

Comprehensive Web Security

iPrism Web Security, (by EdgeWave) combines simplicity, performance and value to deliver unrivalled protection from Internet-based threats such as malware, viruses, spyware, anonymizers, IM, P2P, and inappropriate content. As a self-contained appliance-based solution, iPrism offers universal interoperability on any platform and in any network environment, delivering Internet security at the perimeter, to help enforce your Internet acceptable use and security policies. In addition, iPrism seamlessly integrates with your directory services to automate authentication for fast and easy deployment throughout your organization. And new Hybrid Remote Filtering assures policy enforcement for all on-premises or remote users without using VPN or DMZ deployments. Simple to set up and requiring virtually zero maintenance, iPrism Web Security allows your organization to mitigate the risks of legal liability, defend against security breaches, and prevent productivity loss.



Secure Content Management Portfolio

iPrism Web Security

Email Security

Archiving eDiscovery

Data Leakage Prevention

Health & eReputation

Highlights

Multi-Layered Protection

iPrism Web Security's robust antivirus combines with the powerful, proprietary iGuard database to give you multi-layered protection from malware/viruses, spyware and phishing — perimeter defense you won't find in other solutions.

Proprietary Technology

Our exclusive transparent bridge deployment won't introduce latency to your network traffic no matter how busy your network gets. Even networks with the largest pipelines are easily managed by a combination of seamless in-line deployment and kernel-level filtering technology.

Hybrid Remote Filtering Requiring no VPN or Hardware in the DMZ

With our exclusive hybrid technology, you can manage remote users easily with no VPN tunnels, no DMZ deployments and no browser-specific PAC files required, assuring bandwidth conservation and no latency. iPrism's hybrid technology uses a location-aware remote filtering client and a powerful, elastic, in-the-cloud data center to ensure enforcement of your AUP across all users, on or off-premises.

Most Comprehensive and Accurate URL Database

EdgeWave maintains its own URL database, now with 80 categories containing millions of websites. This allows you to easily customize your filtering to fit the exact requirements of your acceptable use policy. Your iPrism Web Security subscription includes automatic, daily database updates, with the crucial security category, covering spyware, malware and phishing sites, updated hourly.

Unrivalled Anonymizer Defense

iPrism Web Security blocks anonymizer sites by employing an unparalleled multi-layered approach that combines human-reviewed URL classification, deep packet inspection and unique proxy blocking to deliver the most effective anonymizer protection on the market.

Enhanced Provisioning Interface



Features

Exclusive Transparent Bridge Mode Deployment

Our standard Transparent Bridge Mode deployment and proprietary kernel-level filtering combine the accuracy and security of pass-through filters with the speed of a pass-by or sniffer-type solution, giving you the best of both worlds. The benefits are significant:

- Because both pass-through and pass-by traffic is monitored, comprehensive security is assured
- Kernel-level filtering means latency is never introduced into the filtering process
- Flexible transparent deployment assures that the EdgeWave appliance can still function as a direct proxy when deployed in Transparent Bridge Mode.
- Functioning in both modes simultaneously allows greater flexibility in deployment.
- Proxy functionality is available for remote users who may not use the same gateway to the Internet as on-site users
- Our flexible deployment works seamlessly in a wide range of network scenarios involving mixed platforms, legacy systems and other variants.

Exclusive Hybrid Remote Filtering

iPrism's Remote Filtering extends comprehensive, flexible Web security to your corporate laptop and other remote users with an exclusive hybrid technology that makes deployment simple and seamless. Unlike any other remote filtering solution on the market, the proprietary iPrism technology delivers powerful Web security to your remote users without using your VPN and without adding any hardware in your DMZ or requiring browser-specific PAC files. Using a combination of our Remote Filtering Client (for both Windows and Mac) and a powerful distributed data center cloud service, iPrism Remote Filtering delivers comprehensive Internet security to your employees no matter where they are located. Our Remote Filtering's centralized administration and reporting assures AUP and security policy enforcement as well as comprehensive reporting across your organization.

Multiple Administration Roles with Granular Override

iPrism gives you the flexibility to define roles for policy and other facets of management with eight pre-defined and customizable roles that you can delegate to any person within the organization (local or authenticated users). And unlike any other solution, ours has a granular override feature that allows you to delegate override privileges to a secondary administrator or even provide self-override roles to some end-users. This is ideal for situations requiring more flexible policy enforcement, or for large organizations trying to optimize resources.

Antivirus

iPrism Web Security's antivirus features a unique four-factored system for detecting and blocking Internet-based viruses that includes a massive signature database, advanced heuristics, emulation and neural network detection. This technology adds a critical layer of antivirus protection for your network while minimizing false positives and false negatives.

iGuard Database with Automated Rating Protocol (iARP)

The 100% human-reviewed iGuard database includes the iARP feature, which further refines Web filtering by sending your most frequently accessed unrated URLs to the iGuard team automatically to be added to your database.

Enhanced Directory Integration

iPrism Web Security eases administration duties by integrating seamlessly with all major network directories including Novell Network Directory Services (NDS), Windows Active Directory, including Window 7 and also Mac clients using AD 2003/2008 and Mac OSX Snow Leopard. In addition, as an LDAP variant, it is possible to integrate EdgeWave Web Filtering with OSX Server Open Directory (LDAP v2/v3).

Centralized Admin and Reporting with SSO

Our Java-based UI with a browser-based interface offers single sign-on (SSO) for comprehensive administration and reporting capabilities using a single interface via any Web browser. In addition, multiple administrators can log into the UI simultaneously for increased efficiency.

iPrism Web Security iLearn Center – Embedded Tutorials

The iPrism iLearn Center offers exclusive video tutorials that are embedded in the new user interface. This enhanced user support feature allows you to manage your Web security configuration and policy settings on-the-fly, shaving hours off the time you spend on IT administration tasks. The iLearn Center houses a series of short video tutorials that walk you through specific tasks without requiring you to log out and access a manual or knowledgebase. These concise, easy-to-use materials include text as well as videos covering a wide range of capabilities. The iLearn Center tutorials are conveniently accessible through the iPrism Web-enabled user interface from a central help page and also via icons located at relevant points throughout the UI.

Anonymizer Defense

Employees who try to circumvent iPrism Web Security by using anonymizer websites and proxies will have their attempts blocked at every turn. Our multi-layered approach uses a variety of techniques:

Spoofed SSL: Only the EdgeWave solution can detect and block anonymizer traffic that tries to spoof secure traffic.

Concealed Surfing: Administrators always know where users are going on the Web because HTTPS traffic is reported using domain names, instead of IP addresses.

Dynamic Proxy Detection including:

- UltraSurf domain
- The Google-web-accelerator domain
- The http-proxy domain

Real-time Updates: Proxy URLs are collected and message groups are monitored daily for new anonymizers.

Active Domain IP Address Mapping: The ability to circumvent our solution using IP addresses is blocked with this mapping feature.

[See the Anonymizer Data Sheet for more details on this feature.](#)

EdgeWave h-Series Appliances

EdgeWave's powerful line of high-performance hardware offers a full range of appliances designed to deliver optimum performance and Web filtering throughput speeds to organizations of all sizes no matter how big their pipelines. All of the h-Series models share a hardened and optimized OS for complete interoperability and unrivalled power and performance.

[See our h-Series Data Sheet for detailed appliance specifications.](#)

About EdgeWave

The EdgeWave portfolio of Web, Email and Data Protection Technologies deliver comprehensive secure content management to 7,000 customers worldwide. Our award-winning iPrism Web Security and Red Condor Email Security products are now complemented by new e-Reputation, Email Archiving and Data Protection Solutions, delivered as hosted, on-premises, and hybrid services. EdgeWave solutions protect your organization's bottom line with unrivalled ease of deployment and the lowest TCO on the market.

Seamless Terminal Server Integration

The unique auto-login feature allows terminal server users to maintain their productivity without incessant authentication requests. Our unique "session based" authentication technology lets you to use Auto-login to simplify the authentication process without installing any software on your terminal or AD servers. This seamless integration is verified by the fact that iPrism Web Security is the only **Citrix Ready appliance-based Web Security solution** on the market, assuring consistent policy application whether your users are Web surfing from their desktops or via Citrix or other terminal server systems.

Comprehensive On-Box Reporting

iPrism Web Security includes comprehensive on-box reporting that requires no additional hardware or software. A variety of report templates are available and reports can be scheduled by day week or month and can run in the background — freeing you to take care of other projects while your reports are automatically generated. You can assign users the right to run the Reports Manager, too.

If you have multiple appliances deployed across your large enterprise and distributed network, the iPrism Enterprise Reporting Server (ERS) delivers comprehensive aggregate reports on all Web activity quickly and easily.

[See the iPrism ERS data sheet for details.](#)

Corporate Office

15333 Avenue of Science
San Diego, CA 92128



Phone: 858-676-2277
Toll Free: 800-782-3762

Fax: 858-676-2299
Email: info@edgewave.com