Client Reputation

Improving security decisions and adding an extra layer of protection

Client Reputation provides an additional layer of protection on top of Kona Site Defender. It provides a reputation score for each IP address in respect to the potential risk it poses to each individual customer. It can significantly improve your security decisions.

Security is not black and white, but has many different shades of grey. Many attackers, and their associated IP addresses, only target specific industry segments or remain active for only a short period of time. Those IP addresses are also used by legitimate users. Simply blocking an IP address could affect the legitimate users, which causes a negative business impact.

The changing threat landscape also forces enterprises to constantly improve their ability to act on suspicious client behaviors in a way that further reduces the risk of successful DDoS or application layer attacks and at the same time minimizes the impact to legitimate users. Client Reputation increases the accuracy of security decisions that separate malicious traffic from legitimate traffic. Kona Site Defender primarily focuses on threat vectors, while Client Reputation provides a complementary view on clients — the potential attack sources.

Many IP reputation solutions that are on the market today create only a single score per client or IP address, which is the same for all customers. Client Reputation, however, uses a state-of-the-art, proprietary risk analysis engine that computes a risk score for every source IP address, customized for every customer. This custom risk-based scoring model is significantly more accurate than generic scoring, and it has shown that actions taken based on the risk score are less likely to negatively impact legitimate clients and users. The quality of risk scoring is driven by the knowledge that can be extracted from Big Data. Akamai leads the Content Delivery Network market as a central hub in the Internet ecosystem, serving 15-30% of all web traffic at any given moment, interacting with 1.3 billion client devices every day. The data is analyzed by Cloud Security Intelligence, Akamai's Big Data security platform. The breadth and scope of this platform enables Akamai to deliver a client reputation service well beyond anything available in the market today.

Comprehensive insight drives the quality of Client Reputation, which provides the following features:

Cross-customer correlation: Correlation of client requests across different customers and identification of malicious intent.

Multiple risk score categories: Ability to associate potentially malicious activity with the following types of attackers:

1. **Web attackers –** Actors performing generic web-oriented attacks such as SQL injection (SQLi), remote file inclusion (RFI), or cross-site scripting (XSS).
2. **DoS attackers –** Web clients or botnets that use automated tools to launch volumetric DoS attacks.
3. **Scanning Tools –** Tools used to scan web applications for vulnerabilities.
4. **Web Scrapers –** Automated tools used to harvest information, like pricing data from websites.

BENEFITS TO YOUR BUSINESS:

- Improved security decisions
- Additional layer of application security
- State-of-the-art risk analysis engine
- Custom risk-based scoring
- Visibility into 15-30% of all web traffic
- Interaction with 1.3 billion devices/day

THE ANALYTICAL PROCESS INCLUDES:

- Sophisticated attacker behavioral profiling
- Detection of malicious payloads and zero-day attacks
- Analysis of common malicious traffic patterns
- Clustering of malicious activities performed by botnets

Client Reputation

Client risk score: Based on previous behavior, like attacker persistency, number of targeted applications, severity of the attack, magnitude, industry, and previous attacks targeting customer's applications.

In conjunction with the risk score, Akamai customers can further adjust the security measures by applying additional conditions, like:

- The source IP's autonomous system number (ASN)
- IP or GEO network lists
- IP address/CIDR
- Specific HTTP header names and/or values
- Specific HTTP cookie names and/or values
- Target hostname
- Target HTTP request path

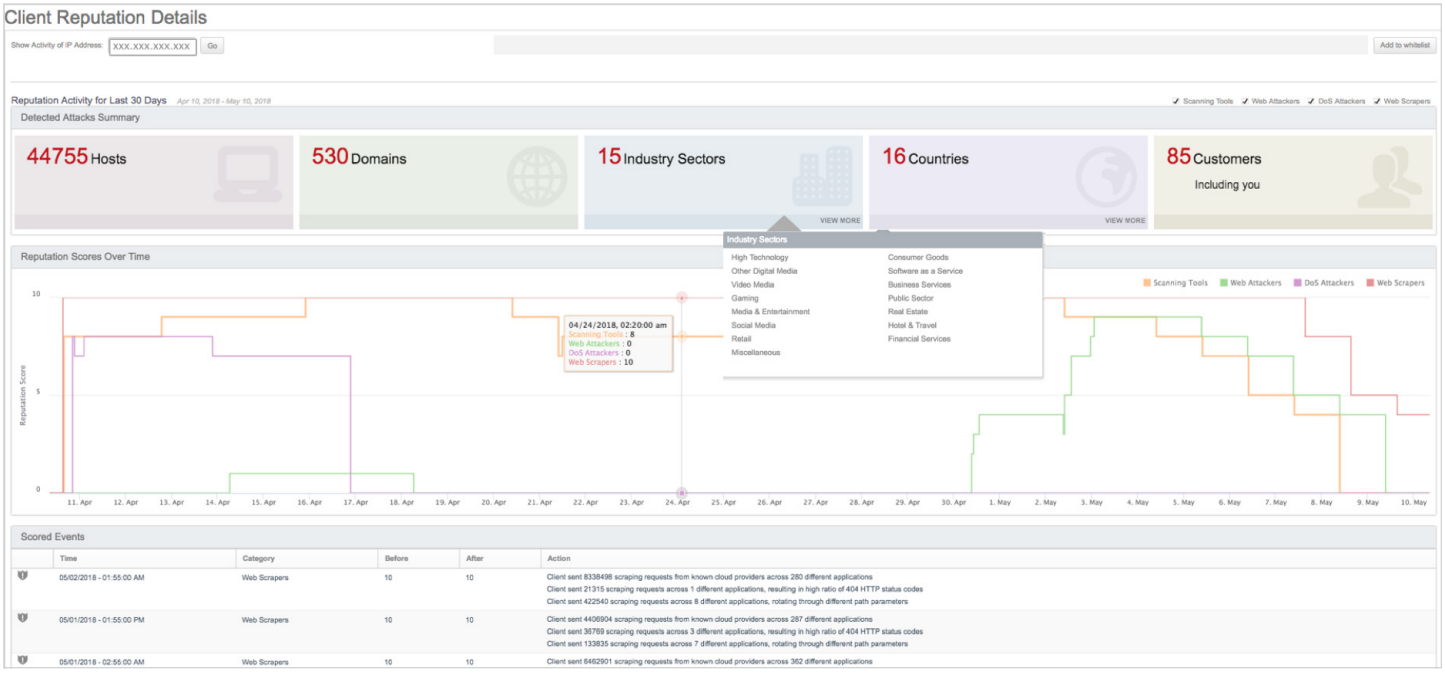
Reputation controls: An interface to filter malicious clients based on their behavior and risk score by either alerting or denying access.

Header injection: Additional request header with information on behavior and risk score so that back-end systems can act upon it.

Client investigation: Access aggregated data to investigate the cause of a risk score in the last 30 days. Aggregated information is collected for each score-changing event.

Client Reputation scores are constantly updated to automatically reflect the latest risks of clients. This automation significantly reduces the maintenance efforts for customers and immediately allows them to use Client Reputation in deny mode. A powerful dashboard provides detailed historical client information on category, risk score, reputation activity, detected attacks per hosts, domains, industry sectors, countries, customers, and much more.

Client Reputation provides deep visibiity into client activities and adds an additional, very sophisticated intelligence-based protection layer to our customers' web application delivery.



Akamai

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7/365 monitoring. To learn why the top financial institutions, online retail leaders, media and entertainment providers, and government organizations trust Akamai, please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. Published 07/18