imperva

DATASHEET

Account Takeover Protection

Safeguard your login pages and protect your customer accounts and data

Account takeover fraud has become a significant threat to businesses across all industries. This type of fraud can compromise customer data, sensitive information, and even entire enterprise networks and the supply chain, leading to severe financial and reputational damage. As we move more of our daily activities and the services we consume online, cybercriminals have a growing number of accounts to target and exploit. They utilize creative and evolving tactics like credential stuffing, credential cracking, brute force, dictionary, and others. With the increasing commoditization of cybercriminal tools, such as credential dumps and bot infrastructure, account theft has become more frequent and accessible. Despite expert advice, consumers continue to reuse passwords and often do not change them after breaches have been disclosed, exacerbating the problem. To safeguard their businesses and customers, organizations must prioritize addressing the risks and negative impacts of account takeover and account-based fraud.

Imperva Account Takeover Protection

Imperva Account Takeover Protection empowers organizations to mitigate malicious Account Takeover attacks without affecting legitimate users in the process. Imperva accurately determines if the interactions with a website have the characteristics of an account takeover attempt through a multilayered process that includes reputational analysis, an advanced client classification engine, and proprietary machine learning algorithms developed by Imperva. Most importantly, it 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 DISCOVERY

Mitigate all bot-driven account takeover attacks and other account-based fraud

Minimal false positives, no impact on performance

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

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

Discover accounts at riskof fraudulent activity

Deployed in minutes

INNOVATIVE DETECTION

Built on top of Imperva's multilayered detection approach

Patented user-behavior Anomaly Detection & Site Profile Based Detection

ADVANCED MITIGATION

Mitigate attacks from the first request

Multiple responses options, including BLOCK, TARPIT AND CAPTCHA

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 lets us immediately detect and mitigate all risks at the edge without requiring distant processing centers.

Preserves customer user experience

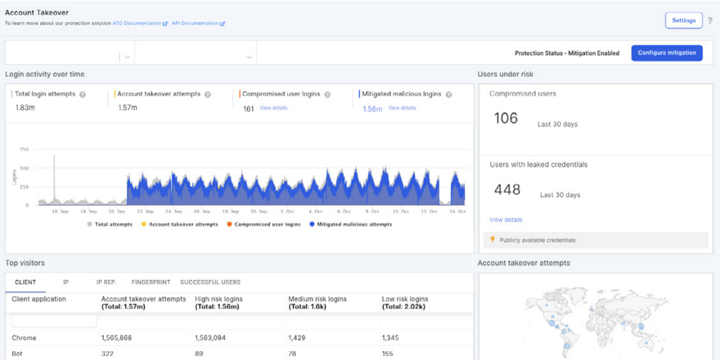
CAPTCHA challenges are commonly used to identify bad bots, but this process generates friction that often frustrates users and leads to reputational damage. Our multilayered detection approach provides laser-focused detection with low false positives, reducing the need to use CAPTCHA challenges and preserving the user experience.

Empowers 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.

Site Profile-Based Detection

In addition to the Imperva multilayered detection process, this patented technology generates a unique profile for each protected website, representing normal and attack traffic patterns. The profile, based on granular details, features, and parameters, allows for the analysis of each login request for anomalies. Any anomalous request is assigned a risk score, determining whether mitigation is necessary based on the site's policy.



Account Takeover

To learn more about our protection solution ATO Documentation API Documentation

Protection Status - Mitigation Enabled

Login activity over time

Total login attempts 1.83m

Account takeover attempts 1.57m

Compromised user logins 161 View details

Mitigated malicious logins 1.56m View details

Users under risk

Compromised users 106 Last 30 days

Users with leaked credentials 448 Last 30 days

View details

Publicly available credentials

Top visitors

Client application	Account takeover attempts (Total: 1.57m)	High risk logins (Total: 1.56m)	Medium risk logins (Total: 1.6k)	Low risk logins (Total: 2.02k)
Chrome	1,565,868	1,563,094	1,429	1,345
Bot	322	89	78	155

Account takeover attempts

IMPERVA APPLICATION SECURITY

Client-side 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)

API Security

Distributed Denial of Service (DDoS) protection

Advanced Bot Protection

Account Tekaover Protection

Runtime Application Self Protection (RASP)

Actionable security insights

Security-enabled application delivery

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

Imperva is the cybersecurity leader that helps organizations protect critical applications, APIs, and data, anywhere, at scale, and with the highest ROI.