Akamai Raises the Bar for Web Security with Enhancements to Kona Site Defender

Submitted by: Ascendant Communications
Monday, 25 February 2013

Akamai Raises the Bar for Web Security with Enhancements to Kona Site Defender

Cloud-Based Solutions Apply Protections at the Network Edge; Adds Greater Intelligence, Flexibility and Simplicity to Fighting Web Attacks

SAN FRANCISCO – RSA® Conference 2013 (Booth #1630) – February 25, 2013 – Akamai® Technologies, Inc. (NASDAQ: AKAM), a leading cloud platform for delivering secure, high-performing user experiences to any device, anywhere, today unveiled several feature upgrades to the company's Kona Site Defender web security solution. The enhancements are designed to add greater intelligence, flexibility and simplicity to the defense of web site and application attacks, giving businesses the tools to help organizations of all types better protect web sites and applications from an ever changing threat landscape.

Included in the new version of Kona Site Defender are upgraded Web Application Firewall (WAF) capabilities and network layer controls, new user validation capabilities and improved configuration and automation tools that speed both initial deployment and response time to changing attacks. Further, Akamai has developed Application Programming Interfaces (APIs) and other modifications to Kona Site Defender. These are designed to make the technology easier to use by Managed Security Services Providers (MSSP) as well as to facilitate tighter integration with existing on-premises security technology.

Kona Site Defender is an always-on cloud-based web security solution designed to protect an enterprise's most critical online business functions against attacks that can result in millions of dollars in lost transactions and business productivity each year, and even greater harm to brand value and reputation. Using the Akamai Intelligent Platform™ as its foundation, the solution offers highly flexible and scalable protection – that does not negatively impact performance – to customers against a variety of attack vectors including DDoS, as well as web application attacks such as SQL injection, Cross Site Scripting and others.

Enhancements to Kona Site Defender include:

• Akamai Common Rules: In addition to the baseline WAF security offered by the OWASP ModSecurity Core Rule Set (CRS), organizations can now benefit from the extended security offered by the newly introduced Akamai Common Rules set. Each time the Akamai threat intelligence team experiences a new attack tool or a new version of an existing attack tool used against the platform, the company develops a rule to counter the attack. These rules are uniquely available to Akamai customers. To date, Akamai has developed and implemented rules to counter attacks such as LOIC (Low Orbit Ion Cannon) and HOIC (High Orbit Ion Cannon), among others.

• New Rate Control Capabilities: To help determine if anomalous traffic is being generated by users accessing the Internet from behind a proxy server and if that traffic is legitimate or malicious, Kona Site Defender features upgraded rate control capabilities. For example, IP addresses that might previously have been flagged as being the source of malicious content based on request volume can now

easily be identified as a web proxy. This increased security intelligence is designed to enable customers to make better decisions about which traffic to block and which traffic to let through to their sites or web applications. Improved protection against slow-moving DDoS attack vectors better allows customers to fight “resource starvation” attacks that bring down sites and applications by tying up CPU power versus simply flooding with massive traffic levels.

• User Validation Capabilities: New to Kona Site Defender, the user validation module provides a way to better understand who or what is generating traffic aimed at your web site or web application. If traffic is identified as potentially malicious, the browser is redirected to a JavaScript confirmation page. If the browser passes, the client request is further processed. The user validation module helps reduce an enterprise’s exposure to machine-based attacks.

• Cloud Security Intelligence: The massive scale of the Akamai Intelligent Platform gives the company tremendous visibility into emerging attack vectors and other malicious activity that can negatively impact organizations doing business online. The intelligence derived from the processing and analysis of aggregated security data is designed to make Akamai services simpler, more automated and more efficient.

• Site Assessment and WAF Rule Update Services: To help identify potential site vulnerabilities and develop appropriate web security strategies, organizations can now engage with Akamai security experts for web site scanning and analysis. This one time professional services engagement is intended to provide customers with a deeper understanding of potential exposure to attack and options for mitigating risk. In addition, customers now can work with Akamai’s professional services organization for ongoing WAF rules updating and tuning.

• APIs and MSSP Flexibility: Understanding that customers may wish to use Kona Site Defender in conjunction with existing on-premises appliances or through relationships with MSSPs, Akamai is developing APIs and other modifications intended to ease integration with these environments. The APIs will enable on-premises security controls to tightly integrate with the DDoS mitigation functionalities delivered by Kona Site Defender. The ability for MSSPs to include Kona Site Defender in their portfolio of supported technology gives customers greater choice in how they deploy and take the best advantage of the solution according to their unique requirements.

“The threat landscape is constantly evolving and web security professionals need a solution that can keep pace with the array of challenges they face every day,” explained John Summers, vice president, Security Business, Akamai. “Customers that have deployed Kona Site Defender have been able to deal effectively with these new adversaries, new tools and new attacks. Mitigating the Operation Ababil attacks that began in September 2012 are just one example of our success.”

Kona Site Defender is part of the Akamai Kona Security Solutions family. Akamai customers across industries are using Kona Security Solutions to better protect their valuable web sites and web applications by extending the security perimeter outside the data-center and to provide protection from the increasing frequency, scale and sophistication of web attacks. To date, 27 of the Fortune 100, 37 of the Internet Retailer 100 (including 10 of the top 20) and 27 of the Mobile 100 use Kona Security Solutions to protect their online businesses.

For more information about Kona Security Solutions please visit http://www.akamai.com/html/solutions/kona-solutions.html.

About Akamai

Akamai® is a leading cloud platform for helping enterprises provide secure, high-performing user experiences on any device, anywhere. 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.

Akamai Statement Under the Private Securities Litigation Reform Act

This release contains information about future expectations, plans and prospects of Akamai's management that constitute forward-looking statements for purposes of the safe harbor provisions under The Private Securities Litigation Reform Act of 1995. Actual results may differ materially from those indicated by these forward-looking statements as a result of various important factors including, but not limited to, failure of Akamai services to operate as expected or to address intended market needs, a failure of Akamai's network infrastructure, and other factors that are discussed in Akamai's Annual Report on Form 10-K, quarterly reports on Form 10-Q, and other documents periodically filed with the SEC.

Nathalie Agnew
Consultant
Ascendant Communications
Mobile: +44 (0) 7985 595510
Email: nagnew@ascendcomms.net
Web: www.ascendcomms.net
Twitter: http://twitter.com/AscendantPR

“Experts in European B2B Public Relations”

A global member of TAAN