imperva

DATASHEET

Account Takeover Protection

Each year, cybercriminals silently attack thousands of enterprises using brute-force attacks to compromise customer user accounts by guessing weak passwords, or more effectively by leveraging stolen credentials (a.k.a. “Credential Stuffing”). Once authenticated, cybercriminals gain immediate access to sensitive customer information such as credit card data, account funds, health records, retail reward points, and more - thereby guaranteeing a profitable attack. In other cases, hackers exploit employee accounts to gain access to the broader enterprise network and execute malware which can then be used in more elaborate and sophisticated ways, compromising business operations and the supply chain.

The frequency and severity of account takeover (ATO) attacks have forced organizations to recognize their material threat to their business; they negatively affect brand reputation and revenue, and forcing users to leave and do business with competitors. Furthermore, organizations now 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.

Imperva Account Takeover Protection

Imperva Account Takeover Protection empowers organizations to mitigate malicious Account Takeover attacks without affecting legitimate users in the process. Imperva is able to accurately determine if the interactions with a website have the characteristics of an account takeover attempt through a multilayered process which includes reputational analysis, an advanced client classification engine, and proprietary algorithms developed by Imperva. Most importantly, Imperva’s solution produces insights that are easy to understand and act upon. It is built on top of Imperva’s integrated single-stack architecture and 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.

KEY CAPABILITIES

Mitigate all bot-driven account takeover attacks: credential stuffing, credential cracking, bruteforce, dictionary.

Deployed in minutes

Minimal false positives, no impact on performance.

See which of your users’ credentials were exposed online, putting them at risk of an account takeover.

Discover accounts at risk of fraudulent activity

Clear visibility into attack attempts, users at risk, compromised user accounts and sussessful logins.

Imperva is an analyst-recognized **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.

Prevent illegitimate access of your users' accounts

Global community intelligence

Imperva captures a worldwide view of Account Takeover 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, but this process generates friction that often frustrates users and leads to reputational damage. Our multilayered detection approach provides laser-focused detection with low false positives, reducing the need to use CAPTCHA challenges and preserving the user experience.

Supports better fraud investigation

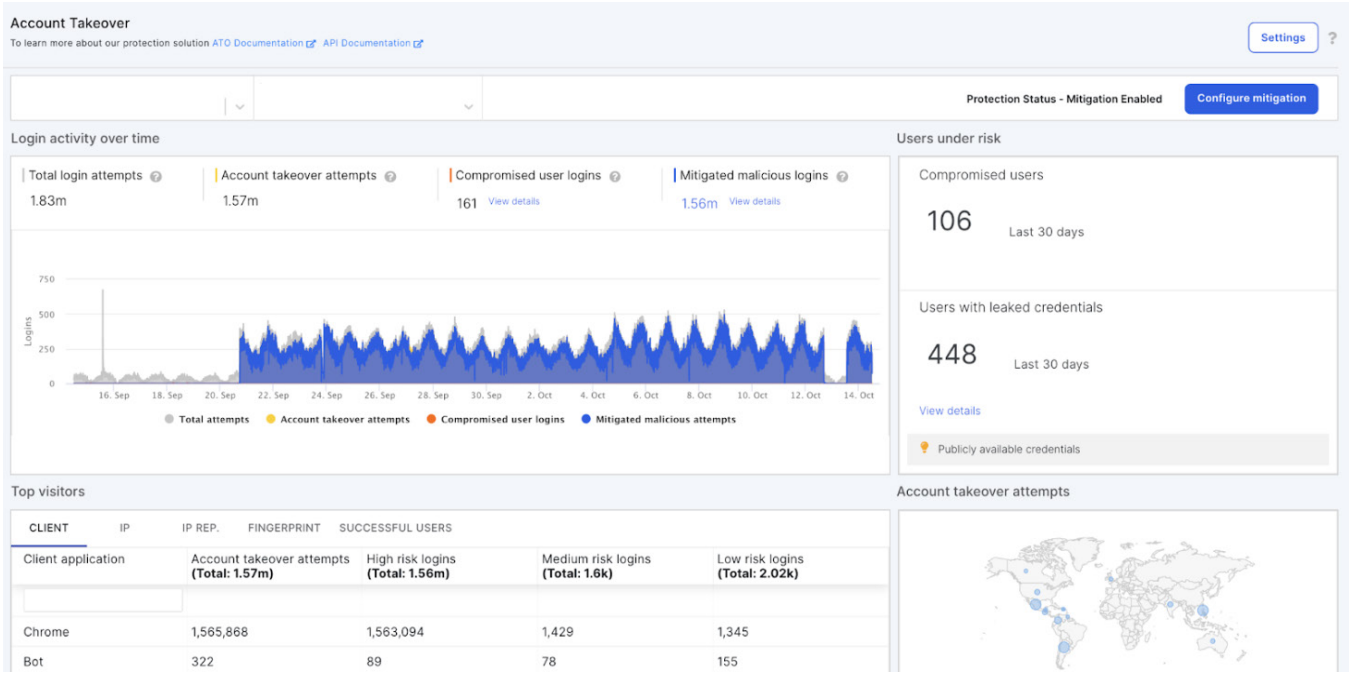
Unique and intuitive dashboards provide security and fraud teams with clear visibility and actionable insights into attack attempts, leaked user credentials, compromised user accounts and successful login attempts. User behavior anomaly detection pinpoints accounts at risk of fraudulent activity.

IMPERVA WEB APPLICATION & API PROTECTION (WAAP)

Account Takeover Protection is a key component of Imperva's Web Application & API Protection (WAAP), which reduces risk while providing an optimal user experience. Our solutions safeguard applications on-premises and in the cloud with:

- Web application firewall (WAF)
- Distributed Denial of Service (DDoS) protection
- Advanced Bot Protection
- API Security
- Runtime Application Self Protection (RASP)
- Client-Side Protection
- Actionable security insights
- Security-enabled application Delivery

Learn more about Imperva Application Security at +1.866.926.4678 or online at impverva.com



Imperva Account Takeover Protection

Copyright © 2022 Imperva. All rights reserved