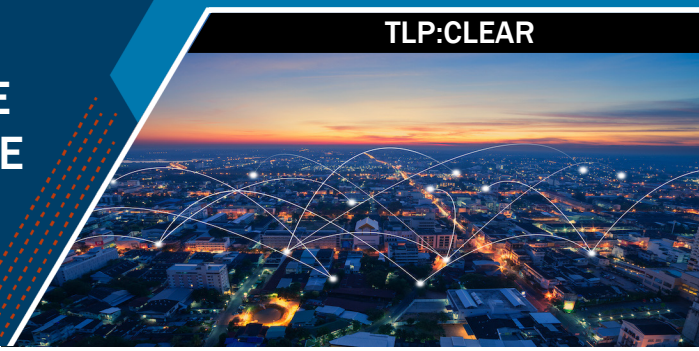
TLP:CLEAR

PROTECTIVE DOMAIN NAME SYSTEM RESOLVER SERVICE FACT SHEET



BACKGROUND

The Protective Domain Name System (DNS) Resolver service allows the Cybersecurity and Infrastructure Security Agency (CISA) to detect and prevent cyberattacks and threats targeting federal civilian executive branch (FCEB) agency networks. Protective DNS also offers a range of capabilities to safeguard assets that may otherwise be challenging to protect such as cloud, mobile, and nomadic devices. Since the service became available to FCEB agencies in September 2022, more than 104 agencies have onboarded to Protective DNS and an average of 1.6 billion queries have been secured daily. The service has also maintained a 99.999% resolver uptime rate – the percentage of time the service has been active and operational without outages. CISA provides this service to agencies as part of its broader effort to bring forth high-performing cyber solutions to secure federal networks and enhance the U.S. government's cybersecurity posture.

PURPOSE

CISA's Protective DNS service prevents government internet traffic from reaching malicious destinations by using state-of-the-art DNS technologies in combination with CISA's proprietary and commercially sourced threat intelligence. It also fulfills the requirements of the Department of Homeland Security's mandate under Title 6 of the United States Code (USC), Section 663: *Federal Intrusion Detection and Prevention System* to provide capabilities to detect and prevent cybersecurity risks in network traffic.

Additionally, Protective DNS aligns with DNS-related requirements and guidance in OMB M-21-31 and M-22-09. To direct select agencies to take steps toward enhancing the nation's cybersecurity and better protect its critical infrastructure, the current administration issued Executive Order 14028, *Improving the Nation's Cybersecurity*. In January 2022, the Office of Management and Budget authored a memorandum, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, which required agencies to achieve specific zero-trust security goals by the end of fiscal year 2024.

VALUE

CISA's Protective DNS enhances incident detection and response capabilities to support network resiliency in the wake of cyber threats. It does so by granting participating agencies and CISA access to comprehensive log records for analysis, which helps them obtain detailed insights into threat activities, better respond to incidents, and work to prevent future attacks.

FEATURES

CISA's Protective DNS is central to modern network operations, translating human-readable domain names into machine-usable Internet Protocol (IP) addresses through three primary components:

DNS Resolver: The service is geographically dispersed and acts on attempts to access internet resources (e.g., domains, IP addresses) deemed malicious by commercial, government, and agency-furnished threat intelligence feeds. It logs the resulting DNS traffic data for analysis.

Web Application: The service's web application empowers CISA and FCEB agencies with the ability to receive and configure alerts, generate queries to glean insights from the logs, download reports, and view dashboards.

Data Platform: The service uses a data lake to store DNS events from the resolver and to accept direct queries. This provides CISA with enhanced insight into how cyber threats utilize DNS to cause harm. All log data is stored for up to six months before being migrated to cloud storage, where it remains available to agencies and CISA for an additional three years.

FUNCTIONALITY

CISA's Protective DNS service also offers a broad range of enhanced functionality, enabling agencies to provide more efficient operations while mitigating DNS-based threats through:

Expanded Coverage. The service is device-centric, protecting both organizational networks and standalone devices, regardless of network location (e.g., on-premises, roaming/nomadic, or cloud). This functionality provides enhanced security and a greater range of coverage for more devices. In addition to traditional unencrypted DNS:53, the service also supports modern protocols, such as encrypted DNS, over both IPv6 and IPv4.

Enhanced Threat Intelligence. The service leverages a combination of unclassified commercial threat intelligence feeds and indicators sourced from government and industry partners to provide more comprehensive threat detection and prevention.

Real-Time Alerts. The service utilizes an application programming interface to provide real-time updates to participating agencies when potential malicious DNS requests are identified, increasing early response capabilities and preventing security compromises.

Increased Visibility and Accessibility. The service allows participating agencies to access records and threat trends via an intuitive web application. This data also enables CISA to view the same trends and data across the FCEB enterprise, which helps identify common threats and potential targets for further action and threat-hunting operations.

Zero-Trust Architecture Alignment. In alignment with zero-trust concepts, the service protects devices that were previously challenging to protect such as mobile, roaming, and nomadic devices.

SIGN-UP

Protective DNS is currently welcoming full FCEB participation. Those interested in learning more or onboarding should contact CyberSharedServices@cisa.dhs.gov.