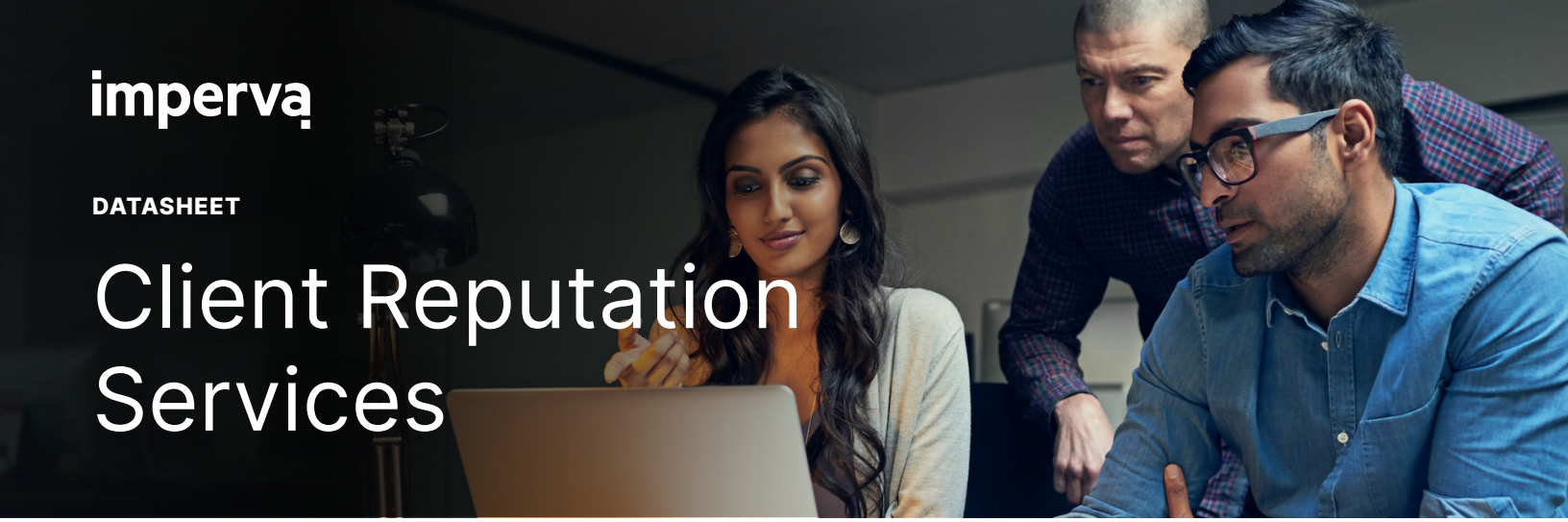
imperva

DATASHEET

Client Reputation Services



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, 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 Client Reputation Services is the premier threat intelligence feed that arms the industry leading[1] Web Application Firewall (WAF) Gateway with the following protections:

- **Client Reputation Services Feed:** Filters traffic based upon latest, real-time reputation of source
- **Client Reputation Services Community Defense Feed:** Adds unique threat intelligence crowd-sourced from Imperva users
- **Client Classification Services Feed:** Detects botnet clients and application DDoS attacks
- **Signature Emergency Feed:** Delivers latest signatures right away to mitigate against zero-day vulnerabilities

Imperva Client Reputation Services is the premier threat intelligence feed that arms the industry leading[1] WAF Gateway.

[1]Gartner's Magic Quadrant for Web Application Firewalls, 13 October 2020

Leverage threat intelligence to stop malicious users and automated attacks

Crowd-sourced threat intelligence to identify new attack vectors

Client Reputation Services employs threat intelligence research from Imperva Research Labs, composed of some of the world's leading experts in data and application security, and combines it with live threat data from the community of WAF Gateway customers.

Early detection and blocking of malicious sources

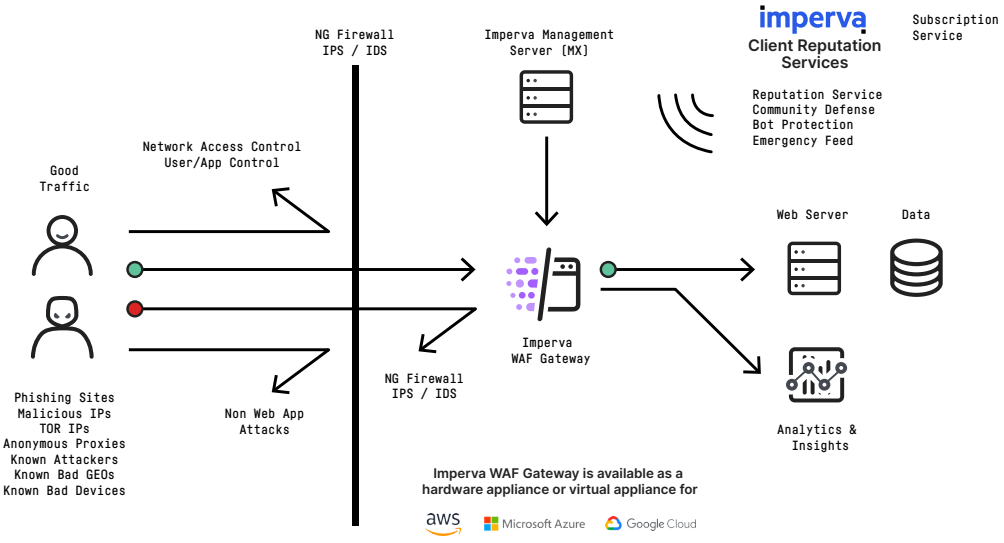
Aggregating attack data from both third-party security providers and WAF Gateway deployments worldwide, Client Reputation Services provides an early detection and comprehensive defense against known malicious sources.

Improve efficacy of threat data and reduce workload of security operations

WAF Gateway 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, attempts and hackers conducting reconnaissance of applications to find weaknesses.

Continuous, automated feed of current attack sources

Client Reputation Services 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.



Streamlined forensic analysis with clear, relevant alerts and reports

Client Reputation Services 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.

Client Reputation Services Feed

Client Reputation Services arms the WAF Gateway 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 attacks
- **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
- **Spandexing:** known active comment spammers URLs

Client Reputation Services Community Defense Feed

Client Reputation Services Community Defense harnesses the collective insight of WAF Gateway deployments around the world and delivers crowd-sourced threat intelligence in near real-time to each WAF Gateway installation. It uses 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 Client Reputation Services relies on security information from leading external security providers, Client Reputation Services Community Defense draws on live attack information aggregated from WAF Gateway deployments around the world. WAF Gateway customers who opt-in to send anonymized attack data to the Client Reputation Services cloud receive Client Reputation Services Community Defense free of charge.

Client Classification Services Feed

Client Reputation Services enables WAF Gateway 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.

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

Client Reputation Services editions

Client Reputation Services bundles the three subscription feeds—Client Reputation Services, Client Reputation Services Community Defense, and Client Reputation Services Bot Protection, into the following two bundles, to make it easy to buy and cost-effective to implement:

Client Reputation Services Community Edition

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

Client Reputation Services Enterprise Edition

This bundle is available to those that OPT-OUT from sharing live attack data from their WAF Gateway installations with Imperva Client Reputation Services repository in the cloud. These customers gain the collective insight of WAF Gateway and Cloud WAF deployments around the world and benefit from the premier threat research from Imperva Research Labs.

Signature Emergency Feed

Signature Emergency Feed delivers the latest signatures right away to WAF Gateway to protect web applications against newly discovered vulnerabilities. Instead of waiting for periodic updates enterprises can gain immediate protection against zero-day vulnerabilities closing the window of exposure to cyber threats.

IMPERVA APPLICATION AND DATA SECURITY

Imperva Application and Data Security is a comprehensive, integrated security platform that includes WAF Gateway, Database and File Security. It scales to meet the data center security demands of even the largest organizations, and is backed by Imperva Research Labs, a world-class security research organization that maintains the product's cutting-edge protection against evolving threats.

Learn more about Imperva Application Security at +1.866.926.4678 or online at imperva.com

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.