Edge Delivery Services
powered by Akamai

Kona Site Defender

Protect your websites and web applications from downtime and data theft

Application security tailored to your business, security posture, and attack surface, powered by our intelligent platform. Enjoy the latest threat protection at unmatched scale, performance, and optimal end-user experience — even under attack.

About Kona Site Defender

In order to thrive in today's fast-moving and hyper-connected digital economy, your business applications are designed to be highly accessible via websites and APIs by consumers and business partners at scale and speed. However, they also offer an attractive entry point to access valuable data and therefore are the main target of serious attacks. Kona Site Defender provides broad protection for websites and applications from downtime and data theft caused by opportunistic and sophisticated web attacks, as well as Distributed Denial of Service (DDoS) attacks. Organizations that use Kona Site Defender are able to aggressively innovate their web offerings to increase delivery performance without the distraction of an increasing number of targeted attacks.

BENEFITS

- Protect Revenue, Customer Loyalty, and Brand Equity
- Maintain Application Performance Even When Under Attack
- Reduce Cost from Spikes in Attack Traffic
- Advanced Integration with IT Infrastructure and DevOps
- Leverage Best-in-Class Application Security Experts
- Get Deep Threat Insight Visibility with Web Security Analytics

Kona Site Defender Overview

Kona Site Defender protects websites and APIs against all types of sophisticated DDoS, web application, and direct-to-origin attacks, leveraging an always-on multi-layered toolset. It is deployed across our intelligent platform, which consists of more than 200,000 servers in more than 3,500 locations across 1,600 networks in 131 countries. This solution blocks attacks at scale at the network edge and far away from your web server and applications.

DDoS Protection Always On

Kona Site Defender's web application firewall absorbs DDoS attacks targeted at the application layer and authenticates valid traffic at the network edge. Built-in automated controls respond to attacks within seconds. For really sophisticated and new attacks that require a custom response, customers' security experts can create custom rules based on individual signatures. In addition, our intelligent platform is architected as a reverse proxy, only accepts traffic via ports 80 and 443, and automatically drops all network layer DDoS attacks. With over 61 Tbps delivered, we have the capacity to absorb the largest network-layer attacks without skipping a beat. DDoS attacks against your DNS infrastructure can be mitigated via the complementary Fast DNS solution.

Web Application Firewall

The web application firewall includes a rich collection of pre-defined configurable application-layer firewall rules. Our Threat Research Team keeps them current with regular updates based on in-house threat intelligence derived from unique visibility into 15 to 30% of the world's web traffic and across various categories, which increases overall accuracy in terms of lowering false negatives and false positives. Rule customizations can serve as virtual patches in which new website vulnerabilities can be mitigated quickly while you update the application based on its regular lifecycle process.

API Protections

Kona Site Defender uses positive and negative security models to protect APIs from malicious calls. Customers can define which types of requests and calls are allowed. 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 are used to mitigate DDoS attacks launched via APIs. Kona Site Defender provides analytics and reporting at an API level.

Security for DevOps

Enterprises are increasingly embracing cloud technologies, automation and DevOps practices, and the need to integrate security with their agile development processes. With Kona Site Defender, organizations have a way to programmatically update security controls and tie them into their development processes. Kona Site Defender provides organizations with a range of management APIs that enable developers and administrators to integrate common security configuration tasks into the CI/CD process.

FEATURES:

Global Cloud Platform
Built on the world's largest cloud delivery platform, Kona Site Defender extends your security infrastructure to the cloud and stops attacks before they can reach your applications.

DDoS Protection
Kona Site Defender defends your applications from the largest DDoS attacks, automatically dropping network-layer attacks at the edge and responding to application-layer attacks within seconds — minimizing any potential downtime.

Web Application Firewall
Kona Site Defender includes a highly scalable web application firewall that protects you from application-layer threats with an automated and highly customizable rule set.

API Protection
Kona Site Defender provides API-centric protections against DDoS and parameter-based attacks, allowing organizations to define their APIs to be protected, and configure protections and report on security events on a per-API basis.

Rule Updates
With visibility into the latest attacks against the largest and most frequently attacked organizations online, we continuously and transparently update Kona Site Defender's security rule set, leaving you in control of activation.

Virtual Patches
Your security team customizes rules, providing a virtual patch for your applications, quickly securing new vulnerabilities or simply tailoring protection for your website traffic.

100% Availability and Uptime
Kona Site Defender is built on a highly resilient and self-healing platform that comes with a 100% uptime SLA. Included Site Failover takes advantage of the platform to keep your website up — even if your servers go down.

SureRoute
Kona Site Defender includes our SureRoute technology to help your users always find the most optimal route to your website, mitigating network issues outside of your control and improving performance and availability.

Improved Performance
Benefit from performance capabilities built into the CDN, such as caching, advanced offload capabilities, and TCP optimization, to improve website performance for users even through the largest attacks.

Management APIs
Management APIs for common configuration tasks enable organizations to integrate security controls into their software development and delivery pipeline.

Advanced Web Security Analytics
Detailed assessment of security events allows your security team to better evaluate changes needed to maintain an optimal security configuration tailored to your specific business needs.

Additional Options to Increase Protection

Client Reputation
This optional module can further improve security decisions in a difficult environment by providing the ability to filter malicious clients based on their behavior and risk score.

Managed Security
Offload security management, monitoring, and threat mitigation to our security experts. Designed to help you build a responsive cloud security strategy.

For more resources on our industry-leading solutions, visit www.edgedeliveryservices.com/resources or Contact Us for a complimentary consultation.

IBM **Edge Delivery Services**
powered by Akamai