IMPERVA®

ThreatRadar Reputation Services

Leverage Reputation Data to Stop Malicious Users and Automated Attacks

ThreatRadar Benefits

- Protect against botnets and automated attacks
- Monitor and block by country to thwart Web attacks and eliminate unwanted traffic
- Leverage up-to-date attack data from leading security providers and thousands of SecureSphere Web Application Firewalls deployed around the world
- Streamline forensics analysis with user reputation and geolocation data
- Build security policies that combine reputation data with other suspicious activity

Over half of all Web users are not human users at all; they're bots.[1] Some of these bots – like search engine crawlers – are harmless; others are more nefarious, probing sites, scraping Web content, posting spam messages, or attacking Websites. Besides stopping dangerous bots, organizations must protect their applications from hackers, who often use anonymous proxies and Tor networks to cloak their identity.

ThreatRadar Reputation Services, an industry-first security service from Imperva, arms the SecureSphere Web Application Firewall with up-to-date reputation data to stop bots and hackers. With ThreatRadar, SecureSphere can identify known malicious sources and prevent attacks like application DDoS, site scraping, and comment spam. ThreatRadar reputation data feeds includes:

- **Malicious IP Addresses**: IP addresses that have repeatedly attacked other websites
- **Anonymous Proxies**: Proxy servers used by attackers to hide their true location
- **The Onion Router (TOR) Network**: Outbound nodes of the identity and location-obfuscating TOR network
- **IP Geolocation**: Location data of IP addresses, to monitor or block access by country
- **Phishing URLs**: Referring URLs of fraudulent sites used in phishing schemes

ThreatRadar Reputation Services augments SecureSphere WAF defenses to stop automated attacks.

ThreatRadar Community Defense

Harnessing the collective insight of SecureSphere deployments around the world, ThreatRadar Community Defense delivers crowd-sourced threat intelligence to ThreatRadar-enabled SecureSphere Web Application Firewalls. ThreatRadar Community Defense uses patent-pending algorithms to translate attack information it gathers into attack patterns, policies, and reputation data. Community Defense distributes these feeds in near-real time to fortify the entire community against emerging threats.

While ThreatRadar Reputation Services relies on security information from leading external security providers, Community Defense draws on live attacks detected by SecureSphere Web Application Firewalls. ThreatRadar Reputation customers who opt to send anonymized attack data to the ThreatRadar cloud will receive ThreatRadar Community Defense free of charge.

[1] "What Google Doesn't Show You," Incapsula, 2012

Track Malicious Sources on a Global Scale

Aggregating attack data from both third-party security providers and SecureSphere Web Application Firewalls, ThreatRadar provides a comprehensive defense against known malicious sources. ThreatRadar augments SecureSphere's existing layers of protection –such as Dynamic Profiling technology, attack signatures, and bot mitigation rules – to provide additional context on suspicious requests. SecureSphere owners can build custom policies that correlate ThreatRadar reputation and geolocation data with other SecureSphere defenses to accurately pinpoint attacks.

Continuous, Automated Feed of Current Attack Sources

ThreatRadar delivers multiple attack feeds, in near real time, to SecureSphere Web Application Firewalls. Security feeds identify sources that have recently executed SQL injection, cross-site scripting, DDoS, or other Web attacks. Imperva continuously updates the feeds, providing current protection against malicious traffic.

Early Detection and Blocking of Malicious Sources

ThreatRadar dramatically reduces application visibility to attackers. By blocking Web requests based on user reputation, hackers have virtually no opportunity to explore the Web application for possible weaknesses and are less likely to launch a successful attack.

> *"The ability to block malicious IP addresses with ThreatRadar Reputation Services was extremely valuable. Traffic from bots and other automated attacks comprises about 25 percent of our site visits."*
>
> **Jeff Mathena, TicketNetwork**

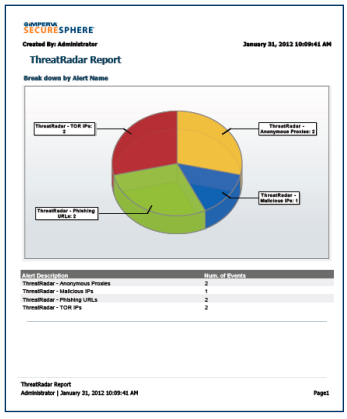
Crowd-Sourced Threat Intelligence to Identify New Attack Vectors

ThreatRadar Community Defense enables SecureSphere Web Application Firewalls to detect new attack patterns without blocking legitimate requests. Community Defense uses patent-pending technology to gather suspicious Web requests, validate that requests are attacks, and transform identified attacks into signatures. Equipped with Community Defense, SecureSphere Web Application Firewalls can spot attacks witnessed by other SecureSphere-protected websites.

Streamlined Forensic Analysis with Clear, Relevant Alerts and Reports

ThreatRadar takes the guesswork out of security event analysis. User reputation and geographic location data provide additional context, enabling precise incident response and minimizing operational workload.

ThreatRadar Reputation Services provides geographical context on Web attacks.



Security alerts show requests from malicious sources. Reports summarize attacks from anonymous proxies, TOR networks, malicious IP addresses and phishing sites.

www.imperva.com