ReputationWatch™

Prevents DDoS Attacks Automatically with Real-Time IP Reputation Intelligence

ReputationWatch Benefits

- ***Eliminates costly downtime by ensuring your network is always up***
- ***Reduces operational costs by automatically delivering threat intelligence***
- ***Protects organization's investment in IT infrastructure***

The ReputationWatch Security Edge

- ***Identifies known threat entities***
- ***Automatically stops DDoS attacks***
- ***Provides threat intelligence by logging data from threat sources for historical analysis***
- ***Enforces security policy based on national origin of IP addresses***
- ***Customizes content delivery to and from specific nations***
- ***Enhances Corero's industry leading defense against all types of DDoS attacks***

The First Line of Defense for an organization, ReputationWatch™ is a service that provides context-based security to Corero's leading DDoS Defense System (DDS), preventing Distributed Denial of Service (DDoS) attacks. ReputationWatch delivers dynamic protection by identifying constantly changing IP addresses — even hidden ones — and automatically blocking traffic from "known bad" sources in real time.

In addition to stopping attacks from malicious IP addresses, ReputationWatch features Corero's latest geolocation technology advancements, which further empower organizations by allowing them to prevent access or specify security policy based on national origin of IP addresses.

DDoS attacks are increasing in frequency and sophistication, yet are easier to perpetrate. Attacks range from bandwidth-gobbling strikes to those that target applications and fall under the bandwidth consumption radar. Every organization that relies on the Internet to conduct business is a potential victim. As a result, organizations around the world are experiencing costly downtime. Corero's DDS stops virtually all forms of attacks, eliminating disruption, reducing operational costs and protecting organizations' IT infrastructure.

ReputationWatch leverages contextual awareness by assessing the current state of an IP address in a fluid Internet threat environment. IP addresses can go from good to bad in a matter of minutes and vice versa. Computers are hijacked and added to botnets, and bot computers are identified and remediated. It is impossible to maintain up-to-date security configurations manually as these attack sources change.

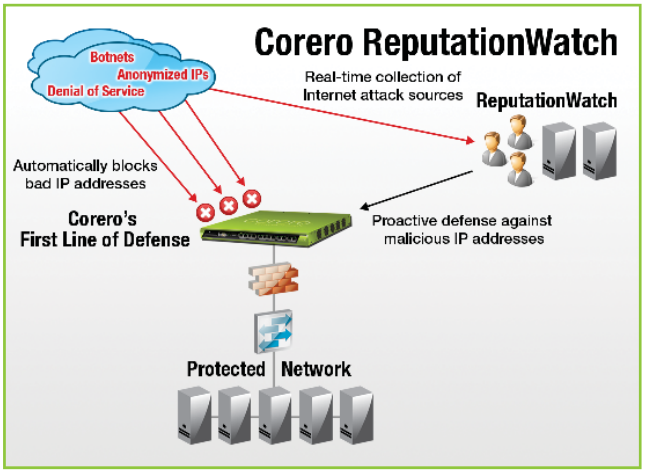

Figure 1. Corero's ReputationWatch continually gathers global intelligence on known attack IP addresses, such as botnets and DDoS attack sources, including "anonymized" or hidden IPs. Corero maintains a real-time threat update feed to Corero's DDoS Defense System, which is configured to automatically block traffic from these IP addresses.

corero
FIRST LINE OF DEFENSE

Corero ReputationWatch

ReputationWatch solves this problem, automatically identifying known malicious sources on the Internet and delivering a continuous, dynamic global intelligence feed. It automatically changes configurations in response to the latest intelligence and blocks “bad” addresses automatically so that your DDS appliance is always defending against the latest threats, such as:

- Known sources of DDoS attacks
- Bots that fall within identified botnet command structures
- Systems delivering specially crafted denial-of-service exploits, such as KillApache
- Identified sources of malicious content attacks
- Phishing sites
- Spam sources

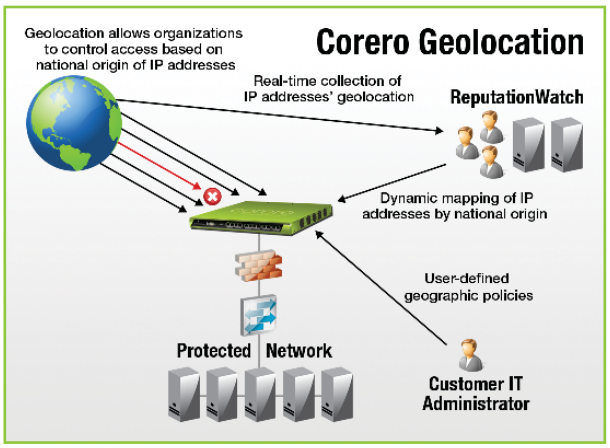

Figure 2. ReputationWatch’s geolocation technology categorizes IP addresses by nation and updates Corero’s DDoS Defense System. IT administrators set policies for each nation, allowing organizations to deny access or control the rate of traffic from countries with which they do not do business.

Frequent, real-time updates reflect the need to respond dynamically to an Internet attack environment that is in a state of constant flux; ReputationWatch feeds also can be delivered at user-customizable intervals to meet each organization’s requirements.

The geolocation capability introduced with ReputationWatch enables enterprises to enforce security policies based on the national origin of IP addresses. Geolocation allows organizations to limit or even exclude traffic from countries with which they do little or no business, or countries associated with high numbers of attacks. For example, an enterprise, service provider or government agency could elect to block or set rate limits on all traffic to control access from a particular nation, and set exceptions for those IP addresses with which they have legitimate business.

ReputationWatch augments Corero’s patented DDoS Defense capabilities that stop cold virtually all forms of DDoS attacks at the enterprise gateway, making it the first line of defense for organizations, ensuring that their IT infrastructure is protected and carrying out their functions as intended.

DDS leverages rate-limiting capabilities and deep-packet inspection to identify and stop both application-layer and network-layer attack traffic. DDS applies a debit and credit behavioral model that shuts down malicious traffic before it can disrupt its target.

With the introduction of ReputationWatch to the DDS arsenal, the first line of network protection is even stronger. Dynamic, real-time reputation-based identification of known bad sources and policies based on geolocation data enable organizations to proactively block threats and preempt all forms of DDoS attack.

About Corero Network Security

Corero Network Security, an organization’s First Line of Defense, is an international network security company and the leading provider of Distributed Denial of Service (DDoS) defense solutions. As the First Line of Defense, Corero’s products and services stop DDoS attacks, protect IT infrastructure and eliminate downtime. Customers include enterprises, service providers and government organizations worldwide. Corero’s appliance-based solutions are dynamic and automatically respond to evolving cyber attacks, known and unknown, allowing existing IT infrastructure — such as firewalls — to perform their intended purposes. Corero’s products are transparent, highly scalable and feature the lowest latency and highest reliability in the industry. Corero is headquartered in Hudson, Massachusetts with offices around the world. www.corero.com.

Corporate Headquarters
1 Cabot Road
Hudson, MA 01749
Phone: +1.978.212.1500
www.corero.com

EMEA Headquarters
68 King William Street
London, England
EC4N 7DZ
Phone: +44 (0) 207.959.2496