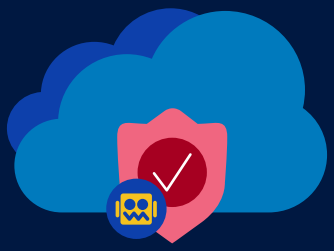
DATA SHEET



F5 Distributed Cloud Bot Defense

Key benefits

Increased efficiency
Simplify protection with automatic detection and mitigation.

Long-term efficacy
Use rich client-side signals, aggregated data, and machine learning assistance for up-to-date security while avoiding false positives.

Code protection
Prevent tampering to block attackers from bypassing detection.

Reduced friction
Improve security and enhance customer experience by eliminating CAPTCHA checks, avoiding account lockouts, and decreasing the frequency of multi-factor authentication.

Mitigate the most advanced bot attacks

From search engine crawlers that facilitate information access to chatbots that engage and influence customers, bots are essential to the Internet and modern business operations. However, they can also be used for malicious purposes—like large-scale, automated cyberattacks that create significant customer frustration, cause financial harm, and degrade application performance.

Bot attacks can lead to the exposure of gift card codes, the creation of fake accounts that are used to commit fraud, account takeovers, multi-factor authentication bypasses, and many other issues. Bots are also increasingly being used by scalpers to hoard and resell inventory.

Traditional defenses such as web application firewalls are insufficient against modern bot-based threats. Criminals are continually adapting their strategies so they can get around defenses, use valid IP addresses, solve CAPTCHAs with AI, mimic human behavior, and add randomness, all of which make conventional methods ineffective.

To counteract this, F5® Distributed Cloud Bot Defense employs client-side signals, code obfuscation, data collection, and AI capabilities for effective defense with minimal false positives, ensuring that legitimate bots still get the access they need. Because F5 protects top-targeted sites such as major banks, retailers, and airlines, we can detect advanced attacks early and apply our learnings to help ensure your organization is safeguarded.

Bot protection made simple

Getting up and running with Distributed Cloud Bot Defense is a painless process. Our managed services team can help you onboard up to two fully qualified domain names. You'll also meet with our bot protection experts to tune your protection policy thresholds. And of course, you'll receive 24x7 email, phone, and ticketing support whenever it's required.

Distributed Cloud Bot Defense is delivered via compute instances dedicated solely to your organization, including production and QA environments.

Key features

Device fingerprinting (optional)
Identify and track web users or mobile devices to flag repeat visitors and prevent fraud.

Proactive alerting and rule management
Create customized alert thresholds, notification processes, and bot detection rules.

Visualization
Generate graphic representations of bot and human traffic, including types of bots and business flows under attack.

Reporting
Create reports showing how you compare to industry peers and detailing top user agents, ASNs, IP addresses, and geographies.

Distributed Cloud Bot Defense package tiers

Distributed Cloud Bot Defense for Web and Distributed Cloud Bot Defense for Mobile are self-service solutions designed to protect web-based and mobile native applications from malicious bot activity. Both offerings include:

- Up to 500,000 transactions per day
- Initial onboarding and setup support for up to two fully qualified domain names (FQDNs)
- One bot engine (one production in two regions, one QA in one region)
- Dedicated, tailored policies to manage bot traffic effectively
- Global bot detection updates that continually refresh detection rules
- Device fingerprinting that identifies and tracks devices to detect repeat or suspicious behavior

Available add-ons (sold separately) include:

- Content scraping protection
- Mobile SDK integrator
- F5 Distributed Cloud Mobile App Shield
- F5 Data Intelligence (Basic, Advanced, Premium)
- Additional bot engines and regions

These offerings are ideal for organizations seeking streamlined, scalable bot protection with minimal friction and strong baseline capabilities.

Bot Defense for Web	Bot Defense for Mobile
Self-service offering for protecting web-based applications from bots	Self-service offering for protecting mobile native applications from bots
INCLUDES	
Up to 500K transactions per day	Up to 500K transactions per day
Initial onboarding and setup (up to 2 FQDNs)	Initial onboarding and setup (up to 2 FQDNs)
Includes 1 bot engine (1 production in 2 regions, 1 QA in 1 region)	Includes 1 bot infrastructure (1 production in 2 regions, 1 QA in 1 region)
Dedicated bot policies	Dedicated bot policies
Ongoing updates to global bot detection rules	Ongoing updates to global bot detection rules
Device fingerprinting	Device fingerprinting
ADD-ONS	
Paid features	
Additional transactions per day (unit: 500K/day)	Additional transactions per day (unit: 500K/day)
Content scraping	Mobile SDK Integrator
	Mobile App Shield
	Mobile integration services
Data Intelligence (Basic, Advanced, Premium)	Data Intelligence (Basic, Advanced, Premium)
Additional regions/bot engines (1 production, 1 QA)	Additional regions/bot infra (1 Prod, 1 QA)
Managed threat intelligence (Expert-led monitoring, threat and re-tool detection, and TI package upkeep)	Managed threat intelligence (Expert-led monitoring, threat and re-tool detection, and TI package upkeep)
Managed services (Standard, Enhanced, Enhanced Plus); Enhanced and Enhanced Plus included managed threat intelligence	Managed services (Standard, Enhanced, Enhanced Plus); Enhanced and Enhanced Plus included managed threat intelligence

*Note: Please refer to managed services description documentation for service levels.

The Distributed Cloud Bot Defense Advanced and Distributed Cloud Bot Defense Premium bundles are comprehensive, managed offerings that include both Distributed Cloud Bot Defense for Web and Distributed Cloud Bot Defense for Mobile capabilities, delivering scalable protection, expert support, and advanced threat intelligence.

Distributed Cloud Bot Defense Advanced

- Includes Distributed Cloud Bot Defense for Web and Distributed Cloud Bot Defense for Mobile
- Managed service with Enhanced-level support (named resource)
- Up to 1M transactions per day
- 6 bot engines provisioned
- Dedicated bot policies and global detection rule updates
- Device fingerprinting and Data Intelligence (Basic)
- Content scraping protection included
- Managed threat intelligence, with 24x7 SOC monitoring, custom detection rules, threat briefings, and on-demand tactics support

Distributed Cloud Bot Defense Premium

- Includes Distributed Cloud Bot Defense for Web and Distributed Cloud Bot Defense for Mobile
- Managed service with Enhanced Plus-level support (dedicated resource)
- Up to 1M transactions per day
- Unlimited bot engines provisioned in any geographic region
- All features of the Advanced bundle, plus:
    - Support for custom deployment architectures
    - Data Intelligence (Advanced and Premium tiers)

These bundles are ideal for organizations that need robust, enterprise-grade bot protection with flexible infrastructure and expert-led threat response.

Bot Defense Advanced Bundle	Bot Defense Premium Bundle
Managed offering (Enhanced level) for protecting web and mobile applications from bots	Managed offering (Enhanced Plus level) for protecting web and mobile applications from bots with option to provision unlimited number of bot engines in any geographic region
Up to 1M transactions per day	Up to 1M transactions per day
On-demand support for onboarding and setup	On-demand support for onboarding and setup
Up to 6 bot engines provisioned	Unlimited number of engines provisioned
Dedicated bot policies	Dedicated bot policies
Includes content scraping protection	Includes content scraping protection
Device fingerprinting and Data Intelligence Basic	Device fingerprinting and Data Intelligence Basic
Managed services (Enhanced*— named resource)	Managed services (Enhanced Plus*—dedicated resource)
Managed threat intelligence (24x7 SOC monitoring and alerting, custom detection rules, threat briefings, on-demand tactics support)	Managed threat intelligence (24x7 SOC monitoring and alerting, custom detection rules, threat briefings, on-demand tactics support)
	Support for custom deployment architectures
ADD-ONS	
Paid features	
Additional transactions per day (unit: 500K/day)	Additional transactions per day (unit: 500K/day)
Mobile SDK integrator	Mobile SDK integrator
Distributed Cloud Mobile App Shield	Distributed Cloud Mobile App Shield
Data Intelligence (Advanced and Premium)	Data Intelligence (Advanced and Premium)
Additional regions/bot engines (1 production, 1 QA)	Additional regions/bot engines (1 production, 1 QA)

*Note: Please refer to managed services description documentation for service levels.

Threat Briefings in Distributed Cloud Bot Defense

Threat Briefings are a key component of the Managed Threat Intelligence service included in the Advanced and Premium bundles of Distributed Cloud Bot Defense. These briefings provide organizations with expert-led insights into evolving bot threats, including:

- Custom detection rules tailored to your environment
- 24x7 SOC monitoring and alerting
- On-demand tactics support to respond to emerging threats
- Regular briefings that keep your team informed on attacker behavior, re-tooling trends, and mitigation strategies

These briefings help ensure your bot defense posture remains proactive, adaptive, and aligned with the latest threat landscape.

Resources

From Bots to Boardroom: How Bad Bots Negatively Impact Your Balance Sheet

Experience F5 Distributed Cloud Bot Defense

2025 Advanced Persistent Bots Report

You Can't Spell API Security without Bot Defense

More information

Contact an expert to learn more.

DC 07.2025 | JOB-CODE-1664534466