imperva

CAPABILITY BRIEF

Account Takeover Prevention

Mitigation of ATO attacks

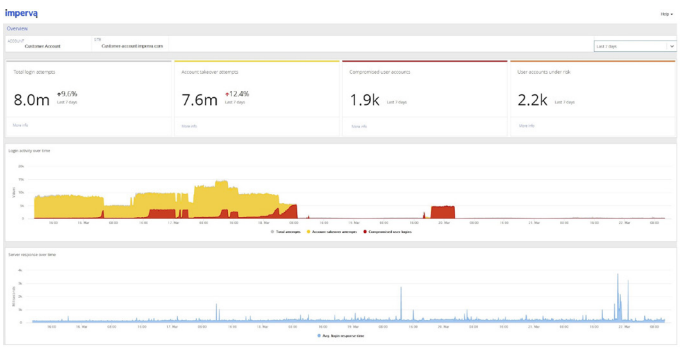
Each year, thousands of enterprises are silently attacked by cybercriminals who seek to compromise customer user accounts through the use of brute-force attacks, guessing weak passwords, or more effectively by leveraging stolen credentials (aka “Credential Stuffing”). Once authenticated, cybercriminals have immediate access to sensitive customer information such as credit cards, currency, health records, and retail reward points - thereby guaranteeing profit. Account takeover (ATO) attacks have pressured organizations to realize that they represent a material threat to their business, affecting brand reputation and revenue, with users often leaving towards competitors. Furthermore, organizations understand that malicious bot traffic consumes expensive bandwidth and compute resources, significantly increasing operational costs. Defenseless, organizations are looking for security solutions that can help to block these sophisticated attacks and allow legitimate, business-critical traffic to pass through unaffected.

KEY CAPABILITIES

- Mitigates all ATO attacks: credential stuffing, bruteforce, dictionary
- Accurate detection with minimal user disruption
- No added latency and performance impact
- Global view of real-time security threats
- Deployed in minutes

Imperva ATO security

Imperva’s ATO protection empowers organizations to mitigate malicious ATO attacks without affecting legitimate users in the process. Imperva is able to accurately determine if the interactions with a website have malicious intent through a multilayered process which includes reputational analysis, an advanced client classification engine, and behavioral machine learning. Built on top Imperva’s integrated single-stack architecture, it ensures that end-users don’t incur latency as they interact with your site. Deployed across the Imperva global network, it guarantees that malicious logins are immediately mitigated closest to where they originate, long before they even have a chance to reach your infrastructure.



Account takeover (ATO) protection service real-time forensics dashboard

Prevent illegitimate access of your user's accounts

Global community intelligence

Imperva captures a worldwide view of ATO behavioral activity across thousands of login pages on our global network that is fed into our multi-stage machine learning models. This allows us to correlate between suspected login attempts and pinpoint credential stuffing attempts even when the attacker uses a fresh credential list.

Real-time protection

Built as part of our single-stack architecture, our detection and mitigation engines are inherent in-line capabilities of our cloud application security solution. This purpose-built architecture allows us to immediately detect and mitigate all risks at the edge without requiring any distant processing centers.

Preserves customer user experience

Captcha challenges are commonly used to identify bad bots, this process often frustrate users and lead to reputational damage. Our multi stage detection approach provides a laser focused security protection with low false positive thus reducing the need to use CAPTCHA challenges and preserves the user experience.

IMPERVA APPLICATION SECURITY

ATO Security is a key component of Imperva Application Security, which reduces risk while providing an optimal user experience. The solution safeguards applications onpremises and in the cloud by:

- Providing WAF protection
- Protecting against DDoS attacks
- Mitigating botnet attacks
- Enabling RASP protection
- Providing actionable security insights
- Ensuring optimal content delivery.

Learn more about Imperva Application Security at www.imperva.com.