

New Era of Fraud

Motivated cybercriminals use a variety of tools, tactics, and techniques to evade detection by bypassing security controls and exploiting the seams between security and fraud teams. By leveraging bots and billions of compromised credentials, attackers can easily weaponize and monetize their attacks—leading to fraud, damaged customer loyalty, and tarnished brand. By abusing business logic and retooling around security countermeasures, sophisticated fraudsters evade detection and render traditional mitigations useless, but your customers are left with a user experience full of friction and frustration.

Read the eBook to learn:

- The many faces of fraud and how cybercriminals leverage bots and automation to scale their attacks
- Why credential stuffing has transformed into a business problem that puts pressure on both the top and bottom lines
- How a dedicated, outcome-based bot mitigation service can provide resilient protection no matter how attackers try to bypass your security controls and org chart