IMPERVA®

ThreatRadar: Web Application Threat Intelligence

DATASHEET

Stop threats before they impact your online business

Cybercriminals exploit vulnerabilities in internet facing web applications as the initial attack vector to bypass traditional security controls, take over accounts, laterally move through your IT infrastructure, and gain access to business critical data and applications. The capabilities of such attackers are growing, their agendas are expanding, and their methods are astoundingly stealthy.

Advanced warning systems to defend against constantly evolving web-based attacks are vital to protect against advanced cyber attacks. This is where threat intelligence from a trusted crowd-sourced platform and community of peers has become extremely valuable. Imperva ThreatRadar is the premier threat intelligence feed that arms the industry leading[1] SecureSphere Web Application Firewall (WAF) with the following protections.

Imperva ThreatRadar is the premier threat intelligence feed that arms the industry leading[1] SecureSphere Web Application Firewall

- Reputation Service: Filters traffic based upon latest, real-time reputation of source
- Community Defense: Adds unique threat intelligence crowd-sourced from Imperva users
- Bot Protection: Detects botnet clients and application DDoS attacks
- Account Takeover Protection: Protects website user accounts from attack and takeover
- Fraud Prevention: Simplifies deployment of best-in-class partner fraud prevention solutions

[1] Gartner's Magic Quadrant for Web Application Firewalls, 15 July 2015

Imperva ThreatRadar Subscription Service

- Reputation Service
- Community Defence
- Bot Protection
- Account Takeover

Leverage Threat Intelligence to Stop Malicious Users and Automated Attacks

Crowd-Sourced Threat Intelligence to Identify New Attack Vectors

ThreatRadar employs threat intelligence research from Imperva Application Defense Center (ADC), which is comprised of some of the world's leading experts in data and application security and combines it with the live threat data from the community of SecureSphere WAF customers.

Early Detection and Blocking of Malicious Sources

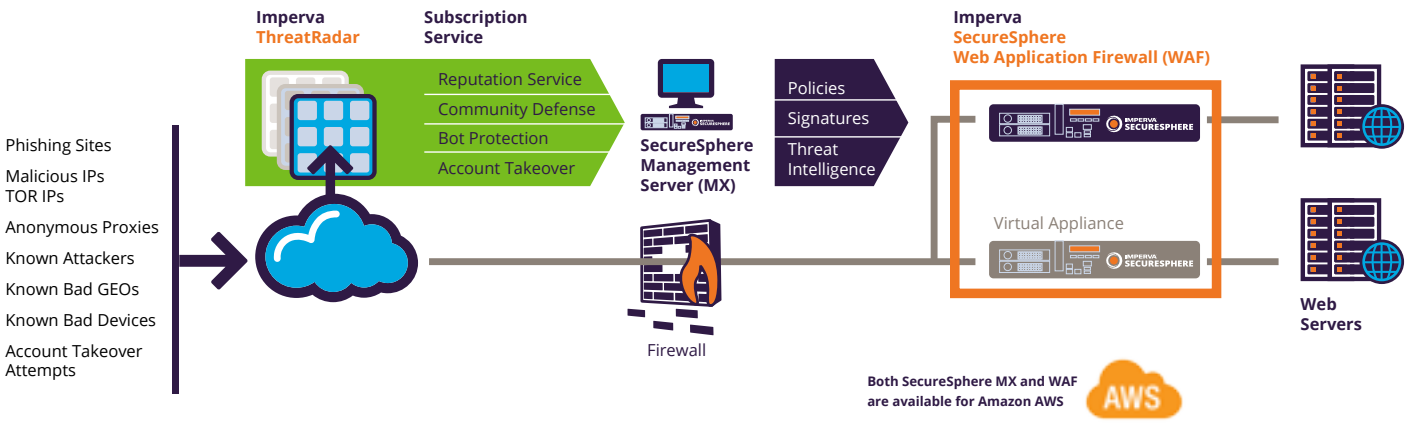
Aggregating attack data from both third-party security providers and SecureSphere WAF deployments worldwide, ThreatRadar provides an early detection and comprehensive defense against known malicious sources.

Improve Efficacy of Threat Data and Reduce Workload of Security Operations

SecureSphere WAF customers can dramatically reduce the workload of security operations related to malicious and unwanted web traffic, by automatically alerting/blocking web requests based on user reputation, botnets, account takeover attempts and hackers conducting reconnaissance of applications to find weaknesses.

Continuous, Automated Feed of Current Attack Sources

ThreatRadar automatically delivers multiple attack feeds in near real-time. Security feeds identify sources that have recently executed SQL injection, cross-site scripting, DDoS, and other Web attacks.



Known Malicious Sources

- 90% of attacks are from known bad actors
- 60% of traffic is from malicious bots
- 50% of web attacks are using stolen credentials

source: Imperva and Verizon DBIR

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 Service

ThreatRadar Reputation Service arms the SecureSphere WAF with real-time threat intelligence on known malicious sources, such as:

- Malicious IP Addresses: Sources that have repeatedly attacked other websites
- Anonymous Proxies: Proxy servers used by attackers to hide their true location
- TOR Networks: Hackers who are using The Onion Router (TOR) to disguise the source of attack
- IP Geolocation: Geographic location where attacks are coming from and block access
- Phishing URLs: fraudulent sites (URLs) that are used in phishing attacks
- Comment Spammers: IP addresses of known active comment spammers

ThreatRadar Community Defense

ThreatRadar Community Defense harnesses the collective insight of SecureSphere WAF deployments around the world and delivers crowd-sourced threat intelligence in near real-time to each SecureSphere WAF installation. It uses patent-pending algorithms to translate live-attack data that it gathers into attack patterns, policies, and reputation data and delivers near real-time threat intelligence that is seen by Imperva WAF customers.

While ThreatRadar Reputation Services relies on security information from leading external security providers, ThreatRadar Community Defense draws on live attack information aggregated from SecureSphere WAF deployments around the world.

SecureSphere WAF customers who opt-in to send anonymized attack data to the ThreatRadar cloud receive ThreatRadar Community Defense free of charge.

ThreatRadar Bot Protection

ThreatRadar Bot Protection Service enables SecureSphere WAF to accurately distinguish incoming traffic between human and bot traffic, identify “good” and “bad” bots; classify traffic by browser type, and more.

Malicious bots account for more than 95% of all website attacks, including DDoS attacks, injecting comment spam, and scraping website content. By eliminating unwanted/unwelcome bots, which account for up to 30% of all website traffic, it improves website performance and security.

Imperva SecureSphere Cyber Security

Imperva SecureSphere is a comprehensive, integrated security platform that includes SecureSphere web, database and file security. It scales to meet the data center security demands of even the largest organizations and is backed by the Imperva Application Defense Center, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

ThreatRadar Account Takeover Protection

Criminals use stolen credentials from malware and phishing attacks to gain unauthorized access to customer accounts, to transfer money, execute fraudulent transactions, and bring down reputations of companies. ThreatRadar Account Takeover Protection enables SecureSphere WAF to detect and mitigate such unauthorized access in real time by leveraging credential/device threat intelligence.

Credential Intelligence: Detect and mitigate

- Credential stuffing using harvested credentials
- Dictionary attacks using weak passwords
- Privileged account default password attacks

Device Intelligence: Detect and mitigate

- Device logins from high-risk devices
- Transactions from devices behind TOR/proxies
- Geo-based high risk locations – ISPs, Geo/IP mismatches
- Multiple devices accessing single account, or single device accessing multiple accounts in a short period of time

ThreatRadar Fraud Prevention

ThreatRadar Fraud Prevention connectors for Imperva SecureSphere WAF enables organizations to rapidly integrate with best-in-class fraud prevention partners with complete transparency to the applications protected.

SecureSphere WAF integrates with the following fraud monitoring solutions, allowing businesses to centrally manage fraud policies.

- iovation ReputationManager 360
- ThreatMetrix TrustDefender ID

ThreatRadar Editions

ThreatRadar bundles the three subscription feeds – Reputation Services, Community Defense, and Botnet Protection, into the following two bundles, to make it easy to buy and cost-effective to implement.

ThreatRadar Community Edition

This bundle is available to those that OPT-IN to share live attack data from their SecureSphere WAF installations with Imperva global ThreatRadar repository in the cloud, after any customer specific data has been automatically anonymized.

ThreatRadar Enterprise Edition

This bundle is available to those that OPT-OUT from sharing live attack data from their SecureSphere WAF installations with Imperva ThreatRadar repository in the cloud. These customers gain the collective insight of SecureSphere WAF deployments around the world and benefit from the premier threat research from Imperva ADC.