URL FILTERING

We increasingly use the Internet to conduct our business and personal lives, but web-borne threats are more prevalent than ever. Software and hardware vendors offering a safe, secure connected experience enjoy strong differentiation from competitors and new recurring revenue streams.

Ultimately success depends on the ability to deliver a great User Experience (UX). High-latency (slow response) and inaccurate classification (wrongly blocking or not blocking sites) are the enemies of a great UX.

CYREN Embedded URL Filtering overcomes the limitations of previous solutions to provide the most highly relevant Web coverage, uncompromising accuracy, and zero-hour security - all delivered in a low-latency model, high-accuracy model that delights users.

UNIQUE APPROACH

The size of the Internet, coupled with the unique browsing habits of each user mandated moving the URL database "to the Cloud". This overcomes local storage limitations, and gives CYREN partners flexibility with:

- Global, diversified data sources processing billions of transactions daily
- Massive, centralized database hold all the URL classifications you need
- Lightweight, economical local clients that store only the data you need, when you need it, eliminating resource-intensive updates

BROAD COVERAGE, UNPARALLELED ACCURACY

CYREN Embedded URL Filtering intelligently determines when and how to deeply scan each site, using multiple methods:

- Customer-oriented classification, triggered by each new site visited
- Analysis of site dynamics and user behavior determines scan depth
- Continuous tracking ensures exact URL classification at every moment

THE BEST ZERO-HOUR SECURITY

- Predictive detection recognizes harmful sites before users are exposed
- Zero-hour capabilities leveraged from all CYREN security products
- CYREN Security Alliance partners augment security data for maximum accuracy

BENEFITS

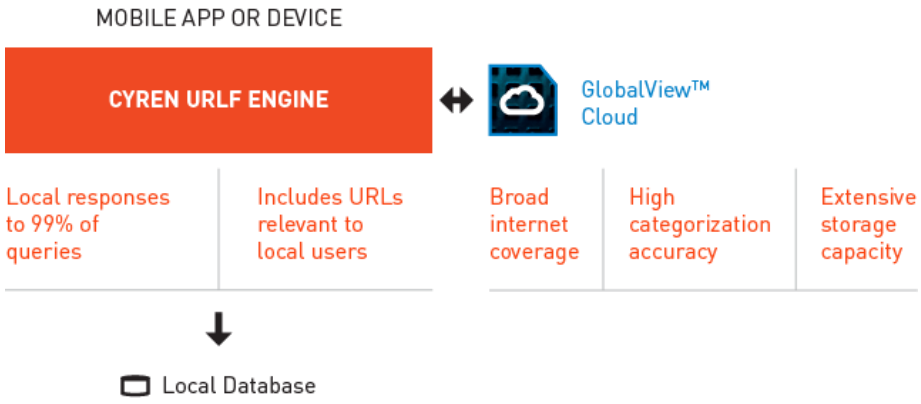
- **Ultra-low latency –** More than 99% of all queries are satisfied on the local device
- **Accuracy –** self-learning caches adapt to local conditions, removing the need for the traditional 'one size fits nobody' approach
- **Broad coverage –** CYREN augments the GlobalView Cloud data with 200+ data sources to provide the broadest, most relevant global coverage
- **Fresh, relevant data –** CYREN holds 'up to the minute' data on ~140 million of the **most relevant** URLs. Large URL databases are useless if the data they hold is stale
- **Fits the smallest platforms –** the unique CYREN 'Direct To Center' deployment model means that URL filtering can be deployed on almost any platform – even when no local storage is available

"CYREN Web filtering technology gives our ProSecure STM Series the power to protect our SMB customers."

Jason Leung
Sr Product Line Manager, SMB
NETGEAR

CYREN

HOW IT WORKS



CYREN Embedded URL Filtering categorizes user URL requests as follows:

1. The Embedded URL Filtering (URLF) engine is installed on the partner device, e.g. a Web Security Gateway
2. The partner device receives an http request
3. The device uses the engine to check the URL classification. The URLF engine first checks the local cache for values; typically more than 99% of queries are resolved locally by the cache, minimizing latency
4. If necessary, the URLF engine queries the GlobalView™ Cloud for relevant updates
5. The partner device blocks, allows, or removes content according to the classification it receives from the GlobalView URLF engine.

SPECIFICATIONS

- 64 categories, 8 of which are security related - returns up to 5 per URL
- Language and content-agnostic; vast coverage of global sites
- Database contains ~140 million of the most relevant URLs
- Configurable cache footprint with auto-tuning of cache contents
- High-performance: >50,000 queries/ second, with low resource utilization
- Supports http, https, ftp and other protocols

APPLICATIONS

Using CYREN Embedded URL Filtering, partners can create applications, such as:

- **Security –**real-time protection from emerging Web threats including malware, phishing, and Zombies/bots
- **HR compliance/regulation –** block access to questionable content, e.g. pornography or hate sites

  Productivity – block or monitor browser use to optimize employee productivity
- **Bandwidth regulation –** identify sites consuming excessive bandwidth, e.g. movies, music
- **Parental control –** restrict access to inappropriate Web sites