



Circumvention Defense Network (CDN)

Circumvention Tools are a Dangerous New Trend

Restrictive governments such as China and Iran are attempting to stringently monitor and control Internet access in their countries, resulting in an explosion of sophisticated technologies aimed at thwarting these censorship attempts. In fact, oppressive censorship actions have laid the groundwork for an ongoing 'arms race' between pro-censorship authorities and anti-censorship programmers, some of whom are hackers. The types of technologies being leveraged include Peer-to-Peer, Mixed Cascade, Onion Routing and LocalHost as well as other evasive circumvention tools designed to bypass Internet access controls. These tools are distributed in a variety of ways including through professional organizations, whose users can include younger professionals, students or disgruntled employees. The tools can be installed off-premises or even brought into your organization via portable devices such as thumb drives.

Defense is Difficult

Most of the tools being used in circumvention attempts are client-side applications that are hard to detect and block because new versions are constantly being released, which will change their communication behaviors. These tools work by connecting to a growing number of externally-hosted servers that proxy or re-route the original Web request, allowing anonymous browsing and its inherent risks such as exposing corporate networks to damaging malware and data loss. Because these circumvention tools are changing so fast, it's almost impossible for any IT administrator to keep up. Vendors trying to solve this problem by using only on-box behavioral techniques will find their efforts rendered useless as new circumvention tool versions pop up continuously. Even worse, their customers frequently find themselves waiting months or years until their on-box device catches up – an unacceptable situation considering how fast circumvention technology is evolving.

EdgeWave Technology offers Superior Anti-Circumvention Defense

iPrism's new Circumvention Defense Network (CDN) blocks attempts by circumvention tools to connect to their network proxy or re-routing servers, rendering them harmless and protecting your organization from the damage circumvention can cause including regulatory compliance infractions, data leakage and exposing your network to security breaches. Once the circumvention threat has been blocked, iPrism's Email Alerts and Real-Time Monitor features can be used to address the transgressors and take more serious action if required. iPrism's historical reporting features can document that regulatory compliance, and your acceptable use policy and security policies are being enforced. The EdgeWave CDN stops circumvention attempts and:

- Creates no known false positives which eliminates over-blocking, or requiring SSL certificates on each workstation for traffic decryption techniques
- Mitigates both intentional acceptable use violations and unintentional security breaches and data leakage
- Delivers continuous protection without incurring any network latency



Secure Content Management Portfolio

iPrism Web Security	Email Security	Archiving eDiscovery	Data Leakage Prevention	Health & eReputation
---------------------	----------------	----------------------	-------------------------	----------------------

Enhanced Provisioning Interface



How EdgeWave CDN Works

EdgeWave Leverages hundreds of frequently-reset virtual machines that are hosted in our scalable cloud data center to detect thousands of externally-hosted non-web servers used by various circumvention tools to proxy or re-route users' web requests. We then correlate and filter these IP addresses against those shared with known legitimate websites to eliminate false positives. The results are synchronized with your on-premises iPrism and you get immediate protection. This transparent process enables iPrism to inspect outbound traffic and block circumvention tools from connecting to their server networks outside. Currently, iPrism monitors and blocks UltraSurf, Tor and JAP. However, new circumvention attempts are continuously being detected in the cloud, so your iPrism will have the capacity to stay ahead of emerging threats:

- When new versions of circumvention tools are detected, they are quickly loaded into CDN and onto your iPrism where they start working immediately. This process doesn't require your IT staff to update the iPrism or to wait for a new iPrism release.
- iPrism has placeholders for Client Anonymizers, including FreeGate, so that if our customers experience a significant issue with any of the less frequently used client-based applications, we can repeat the process without version updates and long delays.

About EdgeWave

The EdgeWave portfolio of Web, Email and Data Protection Technologies deliver comprehensive secure content management to 6,500 customers worldwide. Our award-winning iPrism Web Security and EdgeWave Email Security (powered by Red Condor) products are now complemented by 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.

Corporate Office
15333 Avenue of Science
San Diego, CA 92128



Phone: 858-676-2277 Fax: 858-676-2299
Toll Free: 800-782-3762 Email: info@edgewave.com