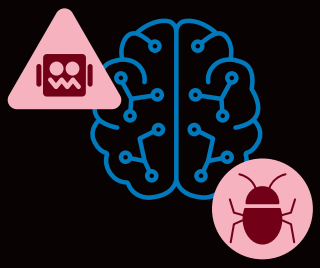
Overview



Setting the Record Straight: Addressing Automated Attack Myths

Block sophisticated and automated cyber threats

Together, F5 and AWS enable you to detect and defend against DDoS attacks, malicious bots, and other advanced cyber threats. Now you can improve your visibility, keep pace as bad actors evolve, and centralize policy enforcement to mitigate cyberattacks and bolster application security postures.

Learn more at **f5.com** or find F5 Distributed Cloud Services on **AWS Marketplace**.

Automated attacks, driven by advancements in AI, are on the rise. From malicious bots to sophisticated DDoS attacks, organizations of every size need a proactive and adaptive approach to stay ahead of evolving threats.

Think your security is up to snuff? See some common myths and learn key insights to bolster defenses from new and persistent attacks.

Myth #1

Web application firewalls (WAF) are antiquated.

Truth: While it's true that traditional WAFs use static rules, generate false positives, and cannot easily scale protections in the cloud, new technology has changed the story. F5® Distributed Cloud WAF uses a next-gen, SaaS-based approach that provides signature and behavioral-based threat detection—wherever apps are deployed. Block OWASP Top 10 threats and zero-day attacks, improve visibility into security events, and centralize policy enforcement to standardize protections for AWS and non-AWS workloads.

Myth #2

Bot prevention is outpaced by attacker retooling.

Truth: Modern bots can and should adapt and evolve with threats. F5® Distributed Cloud Bot Defense provides AI-powered protection to unmask bad actors and rapidly discover retooling attempts. Easily add bot protection to Amazon CloudFront to analyze massive traffic volumes to pinpoint malicious activity and block bad bots. Advanced obfuscation techniques prevent reverse engineering by attackers.

Myth #3

DDoS attacks only happen at the network level.

Truth: L7 attacks are increasing, requiring organizations to deploy DDoS protection at both the network and application layers. F5 and AWS multi-faceted DDoS protection enable consistent cloud-based perimeter security to mitigate L3-L7 attacks in every environment. Safeguard against volumetric network-level attacks while preventing bad actors from consuming critical resources that degrade app performance and reliability.

DC 08.2024 | JOB-CODE-470831091

aws PARTNER