2025 E-commerce Industry Security White Paper

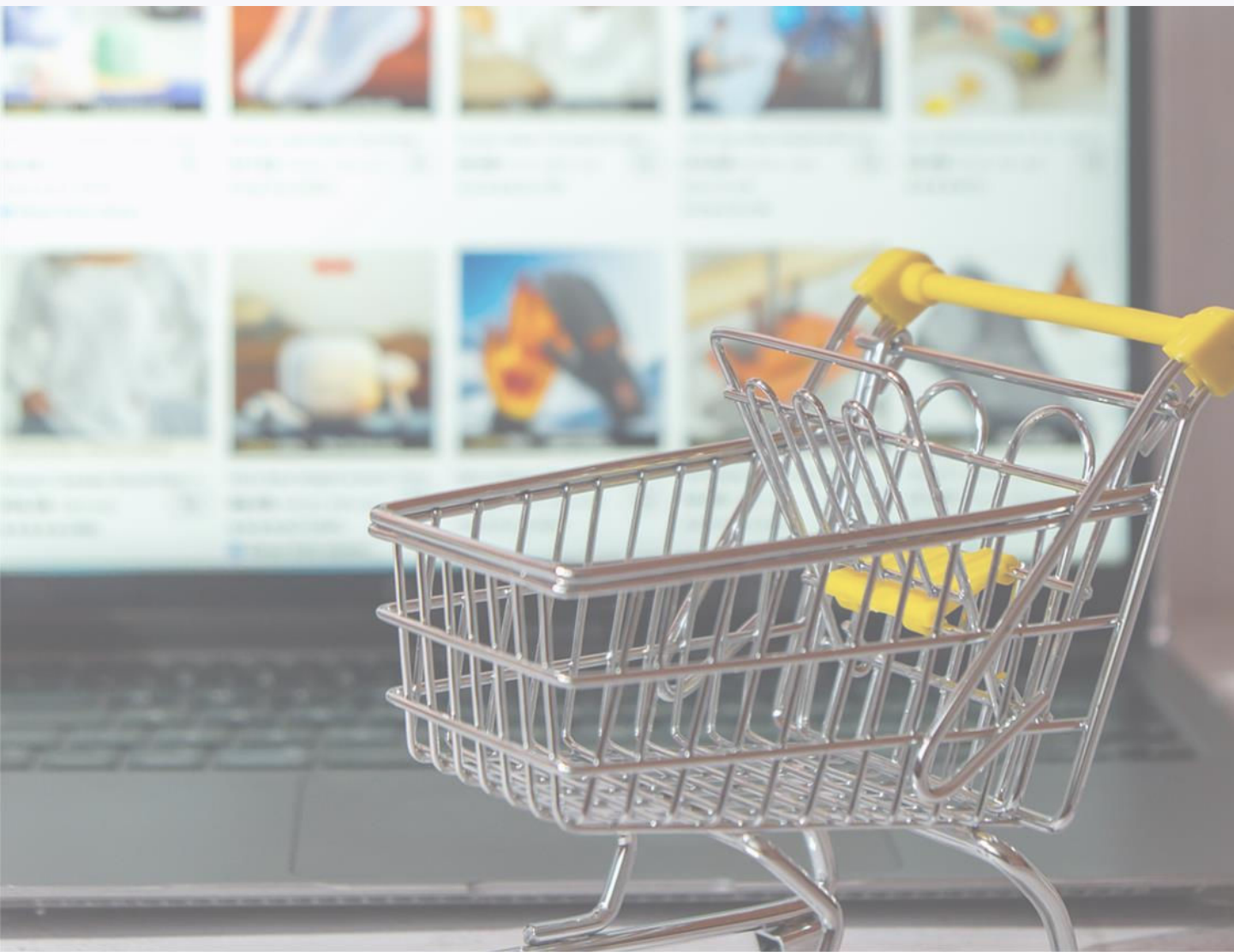
WUHAN JIYI NETWORK TECHNOLOGY CO., LTD

Published in July 2025

Introduction

This white paper provides a thorough analysis of the security challenges facing the e-commerce industry. It presents GeeTest's comprehensive, scenario-based security solutions and real-world applications, while exploring technology-driven trends that are shaping the future of e-commerce security. The insights offered aim to support informed decision-making and promote sustainable growth across the industry.

We hope this report serves as a valuable resource for your strategic planning.



Preface

With the rapid rise of the digital economy, e-commerce has become a key engine of global growth. However, security threats are escalating just as quickly. In 2024, over 65% of platforms faced large-scale bot-driven registration attacks, and 47% of promotional resources were hijacked during sales events. Transaction fraud losses rose by 18% year over year, posing serious risks to both platform operations and user trust.

As a leader in business security, GeeTest leverages 13 years of experience to deliver full-chain protection across scenarios like registration, login, transactions, and promotions. Powered by behavioral verification, device fingerprinting, and risk-based business rules decision engine, GeeTest supports 360,000+ enterprises with over 1 billion daily interactions, safeguarding e-commerce operations at scale.

Abstract

E-commerce Growth

E-commerce is driving global growth but is increasingly exposed to complex security threats.

Key Pain Points

Risk analysis in key scenarios includes scalping bots, payment fraud, and limitations of traditional verification methods.

Full-Path Solution

GeeTest secures every step—registration, login, transactions, coupons, and rewards—while ensuring compliance and user experience.

Case Study

Successful deployments on major e-commerce platforms show how GeeTest enables both security and growth in global markets.

Future Outlook

Future trends include AI-driven security, privacy protection and GeeTest's strategic focus on ecosystem and SECaaS partnerships.

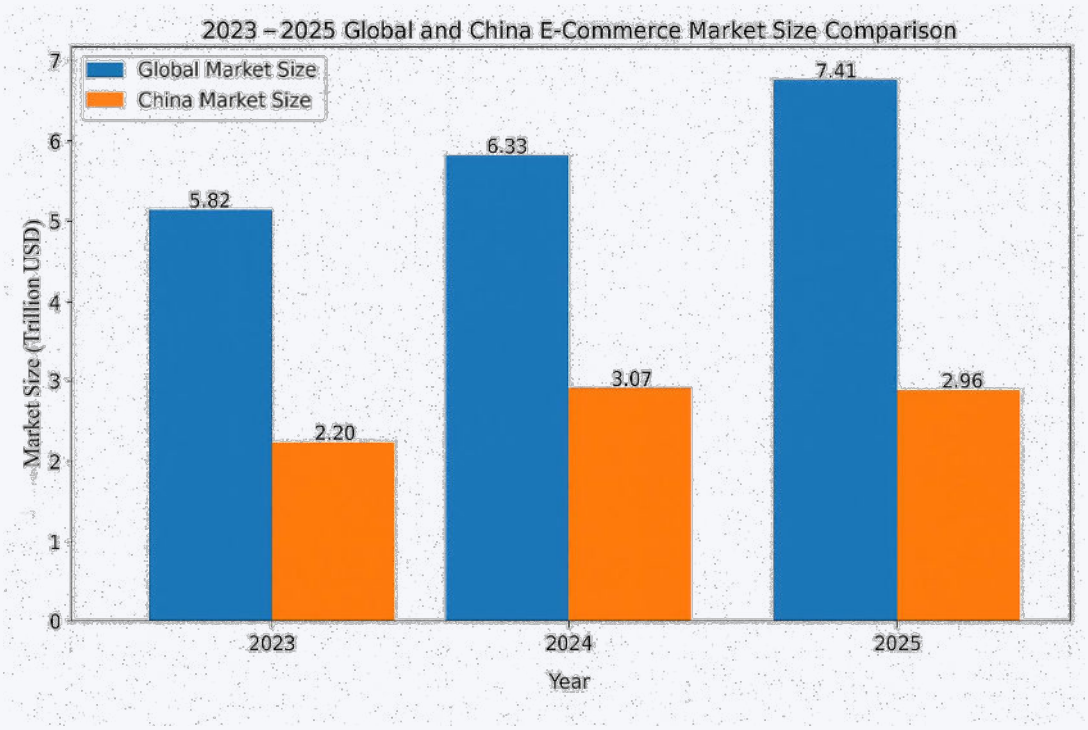
Table of Contents

1. E-commerce Landscape and Threats

1.1 The Growth of Global E-commerce

According to Statista, the global e-commerce market reached USD$ 4.117 trillion in 2024, representing a 15 percent year-over-year increase. Asia played a pivotal role in driving this growth, with China at the forefront, contributing USD$ 1.469 trillion in retail e-commerce sales and accounting for 35.7% of the global total.

In parallel, China's cross-border e-commerce sector continued its robust expansion, with total trade volume reaching approximately USD$ 370 billion, reflecting a 10.8% increase compared to the previous year. Supported by strong consumer demand and favorable government policies, China's online retail sales reached USD$ 507 billion in the first quarter of 2025, further consolidating the country's position as a global leader in the e-commerce landscape.



*Source: GeeTest internal data, 2025.

2025 Market Flashpoint: In April 2025, the U.S. administration implemented a 125% tariff increase on imported goods from China, triggering significant volatility across global markets. Despite this, cross-border e-commerce platforms originating from China saw a sharp surge in international adoption. By mid-April, Chinese platforms dominated the U.S. App Store's e-commerce rankings, with DHgate taking the No.1 spot, followed closely by Taobao and SHEIN. Other Chinese e-commerce apps similarly saw record-breaking downloads and engagement.

This trend coincided with a viral surge in related discussions on platforms like TikTok, where interest in “Chinese e-commerce” topics fueled a 940% spike in daily app downloads. The phenomenon underscores the growing global competitiveness of decentralized supply chains and highlights the resilience of tech-enabled cross-border commerce in times of geopolitical and economic uncertainty.

Trend Insight: Cross-border e-commerce is shifting from price-driven to tech, supply chain, and security–driven competitiveness, with security emerging as a key entry threshold.

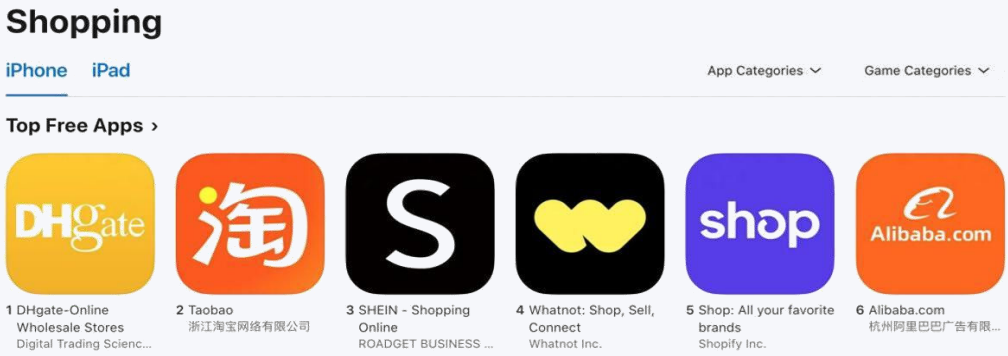


*Image source: From the public internet, 2025

1.2 Evolving Threats in E-commerce Security

In the current complex and dynamic environment, the e-commerce industry faces multifaceted challenges, categorized into three core threat dimensions:

1. AI-Driven Attacks:

- Deepfake fraud has surged by 3000%, with 38% of reviews now AI-generated.
- Scalping scripts iterate in just 4 hours, down from 72 hours.

2. Industrialized Data Breaches:

- User data on the black market has dropped a lot, cutting attack costs by 70%.
- 56% of breaches result from internal leaks, mainly due to low employee security awareness.

3. Tightening Regulatory Pressure:

- The EU's DSA has issued fines up to €230 millon in a single case.
- China's Data Security Law mandates security assessments for cross-border data transfers.

Threat Type	Manifestation	Impact	GeeTest Capabilities
AI-Driven Attacks	Deepfake reviews, automated scalper bots	3,000% fraud increase	Behavior Verification 4.0
Industrialized Breaches	56% insider leaks, falling black market data prices	Hundreds of millions in losses	Device Fingerprinting
Regulatory Compliance	€230M GDPR fine, CCPA restrictions	76% of enterprises at risk of fines	Global Compliance Framework & Multi-language Support

**Source: GeeTest internal data, 2025.

2. Security Challenges in E-commerce Industry

2.1 Account Security Risk

Fraudulent groups use automated tools and massive fake identities to conduct bulk account registrations, posing significant security risks to e-commerce platforms. According to 2023 police data, a crime syndicate used software like “Booster Assistant” to provide fake order services for nearly 3,000 merchants, generating over 11 million fake orders and 21 million fake reviews and likes. These fake accounts are widely used for malicious activities like fake orders, reviews, and reward exploitation, severely disrupting platform operations. Statistics show fake orders can inflate product sales by over 50% and fake positive reviews by 80%, misleading consumer decisions.

Meanwhile, credential-stuffing attacks are surging. Cybercriminals use stolen user credentials from other platforms to attempt logins on e-commerce sites. In 2024, police reported an app faced 13 million such attacks, successfully compromising over 300,000 accounts, causing millions in user financial losses and 10%-15% user churn for the platform.

2.2 Malicious Scalping Risk

Promotional events on e-commerce platforms are frequent targets of bot-driven scalping attacks. Fraudsters deploy automated scripts to instantly grab coupons, flash sale items, and limited-stock products the moment an event begins. These scripts are capable of submitting thousands of orders in mere seconds, far beyond the speed of any human user.

Data from major sales campaigns indicates that bot-generated orders can account for 30%–40% of total transactions, significantly reducing the chances for genuine consumers to place successful orders. In one high-profile case, over 80% of discounted items were purchased by bots within the first five seconds of a flash sale. Legitimate users were left refreshing pages in vain, leading to thousands of customer complaints and a marked decline in platform trust and future campaign participation.

Malicious scalping not only distorts sales performance but also damages brand reputation and undermines consumer loyalty, making it a critical threat to address in today's e-commerce ecosystem.

2.3 Transaction and Payment Risk

As the core of e-commerce operations, the payment process remains a primary target for fraud. One common tactic is phishing, where attackers distribute fake links impersonating legitimate platforms to trick users into entering sensitive payment information (passwords and card numbers), resulting in unauthorized transactions and financial loss. Beyond direct user impact, such incidents erode trust and damage platform credibility.

Payment fraud also manifests through account takeovers and card data theft. Domestically, attackers often exploit stolen payment credentials to perform unauthorized purchases. In cross-border scenarios, fraudsters may acquire credit card details (e.g., card numbers, CVVs) and exploit weaknesses in international payment systems to conduct card-not-present (CNP) fraud. These cases are often harder to trace, complicating accountability and dispute resolution.

Securing payment transactions remains a complex challenge due to diverse payment channels, dynamic environments, and the need for real-time processing.

2.4 Product Information Risk

Fraudulent groups employ web scraping to extract vast amounts of product data from e-commerce platforms, including prices, inventory, and reviews. A 2024 report by the International Cybercrime Prevention Organization revealed that active crawlers can harvest millions of product records daily. This data is exploited to analyze competitors' strategies, conduct price comparisons, and perform market research, significantly harming platforms and merchants.

For instance, competitors use scraped pricing data to engage in predatory pricing, reducing affected product prices by 15%-20%, disrupting market stability. Unscrupulous merchants analyze user reviews to generate fake positive feedback, with fake review rates exceeding 70%, misleading consumers. Such data breaches erode user trust, decreasing platform loyalty by 10%-15% and weakening market competitiveness.

2.5 Fraudulent Manipulation Risk

Some unethical merchants manipulate store rankings and product sales by generating fake orders and reviews. They employ organized "brushers" or automated bots to create fraudulent transaction records and positive feedback. A 2023 study revealed that 30%-40% of merchants in popular categories engage in such practices, inflating sales by several times and achieving fake review rates up to 90%.

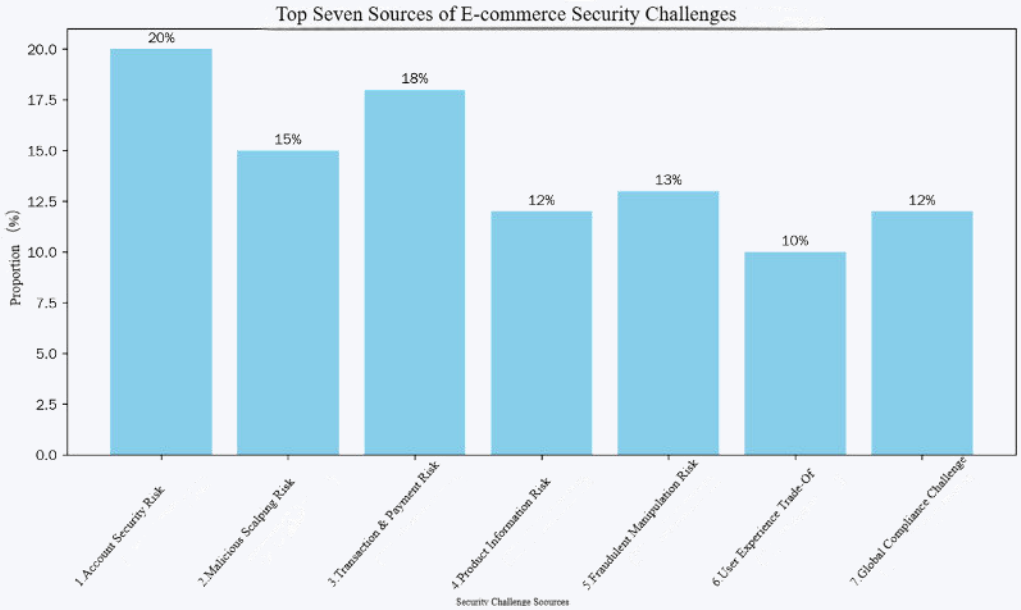
This deception misleads consumers, obscuring authentic product information and skewing purchasing decisions. It also undermines platform credibility and fair competition. Over time, such fraudulent practices reduce user satisfaction by 20%-30% and loyalty by 15%-20%, significantly impeding the healthy development of the e-commerce industry.

2.6 User Experience Trade-Off

Traditional verification methods, such as SMS codes and image-based CAPTCHAs, enhance security but compromise user experience. A 2024 industry report indicates SMS verification takes an average of 15 seconds, while image CAPTCHAs have a completion rate of only 68%, with complex processes causing 23% of users to abandon registration or payment. Testing by a cross-border e-commerce platform shows that each additional second of verification time reduces mobile conversion rates by 8% and desktop rates by 5%, with order abandonment rates reaching 17% during promotional periods due to verification delays.

2.7 Global Compliance Challenge

As e-commerce globalization accelerates, stringent data privacy regulations, such as the EU's GDPR and the US's CCPA, impose higher standards for user verification. According to the 2024 TrustArc compliance report, 76% of cross-border e-commerce platforms face fines for non-compliant data handling, with penalties reaching up to 4% of global annual revenue per violation.



*Source: GeeTest internal data, 2025.

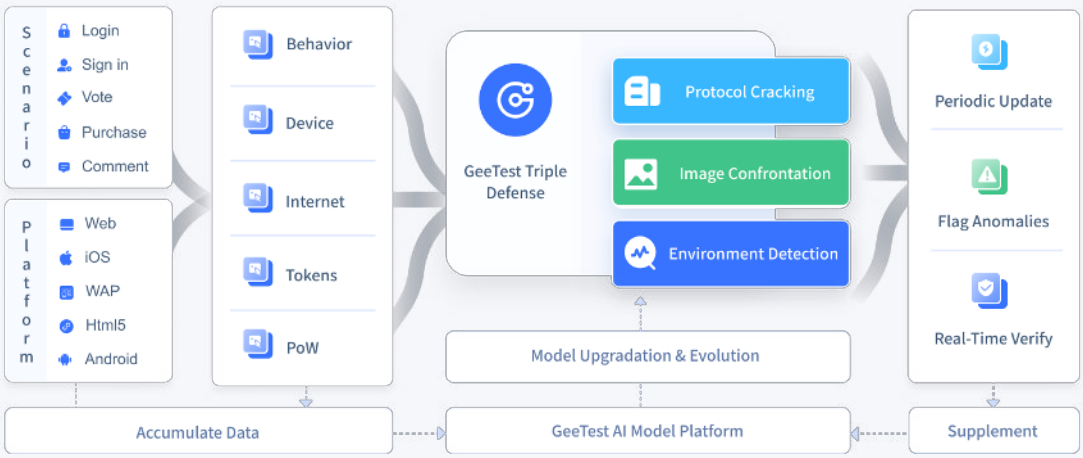
3. GeeTest E-commerce Security Solutions

GeeTest, with **13 years** in internet business security, serves diverse industries, with e-commerce comprising **20%** of its client base.

By April 2025, GeeTest powered over **66% of top U.S. App Store e-commerce apps**, achieving a 99%+ transaction success rate amid global trade challenges. One major platform using GeeTest thwarted over 1M daily malicious attacks, supporting seamless transactions for 3,000 overseas buyers. Another saw a 483% month-on-month download increase, with over 320,000 daily overseas user registrations. These results underscore GeeTest's critical role in enhancing e-commerce resilience and growth.

GeeTest's Triple Defense Against Fraud

To meet evolving security needs and combat common fraud tactics, GeeTest has developed a "Triple Defense" CAPTCHA strategy. It strengthens image resistance, protocol reverse engineering detection, and environment fingerprinting. This solution enables rapid deployment and helps reduce automated attack risks across gateways, SMS, and API scenarios, providing multi-layered protection for business operations.



3.1 Account Protection: Building a Secure Fortress

GeeTest leverages user behavior and environmental data to build an AI-powered bot detection model. It analyzes over 200 data points, including mouse movement (sampled at 100Hz), click pressure (±5% accuracy), and device fingerprinting. The system monitors registration and login requests in real time and triggers adaptive verification when traffic from a single IP exceeds 50 requests per minute or behavioral similarity drops below 60%. The slide CAPTCHA maintains a 98.7% pass rate, while click verification keeps false positives below 0.3%.

This solution increases fake registration blocking to 92% and achieves 99.8% accuracy in detecting unauthorized logins. One major e-commerce platform reduced account takeover attacks from 1.2% to 0.15% using GeeTest.

Frictionless verification achieves an 85% silent pass rate. As a result, registration time is reduced by 40% and login conversion improves by 35%, effectively balancing security and user experience.

Technical Dimension	Traditional Solution	GeeTest Solution	Improvement Effect
Malicious Order Blocking Rate	68%	99.3%	46% increase
False Positive Rate	2%-5%	Below 0.1%	95% Reduction

*Source: GeeTest internal data, 2025.

3.2 Malicious Scalping Mitigation: Building a Dynamic Defense

GeeTest's dynamic defense architecture protects the full transaction chain, including front-end validation, traffic scrubbing, and business-level failover. Key components include:

1. Front-End Interaction Layer: Utilizes 12 CAPTCHA variants (e.g., slide puzzle, sequential click) to reduce automated script pass rates from 75% to 12%;

2. Device Fingerprint Layer: Generates unique fingerprints with 180+ features (hardware ID, network environment), triggering risk alerts for devices reused more than 3 times;

3. Behavior Analysis Layer: Leverages over 80 billion historical scalping behavior samples to compute user actions in real time, identifying abnormal scalping with <200ms latency;

4. Traffic Risk Control Layer: Processes over 1 billion daily requests with an abnormal traffic filtering rate of 95%. One platform blocked 3.2 million malicious orders during a major sales event;

5. Business Failover Layer: Automatically activates when over 30% of traffic is flagged as abnormal. Redirects traffic within 5 seconds to ensure 99.99% service availability.

Deployment results show a rise in real-user participation during promotions from 58% to 83%, and a drop in scalper-driven orders from 42% to 9%. For a cross-border e-commerce platform's Black Friday event, GeeTest drove a 27% GMV increase while cutting promotional costs by 40%.

3.3 Payment Protection: Safeguarding Transactions

GeeTest's payment protection solution combines a three-layer defense system:

1. Biometric Behavior Verification: Utilizes AI to analyze 15 biometric features, such as finger swipe acceleration (±0.5m/s² error) and screen contact area (±2mm resolution), achieving a 99.92% human-machine identification accuracy;

2. Device Fingerprint System: Generates unique identifiers with 200+ dimensions, including sensor data and app environment, with a 98% detection rate for device anomalies, reducing payment fraud losses by 78% for a banking client;

3. Real-Time Risk Decision: A risk engine evaluates over 80 indicators, including IP address, device location, and transaction history. Response time is under 50 ms, with over 95% accuracy in blocking fraudulent transactions.

The data shows GeeTest's solution reduces user drop-off rates during payment processes from 12% to 3.5% and boosts payment success rates from 85% to 97.3%. In 2024, it intercepted 1.76 million phishing link attacks, contributing to a 70% year-on-year decline in payment fraud losses.

3.4 Data Protection: Securing E-commerce Data Assets

GeeTest's anti-scraping system builds a robust data protection framework through dual-layer validation combining behavioral patterns and device fingerprints:

1.Crawler Behavior Detection： Monitors 30+ behavioral metrics, such as request frequency (>200/min triggers alerts) and page depth (>5,000 pages/day per IP flagged as abnormal), achieving 99.1% malicious crawler identification accuracy；

2.Device Environment Validation: Uses device fingerprinting across 150+ parameters, including browser configuration and plugin data, to identify emulators and tampered devices. In 2024, the system blocked 21.7 billion automated crawler attempts；

3.Dynamic Path Disruption: Applies real-time content obfuscation with over 100,000 layout variations generated daily and 5 CAPTCHA variants updated every minute. This reduces crawler script effectiveness duration from 4 hours to 15 minutes.

After implementation by a cross-border e-commerce platform, product scraping volume dropped by 89%, competitor price tracking costs decreased by 60%, and user data breach incidents fell by 85%. The solution is certified under ISO/IEC 27001 for information security management.

3.5 Fraud Prevention: Protecting a Fair Competitive Environment

GeeTest's seamless probe system analyzes over 300 behavioral indicators in real time to detect fraudulent activities:

1. Order Fraud Detection Model: Flags suspicious patterns such as bulk order creation within 30 seconds, repeated shipping addresses (>5 triggers alerts), and shared payment accounts across multiple recipients (over 10). The detection accuracy for fraudulent orders reaches 96%;

2. Fake Review Filtering: Uses NLP to identify repeated keywords (>40%), abnormal posting frequency (20+ reviews per day), and behavioral anomalies (10+ reviews from newly registered users). The false review blocking rate reaches 88%;

3. Smart Enforcement Framework: Implements tiered penalty strategies such as warnings, visibility reduction, and account suspension. After deployment, one e-commerce platform reduced the rate of seller fraud from 28% to 5.7%, and user trust in product reviews increased by 35%.

In 2024, GeeTest helped eliminate 1.2 million malicious accounts and 31 million fake orders. Search accuracy improved by 22%, and top merchants saw an 18% increase in traffic conversion.

3.6 Intelligent Verification: Balancing Security and User Experience

GeeTest found that traditional verification causes user loss due to three key points:

1. Cumbersome Operations: SMS verification requires waiting for receipt, while image CAPTCHAs suffer from unclear characters and network delays, with users averaging 2 or 3 attempts to pass;

2. Security Risks: In 2024, 18% of users experienced SMS code interception via sniffing attacks, and 29% encountered phishing pages that mimicked legitimate verification interfaces;

3. Compatibility Challenges: Elderly users achieve less than 50% recognition rates for image CAPTCHAs, and users face a 35% SMS delivery failure rate due to carrier restrictions.

GeeTest's behavioral verification methods, including slider CAPTCHA and invisible verification, reduce average verification time to 1.4 seconds and raise completion rates to 99%. One leading e-commerce platform improved registration conversion from 15% to 42% and increased payment success by 27% after adopting the solution.

Impact of GeeTest on Another Cross-Border E-commerce Platform

Metric	Before	1 Month	3 Months	Improvement
Daily Fake Registrations	50,000	12,000	4000	92% Decrease
Payment Success Rate	82%	89%	96%	14% Increase
Data Leakage Incidents	37% of product data	0	0	Eliminated

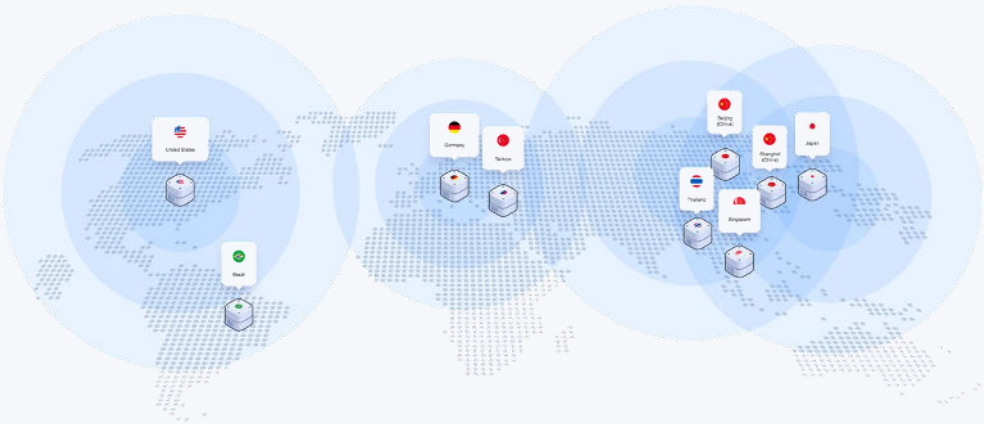
*Source: GeeTest internal data, 2025.

3.7 Global Compliance: Building Cross-Regional Risk Control

To address data compliance and regional risk challenges in cross-border e-commerce, GeeTest has developed a globally adaptive risk control and data governance framework. This solution empowers enterprises to respond quickly and manage risks effectively across diverse markets.

1. Global Multi-Cluster Deployment: GeeTest has established 7 service nodes worldwide to ensure that CAPTCHA requests from end users are processed by the nearest data center. This significantly reduces response time and enhances system stability.

GeeTest Global Service Node Distribution Map



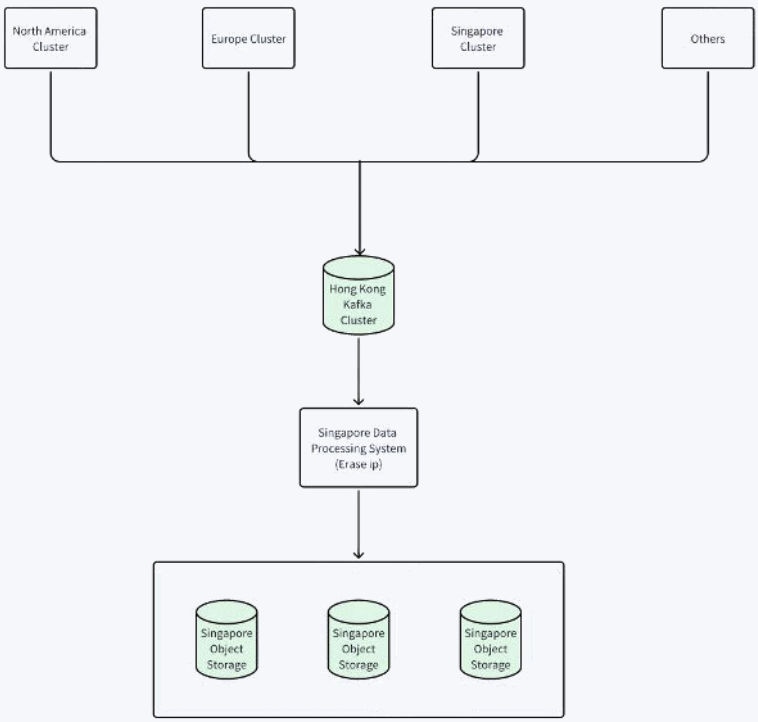
2. Customized Language Adaptation: GeeTest optimizes user experience across diverse linguistic and cultural contexts, such as Arabic and Spanish. The CAPTCHA solution supports 78 languages, ensuring intuitive, accessible interactions for users worldwide.

3. Localized Storage and Processing: GeeTest's architecture supports regional compliance with CCPA and GDPR, holding certifications including ISO/IEC 27001, ISO/IEC 27701, and China's MLPS. It supports multilingual privacy policies and data anonymization, with localized servers in the EU and North America to ensure data security and regulatory alignment.

View GeeTest's Privacy Policy: https://www.geetest.com/en/Service

4. Isolated Data Services for International Markets: To meet strict cross-border data requirements, GeeTest operates dedicated data centers in Singapore to isolate user behavior data from domestic systems. This includes physically separated database clusters, role-based access limited to regional compliance teams, and a cross-border transmission whitelist mechanism. These measures ensure no data return or co-storage, effectively mitigating cross-border compliance risks.

GeeTest Data Isolation Flow Chart



4. Case Study

GeeTest Empowers a Leading Cross-Border E-Commerce Platform for Security and Growth:

A top-tier cross-border e-commerce platform, expanding rapidly across more than 200 countries and regions, faced significant security challenges during rapid global expansion:

- **Massive Fake Account Registrations:** Over 50,000 fake account registrations occurred daily, with approximately 30% used for coupon abuse and subsidy fraud.
- **Data Breaches:** Automated scraping led to the leakage of 37% of product pricing data, enabling competitors to undercut promotions in real time.
- **Promotional Fraud:** During peak sales, 45% of orders came from scalpers. For instance, a French consumer reported that a limited-edition sneaker sale was exhausted in 0.3 seconds, with 90% of the inventory snapped up by scalping scripts and resold at inflated prices via unauthorized distribution channels. Such incidents triggered over 5,000 complaints per day during promotions, leading to erosion of customer trust.
- **Operational Inefficiencies:** A professional fraud team exploited 10,000 fake accounts to siphon $500,000 in new-user subsidies within three hours, depriving genuine users of benefits. Manual verification of suspicious accounts consumed significant resources, further reducing operational efficiency.

Security Vulnerability created a growth-risk cycle, where rapid expansion amplified exposure to fraud and data breaches.

4.1 Solution & Technical Implementation

GeeTest tailored a comprehensive security protection system for the platform, integrating Behavior Verification 4.0 across critical touchpoints: registration, login, and checkout. The system analyzes over 200 behavioral indicators, such as mouse trajectory, device environment, and click frequency, to detect anomalies in real time. By combining seamless validation with dynamic challenges, it creates an intelligent risk control model that enhances security while maintaining a smooth user experience.

Core Capability	Application Scenario	Defense Mechanism
Behavior Verification 4.0	Blocking Fake Registrations	Real-time identification via 200+ indicators, blocking malicious requests in 0.2 seconds.
7-layer dynamic protection	Countering Scalping Scripts	During Black Friday, the AI model detected new variant scripts, achieving a 99.3% interception rate.
Global Compliance Framework	EU User Data Protection	Deployed local servers in Frankfurt with data anonymization to meet Article 44 of the GDPR

*Source: GeeTest internal data, 2025.

4.2. Enhanced Security Capabilities

GeeTest provides a visual risk logging system with over 30 query dimensions, including verification ID, IP address, and device fingerprint. It achieves 99.2% accuracy in detecting abnormal behavior with a false positive rate below 0.1%. A domain-based allowlist mechanism is also implemented to block unauthorized CAPTCHA requests, boosting bot detection rates from 68% to 94% and reducing product data scraping by 85%.

According to the platform's business lead, during last year's Black Friday peak hours (from midnight to 2 a.m.), the proportion of abnormal requests dropped sharply from 18% to just 2%. The team no longer needed to remain vigilant, manually blocking suspicious traffic. Instead, the the visual dashboard clearly showed that malicious traffic was accurately intercepted, reducing backend workload by over 70%.

4.3 Optimizing Global User Experience

GeeTest's hybrid of slider and invisible CAPTCHA reduced verification time from 8 to 1.2 seconds, boosting mobile registration conversions by 27% and eliminating internal trade-offs between security and user experience.

Deployment of localized nodes in seven regions reduced network latency 60% and ensured 99.99% availability by processing requests locally. Consequently, timeout complaints were prevented even during promotional traffic peaks.

The system supports 78 languages, with customized prompts in 15 key languages. This localization reduced user confusion during verification by 90% across international markets.

GeeTest Serving Over 25 Countries Worldwide

4.4 Implementation Results

After deploying the solution, the platform saw a 92% reduction in fake registrations and a decrease in malicious scalping orders from 45% to 7%, with genuine user reach during promotions rising to 88%. Meanwhile, price data leaks were completely prevented, significantly enhancing data security. These improvements supported 35% annual GMV growth, positioning the platform as a benchmark for secure, user-friendly, and scalable cross-border e-commerce.

The review team's workload was significantly reduced cause they no longer had to manually monitor and filter fraudulent accounts daily. This allowed them to shift focus toward optimizing the login process, ensuring genuine users a better shopping experience. During major sales events, complaints regarding fake promotions and system errors dropped sharply. Order success rates improved notably, and consumers who previously struggled with bot interference were now able to purchase their desired items with ease.

Core Capability	Application Scenario	Implementation Outcome
7-layer dynamic Defense System	Blocking Scalper Purchases	Malicious order rate reduced to 7%
Invisible Probe System	Combating Fake Orders & Reviews	88% fake review interception rate
Global Compliance Framework	EU User Data Governance	67% reduction in GDPR compliance audit costs

*Source: GeeTest internal data, 2025.

Comparison of Implementation Outcomes by Stage

Metric	Before Deployment	1 Month After	3 Month After
Daily Fake Registrations	50000	12000	4000
User Payment Success Rate	82%	89%	96%

*Source: GeeTest internal data, 2025.

5. Future Outlook

5.1 Driving the Future with Technological Innovation

1. AI-Powered Security Systems Take the Lead

Traditional static verification is rapidly evolving toward intelligent systems with continuous risk monitoring and dynamic strategy adjustments. GeeTest data shows that in 2025, 68% of e-commerce platform attacks involve AI-driven threats, such as intelligent credential stuffing and adversarial crawlers, necessitating a shift from point-in-time interception to end-to-end behavioral analysis.

2. Privacy Protection Reshapes Security and Experience Balance

As privacy regulations take effect in 32 countries and regions, including the GDPR and CCPA, protecting personal data has become central to balancing security with user experience. Privacy-first risk assessment enables effective threat detection without exposing original data. This approach builds user trust while reducing the data requirements, improving both speed and success rates.

3. GeeTest's Compliance-Focused Data Governance

GeeTest complies with the GDPR and the Schrems II ruling by the European Court of Justice. For users in the EU and EEA, GeeTest implements a strict data localization policy. Regional data centers in countries such as Singapore and Germany ensure that all behavioral data is stored and processed locally in full compliance with Article 44 of the GDPR.

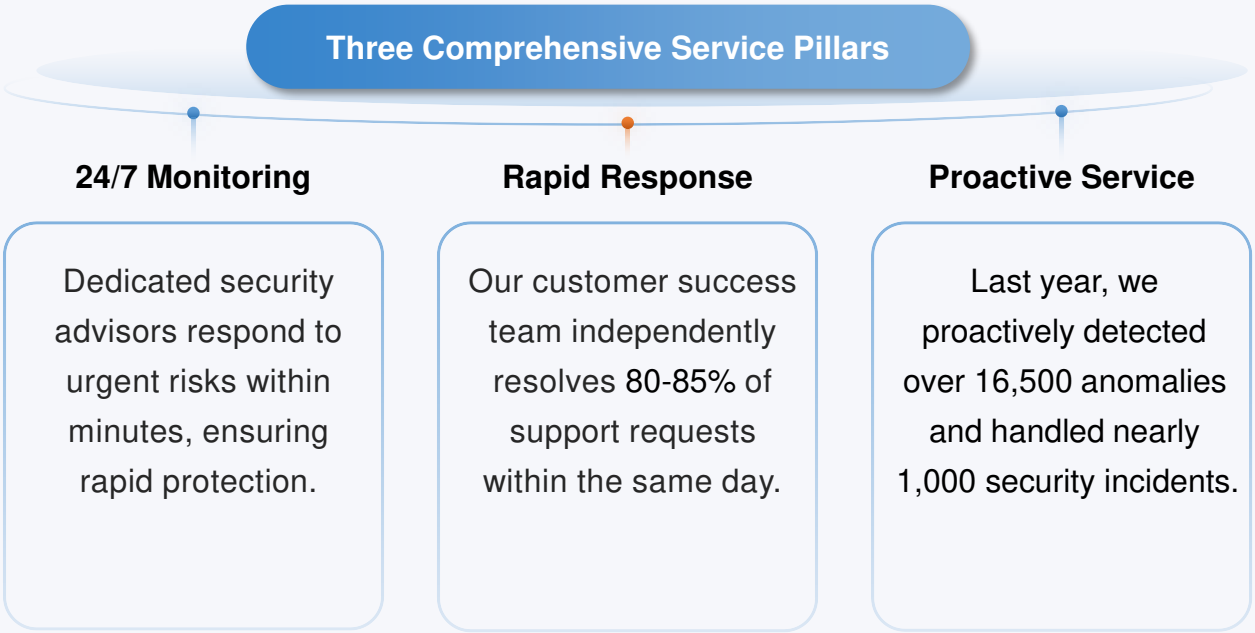
5.2 GeeTest Strategic Roadmap

1. Building a Global Security Ecosystem

To counter evolving security threats, GeeTest will continue investing in technological innovation and strengthening partnerships worldwide to foster an open, collaborative security ecosystem. Our efforts include expanding our global service network, strengthening cross-border threat detection capabilities, and enhancing industry-wide defenses through shared threat intelligence. GeeTest also plans to introduce more localized products and services tailored to regional compliance frameworks, enabling businesses to navigate complex international regulations and operate securely on a global scale.

2. Security as a Service (SECaaS) Long-Term Partnership Model

At GeeTest, we focus on service as a core value, fostering enduring client partnerships. Our SECaaS model is designed for long-term value creation, reshaping industry standards through three comprehensive service pillars:



This continuous service model empowers businesses to respond swiftly during critical moments while enhancing long-term security outcomes through sustained collaboration.

Service	Core Features	Key Metrics
24/7 Monitoring	Dedicated security advisors provide real-time monitoring with minute-level response to critical risks.	Response Time: <10 minutes Coverage: Global real-time threat alerts
Rapid Service Response	Customer Success team resolves 80-85% of client issues within 24 hours.	Daily Resolution Rate: 80-85% Average Handling Time: Within 24 hours
Proactive Service	Minute-level risk monitoring system detects risks in business scenarios and facilitates collaborative client resolution.	2024 Traffic Anomaly Detections: 16,500+ Security Incidents Addressed: ~1,000

*Source: GeeTest internal data, 2025.

Conclusion

E-commerce is transforming the global economy, with security now a vital enabler of sustainable growth.In the face of increasingly sophisticated fraud, frequent data breaches, and mounting compliance pressures, businesses must respond with innovation, collaboration, and strategic foresight.

This white paper examines the core challenges and solutions in e-commerce security, including account protection, bot mitigation, payment fraud prevention, and risk management. GeeTest's intelligent system illustrates how advanced technology delivers measurable results: reducing fake registrations by 85%, cutting fraud losses by 70%, and protecting over 99% of transactions, supporting global growth.

Looking ahead, AI-driven protection, enhanced privacy, and evolving compliance will shape the future of e-commerce security—focused on prediction, real-time response, and measurable value. We call on all stakeholders to help build an open and trusted security ecosystem.

- Enterprises should treat security as a strategic priority and adopt Security-as-a-Service (SECaaS).
- Security providers should accelerate innovation and offer cost-effective solutions for SMEs.
- Regulators and industry groups should enhance global standards and foster cross-border cooperation.

Security is no longer just a necessary cost—it's a strategic driver of business growth.

When every order, click, and user interaction is effectively safeguarded, e-commerce can unlock a new era of trust and sustainable value.

Thank you for your attention.

GeeTest Insight

E-commerce security has evolved from a defensive cost into a strategic growth enabler. Businesses must build security systems that combine proactive defense, adaptive compliance, and ecosystem collaboration. By 2025, security and compliance will become a key competitive edge for cross-border e-commerce, enabling global expansion and regulatory readiness.

Legal Disclaimer

This white paper is intended solely for industry professionals, researchers, and relevant institutions in the e-commerce sector for informational, analytical, and technical exchange purposes only. It does not constitute commercial promotion, a product offering, or a solicitation of services. It is not associated with any paid access, downloads, or advertising activities. All technical solutions and best practices mentioned are based on general industry use cases and are not directed at any specific organization or competitive relationship. GeeTest retains all rights to interpret and revise this white paper. No organization or individual may reproduce, distribute, or use this document for commercial purposes without prior written authorization.

All data referenced herein are derived from public sources. Case studies have been anonymized to avoid disclosure of confidential business information or infringement of intellectual property rights. GeeTest is committed to complying with applicable global laws and regulations on cybersecurity, data privacy, and intellectual property, and to protecting the data security and commercial interests of its clients.

If you believe any content in this white paper infringes on your legitimate rights or may unintentionally affect any party's interests, please notify us in writing at service@geetest.com, and we will promptly review and take appropriate corrective action, including removal or revision.

GEETEST

Looking forward to our collaboration

Website：www.geetest.com
Email：international@geetest.com
Blog：blog.geetest.com/en

GEETEST

GeeTest