Kona Site Defender

Multi-layered defense to protect websites against the increasing threat, sophistication and scale of attacks

Akamai

Billions of people, tens of billions of devices and countless petabytes of information are all connected online. With rapid online innovation, new security threats are emerging with equal speed. The challenge for companies is to innovate fearlessly and deliver the fast, fluid online experience consumers and business users expect while protecting against threats that cause downtime, drive up costs and put confidential information at risk. To succeed, companies need to continue to expand their online offerings without constantly watching the door.

Some of the biggest brands in the world – many of which are targeted for attack on a regular basis, trust Akamai's web security solutions to protect their online presence.

Akamai's Kona Site Defender

Akamai's Kona Site Defender extends security beyond the data center while maintaining site performance and availability in the face of fast-changing threats. It leverages the power of the Akamai Intelligent Platform™ to detect, identify and mitigate Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks before they ever reach the origin.

How it Works

Kona Site Defender thwarts DDoS attacks by deflecting network-layer DDoS traffic and absorbing application-layer DDoS traffic at the network edge. Mitigation capabilities are implemented natively in-path to protect against attacks in the cloud before they reach the customer origin. Kona Site Defender also incorporates a highly scalable Web Application Firewall (WAF) that protects against application-layer attacks in HTTP and HTPS traffic, such as SQL injections and cross-site scripting (XSS).
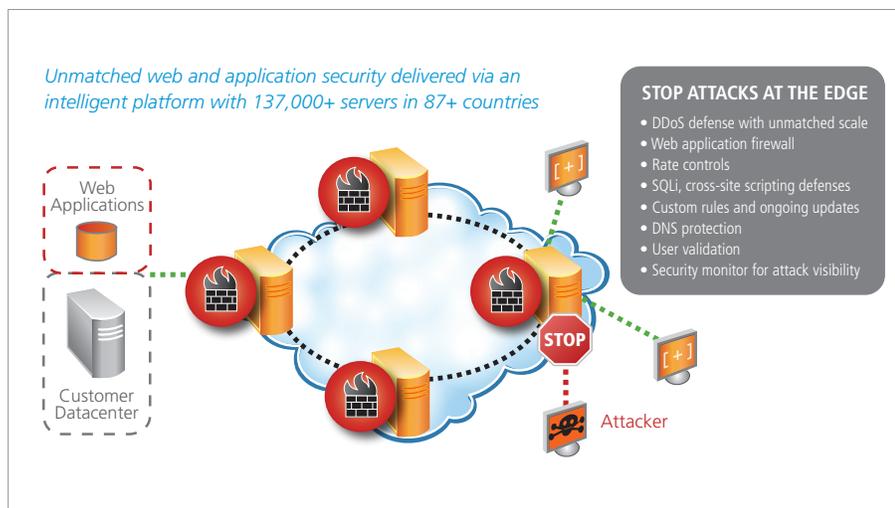
BENEFITS TO YOUR BUSINESS

- **Reduce downtime and business risk** with the scale to deflect/absorb the largest DoS and DDoS attacks

- **Reduce the risk of data theft** with a highly scalable Web Application Firewall

- **Maintain performance** during attacks through Akamai's globally distributed architecture

- **Reduce costs** associated with web security by leveraging Akamai's globally distributed web security platform

- **Protect against new and evolving threats** with Kona Rules regularly updated by Akamai's Threat Intelligence Team

Unmatched web and application security delivered via an intelligent platform with 137,000+ servers in 87+ countries

Web Applications

Customer Datacenter

STOP ATTACKS AT THE EDGE
- DDoS defense with unmatched scale
- Web application firewall
- Rate controls
- SQLi, cross-site scripting defenses
- Custom rules and ongoing updates
- DNS protection
- User validation
- Security monitor for attack visibility

STOP

Attacker

"We're always planning for growth. With Akamai we're confidently positioned to drive more site traffic and revenues while safeguarding our brand and shoppers' information.

— **Jason Miller,** VP of Technology, Motorcycle Superstore

Kona Site Defender

Key Capabilities

- **Kona Rules:** Akamai's Threat Intelligence Team develops and updates WAF rules continually to address new and emerging web application attacks, such as SQL injections, cross-site scripting, remote file inclusion and more. Scheduled reviews by the Akamai Professional Services team analyze logs and recommend configuration tuning/optimization to maintain an effective security posture even as applications change and new threats emerge.

- **Application-Layer Controls:** A collection of pre-defined, configurable application-layer firewall rules address categories such as Protocol Violations, Request Limit Violations, HTTP Policy Violations and more. You can also create policy-based rules enforced after the execution of application layer controls.

- **Adaptive Rate Controls:** Automatically protect applications against application-layer DDoS and other volumetric attacks by monitoring and controlling the rate of requests against them. Set behavioral rules to respond to bursts of requests in seconds, selectively alert/block attackers based on IP address and other parameters, and mitigate slow POST DDoS attacks.

- **Network-Layer Controls:** Automatically drop network-layer DDoS attacks at the network edge. Define and enforce IP whitelists and blacklists to allow/restrict requests from certain IP addresses or geographical regions to protect your website.

- **Site Shield:** Cloak your origin from the public Internet to further protect against direct-to-origin attacks without impeding quick, reliable content delivery

- **Security Monitor:** Real-time visibility into security events and the ability to drill down into attack alerts to learn what's being attacked, by whom, what defense capabilities triggered the attack declaration and what specifically in the requests triggered site defenses

- **Logging:** Increase your threat posture awareness by integrating WAF event logs with your security information and event management (SIEM) or other reporting solution through Akamai's Log Delivery Service (LDS)

- **Fast DNS:** Leverage Akamai's authoritative name servers to allow your end users to quickly get to your websites. Fast DNS is designed to improve the performance and availability of your DNS infrastructure while also protecting against the threat of DDoS attack.

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 kept all sites of the 2012 London Olympics up through a 40x increase in attack traffic with 23 different attack types including SQL injections and XSS.*
>
> We can use a content distribution network, so it's very hard to launch a DDoS on us, because our front end is so dispersed.
>
> **— Gerry Pennell, CIO,** London Games Organizing Committee

Akamai FASTER FORWARD