DATA SHEET

F5 Bot Defense features for Agentic AI

Take control of AI agents–reduce fraud, protect revenue, and enable trusted automation.

THE SHIFT:

Agentic AI is already hitting your apps

Agentic AI doesn't just scrape pages: it browses, fills forms, creates accounts, resets passwords, places orders, and chains actions autonomously. They can be helpful (price checkers, shopping assistants, customer agents) or harmful (fraud bots, credential stuffers, inventory scalpers, content scrapers). Traditional bot tools tuned for scripts and headless traffic struggle to distinguish human users from increasingly human-like AI agents.

The risk

Misclassification of AI agents
As malicious bots disrupting normal user workflows, causing failed transactions, customer friction, and direct revenue losses.

Identity and accountability ambiguity
Obscuring who is taking an action and who should be held responsible for the consequences.

Operational disruption
Expose sensitive data, disrupt workflows, increase security risk, and cause potential data loss.

Authorized, economically harmful at scale
Allowed actions at volume that cause financial loss, service degradation, or business logic abuse.

WHAT'S NEW:

Bot Defense for Agentic AI

1 **Detection signals for agentic browser traffic**
Finally, you will know when an **AI agent—not a human—is interacting** with your website or APIs. Purpose-built telemetry and behavioral models surface agentic patterns across modern browsers, extensions, headful automations, and tool-augmented sessions.

2 **Trusted agent traffic management**
Only **authorized, unmodified, policy-compliant AI agents** can take actions on your apps. Enforce allowlists, integrity checks, and policies tied to identity, source, and purpose—**no more guessing who's at the door**.

3 **Purpose-built management & reporting of agent traffic**
Clear **visibility** into which agentic traffic is hitting which endpoints, what it's doing, and how it impacts KPIs. Out-of-the-box dashboards help security, fraud, and application teams **decide and act**.

4 **Out of the box integrations**
Evolving security partnerships to enable organizations to manage **traffic from agents**, **curb automated abuse**, and **monetize verified AI activity**, while ensuring robust controls to prevent exploitation and abuse.

Ideal use cases

- Allow trusted agents to access product details and checkout flows.
- Deny agents access to flows you want human only access (ex. sensitive data, login endpoints).
- Login and account flows, checkout and payments, promotions and loyalty.
- High value product and pricing pages, inventory and reservations.
- Enable monetization of content with AI Platforms.

How Bot Defense helps

- **Detect and classify** humans, agents, and bots, and apply the right policy to each.
- **Provide real-time visibility** into agent traffic showing intent, activities, session behavior, and top targeted routes.
- **Protect sensitive endpoints** from AI Agents to ensure your proprietary data remains secure.
- **Disrupt abusive automation** before workflows are exploited by blocking known automation frameworks and detecting malicious agentic behaviors.

How it works (At a glance)

1. **Detect:** Out-of-the-box detection based on traditional and agentic specific detection methods.
2. **Authorize** trusted agents using pre-configured controls.
3. **Manage:** Granular permission management to control access and rate of access across the various parts of the website
4. **Monitor:** Continuously monitor agent traffic for compliance.

Bottom line

AI agents are here. The question is whether you control them–or they control your risk.

With F5 Bot Defense for Agentic AI, you're in control.

Contact your F5 account team for more information or to enable in your environment.