Barbarians at the Gate: Shoring Up Web Application Defenses with Client Reputation
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>The Necessity of WAF Best Practices</td>
<td>3</td>
</tr>
<tr>
<td>Improve Security Decisions with Client Reputation Monitoring</td>
<td>4</td>
</tr>
<tr>
<td>Cloud Security Intelligence (CSI) – Akamai’s Approach</td>
<td>5</td>
</tr>
<tr>
<td>Threat Visibility for Superior Security Decision Making</td>
<td>5</td>
</tr>
<tr>
<td>Why Collective Intelligence is Important</td>
<td>6</td>
</tr>
<tr>
<td>Recommendation: Adopt a Multi-Layered Defense</td>
<td>6</td>
</tr>
<tr>
<td>Conclusion</td>
<td>7</td>
</tr>
</tbody>
</table>
**Introduction**

Defending your web applications against data theft and your websites against defacement is an on-going challenge. Web applications are particularly vulnerable to cyberattacks, as well as disruptions to application performance and availability. Case in point: In June 2015, personal information of 4 million federal employees may have been stolen as a result of one of the biggest hacks ever against the U.S. government.

In building a robust cyber defense, it is common practice for security teams to adopt a layered approach to protect their online assets – rate controls, payload detection and client reputation monitoring. For example, many people invest in home security systems if neighbors have been burglarized, especially when crime increases compared to previous years. Rate controls similarly alert you and protect you from an increase in malicious web activity. With an alarm system monitoring windows and doors, it becomes much more risky and difficult for an intruder to steal the goods, which is akin to how a Web Application Firewall (WAF) stops individual requests based on their payloads. And like a perimeter camera that can compare known burglars to a person on the porch and alert police to stop a crime before it is committed, Akamai’s client reputation monitoring service can alert on and block known sources of malicious traffic.

This white paper will explore the benefits of adding client reputation intelligence at the web application level to provide score-based Internet Protocol (IP) client behavior over time. Armed with this client reputation data, organizations get enhanced visibility to make better cloud security decisions and block threats from malicious IP addresses that may target their businesses.

**The necessity of WAF best practices**

In today's high threat landscape, a multi-layered defense is essential. Rate controls are the first line of defense and can be used to protect web applications against Layer 7 distributed denial of service (DDoS) volumetric attacks by monitoring and controlling the rate of requests against them. Behavioral rules can be set to respond to bursts of requests in seconds and selectively alert on and block attackers based on IP addresses and other parameters.

The next line of defense is typically a WAF, which is used to protect web applications against malicious attacks. The WAF is like a sentinel in the middle of an HTTP conversation that monitors traffic and relies on rule sets to decide if an IP request is malicious or legitimate. WAFs come with examples of rule sets to help alleviate the complexity, but the challenge lies in the ability to adjust the rule sets, sometimes very subtly, to the day-to-day realities of the business environment.
WAFs excel at flagging potentially malicious client requests, but it is important to avoid blocking legitimate requests from vendors and customers who expect high availability and performance. WAF best practices demand that rules must be changed and modified on a regular basis to keep pace with evolving attack vectors, but without compromising the ability to allow legitimate HTTP traffic through or adversely affecting the user experience. Unfortunately, a 2015 research survey on WAF usage habits conducted by the Ponemon Institute and sponsored by Akamai reveals that many WAFs are not being properly maintained because there is a shortage of IT talent with the specialized web application security knowledge.

In the same Ponemon study, despite the escalation of web application-based attacks, 30 percent of the respondents who had purchased WAFs indicated that they have not deployed them, which reflects the challenge of finding experienced people to manage a WAF. Yet, two-thirds of the respondents expected a WAF to provide a high level of security while preserving application performance.

One demonstrated solution for implementing WAF best practices while maintaining web application performance is to engage a cloud-based security service provider. With a managed cloud security solution, customers can augment the best practice of a secure software maintenance lifecycle with a scalable WAF solution from the services provider, coupled with expert guidance from security operations center (SOC) experts. Other advantages of a cloud-based WAF are superior performance due to its scalability and minimal latency.

Even if an organization has the time and money to manage a WAF in-house, using a solution that reduces some of the noise that the WAF produces will make the job easier for IT security. One way to enhance cyber defenses is with a new web application security service called client reputation monitoring that compliments a well-configured WAF and enables web application security threats to be blocked at the source before they reach the WAF. In essence, instead of focusing on cleaning up after a break-in, it’s now possible to identify and stop a crime before it happens.

Client reputation monitoring and a WAF can work together seamlessly to block the source of bad requests as well as the requests themselves.

**Improve security decisions with client reputation monitoring**

More organizations are taking a proactive approach to securing not only web applications, but their entire web-facing environment. Client reputation monitoring complements WAFs and other cyber defenses, such as DDoS protection, with an additional layer of protection against — and visibility into — malicious actors at the source.

Client reputation monitoring provides this additional protection by focusing on the source of the threat – web clients as opposed to attack vectors – and stopping the attack before any of the bad requests reach the WAF for inspection.
This approach uses advanced algorithms on the data collected from a large number of web clients to identify malicious actors. The malicious web clients are scored according to their past behavior and current likelihood of engaging in four types of attack behavior: application layer attacks, website scanning and scraping, other web attack launches and denial of service DoS attacks.

Most importantly, client reputation monitoring gives organizations the ability to look at a particular client IP address and predict, based on past behavior, whether that client will engage in future attacks on their web application platform. In addition, the data can help to predict the intent of future requests from a particular client IP address.

Cloud Security Intelligence (CSI) – Akamai’s approach to client reputation monitoring

Akamai’s Cloud Security Intelligence (CSI) is a security platform that interacts with billions of client IP addresses every quarter, and collects data for the client reputation monitoring service. The more data feeding it, the better the reputation service can be.

Akamai stores 4 petabytes of data, made up of more than 20 terabytes of daily attack data in Hadoop clusters. Data sources include WAF triggers and other data from Akamai customer WAFs and content delivery network (CDN) logs. Akamai data scientists query this data hourly, using heuristics to identify attack patterns and client behavior, and to reduce false positives.

Threat visibility for superior security decision making

Akamai’s client reputation monitoring service provides organizations with two core abilities. The first is the ability to determine whether or not you want to block a particular client accessing your servers based on the combination of level of client risk scoring or type of attacker, such as data scrapers and scanners, DDoS, or web application attack. The second is the ability to choose at what level you want to block access. This combination of flexibility and control is made possible by a number of key capabilities:

- **Correlate data across customers** – Correlate client requests across many customers and identify malicious intent, resulting in threat intelligence that can improve security decisions around specific clients.

- **Sort by multiple categories** – Associate malicious behavior with web attackers participating in web vulnerability exploitation attempts. This includes SQL injection (SQLi), remote file inclusion (RFI) or cross site scripting (XSS) – and DDoS attackers using tools such as low orbit ion cannon (LOIC) and high orbit ion cannon (HOIC) to launch denial of service attacks, and scanners performing web application vulnerability scanning, and web scrapers.

- **Score by client risk** – Score risk in a range based on the persistency of the attacker, attack severity, attack magnitude and distribution across multiple hosts, thereby providing sufficient granularity on which to base decisions.

- **Filter by reputation** – Filter malicious clients based on their behavior and risk score and either alert or deny access.

- **Add header injection** – Add a request header with information on client behavior and risk score so that back-end systems can act upon it.

- **Drill down to investigate** – Access aggregated data to investigate the cause of a risk score in the last 30 days. Aggregated information should be collected for each score-changing event.
Why collective intelligence is important

Recently, a WAF at an Akamai customer site detected a web application attack. Akamai was asked to investigate. Akamai SOC technicians identified a remote file inclusion (RFI) attack against a WordPress application, a common attack strategy. However, this attack differed in that it targeted a hypertext preprocessor (PHP) site, even though it appeared to be scanning for vulnerabilities in many areas, not just PHP.

Akamai SOC technicians began searching for common attack characteristics among this client and other clients known to be malicious. Analysis showed that the client was part of a 272-member botnet that had targeted nearly 1,700 different web applications with more than 1.3 million attacks. This research illustrates the value of correlating malicious activity across multiple websites and, while this process was completed manually by SOC technicians, with the introduction of Akamai’s client reputation monitoring service, it now occurs automatically on an ongoing basis.

Because Akamai handles 15-30 percent of all web traffic every day, it has deep visibility into how legitimate users use web applications, attacker behavior and how attack vectors are evolving. Akamai leverages this data visibility within our CSI platform to continually strengthen and refine our security rules and provide customers with more effective cloud security protection, higher accuracy, and better ability to mitigate new types of attacks.

All Akamai customers using client reputational monitoring can benefit from this intelligence to make an informed decision on whether or not to block requests coming from a particular client in the future.

Recommendation: adopt a multi-layered defense

Web applications have become a staple of the Internet, from business-driven software-as-a-service (SaaS) applications to consumer mobile apps. For example, Gartner expects that by 2016 about 25 percent of large banks will deploy a banking app store to improve app discovery, user experience and collaboration\textsuperscript{1}. Unfortunately, the increase in web applications will result in an increase in data theft targets for cyber attackers. Simply, malicious actors will follow the money up the application stack, making a WAF even more essential.
Web application attacks are being launched not only from large and established botnets, but also from smaller botnets that hide within mobile carrier networks and are harder to detect. With any type of cloud security solution, the ability to stay ahead of the changing threat landscape is paramount. Consequently, there has been rapid growth in security services to help remove the heavy burden on in-house security teams of having to continually update WAF rules and attack signatures. However, there is no silver bullet when it comes to web application protection. As a result, most security practitioners recommend a defense in depth approach, such as a combination of interactive cyber protection technologies to provide a multiple layered defense, including the following:

**Rate controls**
- Inspection of multiple HTTP transactions
- Detection over a short period of time
- Triggers on excessive rate of client requests

**Web Application Firewall (WAF)**
- Inspection of single HTTP transactions
- Attack detection in real-time

**Client reputation monitoring**
- Stop malicious actors at the source
- Behavioral analysis on all cloud platform logs
- Triggers on malicious intent to forecast potential attacks

**Conclusion**

As with the best home security systems that work at multiple perimeters, today's organizations need to take a similar approach to cybersecurity. While it used to be enough to monitor doors and windows, today's home security systems now include motion sensors and cameras. Similarly, enterprises need multiple defenses in place, each focused on different aspects of a potential cyberattack (origin and target). It's an accepted industry best practice. While rate controls and a well-tuned WAF are useful and necessary, client reputation monitoring, like that camera on the porch, strengthens defenses even more.

Adding client reputation monitoring to a cloud security strategy not only helps stop malicious attacks at the source but also provides the security intelligence needed for improved security decisions and risk evaluation. Most of all, by providing an increased layer of web application security, it is possible to protect the integrity, availability and performance of critical web applications, resulting in improved brand and customer confidence and reduced business risk from under-provisioning WAFs.

Rate controls, WAFs, client reputational monitoring, DDoS defense, and other cloud security approaches should be used in combination as part of a comprehensive defense against all types and sizes of cyber threats. It can be a daunting task to manage, coordinate, tune and update all of these defensive layers, which is why many organizations leverage the services of cloud security providers.