Oriented

SENTRY® products take control of domain name query resolution for internal and external network services within enterprises. They are equipped with the industry's pioneering ScoutEye correlation threat analysis module, an advanced tool developed for cybersecurity teams to swiftly respond to high-risk connections.

ScoutEye supports various risk indicators to classify endpoint connection behaviors, risk scoring, and threat content forensics. This makes DNS activity content transparent and enhances preventive measures against cybersecurity threats such as amplification attacks, tunneling attacks, botnets, sensitive data theft, and public cloud service posture. This significantly reduces the risk of human error and long processing times when manually reviewing vast amounts of information, making it the optimal cybersecurity strategic tool for medium to large network environments.

In terms of cybersecurity defense mechanisms, URMAZI's team of intelligence analysts has embedded a DNS-specific threat intelligence database within SENTRY®, offering over 60 categories of intelligence content, including phishing, probing, ransomware, DGA, C2, and malware. Its integration with DNS firewall blocking and honeypot hunting technology, along with a highly flexible automated security response mechanism, ensures that malicious connection activities are blocked and precisely identified at the endpoint request stage. The system also supports retaining DNS connection trace data and event content, which can be integrated into EDR/SIEM analysis platforms to expand the interpretation and utilization of related cybersecurity content.

SENTRY®series products offer numerous application advantages for enterprises:

- The most convenient cybersecurity defense solution without altering network architecture.
- Insight and response capabilities before attack patterns form.
- Control over endpoint connection behaviors and threat risk ratings.
- DNS-related data to assist in cybersecurity incident forensics.
- Compliance with ISO-27001/27002 cybersecurity regulations.
- Early detection of sensitive data leakage signs and sources.
- Prevention and reduction of lateral movement attacks within the internal network.

URMAZI is a technology development team focused on PDNS cybersecurity applications. Established to create a robust DNS-level cybersecurity ecosystem for enterprises, URMAZI builds core resources for autonomous management of enterprise-specific threat intelligence and implements responses to unknown risks before they become threats. DNS is not only a essential service for the network operations of all industries but also the primary key position for endpoint cybersecurity defense within organizations.

URMAZI SENTRY® promotes "Risk-Oriented, Intelligence Governance" initiatives, making DNS your perpetual cybersecurity sentinel.

SENTRY®Product Matrix:

Feature / Model	50	200	300	500	2000	3000
Performance(RPS)	50	200	300	500	2000	3000
DNS Firewall Feature	V	V	V	V	V	V
DNS Recursive Feature	V	V	V	V	V	V
DNS Server Feature	X	V	V	V	V	V
Inbound Multihoming/Domain	X	Opt.	Opt.	V/2	V/2	V/2
DNS Threat Intelligence	V	V	V	V	V	V
ScoutEye Feature Module	X	Opt.	V	V	V	V
Internal Reports	V	V	V	V	V	V

*. URMAZI reserves the right to adjust system features or performance without prior notice.