ThreatRadar

Industry-First Reputation-Based Web Application Security

As the threat landscape evolves, hackers are becoming more industrialized and well resourced. Sophisticated, state-sponsored attacks take advantage of large-scale automation capabilities, such as networks of bots. Effective mitigation of such attacks must be automated and timely, adapting to continuously shifting attack locations and techniques.

ThreatRadar is a unique add-on security service for Imperva's SecureSphere Web Application Firewall (WAF) that provides an automated defense against automated attacks. By integrating credible, timely information on known attack sources into the WAF defense, ThreatRadar can quickly and accurately stop traffic from malicious sources before an attack can be launched.

Track Attack Sources on a Global Scale

Leveraging the security community collective insight, centralized ThreatRadar servers aggregate information on attack sources from credible data providers. These providers monitor global malicious activity originating from anonymous proxies, specific IP addresses, botnets, and phishing sites. ThreatRadar allows organizations to benefit from traffic source reputation data, based on attempted attacks on other websites.

Continuous, Automated Feed of Current Attack Sources

ThreatRadar servers deliver an integrated attack source feed, in near real time, to all ThreatRadar-powered SecureSphere WAFs. ThreatRadar is fully maintained by Imperva and eliminates the manual effort required to identify, subscribe, and maintain these security feeds. ThreatRadar continuously refreshes the feed, providing up-to-date protection against malicious traffic.

Dynamically Adapt Web Security Policies

As SecureSphere WAF receives attack source information, ThreatRadar dynamically adjusts Web security policies to alert or block traffic from newly identified attack sources. Furthermore, custom security rules can use information provided by the feeds to fine-tune the response for specific types of traffic, such as the ability to block only the traffic that comes from a malicious source exhibiting suspicious behavior.

Early Detection, Blocking of Malicious Sources

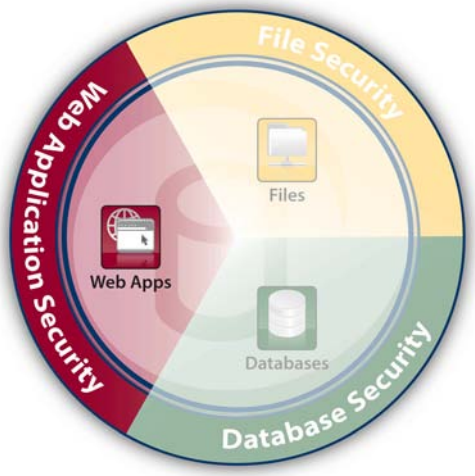
ThreatRadar increases the accuracy of SecureSphere WAF and dramatically reduces application visibility to attackers. By blocking access requests based on traffic source reputation, hackers have virtually no opportunity to explore the Web application for possible weaknesses and are less likely to launch a successful attack.

Streamlined Forensic Analysis and Attack Source Intelligence

ThreatRadar removes the guesswork out of event analysis by providing greater operational insight into attacker origins and methods. Source information, such as malicious IP address and geographic location of the attack, provides additional context on attackers, enabling precise incident response procedures and minimizing operational workload.

ThreatRadar Key Benefits

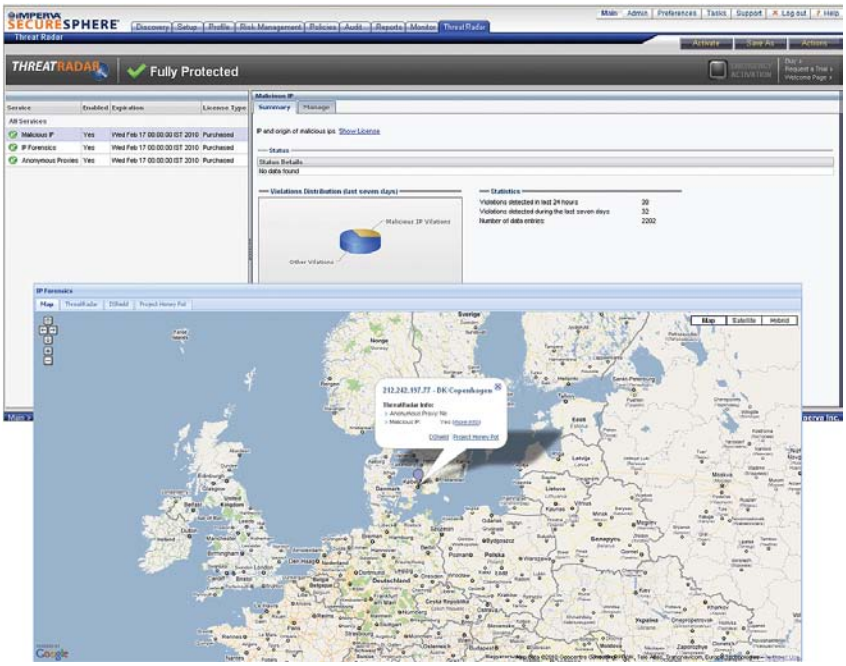
- Centralized, global monitoring of credible attack source data providers
- Automated, dynamic adjustment of security policies
- Block traffic from malicious sources even before an attack is attempted
- Visibility into phishing attacks on the customer's website
- Forensics information on attacks blocked by ThreatRadar



ThreatRadar Data Services Cover Multiple Threats

ThreatRadar specifically protects against:

- **Malicious Sources**: Traffic sources that have repeatedly performed malicious activity on other Web applications. To date, over ten million botnets have executed attacks on behalf of remote hackers.
- **Anonymous Proxies**: Traffic sources that use anonymous proxies. By hiding the identity of the traffic source, anonymous proxies are often exploited by hackers to launch attacks.
- **The Onion Router (TOR) Networks**: Traffic source that use TOR networks to launch attacks without revealing their identity and location.
- **Phishing URLs**: Real-time alerting on phishing incidents against the customer domain.



ThreatRadar: Mitigate automated attacks from known malicious sources and provides geographical context on attack.

About Imperva

Imperva is the global leader in data security

Thousands of the world's leading businesses, government organizations, and service providers rely on Imperva solutions to prevent data breaches, meet compliance mandates, and manage data risk. Underscoring Imperva's commitment to data security excellence, the Imperva Application Defense Center (ADC) is a world-class security research organization that maintains SecureSphere's cutting edge protection against evolving threats.

Imperva
Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com