SOLUTION OVERVIEW

# F5 Distributed Cloud Bot Defense for E-Commerce

Defending e-commerce applications against malicious bots to ensure safe, fast, and seamless customer 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.

## Today's Bots Are Advanced, Persistent, Difficult to Detect, and Increasingly Target E-Commerce

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, steal loyalty points, and carry out account takeovers via credential stuffing.

Of all the bot attacks that impact e-commerce, 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.

Many of these attacks target online retail and e-commerce organizations: As commerce continues to shift online, e-commerce apps are bigger targets than ever, and cybercriminals are developing more creative ways to compromise commercial web and mobile apps with sophisticated automated attacks. Up to 90% of traffic flowing to e-commerce apps is usually from non-human visitors, and while some of these software automations are so-called good bots such as web crawlers, 57% of all attacks on e-commerce sites were bot-driven, according to a report in IT Security News. And the cybercriminal focus on online retail shows no sign of abating: According to research reported in Help Net Security, in 2021 the volume of monthly bot attacks on retail websites year-over-year rose 13%, compared to the same months of the previous year.

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

Why are attacks on e-commerce and online retail increasing? In large part, it's because e-commerce transactions involve the exchange of personal and financial information that is valuable to cybercriminals—they follow the money. Bots are more numerous and more malicious now than ever before and are now capable of learning and retooling in hours to launch more sophisticated attacks. Stolen credentials, bot tools, CAPTCHA bypass services, and proxy services are also sold openly on the dark web, bringing advanced bot capabilities to a much larger audience.

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 WAFs to mitigate bots.

KEY FEATURES

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

**Easy-to-deploy connectors for popular e-commerce platforms**
Deploy easily with prebuilt connectors for BIG-IP, CDNs, application platforms, F5 Distributed Cloud WAAP, and e-commerce platforms such as Salesforce Commerce Cloud (SFCC) and Adobe Commerce.

**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.

> 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

Your ability to identify and thwart fraud caused by bots 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. These attacks may include:

- **Credential stuffing and account takeover,** in which attackers test large numbers of compromised credentials (such as usernames and passwords breached from another site) against another site's website login forms to gain access and control those accounts for monetary gain or to commit fraud.
- **Fake account creation,** when cybercriminals use bots to automate the account creation process and use false accounts to commit fraudulent acts, such as influencing product reviews, distributing false information, spreading malware, abusing incentive or discount programs, or creating and sending spam.
- **Scalpers/Inventory hoarding,** which involves the use of automated bots to purchase online goods or services in bulk the moment they go on sale. By completing the checkout process instantaneously, criminals gain mass control of valuable inventory, which is usually resold on secondary markets at a significant mark-up, leading to artificial scarcity, denial of inventory, and consumer frustration. Limited production sneakers and concert tickets are frequent targets of purchasing bots.
- **Content scraping,** which involves the use of automated bots to collect large amounts of content from a target website in order to analyze, reuse, or sell that data elsewhere. While content harvesting has legitimate uses, such as price optimization and market research, it can also be used for illegal purposes, including price manipulation and the theft of copyrighted content. In addition, scraping can impact site performance and prevent legitimate users from accessing a site.
- **Gift card cracking,** which is a type of brute force attack in which attackers check millions of gift card number variations to identify card numbers that hold value. Once attackers identify card numbers with positive balances, they redeem or sell the gift card before the legitimate customer has had a chance to use it. Travel and hospitality loyalty programs are also targets of these bot-based attacks.

## Automated Bots Target Key E-Commerce Segments

E-commerce and online retail are attractive targets for criminals because these businesses process a massive number of financial transactions and store large quantities of customer and employee data. However, some e-commerce sectors face specific fraud and bot attack challenges.

**Airlines:** The airline industry operates air mile and loyalty programs that are estimated to control billions of dollars in stored value, which customers can redeem for airline tickets, upgrades, or other perks. However, these credits have proven to be a major target for cybercriminals because point programs are easy to access and compromise, as they are usually only protected by a simple username and password combo. Also, the value is easy to transfer and resell, and program members rarely monitor their balances.

Airlines also experience a high level of unauthorized scraping of flight and price information from competitors seeking to gain a competitive advantage or undercut prices. Bots can place temporary holds on seats without purchasing to create the appearance of scarcity and drive ticket buyers to competitor's sites, which can have a direct impact on an airline's bottom line.

**Hospitality:** After years of pandemic lockdown, people are traveling in large numbers again and demand is high for lodging, cruises, and other travel and hospitality businesses. Unsurprisingly, cybercrime directed at the hospitality trade has also increased dramatically as pandemic travel restrictions have eased.

As with airlines, hotel and resort websites are the gateway to guests' financial and personal information, such as names, credit card info, loyalty program numbers, and addresses, making them a target for credential stuffing by malicious bots. If these attacks are successful, cybercriminals can gain access to guest accounts and financial information, syphon off loyalty points, and burden the website with such high levels of automated activity that performance is impeded, or even causing it to crash.

Malicious bots are also involved in inventory hoarding schemes, in which they place large numbers of guest rooms on hold, thereby removing them from inventory and preventing actual guests from making a reservation. Sustained inventory hoarding, and other forms of bot manipulation, can frustrate guests and threaten customer loyalty and brand reputation, to say nothing of impacting revenue.

**Quick service restaurants:** Credential stuffing and account takeover attempts are common exploits, as restaurant gift cards are popular and chain restaurants may have millions of dollars of gift card balance credits in their systems. After gaining access to an active account, the fraudster is free to drain the credit balance and resell it on the dark web for cash. Or the stolen gift cards can be used by scammers to order food to-go or for delivery and later dispute the charges and demand a refund, essentially stiffing the restaurant.

F5 Distributed Cloud Bot Defense protects online retailers and businesses across multiple e-commerce sectors. Read our customer story to learn how Distributed Cloud Bot Defense helped a major international airline combat automated attacks by cybercriminals engaged in the theft of proprietary flight information and the takeover of customer accounts. Learn how the airline mitigated credential stuffing attacks and deflected automated traffic from reaching the airline's website.

TENS OF THOUSANDS OF CUSTOMERS WERE IMPACTED BY ACCOUNT LOCKOUT THAT ARE NO LONGER BEING IMPACTED, THANKS TO F5.

–CISO, Retailer

## Stay Ahead of Attackers with F5 Distributed Cloud Bot Defense

Protect your customers from login to checkout without imposing friction with Distributed Cloud Bot Defense, the solution ranked Best in Class by the Aite-Novarica Group's matrix of bot management vendors.

### Highest efficacy

Employ rich web and mobile client-side signal collection, aggregate data analysis, and AI for unparalleled long-term efficacy and near-zero false positives, all while maintaining access for good bots. Ensure you're ready when bots target your organization with a bot protection solution that is trusted to protect the world's largest e-commerce applications.

HAVING F5 SECURITY USING ARTIFICIAL INTELLIGENCE TO CONDUCT MASSIVE-SCALE BACK-END ANALYSIS AND IDENTIFY THE LIKELY PATTERNS OF ABUSE BEING EXECUTED BY BOTS ALLOWS OUR TEAM TO FOCUS ON DOING MORE THOUGHT-PROVOKING THINGS.

–CISO, Retail

### Lasting security through code protection

Bot protection requires data collection on the client side for both web and mobile. Therefore, to prevent attackers from seeing and tampering with data collection, F5 developed the first virtual machine (VM)-based obfuscation defense in JavaScript, employing telemetry encryption and blocking attackers from reverse engineering detection methods.

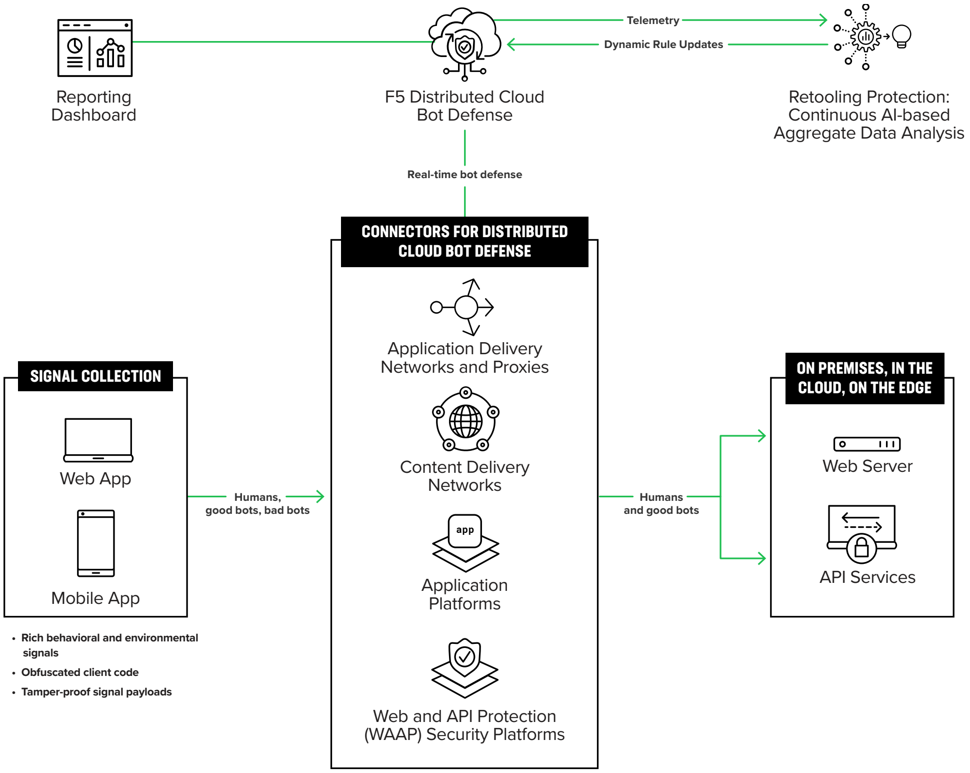
### Remove friction

Increase your security and reduce user friction by getting rid of flow-disrupting CAPTCHA, account lockouts, and multi-factor authentication, leading to happier customers, higher conversions, and greater revenue.

### Easy deployment

Deploy robust bot protections 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). Connectors are also available for Salesforce Commerce Cloud (SFCC) and Adobe Commerce. All the connectors are available with support services tailored to your needs, from self-service to managed service.

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


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

NOW THAT WE KNOW WHAT WE KNOW ABOUT THE ADVERSARY, I DON'T KNOW THAT ANY LEVEL OF STAFFING IS GOING TO BE EFFECTIVE WITHOUT TOOLING THAT RESEMBLES [DISTRIBUTED CLOUD BOT DEFENSE].

–CISO, Retail

## 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 e-commerce operation gains the advantage of a network effect as the platform adapts to retooling attempts across the world's most highly trafficked apps.

## Next Steps

Find out how F5 products and solutions can help you to achieve your goals, contact F5.

Read the Forrester TEI report: retailers report F5 Distributed Cloud Bot Defense reduces the cost of e-commerce fraud by as much as 92%.

**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