Fast & Secure

Deliver Instant Web Experiences While Protecting Your Applications
From Downtime And Data Theft

Akamai's industry leading web performance and security offerings enable enterprises to deliver instant, reliable, and secure Internet experiences.

Akamai offers integrated mobile, web, and API performance optimizations. These are designed to help organizations reduce costs by downsizing infrastructure necessary to deliver mobile content and improve performance in the mobile channel by leveraging key user insight to tailor customers' mobile experiences. Coupled with Akamai Security Solutions, enterprises can defend against all types of DDoS and web application attacks at a high accuracy, without sacrificing application performance.

Akamai Intelligent Platform™

Akamai has deployed the most pervasive, highly-distributed web performance and security platform in the world, with hundreds of thousands of servers in over 110 countries, and within 1,400+ networks. The Akamai Intelligent Platform delivers more than 2 trillion interactions, with an excess of 30 Tbps of volume, accounting for up to 15-30% of web traffic, every day.

The scale of Akamai's Intelligent Platform is architected to exceed the rising expectations of always-connected, globally-distributed end users. The proliferation of connected devices, expansive web and media experiences, and the rise of cybercrime demands a platform with a worldwide distribution, where content delivery and application protection are provided as close as possible to the point of request.

Akamai's web performance optimizations are layered with world class web security technologies, which enable enterprises to offload expensive web infrastructure, deliver sophisticated web experiences for websites, mobile web and apps, all while protecting existing infrastructure by deflecting DDoS traffic and Layer 7 application attacks.

Akamai's integrated web performance and security capabilities are backed by industry leading Service Level Agreements for availability, performance, and the time-to-mitigate attacks.

Web and Mobile Performance

Akamai offers fully-automated solutions for web and mobile performance designed to enable organizations to deliver faster website and mobile app responses to meet the rising expectations of always connected, globally-distributed end-users.

- **Optimize performance for each user.** Akamai applies optimizations adaptively, based on sophisticated analysis of the web application as well as real-time conditions specific to the end user's environment, such as browser, device, network speed, and presence of third-party services. Key capabilities include Edge caching, dynamic page acceleration, API acceleration, network responsive image compression, faster page rendering per device, and more.

- **Simplify development and operations for each experience.** Akamai provides optional modules that reduce development costs while simplifying web operations with easy-to-use tools that push application logic to be executed at the edge of the Akamai Platform, closer to your end users. Key capabilities include edge redirection, semantic URL rewrites, image management, and more.

BUSINESS BENEFITS:

- **Deliver** rich, engaging web experiences that exceed user expectations for speed and availability across devices, networks, browsers, and locations

- **Reduce** risk of downtime, defacement, and data theft

- **Maintain** performance under peak traffic conditions, expected or unexpected

- **Reduce capital expenditure** on application delivery and security hardware and software

TECHNICAL BENEFITS:

- **Simple integration** with existing IT infrastructure

- **Maximize uptime and availability** during expected load or DDoS attacks

- **Defend** web application infrastructure

- **Protect** against direct-to-origin attacks

- **Improve availability** of DNS infrastructure

- **Access** best-in-class performance optimization and application security expertise

Fast & Secure

Application and Website Security

Akamai's Web Security Solutions add a layer of security on top of the the Akamai Intelligent Platform. The security features are designed to thwart DDoS attacks by absorbing DDoS traffic targeted at the application layer, deflecting all DDoS traffic targeted at the network layer, such as SYN Floods or UDP Floods, and authenticating valid traffic at the network's edge.

- **Leverage Internet Intelligence within a Proprietary Rule Set.** Kona Site Defender includes a rich collection of pre-defined, configurable application-layer firewall rules (which Akamai maintains with regular updates) for different attack categories such as: Protocol Violations, Request Limit Violations, HTTP Policy Violations, Malicious Robots, Generic and Command Injection Attacks, Trojan Backdoors, and Outbound Content Leakage. These rules, collectively referred to as the "Kona Rule Set," were developed and are currently updated by continuously analyzing 2PB of security log data collected from delivering up to 15-30% of the Internet's web traffic at any given time.

  The Kona Rule Set also utilizes a concept called "anomaly scoring," whereby each rule contributes to an overall risk score rather than an individual rule blocking a request. Alert/Deny decisions are made based on the total score of combined rules.

- **Manage Application Accessibility by Understanding the Client, not their Requests.** Security teams can prohibit abusive client behavior by configuring rate controls, which provide protection against application-layer DDoS attacks by monitoring and controlling the rate of requests against the Akamai servers and the customer origin. Kona Site Defender can respond to bursts of requests within seconds.

  Kona Site Defender also provides an optional module to provide visibility into the reputation of a web client. Akamai sees billions of IP addresses every quarter and leverages advanced algorithms on the data collected from web clients to identify malicious actors. The malicious web clients are scored according to their likelihood of engagement in various types of malicious behavior, including website scanning, generic web attack launches, and DoS attacks.

- **Simplify Security Operations for each Application.** Kona Site Defender provides a user-friendly interface to configure security policies for individual web applications. The portal also provides security professionals the ability to manage false positives and false negatives by modifying existing rules, or creating their own custom rules. To further reduce security operations, Network Layer Controls afford enterprises the ability to enforce IP whitelists and blacklists. List updates are propagated across Akamai's global network within minutes, enabling a rapid response to attacks. Whitelists and blacklists can be fed automatically through an IP-blocking API.

- **Gain Visibility to your Application.** Kona Site Defender provides security professionals with real-time visibility into security events as well as the capability to drill down into attack alerts to retrieve detailed information on who is attacking, what they are attacking, what defense capabilities triggered the attack declaration, and what specifically was seen in the requests that triggered site defenses. Security Monitor includes the ability to view request/response header details for rule tuning and attack investigations.

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.