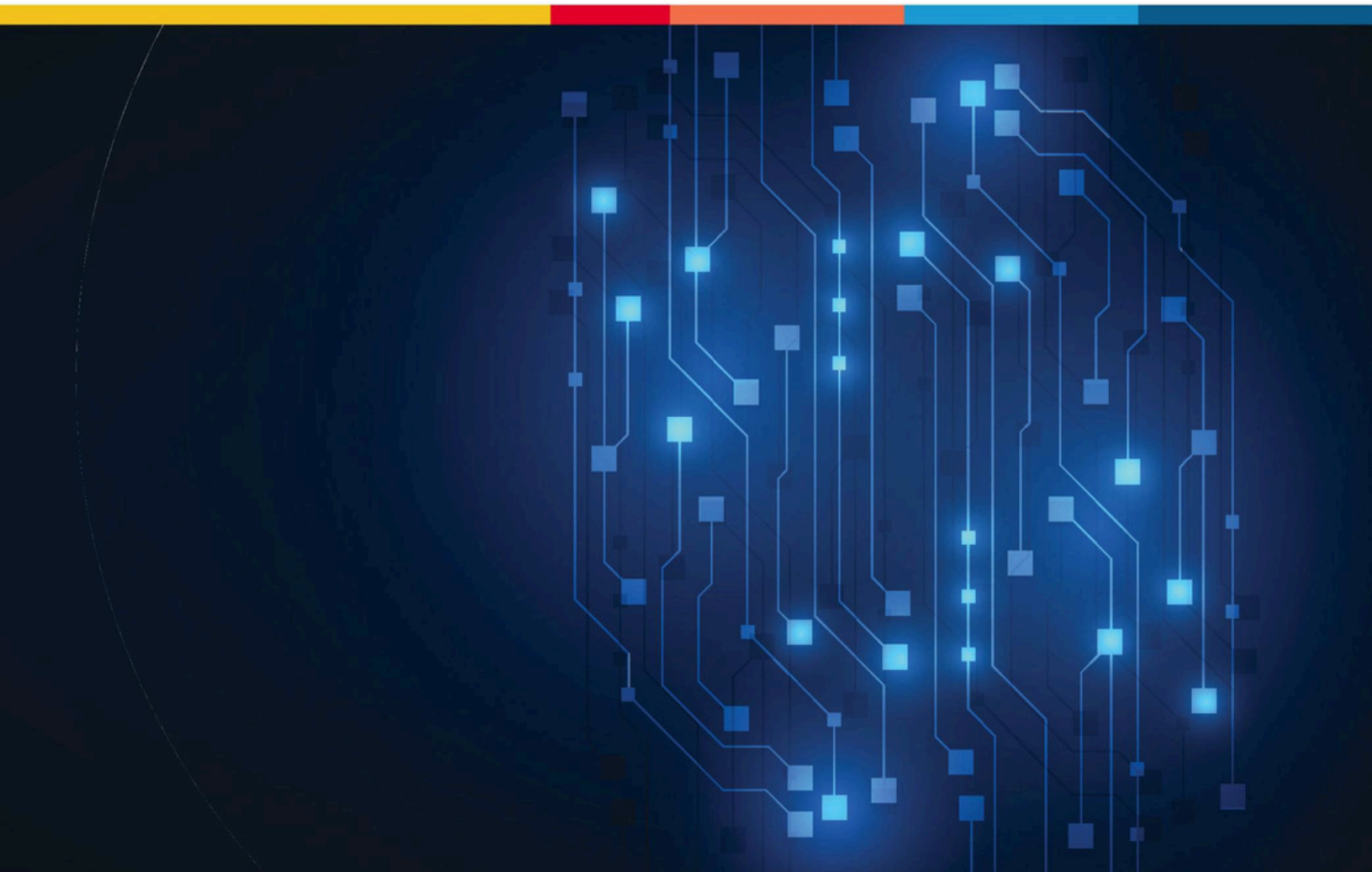
FullProxy

SOLUTION OVERVIEW

F5 Distributed Cloud Bot Defense

Protect applications and web data from malicious bots and sophisticated automated attacks.



KEY BENEFITS

Protect your business
Identify, verify, and stop sophisticated bots.

Protect web and mobile apps, APIs, and social assets
Safeguard your high-value, consumer-facing digital properties.

Remove bad bots from the equation
Optimize the efficiency of your web-facing app experiences.

Stratify trust
Create confidence inside the consumer app experience flow by eliminating 99% of bad bots attacking your systems.

Deliver seamless customer experiences
Stop bad bots without affecting the end-to-end app workflow.

Enjoy fast, flexible deployment
Choose from multiple integration options to adapt to all attack profiles.

The highest incidence of fraud is now conducted against web-facing business channels. Attackers now have more Internet-accessible application paths to attack than ever before. Enterprises find it increasingly difficult to identify, defend, and protect their applications from bot attackers and keep up with the relentless pace and scale of attacks. In a recent internet report, the results revealed that 39% of all internet traffic analyzed was from malicious bad bots, and only 15.2% came from good bots. Bad bots attacks are now highly pervasive.1 Automated bots exploit weak edge security to gain a global deployment footprint that powers distributed, high-scale attack vectors against application origin endpoints. Automated bot attacks evolve rapidly via retooling feedback, which operates at web scale and outpaces most human cybersecurity professionals.

Don't Get Retooled

Cybercriminals retool their bot attacks with lightning-fast efficiency to overcome low-strength, commoditized, and low-value bot protection solutions, which puts security teams on the defensive and strains precious operational resources. Failing to effectively manage bots can have big impacts on your application performance, your customer application experience, and your business.

Attack Vector Intelligence Automation and Mitigation at Web-Scale

There are two stages to a Distributed Cloud Bot Defense deployment: Observation and Mitigation. In the observation stage, Distributed Cloud Bot Defense collects telemetry from an extensively deep set of signals against each client to inform and train the machine learning engine that detects bot behavior and attack personas. The verification engine is the decision-making component, which verifies automated bot behavior transactions. To defeat fraudulent operations, it profiles thousands of client signals to verify malicious automation within the application, network, browser, user, and API layers.

A trusted bot defense solution requires high-efficacy, machine learning-driven bot defense and protection for every industry and attack vector type. F5® Distributed Cloud Bot Defense is a leader in bot management for e-commerce, retail, financial services and travel,2 as well as hospitality, technology, FinTech/banking, airlines and gaming.3

Distributed Cloud Bot Defense operates unobtrusively. Any time the platform determines, in real time, that an application request has a fraudulent source profile, it intelligently blocks the transaction—without introducing any application friction (such as multi-factor authentication, CAPTCHA, etc.) to legitimate human users.

40% OF ALL GLOBAL WEB TRAFFIC IS NOW BOT TRAFFIC, AND THIS NUMBER INCREASES DAILY. 25% OF ALL BOTS ARE MALICIOUS BAD BOTS.2 THEY'RE SOPHISTICATED AND AUTOMATED AND NEGATIVELY IMPACT YOUR CUSTOMERS' WEB EXPERIENCES.

kinecta℠

CREDIT UNION STOPS AUTOMATED ATTACKS WITH A SCALABLE AND ADAPTABLE BOT MITIGATION SOLUTION

Kinecta Federal Credit Union is one of America's largest credit unions, with 245,000 member-owners and assets of $4.7 billion. Kinecta needed a solution to combat an increasing number of online login attacks on its banking website. Without support for 24/7 monitoring and attack mitigation, legitimate customers were experiencing login difficulties and website timeouts due to bad actors. Kinecta saw daily logins spike by 2,400% during automated attacks. Within 48 hours of implementing the Distributed Cloud Bot Defense solution, the credit union was able to:

- Completely mitigate an ongoing attack
- Restore a positive online experience for its customers
- Reduce customer service complaints
- Discover the benefits of machine learning and AI to identify ongoing bot traffic
- Eliminate 90% of attack traffic

Powered by machine learning (ML), Distributed Cloud Bot Defense analyzes all transactions and scrutinizes every bot attack campaign. It proactively recognizes patterns and thwarts future attack vectors via smart Digital Behavior Bot analytics technology and techniques. When attackers attempt to bypass detection by retooling sophisticated bots, Distributed Cloud Bot Defense identifies fingerprinted attack personas using high-efficacy AI. Most importantly, as soon as a new attack technique is observed on one customer, new countermeasures are autonomously deployed, and shared with all other F5 customers. This delivers global anti-bot inoculation across the platform and the user population.

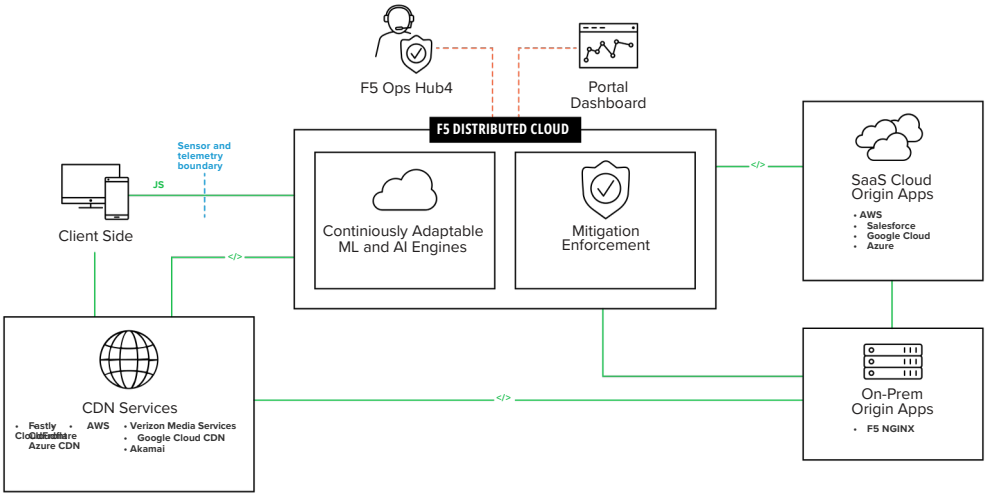


Figure 1: Powered by intelligent Machine Learning (ML), F5 Distributed Cloud Bot Defense analyzes all transactions and scrutinizes every bot attack campaign.

This allows F5 Bot Defense to combat many of the most critical automated attack vectors and known OWASP Bot threats. Such as:

- **Account takeover**–Prevent unauthorized access to accounts and unauthorized transactions.
- **Credential stuffing**–Stop mass brute force verification of stolen credentials on your web properties.
- **Denial of inventory**–Thwart product unavailability by intentionally unexecuted bulk cart purchases.
- **Checkout abuse**–Prevent multiple automated abuse vectors in critical checkout transaction pages.
- **Web scraping**–Stop automated bots from stealing critical data from your apps and web properties.
- **Card cracking**–Block brute force payment card information and code cracking attacks.

KEY FEATURES

Advanced client signals intelligence with deep traffic telemetry
Lightweight telemetry modules collect +3,000 client-side signals and feed data into the platform via rapid asynchronous API transactional flows.

Identify, verify, pattern match at web-scale
Our high-precision, high-efficacy verification engine, pattern matching, and identity platform is horizontally integrated in-line across the end-to-end platform and operates at web speed.

Advanced retooling countermeasures
Industry-leading integrated security protocols, deep obfuscation, and anti-retooling technology thwarts, frustrates, and defeats retooling efforts.

Decide, mitigate, and intelligently self-learn behavior flows
Machine learning and AI behavioral system adapts and learns while executing billions of the observed web transactions.

Report, insight, manage, analyze
Globally available, always-on SaaS dashboard and reporting platform provides deep, configurable insights of client-to-origin application traffic transaction.

Scale as you grow and defend at your pace
Multiple tiers of scale, deployment, and service enables flexible bot defense strategies.

- Fully Managed
- Partially Managed
- Self-Managed
- Hybrid App Stack

Conclusion

Sophisticated attackers continuously and relentlessly retool bot attacks against countermeasures, enhancing bot intelligence to emulate human behavior and evade detection. Security must maintain resilience and effectiveness to protect businesses from cybercrime that can lead to unauthorized access, account takeover, and fraud.

Leverage trusted, high-performance capabilities of behavioral fingerprinting, predictive analytics, and advanced machine learning models to differentiate real users from automated, malicious attacks and accurately identify and block sophisticated threats.

F5 TRUSTED GLOBAL CUSTOMER SUPPORT

Enjoy easy onboarding, best-in-class security expertise, and responsiveness. Experience 24x7 security analyst oversight and Security Operations Center (SOC)4 monitoring to keep your business continuously protected from bad actors and automated bot attacks.

To learn more, contact hello@fullproxy.com or visit www.fullproxy.com.

[1] Sandy Carielli with Amy DeMartine, Isabelle Raposo, Peggy Dostie, Forrester Now Tech: Bot Management, Q4 2021 (November 29, 2021), found at https://www.forrester.com/report/now-tech-bot-management-q4-2021/RES176597

[2] Ibid.

[3] Please contact an F5 representative for more information.

[4] Available with certain deployment service offerings.