IMPERVA®

ThreatRadar: Web Application Threat Intelligence

Stop threats before they impact your online business

Benefits

Augment the market's leading WAF with feeds that:

- Stop threats before attacks impact your business
- Reduce the volume of incidents going to your security team
- Improve incident response with expert insight
- Leverage and enhance your Imperva investment

Modern threats to your online business come from many angles. Attackers are far more malicious, and far better organized, than in the past. Their capabilities are growing, their agendas are expanding, and they are astoundingly stealthy. You can't possibly see them coming from all angles by yourself – look one direction, they'll attack you from another. When they attack, they steal private information, prevent customers from reaching you, ruin your compliance, or even shut your business down.

If you don't see threats coming, they will disrupt your business. You need advance warning to head them off. You need threat intelligence – the power to leverage reliable sources such as experts, trusted peers, and real-time analysis to defend against both present and, more importantly, future threats. Imperva ThreatRadar is threat Intelligence for SecureSphere Web Application Firewall.

ThreatRadar Editions

ThreatRadar Community Edition and ThreatRadar Enterprise Edition combine three of Imperva's powerful ThreatRadar protection products into one highly effective bundle. They are easy to buy, easy to implement, and easy to afford. ThreatRadar supercharges and arms your SecureSphere Web Application Firewall with advanced feeds, such as:

Insights based upon reputation

- Visitors who have attacked other sites, or looked for vulnerabilities on them
- Visitors hiding their identities, or coming from suspicious countries or regions

Insights from the community

- Security policies translated from what others like you are seeing
- Shared back into the community

Insights into bots visiting your site

- Which visitors are human, which are good bots, and which are bad
- More bot visitors than not, are a threat

Insights based upon reputation

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 include:

- Malicious IP Addresses: IP addresses which 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 based upon geography
- Phishing URLs: Referring URLs of fraudulent sites used in phishing schemes
- Comment Spammers: IP addresses of known, active comment spammers

Insights from the community

ThreatRadar Community Defense harnesses 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, ThreatRadar 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 a substantial discount over those who do not.

Insights into bots visiting your site

ThreatRadar Bot Protection Services is an add-on service for SecureSphere Web Application Firewall that accurately distinguishes between good bots, bad bots, and human users, so you can take action accordingly. Using SecureSphere WAF and ThreatRadar Bot Protection Services, malicious bots, a top threat for web applications, can be identified and stopped.

ThreatRadar Bot Protection Services' client classification engine analyzes and classifies all incoming traffic to your site. This engine distinguishes between human and bot traffic, identifies "good" and "bad" bots; classifies traffic by browser type; and more. This granular level of information enables you to control who is allowed access to your website.

This classification information is used to drive WAF policy enforcement decisions, including handling bad and suspected bots. You can choose to have administrators receive an alert (e.g., for monitoring purposes), or have SecureSphere block the bot.

IMPERVA®

www.imperva.com