AKAMAI PRODUCT BRIEF

Account Protector

Is that the account owner or an imposter?
Your customers trust you to know the difference.

Your ability to grow your digital business depends on your ability to build and maintain trust in an environment where trust is rare without adding friction to your customers' experiences. Can you do that with your current systems?

Account-related fraud like account takeover (ATO) presents an expensive and difficult problem for businesses in all industries. The attack appears to be conducted by a human with valid credentials – exactly how the process is intended to work. But as with identical twins who, upon closer inspection, show the small and subtle signs that they're not the same person, there are signs that those credentials are not as valid as they seem. Account Protector evaluates multiple risk and trust signals to find what others might miss and to detect whether the human logging in is the account owner or an imposter.

The risks and fallout of ATO have never been greater as digital business and new digital assets become commonplace.

Digital business is surging. But even as we're all transacting more online, trust in digital experiences has been significantly eroded. People generally trust existing institutions and systems less than ever. Online fraud, disinformation campaigns, deep fakes, and cybersecurity attacks are rampant.

Along with increasing online activity, we've seen a sharp rise in irreplaceable digital assets. There are profitable secondary markets for online assets like gift cards, loyalty points, and airline miles, for example. And there are new valuable digital-only asset classes: cryptocurrencies like Bitcoin, in-game currencies and rare game items, and digital-only artwork, among others. Many of these assets can't be replaced once they're stolen.

Grow your business confidently

If you have significant customer assets at risk, you need to protect your customers and your organization from ATO and related adversarial bot attacks like credential stuffing, inventory manipulation, and others. But you also need to ensure that security doesn't come at the expense of a good online customer experience. We designed Account Protector to detect imposters at the edge, so your customers get through without additional friction. And by reducing ATO and bot-related fraud, you not only protect customers, you reduce the costs and frustrations of fraud. You can unlock explosive digital growth without making trade-offs in terms of cost or protection.

Account Protector provides a comprehensive solution designed to prevent fraudulent human logins and mitigate the sophisticated adversarial bots that often precede ATO attempts. The solution utilizes techniques for understanding the behavior of legitimate account owners, then assesses the risk of each authentication request based on anomalies from the typical behavior profile and devices, as well as other advanced detections.

BENEFITS FOR YOUR BUSINESS

Enhance Trust: Yours and Theirs
Know which interactions are legitimate, reduce friction for users, and protect them from fraudulent activity to fuel trust among consumers, partners, and the organization itself.

Develop Protections Tailored Uniquely to Your Business
Auto-tuning bot detections and the ability to understand user population profiles based on how users interact with your site allow for more customized anomaly detections and protection.

Get Deep Insight and Visibility
Security and fraud teams can confidently take action based on transparent signals and indicators, instead of relying on black box yes/no kinds of analysis.

Reduce Remediation Fallout
Reduce the financial and resource drains of investigating compromised accounts, replacing stolen assets, resetting existing accounts for affected customers, reporting to regulatory and legal authorities when necessary, and addressing user complaints.

Make Better Data-Driven Security and Identity Decisions
Integrate with fraud, SIEM, and other security tools to allow consumption of Account Protector's risk and trust signals to increase the accuracy and enhance your investment in those tools. If you choose to integrate with your user authentication workflow, you can also make more creative and strategic choices about execution, such as when to issue step-up authentication.

Akamai

You can then apply the appropriate response to each request – including taking action at the edge – in real time without affecting the experience of real account owners. You can also use Account Protector's reporting and analytics independently or in conjunction with your existing fraud and analytics tools for more detailed insights.

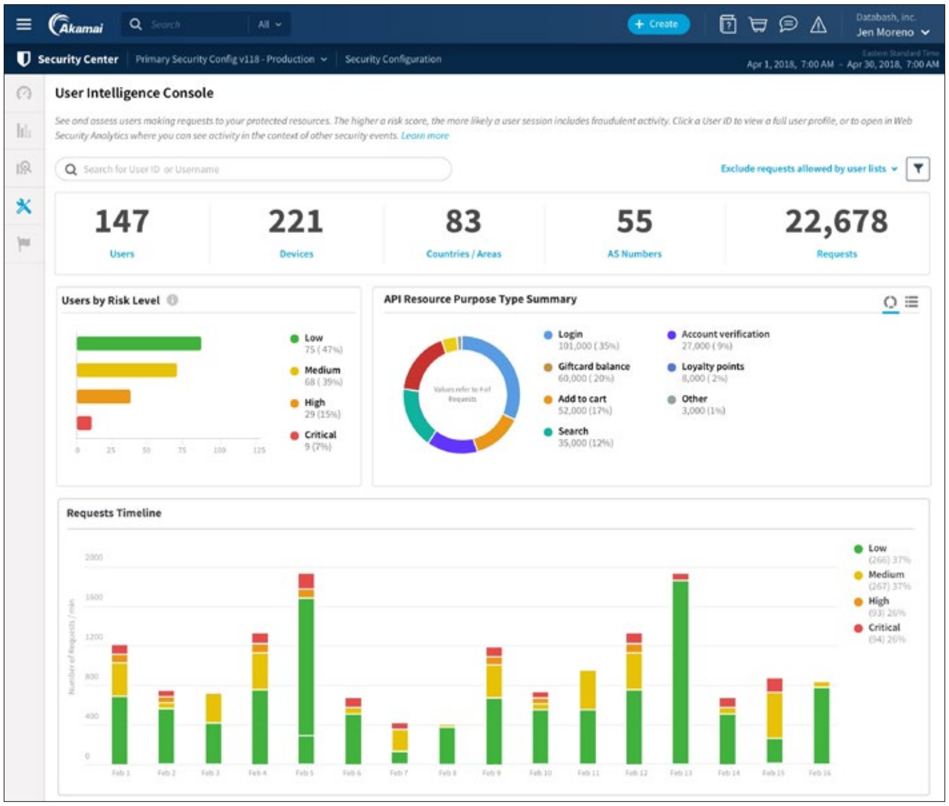
Account Protector enables you to trust the validity of user logins without adding extra friction. That trust, plus a seamless customer experience without unnecessary extra authentication steps, will turn into more sales and higher customer lifetime value.

Disrupt account takeover and adversarial bot attacks

Account Protector uses behavioral detections to profile the activity patterns of account owners, device anomalies, and source reputation. As customer login requests are received, Account Protector assesses in real time the risk that the request does not belong to the legitimate account owner by detecting anomalies compared with the typical user behaviors. The behavior profiles can include device(s) typically used, IP addresses, networks, locations, and frequency and time of logins, among others. And it works even the first time a customer logs in because it can detect anomalies in the first login from the behavior of your entire customer population.

Account Protector also protects you from sophisticated bots that are targeting your organization in automated, large-scale attacks. It detects and mitigates harmful bots using AI and machine learning models and techniques, including user behavior/telemetry analysis, browser fingerprinting, automated browser detection, HTTP anomaly detection, high request rate, and more.

The benefits of Account Protector extend beyond the immediate disruption of ATO attempts. Account Protector provides a rich source of behavior and risk information that you can feed into your existing fraud engines for further analysis and mitigation, increasing the value and effectiveness of your existing investments.



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 a full user profile, or to open in Web Security Analytics where you can see activity in the context of other security events. Learn more

147	221	83	55	22,678
Users	Devices	Countries / Areas	AS Numbers	Requests

Users by Risk Level

Risk level	Users
Low	75 (47%)
Medium	68 (39%)
High	29 (15%)
Critical	9 (7%)

API Resource Purpose Type Summary

Purpose	Requests
Login	101,000 (35%)
Giftcard balance	60,000 (20%)
Add to cart	52,000 (17%)
Search	35,000 (12%)
Account verification	27,000 (9%)
Loyalty points	8,000 (2%)
Other	3,000 (1%)

Values refer to # of Requests

Requests Timeline

Risk level	Requests
Low	(266) 37%
Medium	(267) 37%
High	(93) 26%
Critical	(94) 26%

How It Works

User Profiles

Detect imposters based on anomalies in indicators like an individual's profile of previous devices, locations, network, and activity time observed.

Population Profiles

Detect anomalies from first login based on the behavior profile of the entire user population.

Sophisticated Bot Detections

Catch and mitigate adversarial bots even on the first interaction using unsupervised and supervised algorithms.

Reputation Data

Evaluate the reputation of the source based on past malicious activity observed across all Akamai customers.

Real-Time Risk Scoring

Analyze and score user session risk by evaluating anomalies in user behavior, devices, network/IP reputations, and other advanced detections.

Tuning That's Unique to Your Organization

Evaluate requests using machine learning that is constantly tuning according to your organization's individual traffic and user behavior patterns.

Enrichment

Use Account Protector insights with fraud investigation and SIEM tools for a deeper, more sophisticated understanding of attacks, attackers, and risks.

Key capabilities

Real-time user session risk scoring – Evaluates risk and trust signals during authentication, such as user behavioral anomalies, device anomalies, and the reputation of the user's IP address and network to assess the risk that a user request isn't coming from the legitimate account user.

User behavioral profiles – Constructs a behavioral user profile based on previously observed locations, networks, devices, and activity time.

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

Source reputation – Evaluates the reputation of the source based on 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 that the person logging in is not the legitimate account owner. The indicators are provided together with the final user risk score and can be used for analysis or sent to the origin.

Known-bot directories – Automatically responds appropriately to known bots, and we continuously update our current directory of 1,500 known bots.

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 other insights. Account Protector analytics give you high-level statistics and a detailed analysis that can be imported into your fraud and security information and event management (SIEM) tools for better understanding of intent and for strategic planning, increasing the value of your existing security investments.

Advanced response actions – Provides a wide range of actions that can be applied to stop ATO and credential stuffing attacks, including alert, block, delay, serve alternate content, serve CAPTCHA, proof of work, and more. In addition, organizations can assign different actions based on the URL or time of day, or by percentage of traffic.

Header injection – Sends signals to indicate human fraudulent activity. It injects an additional request header 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.

Protect Trust

Recognize an account takeover attempt as it's happening so you can stop it in real time and protect your users' experience and trust.

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

| Support | | Published 09/21