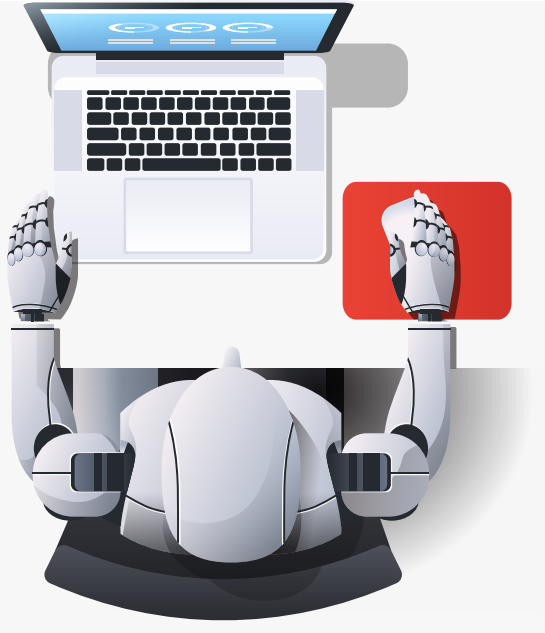
Battle of the BOTS



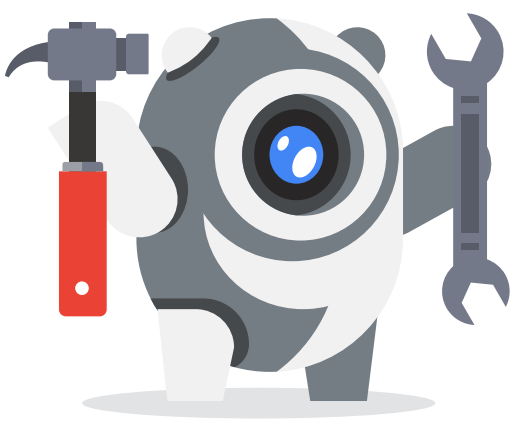
Choose your defenses wisely against cyber fraud

Meet your cybersecurity opponents

Criminals are embracing bots and automation to carry out large-scale attacks with a growing set of sophisticated methods that circumvent traditional defenses:

Account takeover

Attackers test large numbers of compromised credentials against your login application to compromise those accounts for monetary gain.



Fraud

The automated abuse of web pages, like checkout pages to identifymissing credit card values, or repeatedly requesting or submitting content, which skews business intelligence data..

WARNING!

Bad bots account for nearly 40% of all internet traffic.[1]

Bot attacks increased by 41% in the first half of 2021 alone.[2]

Time to get your digital guard up

As these threats are on the rise, how are businesses responding?

Know your weak spots:

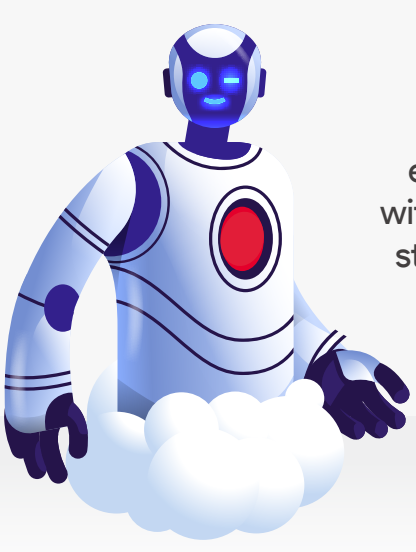
Only 15% of businesses protect against web scraping attacks.[1]

73% of businesses face weekly bot-based attacks.[1]

Credential stuffing and bot-driven attacks are the #1 global app security concern.[2]

Partner with security powerhouses

There's a top-notch tag team that can help your business protect against sophisticated attacks and cyber criminals who constantly adapt.



F5 + Google Cloud

Partners F5 and Google Cloud work to stay ahead of existing and future bad bot tactics, empowering you to battle automated attacks with automated defenses. Innovate your security stack by combining the industry's most trusted cloud with AI-powered F5 SaaS solutions.

A one-two protection knockout

Evolve and adapt more quickly to changing conditions with F5 and Google Cloud.

Protect against bots and human fraudsters

Safeguard digital experiences and reduce fraud to strengthen customer trust, enhance customer experience with your applications, and grow business value. This includes protection from:

- Bot attacks
- Web fraud
- Unauthorized access
- DDoS attacks
- DNS attacks
- API attacks

Trusted cloud for everyone

Google Cloud defends customer data using the same infrastructure and security services used internally, with advanced capabilities normally unavailable to all but the most well-resourced global organizations.

Google Cloud operates with Trusted Cloud requirements:

1. A secure platform that delivers transparency and enables sovereignty
2. A proven zero-trust architecture
3. Shared fate with customers, not shared responsibility

F5 bot defense

Proactive, multi-layered security blocks and drops bad-bot traffic before it can hit your network, mitigating bots that perform account takeovers, vulnerability reconnaissance, and denial-of-service attacks targeted at your network or app layer. Identifying bot attacks leads to reduced web app traffic, CPU load, and infrastructure costs.

Google Cloud's strong security and cutting-edge encryption allow companies to safely store and analyze sensitive personally identifiable information coupled with F5 Bot Defense to provide added protection, enhanced performance, and real-time data monitoring to quickly respond to any threats.

Engage F5 and Google Cloud to win in the cybersecurity ring and make your business the champion.

Discover F5 solutions in the Google Cloud Marketplace or visit f5.com to learn more.

1 Barracuda. "Bot Attacks: Top Threats and Trends," Sept 2021
2 F5 Labs. 2021 Credential Stuffing Report. 3 ZDNet. "Bot Attacks Grow by 41% in First Half of 2021: LexisNexis." 14 Sept 2021