F5 Distributed Cloud Bot Defense

Defend against malicious bots. Ensure safe, fast, and seamless user experiences.
Today’s Bots Are Advanced, Persistent, and Increasingly Difficult to Detect

Bots make the Internet work—from search engine crawlers that bring the world to your fingertips to chatbots that engage and influence your customers early in the buyer’s journey. These are good bots. But then there are malicious bots. These bad bots scale automated attacks that cause significant financial pain, slow web and app performance, scalp goods, and hoard inventory. Malicious bots not only lead to customer frustration, they also enumerate gift cards to steal balances, create fake accounts to commit fraud, and carry out account takeovers via credential stuffing.

Credential stuffing is particularly pernicious. Criminals test credentials stolen from other sites against your customers’ accounts at an alarming rate. In 2020 alone, 1.86 billion credentials were stolen, according to the F5 Labs 2021 Credential Stuffing Report. And because two out of three people reuse passwords across accounts, credential stuffing leads to a remarkably high number of account takeovers. Each account takeover causes financial losses to you and your customers, in addition to privacy violations, subsequent fraud, and brand damage.

Static defenses within a web application firewall (WAF) no longer protect against today’s advanced, persistent bots. Criminals retool bots within minutes to bypass defenses, utilize millions of valid IP addresses, rapidly solve CAPTCHAs, mimic human behavior, and introduce subtle randomness—all making it impractical for conventional defenses to mitigate bots.

Your ability to identify and thwart fraud will be tested by a wide range of creative, complex, and stealthy tactics used by cybercriminals looking to exploit any possible attack surfaces that may exist across your websites and apps. With F5® Distributed Cloud Bot Defense, your sites and apps are guarded against:

Credential stuffing
Stop bots from testing stolen credentials and taking over accounts.

Fake accounts
Prevent criminals from automating fake account creation for fraudulent use.

Scalpers/Inventory hoarding
Mitigate inventory hoarding and retain customer loyalty.

Content scraping
Protect performance and privacy—control how scrapers harvest data.

Gift card attacks
Disrupt enumeration of codes that lead to card cracking.
Stay Ahead of Attackers with F5 Distributed Cloud Bot Defense

F5 stays ahead of attackers and eliminates frustrating security frictions, improving your customers’ safety and experience online.

Highest efficacy
F5 Distributed Cloud Bot Defense uses rich client-side signal collection, aggregate data collection, and AI for unparalleled long-term efficacy and near-zero false positives, all while maintaining access for good bots. From protecting the world’s largest banks to securing global retailers and airlines, Distributed Cloud Bot Defense ensures you’re ready when these attacks target your organization.

Lasting security through code protection
Because bot protection requires data collection on the client side for both web and mobile, F5 deploys innovative technology to prevent attackers from seeing and tampering with any collected data. F5 developed the first virtual machine (VM)-based obfuscation defense in JavaScript, employing telemetry encryption and blocking attackers from breaking detection methods.

Remove friction
F5 increases security and reduces friction, getting rid of flow-disrupting CAPTCHA, account lockouts, and multi-factor authentication, leading to happier customers, higher conversions, and greater revenue.

Easy deployment
Distributed Cloud Bot Defense deploys easily thanks to a set of pre-built connectors for popular content delivery networks (CDNs), Application Delivery Controllers, application platforms, and through the F5 Distributed Cloud WAAP. All the connectors are available with support services tailored to your needs, from self-service to managed service.

Using Our WAF and Traditional Firewalls to Manually Block IP Addresses Was a Horribly Ineffective Way to Mitigate the Very Real Threat Posed by Bots.

—CISO, Major US Retailer
High-Performing Bot Protection Against Today’s Most Sophisticated Bots

Achieve highly effective, industry-leading bot protection based on unparalleled analysis of devices and behavioral signals, which together unmask malicious automations. Your organization gains the advantage of a network effect as the platform adapts to retooling attempts across the world’s most highly trafficked apps.

To learn more, speak with a bot defense expert, or visit F5.com.