Kona Site Defender

Protecting Mission Critical Websites From Downtime and Data Theft

Because websites and applications are accessible from the Internet, they offer a relatively simple entry point to access valuable data and are often subject to attacks. Kona Site Defender protects websites and applications from downtime and data theft caused by opportunistic and targeted web attacks, as well as Distributed Denial of Service (DDoS) attacks. Organizations that use Kona Site Defender are able to expand their web offerings without constantly fearing intruders.

Kona Site Defender Overview

Kona Site Defender protects websites and APIs from sophisticated attacks with a multi-layered toolset. DDoS-defense capabilities are always on, so traffic does not have to be re-routed before mitigation begins. Moreover, Akamai's visibility into 15 to 30% of the world's web traffic provides intelligence into the threat landscape that allows us to constantly evolve rules to thwart the latest attacks. In addition, Akamai's expert services team is available to work with customers to integrate optional components to maximize security.

Kona Site Defender Features

Kona Site Defender provides:

- DDoS attack mitigation
- A customizable Web Application Firewall (WAF)
- Site Shield (protection against direct-to-origin attacks)
- Adaptive caching
- Site failover
- Access control
- NetStorage
- Log Delivery Service
- Out-of-the-box integration with SIEM applications
- and the ISO 27002 Compliance Management module.

DDoS Mitigation

Akamai has delivered web traffic exceeding 46 Tbps. Attacks of tens — or even hundreds — of Gbps are no match for the Akamai Intelligent Platform™. Kona Site Defender protects against all types of DDoS, web application, and direct-to-origin attacks — and our optional Fast DNS solution also mitigates DDoS attacks on DNS infrastructure. Kona Site Defender is deployed across the Akamai Intelligent Platform, which consists of more than 230,000 servers in more than 3,500 locations installed in more than 1,600 networks across 131 countries. Attacks are blocked far from the customers' web server and web applications, at the edge of Akamai's network.

BENEFITS

BUSINESS BENEFITS:

- **Reduce risk** of downtime, defacement and data theft
- **Protect revenue,** customer loyalty, and brand equity
- **Maintain performance** even under attack
- **Reduce costs** from spikes in attack traffic
- **Reduce capital expenditure** on security hardware and software

TECHNICAL BENEFITS:

- **Simple integration** with existing IT infrastructure
- **Maximize uptime and availability** during DDoS attacks
- **Defend** web application infrastructure
- **Protect** against direct-to-origin attacks
- **Scale** on demand
- **Holistic view** of threats in SIEM application
- **Access** best-in-class application security expertise

The Akamai Intelligent Platform is architected as a reverse proxy and only accepts traffic on ports 80 (HTTP) and 443 (HTTPS). All network layer (Layers 3 & 4) DDoS attacks are automatically dropped. This includes traffic such as ICMP, SYN, ACK, RESET, and UDP floods, and UDP fragments.

The Kona Rule Set

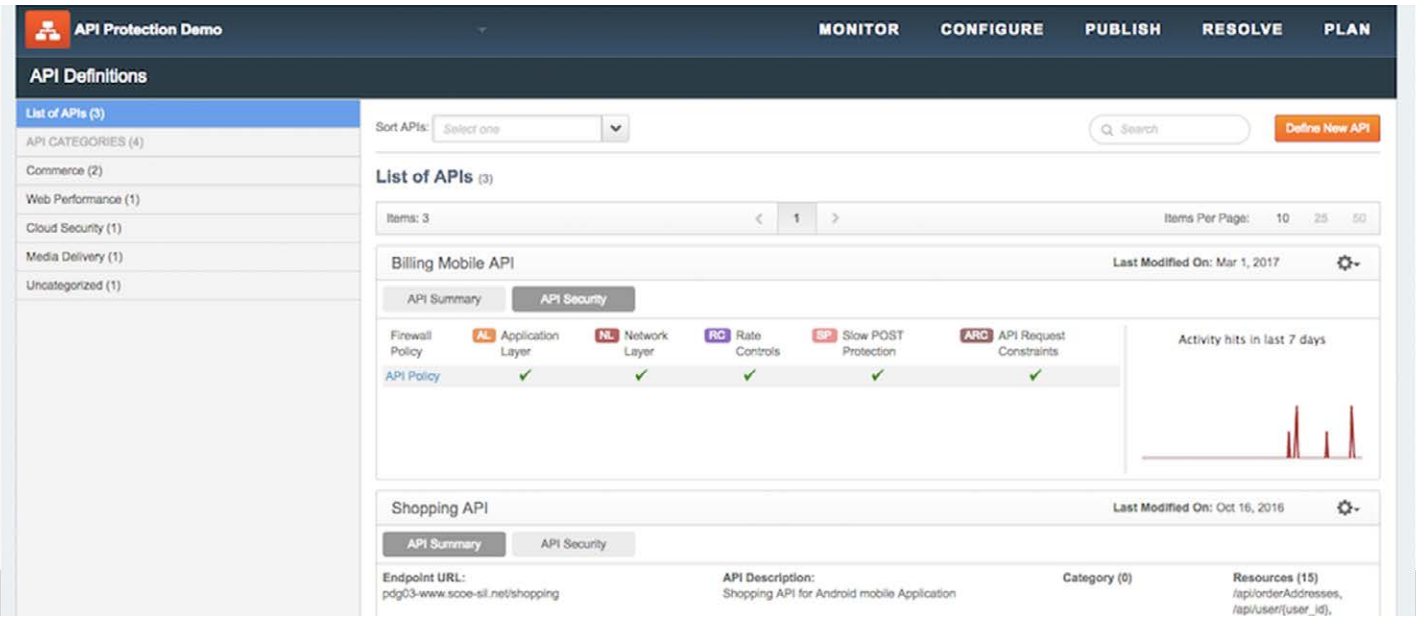
Kona Site Defender includes a rich collection of pre-defined configurable application-layer firewall protections, which Akamai maintains with regular updates for categories such as: protocol, request limit, and HTTP policy violations, malicious robots, generic, and command injection attacks, Trojan backdoors, and outbound content leakage. These rules are collectively referred to as the Kona Rule Set.

The Kona Rule Set addresses even the most recent threats and attacks against our thousands of customers. The rules are updated regularly by Akamai's Threat Research Team, and are available to all Kona Site Defender customers.

Kona Site Defender

API Protections

Kona Site Defender uses positive and negative security models to protect APIs from malicious calls. Customers can define what types of requests and calls are allowed, and Kona Site Defender will inspect the parameters of RESTful APIs against a whitelist of expected values and inspect JSON body and path parameters for risky content. Rate controls can be used to mitigate DDoS attacks launched via APIs, and Kona Site Defender includes analytics and reporting at an API level.



Custom Rule Builder

While Kona Site Defender includes a comprehensive and frequently updated set of rules and our Professional Services team offers Security Optimization Assistance packages that ensure rules are built and customized to meet individual customer needs, an intuitive built-in custom rule builder is provided for customers who prefer to build rules themselves. Custom rules can serve as virtual patches in which new website vulnerabilities can be mitigated quickly before standard rules are defined in the WAF.

Compliance Management

Kona Site Defender includes the ISO 27002 compliance management component, designed to help customers understand and validate how the relationship with Akamai impacts their own compliance initiatives. It includes a core base to address generic requirements coupled with the ISO 27002 module. Additional modules supporting other compliance frameworks are available.

The Akamai Ecosystem

Akamai makes the Internet fast, reliable and secure. Our comprehensive solutions are built on the globally distributed Akamai Intelligent Platform, managed through the unified, customizable Luna Control Center for visibility and control, and supported by Professional Services experts who get you up and running easily and inspire innovation as your strategies evolve.

Akamai FASTER FORWARD