To be successful in today’s hyperconnected world, enterprises need to be able to innovate without fear. Distributed Denial of Service (DDoS), web application and DNS infrastructure attacks represent some of the most critical threats to enterprises today. These attacks are increasingly brazen and target companies across all verticals and geographies. They cause downtime, drive up bandwidth costs and result in the loss of confidential information. Yet despite the risks and challenges, consumers and enterprises expect to be able to see, hear and do more on the web. To be successful in today’s hyperconnected world, enterprises need to continue to expand their web offerings without constantly watching the door for intruders. They need to be able to innovate without fear.

Features
Akamai delivers daily web traffic reaching more than 28 tbps. On the Akamai network, attacks measured in tens — or even hundreds — of Gbps are absorbed with relative ease.

Kona Site Defender defends against all types of DDoS, web application and direct-to-origin attacks — and our optional Akamai FastDNS solution also mitigates attacks on DNS infrastructure. Kona Site Defender is deployed across the Akamai Intelligent Platform™, which consists of over 170,000 servers deployed across more than 1,300 networks in over 100 countries.

DDoS Mitigation
Kona Site Defender, which leverages the Akamai Intelligent Platform, is 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 edge.

This built-in protection is “always on”, and only Port 80 (HTTP) or Port 443 (HTTPS) traffic is allowed. Bursting fees are capped so users are protected from increased service fees caused by DDoS traffic. And flexible caching maximizes offload from origin.

The Akamai Intelligent Platform is architected with worldwide distribution and massive scale to help ensure our clients’ websites stay available. Akamai handles 12 Tbps of traffic daily on average and has handled peak traffic flows of over 26 Tbps. In addition, mitigation capabilities are implemented natively in-path, so protection is provided no more than a few network hops from the point of request – NOT at the customer origin.

Application Layer Protection
Kona Site Defender incorporates a full featured Web Application Firewall (WAF) based upon proprietary technology that provides customers with a highly-scalable layer of protection against application layer attacks. Implemented in-line across Akamai’s globally-distributed platform of tens of thousands of servers, Kona Site Defender helps detect and deflect threats in HTTP and HTTPS traffic, issuing alerts or blocking attack traffic closer to its source before it reaches the customer origin. The Akamai WAF incorporates the Kona Rule Set to protect applications.

Kona Rules
Kona Site Defender includes a rich collection of pre-defined, configurable application-layer firewall rules (which Akamai maintains with regular updates) for different 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 are collectively referred to as the “Kona Rule Set”.

BENEFITS TO YOUR BUSINESS
• Reduce risk of downtime, defacement and data theft
• Protect revenue, customer loyalty and brand equity
• Maintain performance in times of attack
• Reduce costs associated with handling spikes in attack traffic
• Reduce capital expenditure on security hardware and software

OPERATIONAL AND 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
• Improve availability of DNS infrastructure
• Scale on demand
• Access best-in-class application security expertise
Kona Site Defender

The Kona Rule Set addresses the most recent threats and attacks against our hundreds of customers. The rules are updated regularly by Akamai's Threat Research team and are available to all Kona Site Defender customers. They protect against attacks such as: Low Orbit Ion Cannon, High Orbit Ion Cannon, HULK, Dirt Jumper, Havij SQL Injection Tool, Netsparker, ApacheBench, Webhive and others. Kona Rules include:

- Anomaly scoring whereby each rule contributes to an overall risk score. Alert/Deny decisions are made based on the total score.
- Enabling inspection of HTTP Request/Response Headers and HTTP POST Request/Response Bodies through a series of cascading REGEX rules in order to protect against attacks such as SQL Injections and Cross-Site Scripting.
- A variety of features to make upgrading rules easier:
  - An upgrade wizard that allows existing customers to upgrade WAF policies to the latest version of the Kona rules.
  - An evaluation mode that enables customers to maintain legacy rules and protections while simultaneously tuning new KRS rules.
- A rule versioning function that enables customers to adopt new or modified rules at a cadence aligning to their change control processes.

Network Layer Controls afford enterprises the ability to enforce customer-defined IP whitelists and blacklists. List updates are propagated across Akamai's global network within minutes, enabling a rapid response to attacks. Other features include the ability to restrict requests from specific IP addresses to protect customer origin from application layer attacks, and to implement geo blocking. Up to 10,000 CIDR entries are supported – including named lists such as Tor exit nodes. Whitelists and blacklists can also be fed automatically through an IP Blocking API.

Rate Controls 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.

Site Shield Kona Site Defender includes the ability to cloak (hide) a customer origin from the public Internet. Site Shield maps can be configured by Professional Services or by customers from within Luna and through APIs. Site Shield is designed to complement the existing infrastructure and prevent direct-to-origin attacks.

Security Monitor 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.

Kona Site Defender Rule Update Service provides scheduled reviews of Kona Site Defender and Web Application Firewall configurations by the Akamai Professional Services team. This includes false-positive analysis of Kona Security Monitor logs, recommendations on Kona Site Defender and origin configuration tuning and optimization.

Fast Domain Name Server Protection FastDNS provides a robust, reliable and scalable solution designed to ensure end users get directly to their websites. Akamai's FastDNS leverages the globally distributed Akamai Intelligent Platform's secondary authoritative name servers. It requires no change to existing DNS administration processes and provides incredibly robust, reliable, scalable and secure DNS resolution.

Client Reputation (Optional Module) This module complements Kona Site Defender with an additional layer of protection against — and visibility into — malicious actors. Client Reputation provides this protection by focusing on the source of the threat – in other words, Client Reputation focuses on web clients (as opposed to the attack vectors). Akamai sees billions of IP addresses every quarter. Client Reputation 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 three different types of malicious behavior: website scanning, generic web attack launches and DoS attacks.

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 is a leading provider of cloud services for delivering, optimizing and securing online content and business applications. At the core of the company's solutions is the Akamai Intelligent Platform, providing extensive reach, coupled with unmatched reliability, security, visibility and expertise. Akamai removes the complexities of connecting the increasingly mobile world, supporting 24/7 consumer demand, and enabling enterprises to securely leverage the cloud. To learn more about how Akamai is accelerating the pace of innovation in a hyperconnected world, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.