ThreatRadar

Stop Automated Attacks and Web Fraud with Industry-first WAF Security Services

Harnessing the power of automation, widespread malware infections, and off-the-shelf hacking toolkits, cybercriminals can easily launch powerful, large-scale attacks. ThreatRadar is a family of cloud-based security services that provide up-to-date information and analysis of Web users to stop automated attacks and Web-based fraud.



ThreatRadar Services help organizations:

- Block large-scale Web attacks by identifying known malicious sources
- Avoid expensive fraud mitigation costs and brand damage by preventing Web fraud
- Aggregate reputation data from the cloud in near real-time
- Stop automated attacks, like Web site scraping and comment spam, that mimic normal traffic
- Improve security accuracy by correlating user reputation, geolocation, and fraud data with Web attack intelligence
- Automate Web fraud and reputation security, without requiring application changes

Products

ThreatRadar Reputation Services

ThreatRadar Fraud Prevention Services

ThreatRadar Reputation Services

Reputation-Based Security to Stop Automated Attacks

As the threat landscape evolves, hackers have become more industrialized and better equipped. Sophisticated Web 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 Reputation Services provide an automated defense against these attacks by detecting and stopping known malicious sources. As an add-on service for the SecureSphere WAF, ThreatRadar detects Web traffic originating from IP addresses currently attacking other Websites, from anonymizing services, and from undesirable geographic locations.

Track Attack Sources on a Global Scale

Leveraging the collective insight of the security community, ThreatRadar's cloud-based servers aggregate information on attack sources from leading data providers. Armed with this information, SecureSphere gateways can identify and block:

- **Malicious Sources**: IP addresses that have repeatedly performed malicious activity on other Websites. To date, over ten million botnets have executed attacks on behalf of remote hackers.
- **Anonymous Proxies**: Web traffic originating from anonymous proxy servers. By hiding the identity of the traffic source, anonymous proxies are often exploited by hackers to launch attacks.
- **The Onion Router (TOR) Networks**: traffic sources that use TOR networks to launch attacks without revealing their identity and location.
- **IP Geolocation**: IP addresses that are based in a specific geographic location. Geolocation enables organizations to monitor or block access from objectionable countries.
- **Phishing URLs**: real-time alerting on phishing incidents against the customer domain.

Continuous, Automated Feed of Current Attack Sources

ThreatRadar Reputation Services deliver integrated attack source feeds, in near real time, to all ThreatRadar-powered SecureSphere gateways. Fully maintained by Imperva, security feeds can identify sources that execute automated attacks like application DDoS, site scraping, Web comment spam, and automated SQL injection. Imperva continuously updates the feeds, providing current protection against malicious traffic.

Early Detection, Blocking of Malicious Sources

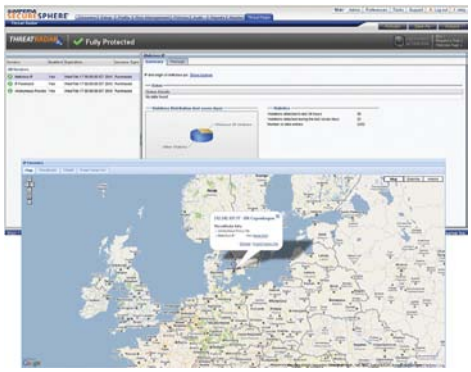
ThreatRadar Reputation Services dramatically reduce application visibility to attackers. By blocking access requests based on traffic source reputation, hackers have virtually no opportunity to explore the Web application for possible weaknesses and are less likely to launch a successful attack.

Streamlined Forensic Analysis and Attack Source Intelligence

ThreatRadar Reputation Services takes the guesswork out of security event analysis. Information provided by ThreatRadar such as an attacker's reputation and geographic location provides additional context, enabling precise incident response and minimizing operational workload.

Dynamic Security Policy Updates

As SecureSphere receives information about attack sources, security policies are dynamically adjusted to alert on or block traffic from newly identified attack sources. Organizations can build custom security rules that correlate reputation data with Web attack intelligence to accurately block malicious users.



ThreatRadar Reputation Services mitigate automated attacks from known malicious sources and provides geographical context on attack.

Reputation Services Benefits

- Aggregate reputation data from the foremost commercial and non-commercial providers to identify known attack sources
- Protect against automated and botnet attacks
- Offer near real-time feeds of global reputation data
- Visualize attack location and summarizes reputation data with integrated forensics tool
- Instantly update SecureSphere WAF policies based on current attack data

"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

ThreatRadar Fraud Prevention Services

Detect and Stop Web-based Fraud

Fraud costs organizations hundreds of millions of dollars in lost revenue, brand damage, and customer churn. Commercial fraud security solutions help mitigate fraud, but they often require extensive Web application changes. In addition, most fraud detection solutions cannot work with one another to maximize accuracy.

ThreatRadar Fraud Prevention Services enable organizations to rapidly provision and manage fraud security solutions without needing to update Web applications. By integrating with leading fraud security vendors, the SecureSphere WAF can transparently identify and stop fraudulent transactions. ThreatRadar Fraud Prevention also provides powerful monitoring and enforcement capabilities, allowing businesses to centrally manage and correlate Web application firewall and fraud policies.

Intelligent Fraud Mitigation Reduces Fraud Expenses, Customer Churn

ThreatRadar Fraud Prevention allows organizations to lower fraud remediation costs, streamline fraud investigations and maintain customer loyalty. By integrating with multiple Web fraud detection vendors, it offers best-in-class protection against online fraud. As an add-on service to SecureSphere, this solution is the cost-effective, simple, and accurate way to detect and stop Web fraud.

Centralized Management of Fraud and Web Security Policies

ThreatRadar Fraud Prevention provides a single integration point to manage and correlate fraud detection technologies with Web Application Firewall rules. For example, organizations can define different fraud policy actions based on user reputation, geographic location, time of day, URL accessed, or user name. By correlating fraud and attack activity, organizations can block fraudulent requests with pinpoint precision.

Rapid Time-to-Security

ThreatRadar Fraud Prevention helps organizations roll out Web fraud prevention quickly and cost effectively. As a simple add-on to the SecureSphere Web Application Firewall, this service enables organizations to implement fraud detection without updating Web applications. ThreatRadar therefore offers rapid fraud provisioning, decreasing the window of exposure imposed by lengthy Web application development processes.

Lower Total Cost of Ownership

ThreatRadar Fraud Prevention eliminates the need to manually update Web applications. By incorporating Web fraud prevention into SecureSphere, organizations can avoid costly development efforts and schedule disruptions. The latest updates and APIs from Imperva's fraud prevention partners are seamlessly incorporated into the service. This enables organizations to take advantage of new fraud prevention features quickly, without costly and protracted Web application changes.

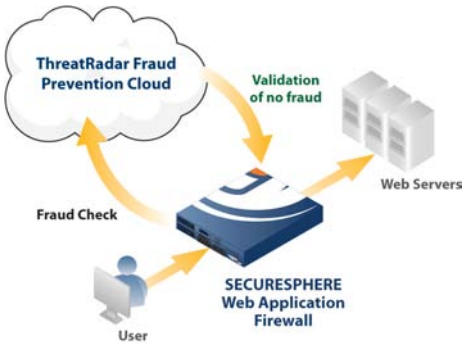
Active Enforcement of Web Fraud Policies

Imperva transforms fraud detection into fraud prevention. Using SecureSphere's intuitive Web-based security policies, organizations can instantly block fraudulent transactions, redirect compromised users to a custom error page, or trigger a risk management system to open a fraud investigation.

Detailed Alerts and Graphical Reporting of Fraud Activity

With SecureSphere's powerful reporting framework, customers can generate executive-level summaries as well as detailed reports of fraudulent events. Security alerts capture full event detail for forensics analysis. SecureSphere's monitoring and reporting capabilities allow organizations to quickly assess risks and investigate fraudulent activity.

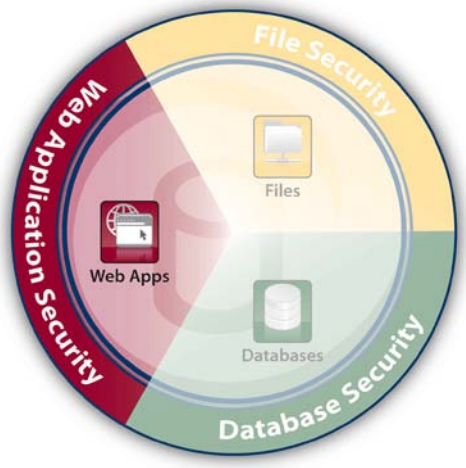
ThreatRadar Fraud Prevention Services



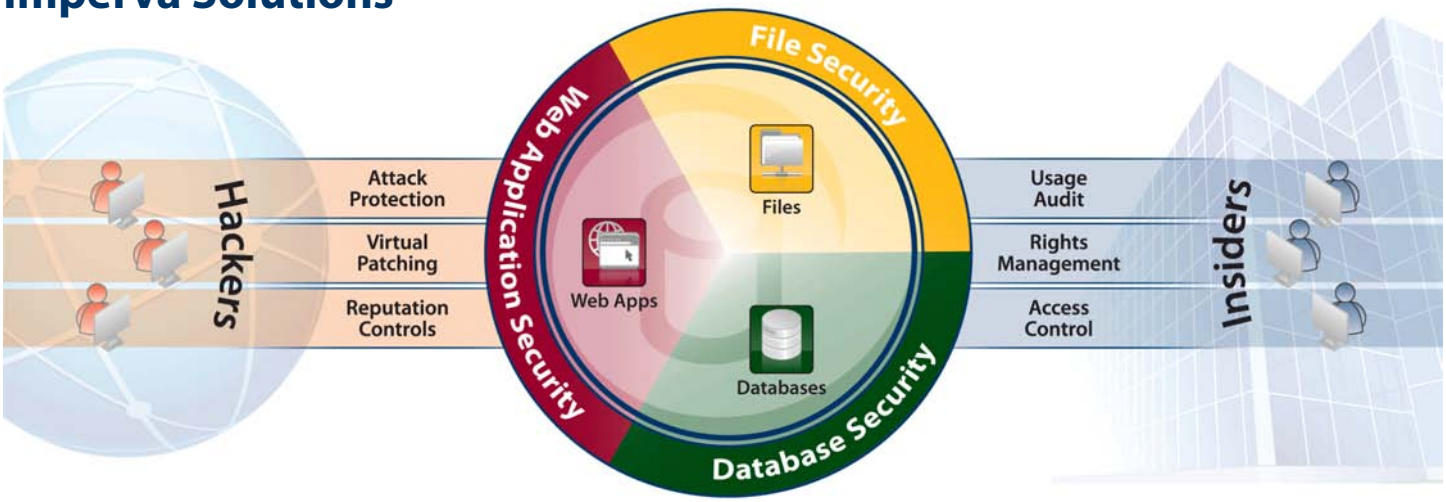
With ThreatRadar Fraud Prevention Services, organizations can quickly detect and stop fraudulent Web transactions

Fraud Prevention Services Benefits

- Maintain brand image and customer loyalty by preventing fraudulent activity
- Correlate fraud and WAF policies for granular identification and blocking of illicit activity
- Rapidly provision Web fraud security, avoiding the cost and time required to manually integrate fraud detection into Web applications
- Reduce the cost and disruption of re-coding applications
- Quickly enforce fraud protection using intuitive Web-based policies



Imperva Solutions



	Family	SecureSphere Product
Management Server	Database	**Database Activity Monitoring** Full auditing and visibility into database data usage **Database Firewall** Activity monitoring and real-time protection for critical databases **Discovery and Assessment Server** Vulnerability assessment, configuration management, and data classification for databases **User Rights Management for Databases** Review and manage user access rights to sensitive databases **ADC Insights** Pre-packaged reports and rules for SAP, Oracle EBS, and PeopleSoft compliance and security
	File	**File Activity Monitoring** Full auditing and visibility into file data usage **File Firewall** Activity monitoring and protection for critical file data **User Rights Management for Files** Review and manage user access rights to sensitive files **SecureSphere for SharePoint** Visibility and analysis of SharePoint access rights and data usage, and protection against web-based threats
	Web	**Web Application Firewall** Accurate, automated protection against online threats **ThreatRadar** Fraud prevention and reputation-based security services to stop Web fraud and automated attacks

Family	Imperva Cloud Services
Web	**Cloud WAF** Easy and affordable cloud-based Web Application Firewall service **Cloud DDoS Protection** Safeguards businesses from the most debilitating and protracted DDoS attacks

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.

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

© Copyright 2011, Imperva
All rights reserved. Imperva, SecureSphere, and "Protecting the Data That Drives Business" are registered trademarks of Imperva.
All other brand or product names are trademarks or registered trademarks of their respective holders. #DS-THREATRADAR-SERVICES-1011rev1