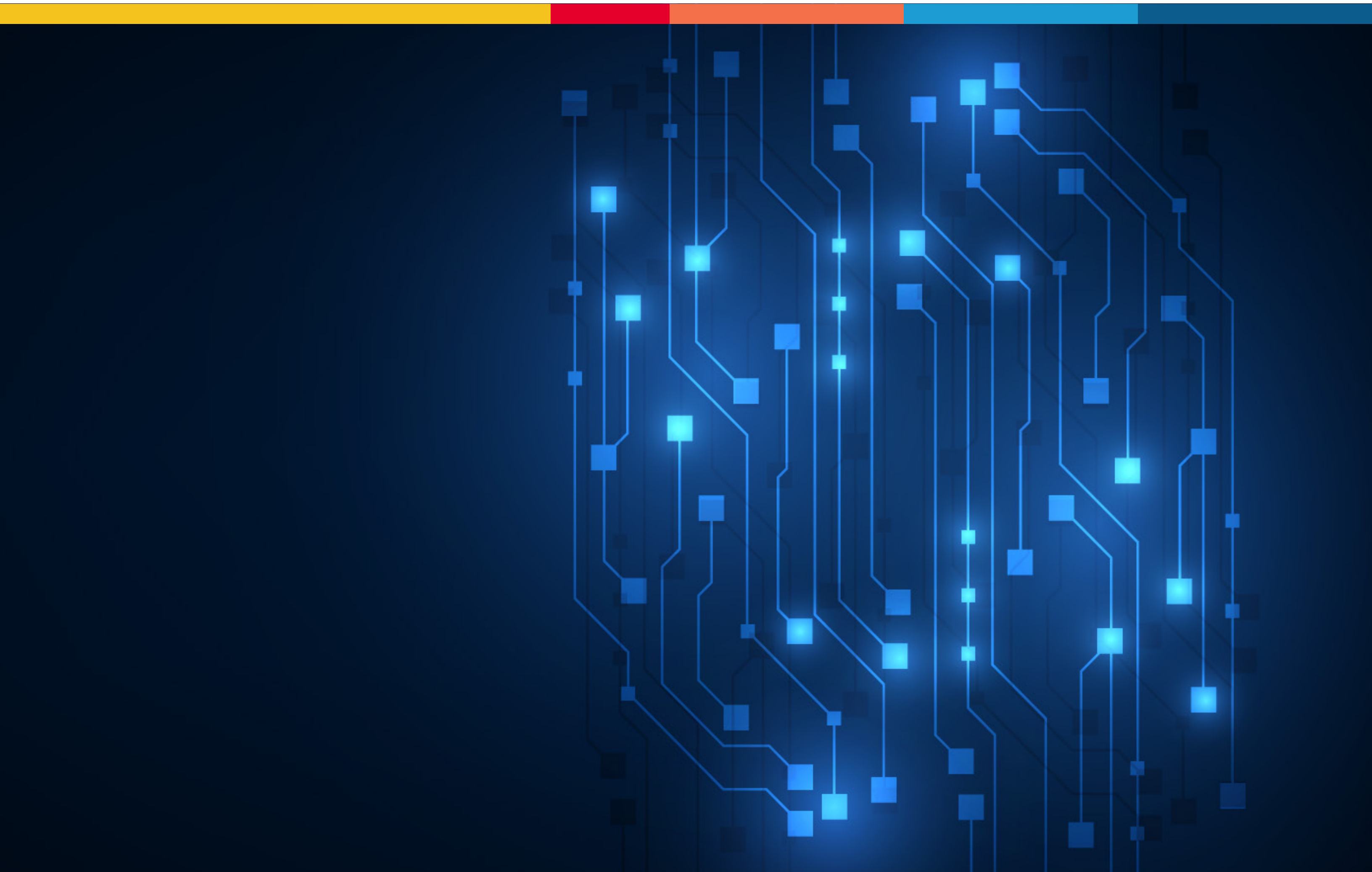
F5 Distributed Cloud Bot Defense

Defend against malicious bots. Ensure safe, fast, and seamless user experiences.



KEY BENEFITS

Reduce fraud
Reduce fraud caused by credential stuffing, account takeover, scraping, and inventory hoarding.

Remove security friction
Mitigate bots without the need for security friction–CAPTCHA, account lockouts, and multi-factor authentication–so that you can improve conversion and increase revenue.

Ease the security burden of fighting bots
Today's sophisticated bots retool within minutes of detection. Eliminate the burden of constantly updating WAF rules with F5 Distributed Cloud Bot Defense.

Improve customer experiences
Prevent scraping bots from slowing down your site and scalping bots from hoarding the inventory that your customers want to buy.

> WITH BOT ATTACKS, THE GAME CHANGES ALL THE TIME. THEY'RE LEARNING AND ADAPTING, AND OUR PRIOR SOLUTION COULD NOT KEEP UP, PUTTING MORE BURDEN ON OUR SECURITY TEAM.
>
> –Engineering director, Retailer

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.[1] 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.

KEY FEATURES

High-efficacy, real-time bot mitigation
F5's domain experts and data scientists continuously research attacker tools, behavioral and environmental signals, and utilize advanced ML to rapidly detect attacker retooling and deploy updated models to mitigate attacks in real time.

Easy deployment with pre-built connectors
Deploy easily with prebuilt connectors for CDNs, Application Delivery Controllers (such as BIG-IP), e-commerce and application platforms, and F5 Distributed Cloud WAAP.

Tamper-resistant code obfuscation and reverse-engineering security protection
To prevent reverse engineering, code tampering, and to block attackers from breaking detection methods, F5 developed the first VM-based obfuscation in JavaScript for bytecode-level obfuscation and telemetry encryption.

Protection for web, mobile, and APIs
Attackers switch attack surfaces whenever they are blocked, going from web to mobile to APIs. F5 Distributed Bot Defense protects each of these attack surfaces so you can provide secure experiences for customers wherever they interact.

> 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

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 Web App and API Protection (WAAP). All the connectors are available with support services tailored to your needs, from self-service to managed service.

F5 DISTRIBUTED CLOUD BOT DEFENSE IS THE MOST TRUSTED APPLICATION BY THE BANKING INDUSTRY FOR SECURITY AND FRAUD PROTECTION. IT WAS AN OBVIOUS CHOICE TO PARTNER WITH THEM AND SET THE SAME HIGH STANDARDS FOR OUR OPEN BANKING SOLUTIONS.

–Simon-Pierre Lebel, Senior Director of IT Operations & Security, Flinks

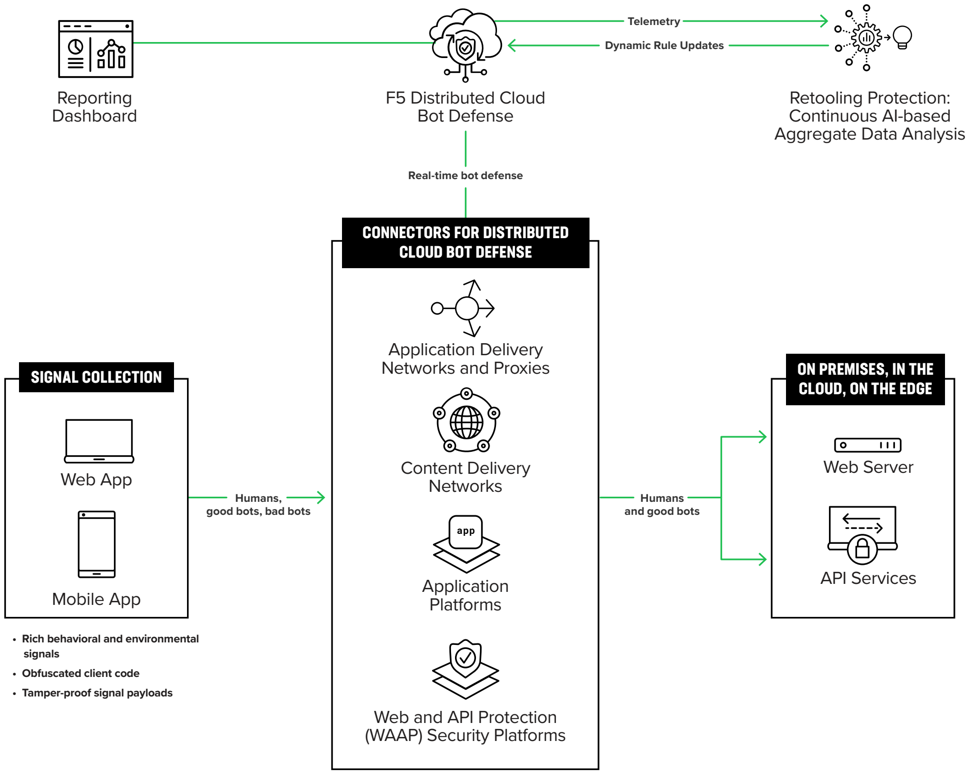

Reporting Dashboard
F5 Distributed Cloud Bot Defense
Telemetry
Dynamic Rule Updates
Retooling Protection: Continuous AI-based Aggregate Data Analysis
Real-time bot defense
CONNECTORS FOR DISTRIBUTED CLOUD BOT DEFENSE
Application Delivery Networks and Proxies
Content Delivery Networks
app
Application Platforms
Web and API Protection (WAAP) Security Platforms
SIGNAL COLLECTION
Web App
Mobile App
Humans, good bots, bad bots
Humans and good bots
ON PREMISES, IN THE CLOUD, ON THE EDGE
Web Server
API Services
Rich behavioral and environmental signals
Obfuscated client code
Tamper-proof signal payloads

Figure 1: Powered by intelligent machine learning (ML), F5 Distributed Cloud Bot Defense analyzes all transactions and scrutinizes every bot attack campaign.

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.

[1] F5 Labs, 2021 Credential Stuffing Report (February 2021), found at https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report