CYREN

Cyren DNS Security

Enterprise Security SaaS

Get automated, comprehensive internet security in minutes for all users at your business locations.

CYREN DNS Security

Keep users safe from threats and block inappropriate content with a cloud service which is easy to deploy and simple to manage.

Ideal for organizations seeking best-in-class web filtering, easy-to-use policy management and automated protection for all web traffic from all users and devices at their business locations. Cyren DNS Security allows you to provision world class security in minutes—just point your DNS to Cyren's global security cloud, choose a pre-formatted security policy (or customize your own), and nearly instantly you will be enforcing web access policies, blocking malicious websites and phishing links, and getting comprehensive visibility across all your web traffic and locations.

World Class Security—The service applies real-time cyber intelligence to protect users against new and emerging threats, taking into account not only known good and bad web destinations, but applying sophisticated reputation analysis to protect users from new, previously unknown threats. Cyren utilizes DNS filtering for HTTP/S and cyber intelligence derived from the analysis of 25 billion internet transactions daily from over 180 countries.

Best-of-Breed Web Filtering—Cyren is a global leader in real-time URL and domain filtering, continuously classifying URLs and maintaining 64 URL categories in a real-time database averaging over 150 million URLs.

All Users, All Devices, All Traffic—Cyren's DNS-based security applies to all your web traffic, including HTTPS, now over half of global web traffic, and therefore enforces policy irrespective of the device being used or if the connection is coming from an employee or visitor. All scenarios are covered.

Enforce and Comply with Acceptable Use Policies—Guarantees enforcement and compliance with regulatory, customer-driven, or organizational guidelines for acceptable use of the internet.

Easy and Automated—Just forward your DNS queries to the Cyren cloud for processing and you can immediately enforce policy. Policy management for locations is simple with our intuitive web dashboard. User-level authentication or policy enforcement is not required.

Optimize Your Bandwidth Utilization—Cyren DNS Security enables you to shape and filter internet traffic. You can optimize network utilization and consistently provide a great user experience.

The advantages of Cyren DNS Security

- A flexible pay-as-you-go SaaS subscription model
- Protect all web traffic at your locations with the industry's largest global security cloud providing real-time protection.
- Any computing device connected to your network is protected from inappropriate content, malware, and phishing, including employee or visitor laptops, smart phones and tablets.
- Provides security filtering for encrypted HTTPS traffic, not just HTTP.
- Enforces "safe search," so users won't see or display inappropriate search images.
- Can be deployed in minutes—just point your DNS and choose a pre-formatted policy template.
- Easily manage multiple sites—our cloud platform consistently applies your policies across locations, or allows you to easily tailor them.

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

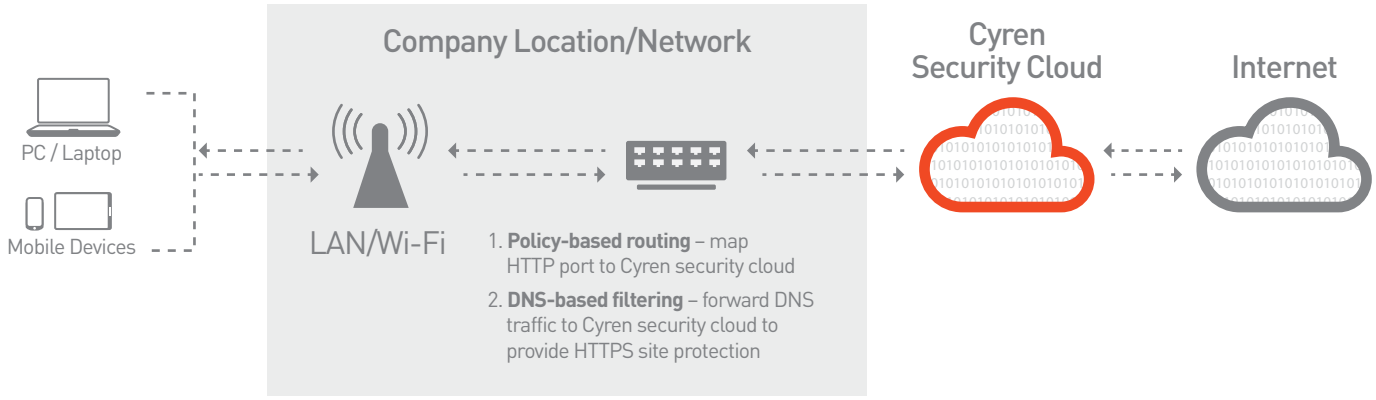
CYREN DNS Security

Cyren DNS Security Features

DNS-based Policy Enforcement—By applying policy to user browsing requests at the DNS level, Cyren DNS Security maintains the strictest privacy for the content of users' traffic. Once the initial request to access a given URL is approved, the user browses directly to the target web site and no further examination of their traffic is performed. This approach also ensures that the user never perceives any delay in accessing their chosen web site, as there is no "middle man" in the transaction.

Flexible URL Filtering and Categorization—Cyren DNS Security offers 64 URL categories as standard (including advanced threats), organized for maximum analysis and control. We provide out-of-the-box user policy templates to guarantee a quick start, which you can customize as needed with your own categories for whitelists and blacklists, and vary by time of day and location, if desired.

File-type and Traffic-type Controls—When used in a proxy deployment model for HTTP traffic, Cyren DNS Security allows you to manage network bandwidth by controlling the types and size of files that can be downloaded and the URLs that can be visited.



How it Works

Users accessing public networks are routed through standard networking configurations to Cyren DNS Security points-of-presence in our global security cloud. Service deployment is simple and almost instantaneous:

1. Point your DNS to the Cyren security cloud
2. In the web admin console, create a location and assign a pre-formatted user policy—or quickly mix-and-match categories for a customized policy.
3. Optionally, map your HTTP port to Cyren and forward your traffic to the Cyren security cloud

Once this is done, using the Cyren DNS Security administrative console, you enter your routing devices' public IP addresses in the system and select the preferred acceptable use policy to be applied to each address. Users are now protected from cyber threats and inappropriate Internet use or content.