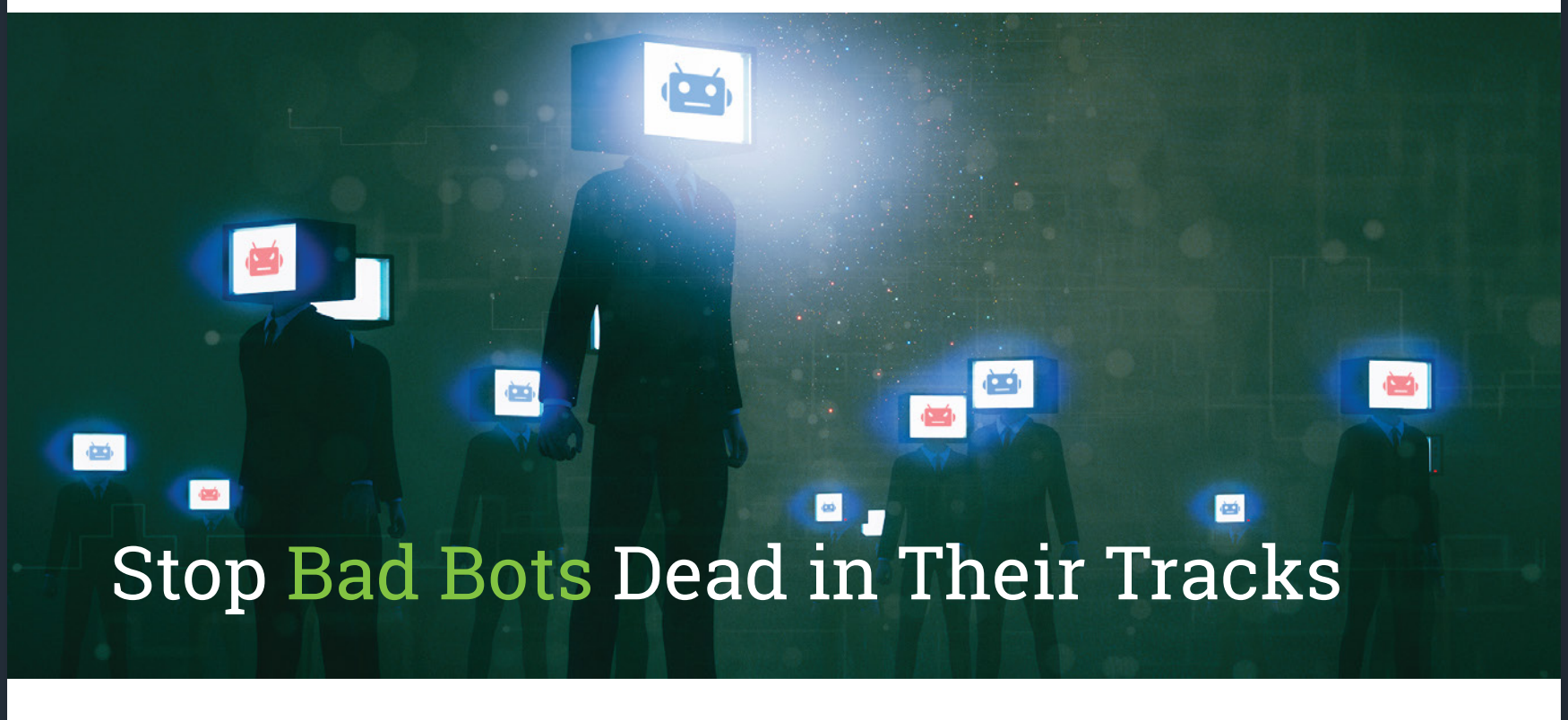
Barracuda

PARTNER LOGO



Stop Bad Bots Dead in Their Tracks

While the “rise of the machines” marched people to their doom in the movie, it is an imaginative story after all. But in the real world, the rise of Internet bots has become a real crisis! Cybercriminals are using bots to do their evil bidding by scraping websites and initiating automated cyberattacks, posing new threats to online businesses of all sizes.

The ongoing coronavirus pandemic also became the “catalyst” with e-commerce and digital transformation leading to a massive increase in bot attacks. Even worse, bots are getting more human-like and smart enough to bypass standard defenses like reCAPTCHA with ease.

Don’t await our doom! Stand up and fight! Barracuda Advanced Bot Protection changes the game in five effective ways:

1. **Power of the crowd** – harnessing crowd-sourced data for anomaly detection
2. **Machine learning based detection** – spotting threats through machine learning, followed by automated real-time responses
3. **Deep visibility with actionable insights** – Advanced Analytics Dashboard offers a unified view of traffic patterns and bot attacks
4. **Efficient verification** – identifying legitimate users with smart, advanced fingerprinting

Stop bad bots with ease, and improve your end customer experience

Barracuda Advanced Bot Protection is a cloud-based service available with the Barracuda WAF or WaaS solution. When enabled, it scans all incoming traffic to identify automated bot traffic to prevent attacks like web scraping, credential stuffing, password spraying, content spam and much more. It protects your websites, mobile applications and API’s against the worst attacks no matter they are OWASP Top 10, DDoS or bot attacks, combating the risk of data breaches, reputational damage and financial disasters. Contact us now!

Contact Us

Forward this to a colleague