AKAMAI PRODUCT BRIEF

Account Protector

Keep fraudsters out — and trust intact — with account abuse protection

How can you tell if a user is genuine or an imposter? Your customers rely on you to distinguish between the two.

As digital transactions and the adoption of new digital assets continue to become more prevalent, the risks and consequences of account abuse are more significant than ever. Your ability to expand your digital business and protect your customers depends on maintaining trust in an environment where fraud tactics are constantly evolving.

Account-related abuse, such as fraudulent account opening (new account fraud) and account takeover (ATO), pose significant challenges and costs for businesses across all industries. Compromised and fake accounts can have severe financial and reputational consequences for organizations. When an account is compromised, attackers can freely exploit it — draining balances, making fraudulent transactions, disabling security features like MFA, or stealing sensitive personal information. Fake accounts, on the other hand, can be used to take advantage of promotions such as free trials and credits, execute SMS pumping, and flood platforms with spam or inappropriate content. The impact of these attacks is significant, and businesses face the risk of customer trust erosion, losing millions to fraud, and grappling with regulatory fines and reputational damage.

Akamai Account Protector

Account Protector is a security solution designed to prevent account abuse across the entire lifecycle of an account, using machine learning and a significant dataset of risk and trust indicators to determine the legitimacy of a user request. It analyzes behavior in real time to identify subtle signs of fraudulent activity from account creation, through login, and beyond. If suspicious or anomalous behavior is detected, Account Protector provides immediate mitigation options to maintain a seamless user experience, such as blocking and taking action at the edge, serving cryptographic and behavioral challenges, serving alternate content, and more.

Benefits for your business

Enhance trust: yours and theirs:
Know which interactions are legitimate, reduce friction for users, and protect them from fraudulent activity.

Develop protections tailored uniquely to your business:
Leverage autotuned bot detections and the ability to understand user population profiles based on how users interact with your site.

Get deep insight and visibility
Confidently take action based on transparent signals and indicators.

Reduce remediation fallout:
Reduce the financial and resource drains of investigating compromised accounts, replacing stolen assets, and more.

Make better data-driven security and identity decisions:
Integrate with fraud tools, SIEM, and other security tools to allow consumption of Account Protector's risk and trust signals to increase accuracy and enhance investment in those tools.

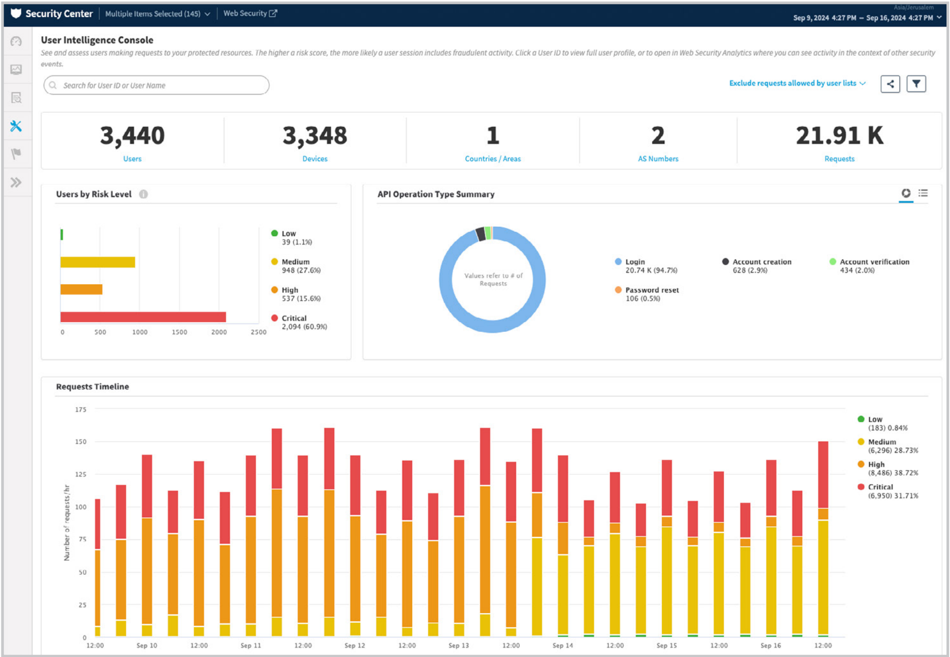
Gain holistic defense against account abuse

Safeguard user accounts against abuse throughout their entire lifecycle — providing advanced protection against account opening abuse, account takeover attacks, and the attack schemes driven by it.

Account opening abuse — Mitigate the creation of fake accounts that are used to take advantage of promotions, carry out SMS pumping, test stolen credit card information, hoard inventory, and more.

Account takeover — Protect against imposters gaining access to legitimate customer accounts to drain them of their value, steal sensitive data, and commit fraudulent transactions.

Sophisticated adversarial bot attacks — Secure user accounts from credential stuffing, inventory manipulation, and other automated attacks often launched in tandem with account opening abuse or ATO to steal valuable products, money, or other valuable assets.



Security Center | Multiple Items Selected (145) | Web Security

Asia/Jerusalem
Sep 9, 2024 4:27 PM – Sep 16, 2024 4:27 PM

User Intelligence Console

See and assess users making requests to your protected resources. The higher a risk score, the more likely a user session includes fraudulent activity. Click a User ID to view full user profile, or to open in Web Security Analytics where you can see activity in the context of other security events.

Search for User ID or User Name

Exclude requests allowed by user lists

3,440	3,348	1	2	21.91 K
Users	Devices	Countries / Areas	AS Numbers	Requests

Users by Risk Level

- Low 39 (1.1%)
- Medium 948 (27.6%)
- High 537 (15.6%)
- Critical 2,094 (60.9%)

API Operation Type Summary

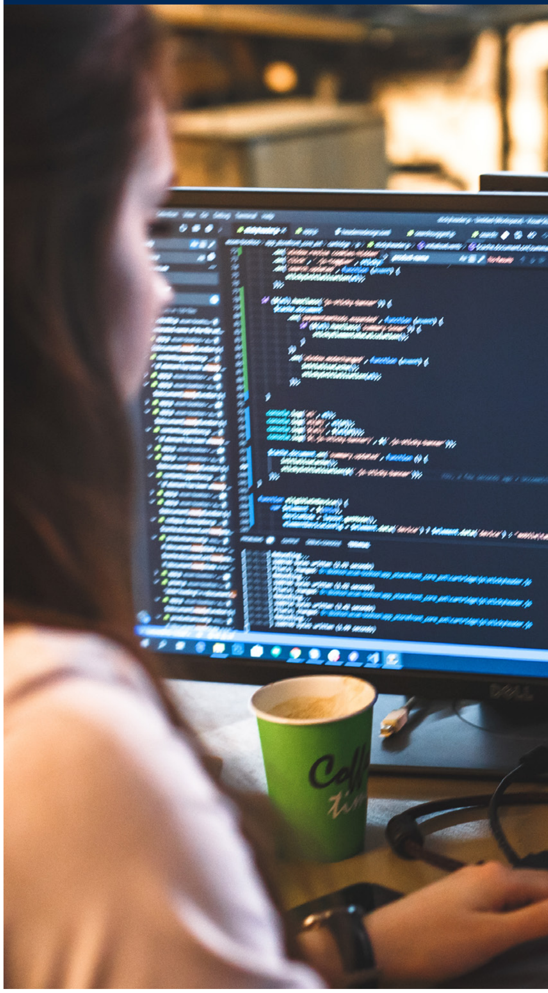
- Login 20.74 K (94.7%)
- Account creation 628 (2.9%)
- Account verification 434 (2.0%)
- Password reset 106 (0.5%)

Requests Timeline

- Low (183) 0.84%
- Medium (6,296) 28.73%
- High (8,486) 38.72%
- Critical (6,950) 31.71%

Protect, trust and user experience

Analyze risk and stop abuse in real time, continuously monitoring accounts throughout their entire lifecycle for signs of suspicious behavior as they happen.



Key capabilities

Comprehensive account lifecycle protection — Identifies and analyzes user risk at any stage, from account creation to post-login activities such as account updates, password changes, and payments.

Real-time user session risk scoring — Evaluates risk and trust throughout the user session to assess whether a user request is coming from a legitimate user or an imposter.

Email address intelligence — Analyzes the syntax of an email address and abnormal use of an email to detect malicious patterns.

Email domain intelligence — Evaluates the activity pattern coming from individual email domains, including disposable domains and excessive use of an email domain.

Global recognition of trusted users — Provides visibility into user behavior across Akamai's network to make more informed decisions regarding the trustworthiness of a login.

User behavioral profiles — Constructs a behavioral user profile based on previously observed locations, networks, devices, IP addresses, and activity time to recognize returning users.

Population profiles — Aggregates the organization's user profiles into a superset, so variances in behavior can also be compared with the entire population of users for anomaly detection.

Source reputation — Evaluates the reputation of the source on the basis of past malicious activity observed across all Akamai customers, including many of the world's largest, most heavily trafficked, and most frequently attacked websites.

Indicators — Feeds the evaluation of each request with risk, trust, and general indicators to assess the risk of account abuse. The indicators are provided together with the final user risk score and can be used for analysis.

Sophisticated bot detections — Detects unknown bots from the first interaction using a variety of AI and machine learning models and techniques. They include user behavior/telemetry analysis, browser fingerprinting, automated browser detection, HTTP anomaly detection, high request rate, and more.

Analytics and reporting — Provides both real-time and historical reporting. Analyze activity on individual endpoints, investigate a specific user, review users by risk level, and gain in-depth insights.

Advanced response actions — Provides a wide range of actions that can be applied to stop abuse, including alert, block, delay, serve cryptographic and behavioral challenge, serve alternate content, and more. In addition, organizations can assign different actions according to the URL, time of day, geolocation, network, or percentage of traffic.

Header injection — Sends user risk information for analysis and real-time mitigation. An additional request header is injected on the forwarded request with information on the user risk score and the risk, trust, and general indicators that contributed to the score for further analysis and real-time mitigation.

Automate with machine learning — Automatically updates the characteristics and behaviors used to identify human fraudulent activity and bots, from behavioral patterns to the latest reputation scores across the Akamai platform.

SIEM integration (optional) — Integrates user risk information into SIEM tools for customers who want more integrated security visibility. You can enrich the value of your existing tools with the insights from Account Protector.

Contact your Akamai representative or visit Akamai.com to learn more.