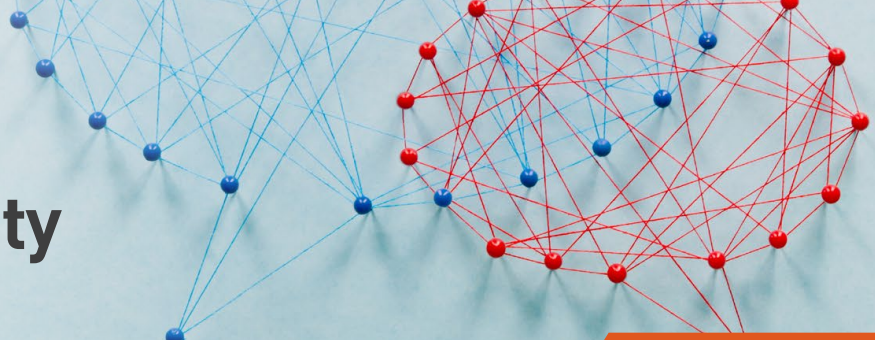
CYREN

Cyren DNS Security for Public Wi-Fi



Enterprise Security SaaS

Protect Your Guests and Customers—and Protect Your Company.

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.

Beyond providing open public internet access, it is critical to consider the risks associated with users exposed to the dangers that lurk on the Internet and your interest in enforcing acceptable use policies. Allowing the potential viewing of inappropriate or offensive content in a public place or on your business premises—even if displayed through search results—can expose your organization to legal liability and damage your reputation.

Businesses must exercise reasonable care in stopping illegal or unwanted acts over the internet access they provide, and threats such as malware or phishing sites are hazardous, not only to visitors, but also potentially to the host organization. Deploying Cyren DNS Security on any public-facing network gives you peace of mind—visitors and your organization are protected from the worst of today's internet threats, including via Safe Search enforcement, and your acceptable use policy is always strictly enforced.

Comply with Acceptable Use Policies—Providers of guest and/or public Wi-Fi-based Internet access can use Cyren DNS Security to comply with regulatory, customer-driven, or organizational guidelines for acceptable use of the Internet.

Easy Integration—Forward your DNS queries to the Cyren cloud for processing and you can immediately enforce policy. Policy management for hotspots is simple with our intuitive web dashboard.

Layered Security—Cyren DNS Security applies up-to-the-moment cyber intelligence to protect users against new and emerging threats. To do this, Cyren utilizes DNS filtering for HTTP/S and cyber intelligence derived from the analysis of 17 billion Internet transactions daily from more than 600 million users in 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. Cyren DNS Security enables network providers to directly manage the application of this database in easily configured policies for public Wi-Fi services and networks.

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

The advantages of Cyren DNS Security

- A pay-as-you-go SaaS subscription model with flexible location-based or user-based pricing
- Protect your users and guests with the industry's largest global security cloud—Cyren processes over 17 billion transactions daily and protects over 600 million users with real-time threat intelligence
- Any computing device connected to your public or guest network is protected from inappropriate content, malware, phishing, and advanced threats, whether a desktop made available to the general public or laptops, smart phones, and tablets linked to your guest network.
- 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

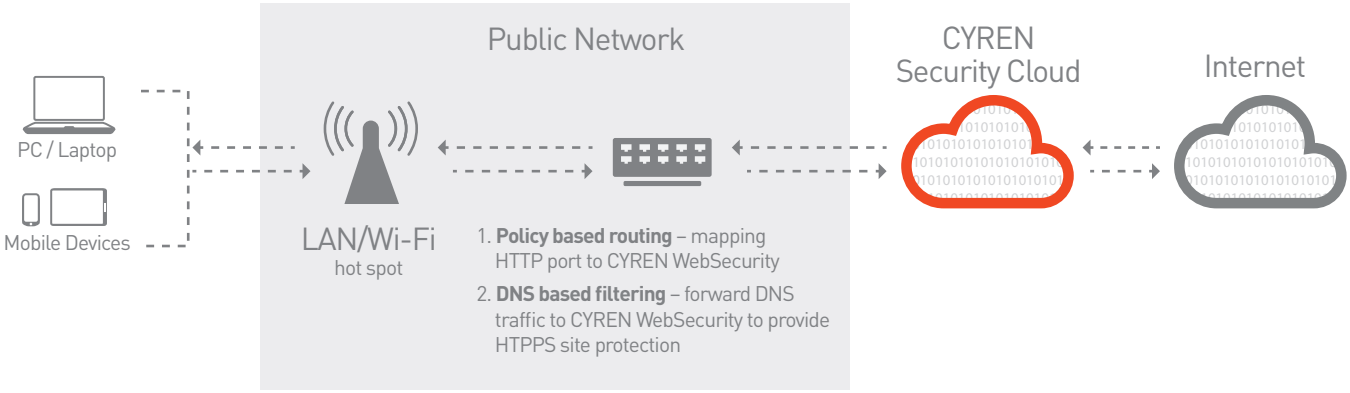
Cyren DNS Security for Public Wi-Fi Features

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 and Traffic-type Controls—When used in a proxy deployment model for HTTP traffic, Cyren DNS Security allows you to manage hotspot 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 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 WebSecurity 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.