AKAMAI PRODUCT BRIEF

Kona Site Defender

Protect Your Websites, Web Applications, and APIs from Downtime and Data Theft

Build trust and reduce risk with the industry-leading web application and API security solution that is tailored to your business, security posture, and attack surface.

Solution Overview

Consumer trust in your security, availability, and brand may be more fragile than ever. Internal trust in your operations, supply chain, and data integrity can also be damaged with a successful data breach. To build and maintain trust, organizations must mitigate both business and operational risk from the latest threats by producing only the highest security outcomes. Kona Site Defender – the industry-leading cloud-based web application firewall (WAF) – harnesses visibility across the Akamai Intelligent Edge Platform to stop the most sophisticated denial-of-service (DoS), web application, and API-based attacks to protect what matters most: trust.

Advanced Firewall and Threat Intelligence

Kona Site Defender includes a rich collection of predefined configurable application-layer firewall protections that are constantly updated by Akamai Threat Research. This intelligence – curated from both machine learning and human analyses – provides the most advanced and accurate detection. Custom rules and automated protection profiles are designed to provide the flexibility and scale to cover entire web and API estates, improve operational efficiencies, and deliver faster time-to-value.

Powerful and Flexible Denial-of-Service Protection

Akamai's globally distributed Intelligent Edge Platform is architected as a reverse proxy to only accept traffic via ports 80 and 443. All network-layer DoS attacks are instantly dropped at the edge with a zero-second SLA. Application-layer DoS attacks, including those launched via APIs, are absorbed by Kona Site Defender while it simultaneously grants access for legitimate users. Non–application-layer DoS and DDoS attacks against your infrastructure can also be mitigated, using Akamai Prolexic and Edge DNS.

Automatic API Discovery and Security

Kona Site Defender automatically inspects API traffic traversing the Akamai platform to provide a list of previously unidentified APIs, including API endpoints, characteristics, and definitions. This visibility enables security teams to stay abreast of changing definitions and easily register APIs for protection. With Kona Site Defender, both positive and negative security models protect APIs from malicious calls. The negative security model automatically parses and inspects XML and JSON traffic for application attacks, while the positive model only allows predefined API traffic. Additionally, real-time alerting, reports, and analytics can all be produced at the API level.

BENEFITS FOR YOUR BUSINESS

- Protect revenue, customer loyalty, and brand equity
- Maintain application performance even when under attack
- Reduce cost from spikes in attack traffic
- Automate application security with CI/CD integration
- Make data-driven security decisions with Akamai Cloud Security Intelligence
- Reduce the burden of maintaining skilled operators with Akamai's SOCC

> "We have been using the Akamai WAF solution for the past five years, and it has delivered *every piece of result* that we, as an organization, require to protect our assets at the edge."
>
> – Senior Cybersecurity Engineer in the Services Industry

Source: Gartner Peer Insights

Integration into CI/CD Processes

With Kona Site Defender, organizations can integrate WAF protections into agile development processes by programmatically managing and tying in security controls earlier in the development cycle. Developers, security, and operations teams can leverage a wide range of management APIs and the command-line interface (CLI) to integrate security configuration tasks into the CI/CD process, enabling security-by-design best practices and the

FEATURES	
Network (IP/Geo) Edge Firewall – IP/Geo controls let you block or allow traffic coming from a specific IP, subnet, or geographic area. This allows you to block malicious requests from specific IP addresses or traffic from The Onion Router (TOR), which bad actors use to hide their identity.	**Site Shield** – Provides an additional layer of protection that helps prevent attackers from bypassing cloud-based protections and targeting your origin infrastructure.
Application Firewall – With Akamai Adaptive Security Engine, Kona Site Defender offers not only flexibility and superior application and API security outcomes compared with WAFs based on traditional rule sets, but levels of automation and simplicity that are designed to demonstrably reduce the effort needed to onboard and maintain the WAF function. Automatic API discovery, self-tuning, and a choice of automatic or manual updates to WAF protections help Kona Site Defender optimize your organization's application and API security posture while delivering significant business and operational benefits.	**Application-Layer DoS Protection (Rate Controls)** – Protect against excessive request rates and DoS attacks by monitoring and controlling the rate of requests. Violators are automatically blocked to protect site origins.
	Custom Rules – Kona Site Defender offers a custom rule builder to quickly and easily generate custom rules that can be used to handle unique scenarios not covered by standard rules or to quickly patch new website vulnerabilities.
Evaluation Mode – Easily evaluate new WAF protections on live traffic, as well as already-active protections, to seamlessly update without impact to end users. While these are continuously and transparently updated by Akamai, you are in complete control of evaluation and activation.	**Response Actions** – Create and serve a wide range of response actions, including fully customized responses. You can send custom error messages; brand pages with your own logo; or define and serve HTML-, XML-, or JSON-based responses, depending on your needs.
Terraform, Open APIs, and CLI – Developers and operations teams can manage Kona Site Defender as code, leveraging Akamai's Terraform provider, open APIs, or the Akamai CLI to fully access, edit, and audit security configurations, giving you the freedom to integrate and customize on your terms.	**Reporting** – Web security reporting tools continually monitor and assess the effectiveness of your protections. You can create real-time reports to monitor daily activities; investigate attacks by type and security policy; and view reports on targeted APIs, DoS traffic, and more.
Advanced Web Security Analytics – Access detailed attack telemetry and analyses of security events to evaluate what changes are needed to improve security protections and optimize configurations for your specific business needs.	**Real-Time Alerting** – Create real-time email alerts using static filters and thresholds that can be easily configured to notify specific recipients only.
SIEM Integration – Prebuilt connectors allow you to use on-premises and cloud-based SIEM applications like Splunk, QRadar, ArcSight, and more.	**Performance and Delivery** – Seamlessly scale to match traffic demands as they vary over time, distribute CPU and memory resources as required, deliver cached content from the edge, and provide continuous protection without interruption for the highest level of performance and delivery.

OTHER SOLUTIONS TO INCREASE PROTECTION	
Client Reputation – Intelligence-based reputation scores driven by Akamai's visibility into prior behavior of individual and shared IP addresses.	**Managed Security Services** – Offload or augment your security management, monitoring, and threat mitigation to Akamai security experts.
Bot Manager – Detect, identify, categorize, and manage bots that are accessing your site. Machine learning algorithms use both bot and human behavior telemetry to allow good bots through while stopping malicious bots from executing attacks like credential abuse and account takeovers.	**Page Integrity Manager** – Protect websites from JavaScript threats – such as web skimming, formjacking, and Magecart attacks – by identifying vulnerable resources, detecting suspicious behavior, and blocking malicious activity.

> "The Kona WAF SaaS has worked flawlessly for us for over four years ... we boast *zero downtime* due to cyberattacks in complete contrast to our previous experience; many of our sites are attack magnets and under 24/7 attack ... according to the logs."
>
> – Head of Architecture, MCIT, in the Finance Industry

Source: Gartner Peer Insights

Contact your Akamai representative or visit akamai.com/kona to learn more.