CYREN

CYREN WebSecurity for Public Wi-Fi

Enterprise Security SaaS

Protect Your Guests and Customers—and Protect Your Company.

CYREN WebSecurity

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 WebSecurity 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.

Benefits

Comply with Acceptable Use Policies—Providers of guest and/or public Wi-Fi-based Internet access can use CYREN WebSecurity 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. Management for hotspots and policy is simple with our intuitive web dashboard.

Layered Security—CYREN WebSecurity 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 200 countries.

Best of Breed URL Filtering—CYREN is a global leader in real-time URL filtering, continuously classifying URLs and maintaining 64 URL categories in a real time database averaging over 150 million URLs. CYREN WebSecurity 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 WebSecurity enables network providers to shape and filter Internet traffic. Providers can optimize network utilization and consistently provide a great user experience.

The advantages of security in the cloud

CYREN WebSecurity for Public Wi-Fi delivers industry-leading, cloud-based security in a proven Security-as-a-Service (SECaaS) model.

With CYREN WebSecurity, any computing device connected to your network—from a desktop owned by you and made available to the general public for their use, to laptops, smart phones, and tablets owned by private citizens and linked to your guest network—is protected from inappropriate content, malware, phishing, and advanced threats.

CYREN WebSecurity applies the cyber intelligence gathered in analyzing over 17 billion Internet transactions every day.

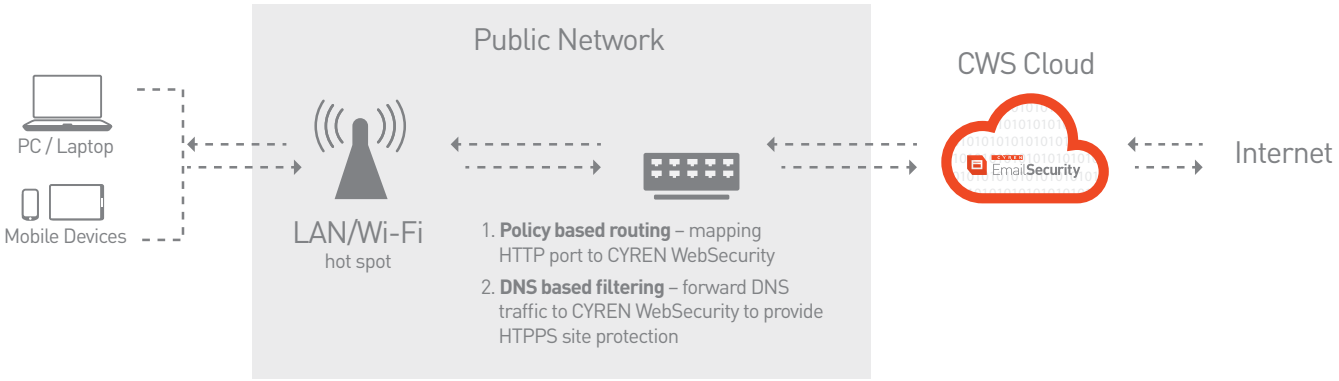
CYREN WebSecurity

CYREN WebSecurity Features

DNS-based policy enforcement—By applying policy to user browsing requests at the DNS level, CYREN WebSecurity 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 WebSecurity 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 WebSecurity 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 WebSecurity points-of-presence in our global security cloud. There are two easy ways to deploy the system:

1. Point your DNS to the CYREN cloud, and, optionally,
2. Map your HTTP port to CYREN WebSecurity and forward your traffic to the CYREN Cloud.

Once this is done, using the CYREN WebSecurity 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.