Barracuda Launches Advanced Bot Protection

Application security leader deploys machine learning to protect organisations against automated threats

Sydney, 24 May 2019 - Barracuda, a leading provider of cloud-enabled security solutions, today announced the introduction of Advanced Bot Protection. Advanced Bot Protection uses artificial intelligence and machine learning to help customers defend against the latest automated threats. It is available for both the Barracuda Web Application Firewall (WAF) and WAF-as-a-Service platforms. Web applications are the number one attack vector for hacks resulting in breaches, according to the 2019 Verizon Data Breach Investigations Report, and malicious bots pose a significant threat to application security. Bots have evolved from using simple scripts to using sophisticated tactics such as headless browsers and machine learning to break through traditional application security defences. Organisations need an application security solution that can keep up with these evolving attacks. According to Gartner: “The main types of bot attacks include distributed denial of service (DDoS), fraudulent purchases, web scraping, and vulnerability scans and exploits. Unsupervised ML can be used to learn the characteristics of typical human-driven traffic, allowing the detection of bots as anomalies. Supervised ML can be used to identify features related to automated behavior.”1 With Advanced Bot Protection, Barracuda WAF customers have access to functionality that includes: Bot spam detection — Reduce referrer spam and block comment spam Credential stuffing prevention — Block credential stuffing to stop account takeover attacks Request risk scoring — Track incoming requests and use advanced behavioral analytics to detect attackers Client finger printing — Track users with better fidelity than IP addresses Dedicated bot mitigation UI — New user interface makes it easy to configure bot mitigation features “To effectively protect their organisations against today’s evolving threats, customers need sophisticated bot mitigation capabilities,” said Tim Jefferson, SVP of Data Protection, Network and Application Security, Barracuda. “Traditional web application firewalls don’t all provide advanced bot protection, and some bot mitigation vendors only offer point solutions that aren’t integrated into WAFs. Advanced Bot Protection is fully integrated into Barracuda’s web application firewalls to provide a complete application security solution that is easy to deploy and manage.” Learn more about Barracuda Advanced Bot Protection, now available with Barracuda Web Application Firewall: https://www.barracuda.com/products/webapplicationfirewall Resources Get information about Barracuda WAF-as-a-Service: https://www.barracuda.com/waf-as-a-service Get information about Barracuda Web Application Firewall: https://www.barracuda.com/products/webapplicationfirewall Read the blog post: http://cuda.co/35615 1Gartner: Assessing the Impact of Machine Learning on Security, Published: 6 May 2019, by Anna Belak, Anton Chuvakin, Augusto Barros About Barracuda At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-enabled, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data and applications with innovative solutions that grow and adapt with our customers’ journey. More than 150,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com. Barracuda Networks, Barracuda and the Barracuda Networks logo are registered trademarks or trademarks of Barracuda Networks, Inc. in the U.S. and other countries.

Contacts

Emma Keen
+61 2 8905 0995
mailto: emma@einsteinz.com.au
Karen Terranova
+61 2 8905 0995
mailto: admin@einsteinz.com.au