# Importance of Protective Domain Name System

## What is Protective DNS

Protective DNS(PDNS) is a policy-implementing, recursive DNS resolver service deployed upstream of organization networks. The service filters DNS queries compared to a range of classified threat intelligence to prevent resolution for known malicious domains and IP addresses. PDNS supports emerging DNS technologies, including encrypted DNS protocol support (DoH/DoT) and IPv6 resolution. DNS log data will significantly enhance the visibility of DNS activities for cybersecurity teams and serve as a reference for formulating security prevention policies.

## Why Does an Organization Need PDNS?

DNS is essential to organizational OA/OT/IT security management integration. With cyber threats evolving in sophistication and frequency, traditional security measures often need to catch up in safeguarding sensitive data and infrastructure. PDNS offers a proactive defense mechanism against many cyber threats, including phishing attacks, malware distribution, and domain hijacking. By leveraging advanced algorithms and threat intelligence feeds, PDNS empowers organizations to identify and neutralize malicious domains before they inflict harm. Moreover, PDNS enhances DNS traffic visibility, enabling organizations to swiftly detect and mitigate DNS-based attacks.


www.urmazi.com
16F, No. 80, Sec. 1, Zhongxiao W. Rd.,Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.)
SF-WP-40320

## The Role of iSafer in PDNS

iSafer stands at the forefront of cybersecurity innovation, offering a comprehensive suite of solutions to mitigate digital risks and safeguard organizational assets. When integrated with PDNS, iSafer enhances threat detection capabilities and augments defensive measures against emerging cyber threats. Leveraging advanced analytics and machine learning algorithms, iSafer complements PDNS by providing actionable insights and threat intelligence to identify and neutralize malicious activities preemptively.

Query Filtering and Blocking

Query Behavior Dynamic Blocking

Sinkhole Tracking


TLD Blocking

DNS DDoS Prevention

Global Threat Intelligence

CyberRisk Indicators

DNS Activity Insight

## Regulation Compliance

iSafer DNS threat intelligence and security can also be expanded and integrated into event management platforms such as SIEM, XDM, or NAC to comply with various industry security regulations, such as CMMC/NIST 800/FISMA/PCI-DSS/HIPAA and the ISO/IEC 27001:2022 specification for certification of control measures.







### Protective DNS is necessary for Next-Gen Security

A proper operational and business resiliency strategy is not just about keeping bad actors out but also protecting organizations where bad actors might already be inside. Unfortunately, everyone will be breached at some point. This is a top-priority concern for many CISOs in the onslaught of modern attacks where threat actors sit inside enterprises undetected for weeks or months.

If you can spot anomalous communications early enough in the cyber kill chain, you can render the attack inert well before data exfiltration and encryption and thus minimize and control any damage. Early warning signals allow you to investigate anomalies before they escalate.

**iSafer – Your Best PDNS Solution**


www.urmazi.com

16F, No. 80, Sec. 1, Zhongxiao W. Rd.,Zhongzheng Dist., Taipei City 100007, Taiwan (R.O.C.)
SF-WP-40320