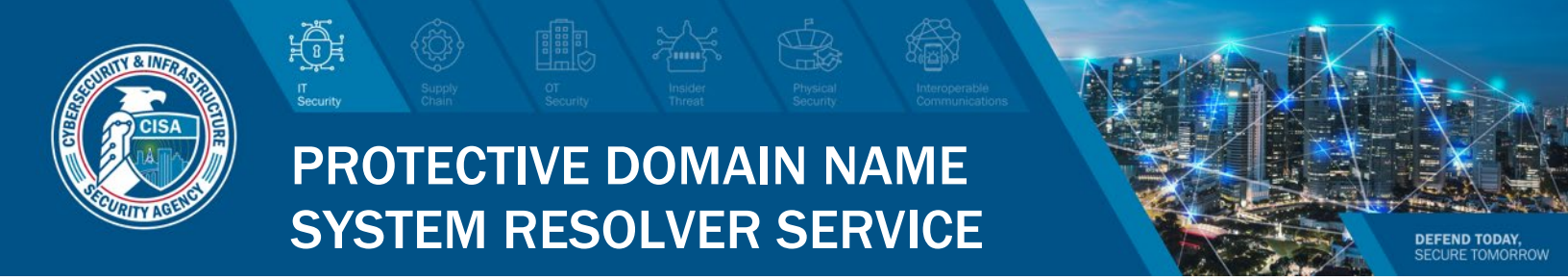


PROTECTIVE DOMAIN NAME SYSTEM RESOLVER SERVICE

OVERVIEW HERE

The Cybersecurity and Infrastructure Security Agency (CISA) will offer its Protective Domain Name System (Protective DNS) Resolver Service as part of CISA's broader effort to provide federal agencies with high performing, cost-effective cyber solutions that secure federal networks and enhance the government's cybersecurity position at large. CISA's Protective DNS Resolver Service is a device-centric service that secures and blocks government web traffic from reaching malicious destinations, and alerts security organizations within agencies when incidents occur. This service uses state-of-the-art DNS technologies and commercial threat intelligence to prevent malicious DNS content from compromising government networks, devices, and information.

BENEFITS

The Protective DNS Resolver Service enhances incident detection and response capabilities and creates an enterprise network that is more resilient to cyber-attacks, helping to better protect federal networks and information. This device-centric service works to protect organizational devices that were previously challenging to protect, such as cloud, mobile, and nomadic devices. This service is also designed to integrate with and complement existing agency protections, helping to streamline service adoption. This service leverages globally scaled commercial DNS providers to ensure a highly scalable and resilient product. CISA will provide its Protective DNS Resolver Service at no financial cost to Federal Civilian Executive Branch (FCEB) agencies.

FUNCTIONALITY HIGHLIGHTS

CISA's Protective DNS Resolver Service offers a broad range of enhanced functionality, enabling agencies to provide greater coverage to more devices, respond faster to malicious activity, and operate more efficiently in mitigating and countering DNS-derived threats through:

Real-Time Alerts: This service leverages an application programming interface (API) to provide real-time updates when incidents occur, increasing early detection capabilities and preventing further security compromises.

Increased Visibility and Accessibility: Participating agencies can view and download their records and threat trends via a web application. This data will also enable CISA to view trends and data across the FCEB landscape at large to aid in identifying common threats and potential targets for further action and threat hunting operations.

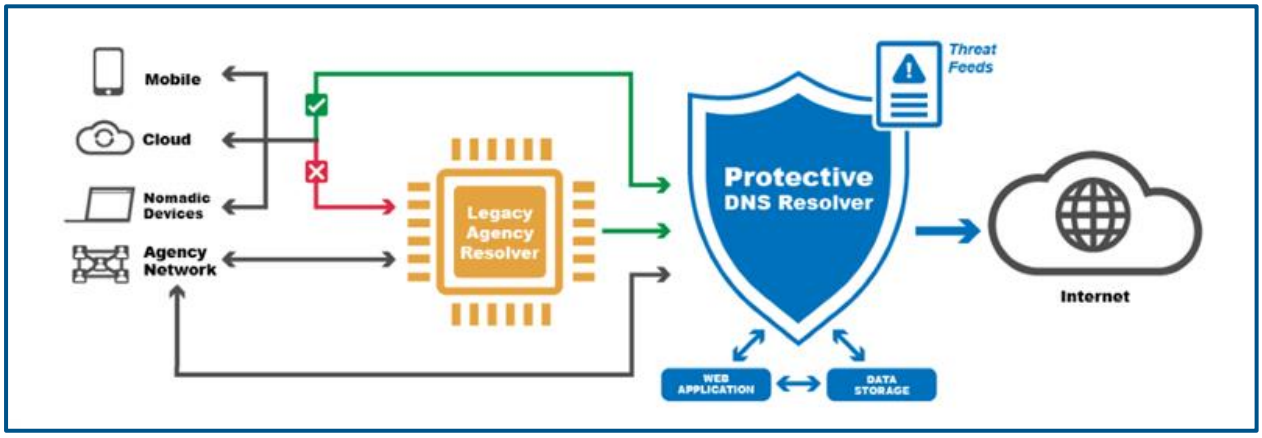
Enhanced Threat Intelligence: Protective DNS leverages a new, robust set of unclassified threat intelligence indicators—together with existing threat indicators—to provide more comprehensive threat detection and blocking capabilities.

Expanded Coverage: This service is a device-centric service that protects organizational devices, regardless of their location (i.e., on-agency-premises, roaming/nomadic, or cloud), resulting in enhanced security and a greater range of coverage for more devices than ever before. In addition to standard DNS over port 53, the service also supports encrypted DNS protocols (DNS over TLS and DNS over HTTPS).

Zero-Trust Architecture Alignment: Protective DNS aligns with zero-trust architecture and enables the protection of devices that were previously challenging to protect, such as cloud, mobile, and nomadic devices.

HOW IT WORKS

The Protective DNS Resolver Service is implemented upstream from agency networks and devices and leverages existing cybersecurity protections used throughout the federal enterprise. Significant volumes and classes of traffic that cannot use existing protections directly – such as traffic from mobile, roaming, and cloud assets – will integrate with the Protective DNS Resolver Service. DNS queries will pass through unclassified threat intelligence indicators and rules for active traffic filtering within the Protective DNS resolver. If a match is found between the requested content and the unclassified threat intelligence feeds, the query response is blocked or sinkholed, and an alert is sent to the origin agency and CISA.



HOW CAN YOU REQUEST SERVICES?

Any agency interested in participating in the trial or receiving additional information should contact CISA's Cybersecurity Quality Service Management Office (Cyber QSMO) at QSMO@cisa.dhs.gov.

ABOUT THE CYBER QSMO

The Cyber QSMO serves as an online, government storefront for high-quality cybersecurity services, aligning with federal governance, requirements, and priorities. Its mission is to centralize, standardize, automate, and offer high-quality, cost-effective cybersecurity services and products for all federal civilian departments and agencies. As part of the end-to-end service management model, the Cyber QMSO is committed to providing integration and adoption support to customers through a unified, shared services platform. The top priorities are to understand our customers' cybersecurity needs, gaps, and risks, and to offer and continually refine service offerings that both meet those demands and align with the ever-changing threat landscape impacting the federal .gov enterprise.

OUR CYBERSECURITY MARKETPLACE

CISA's Cyber QSMO Marketplace offers best-in-class cybersecurity services from CISA, federal, and, eventually, commercial service providers. These CISA-validated services and provider partnerships will evolve and expand as the Cyber QSMO matures. By offering CISA-validated cybersecurity services, the Cyber QSMO Marketplace reduces purchasing agencies' burden of having to conduct their own research to vet and acquire affordable cyber services that comply with federal requirements and standards. The Cyber QSMO's long-term vision is to advance the availability of innovative cybersecurity solutions for federal agencies and SLTT governments to improve mission support functions.