FORTINET

# Key Considerations for Effective Bot Management

# Table of Contents

# Executive Summary

Because of the relentless surge of malicious bots, the need for advanced bot management solutions has never been more apparent. Today, nearly half of all online traffic consists of bots.[1] Bot management solutions must include robust features and capabilities to help security professionals fortify intellectual property, secure online revenue, and protect user accounts against sophisticated bot threats.

According to Gartner®, “Nearly half of all online traffic consists of bots.”[2]

# The Goal: Accurate Bot Detection and Classification

Organizations grappling with the pervasive threat of malicious bots need solutions that offer accurate bot detection and classification. Distinguishing between legitimate users and automated threats is critical. The ultimate goal is not merely identification but also differentiating between good and bad bots.

Any proactive cybersecurity strategy should include accurate bot detection using advanced tools with machine learning (ML) models and behavioral analysis to scrutinize incoming traffic. These techniques go beyond traditional methods, which often falter in the face of sophisticated bot tactics. The goal is to create a dynamic defense system that comprehensively understands the subtle nuances of bot behaviors. It is a powerful tool because ML continuously learns and adapts to evolving bot strategies.

Bot classification involves categorizing identified bots into distinct groups to differentiate between bots with legitimate purposes, such as search engine crawlers, and those that intend harm, such as bots used for account takeovers or distributed denial of service attacks. Accurate classification based on the threat level posed by specific bot behaviors is essential for targeting responses and prioritizing actions.

Accurate bot detection and classification directly contribute to risk mitigation by thwarting potential financial losses, service disruptions, and data breaches. Precise bot detection and classification form the bedrock for safeguarding intellectual property, securing online revenue channels, and maintaining regulatory compliance. Organizations that build resilient defenses can better adapt to the evolution of malicious bot tactics.

# The Method: Continuously Adaptive Detection and Response

Organizations must continuously adapt their detection and response approaches to address the fluid nature of cyberthreats. Bot behaviors are dynamic, and threat actors quickly modify their tactics. Organizations need advanced technologies to continuously analyze and adapt to emerging patterns, such as ML models, which help ensure that detection capabilities remain sharp and effective, even in the face of sophisticated bot tactics like those that closely mimic human behavior.

Adaptive response mechanisms are a crucial line of defense against identified bot threats. The process involves correlating metadata with behavioral factors in real time for swift and targeted responses. For example, when a bot attempts an account takeover or engages in data scraping, the adaptive response mechanism triggers immediate actions to mitigate the threat and help prevent potential financial losses and loss of sensitive data.

The adaptive response mechanism extends beyond immediate responses because it learns from each encounter. By building a repository of bot attack patterns and good bot behaviors, organizations create a robust foundation for training ML models. These models, in turn, enhance their accuracy over time, becoming adept at distinguishing between evolving bot tactics and genuine user behaviors.

Continuous adaptability in detection and response is not just a reactive strategy; it empowers organizations to fortify their defenses, optimize user experiences, and ensure the resilience of digital operations in the face of relentless and sophisticated bot attacks.

# The Expected Outcomes: Adaptive Response Mechanisms

Organizations that adopt a robust bot management strategy by implementing cutting-edge bot management solutions can mitigate the risks of financial losses, service disruptions, and data breaches and improve the overall user experience. The adaptive response mechanisms embedded in bot protection solutions help with:

- **Risk mitigation:** Implementing robust bot management helps reduce the risk of financial losses, service disruptions, and data breaches associated with malicious bot activities.
- **User experience:** Adaptive response mechanisms ensure genuine users experience minimal disruption, which improves user satisfaction.
- **Intellectual property protection:** Comprehensive bot detection safeguards intellectual property by preventing unauthorized access and data exfiltration.

- **Online revenue channel security:** By preventing fraud, inventory scalping, and digital skimming, businesses help safeguard their online revenue streams.
- **Regulatory compliance:** A proactive bot management approach helps organizations meet regulatory requirements related to data protection

# Protect Against Malicious Bots

To fortify networks and applications against malicious bots, security experts must prioritize comprehensive bot detection that addresses as many use cases as possible. Then, they need to focus on the accuracy of the human, good bot-bad bot classifications and practice adaptive response mechanisms. Armed with practical advice to navigate the dynamic cybersecurity landscape, they can take proactive measures to secure intellectual property, online revenue, and user accounts from the pervasive risks posed by sophisticated bots. For more information, learn how Fortinet delivers state-of-the-art solutions powered by ML to detect and mitigate bad bots.

[1] Gartner Research, "Innovation Insight: Bot Management for the IAM Leader," August 4, 2023.

[2] Ibid.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORTINET

www.fortinet.com

January 23, 2024 10:00 PM

2523896-0-0-EN