DATAPRISE DATA SHEET

DNS Filtering: Intelligent Web Protection

Unrestricted DNS traffic is a blind spot attackers can exploit

Our DNS Filtering service delivers flexible protection and visibility at the DNS layer. It uses continuously updated threat intelligence to identify and block malicious domains before connections are established, blocking threats before they reach your network.

With real-time blocking, granular user-level controls, and customizable reporting, the platform adapts to your organization's unique risk profile.

What You Get

- ✓ **Real-time threat detection** that blocks phishing, malware, and command & control domains instantly
- ✓ **Threat Intelligence** to identify trends and defend against emerging threats
- ✓ **Custom Filtering Policies** like allow- and blocklists configured per user, group, or device
- ✓ **Monthly Reporting and Insights** with your Cyber Resilience Score, Top Domains, and Risk Exposure

Why it Matters

Security and Risk Reduction

- **Stops Malware Infections:** Blocks access to malware domains and prevents DNS-based command-and-control activity
- **Prevents Phishing Attacks:** Stops users from reaching spoofed pages designed to steal credentials
- **Reduces Security Incidents:** Blocks threats at the earliest stage before they reach users

Policy and Compliance Gains

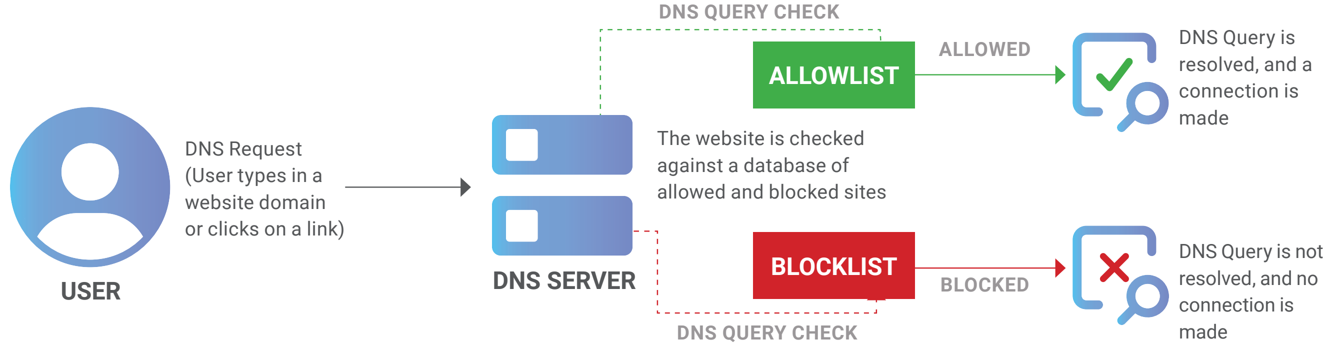
- **Enforces Company Policies:** Prevents users from bypassing acceptable use guidelines organization-wide
- **Enables Audit Readiness:** Maintains DNS query logs for visibility and compliance auditing
- **Supports Compliance Frameworks:** Helps meet requirements for HIPAA, PCI DSS, NIST, and other standards

Operational and IT Efficiency

- **Reduces Lost Productivity:** Frees up bandwidth by blocking distracting or inappropriate content
- **Delivers Visibility into DNS traffic:** Provides IT insight into top-browsed domains.
- **Reduces IT Support Burden:** Lowers volume of reactive support tickets

How DNS Filtering Works:

Domain Name System Filtering works by intercepting DNS requests and determining whether the destination is safe or harmful. Requests to dangerous or banned domains are blocked instantly, keeping users protected and networks running efficiently.


USER
DNS Request (User types in a website domain or clicks on a link)
DNS SERVER
DNS QUERY CHECK
ALLOWLIST
ALLOWED
DNS Query is resolved, and a connection is made
The website is checked against a database of allowed and blocked sites
BLOCKLIST
BLOCKED
DNS QUERY CHECK
DNS Query is not resolved, and no connection is made