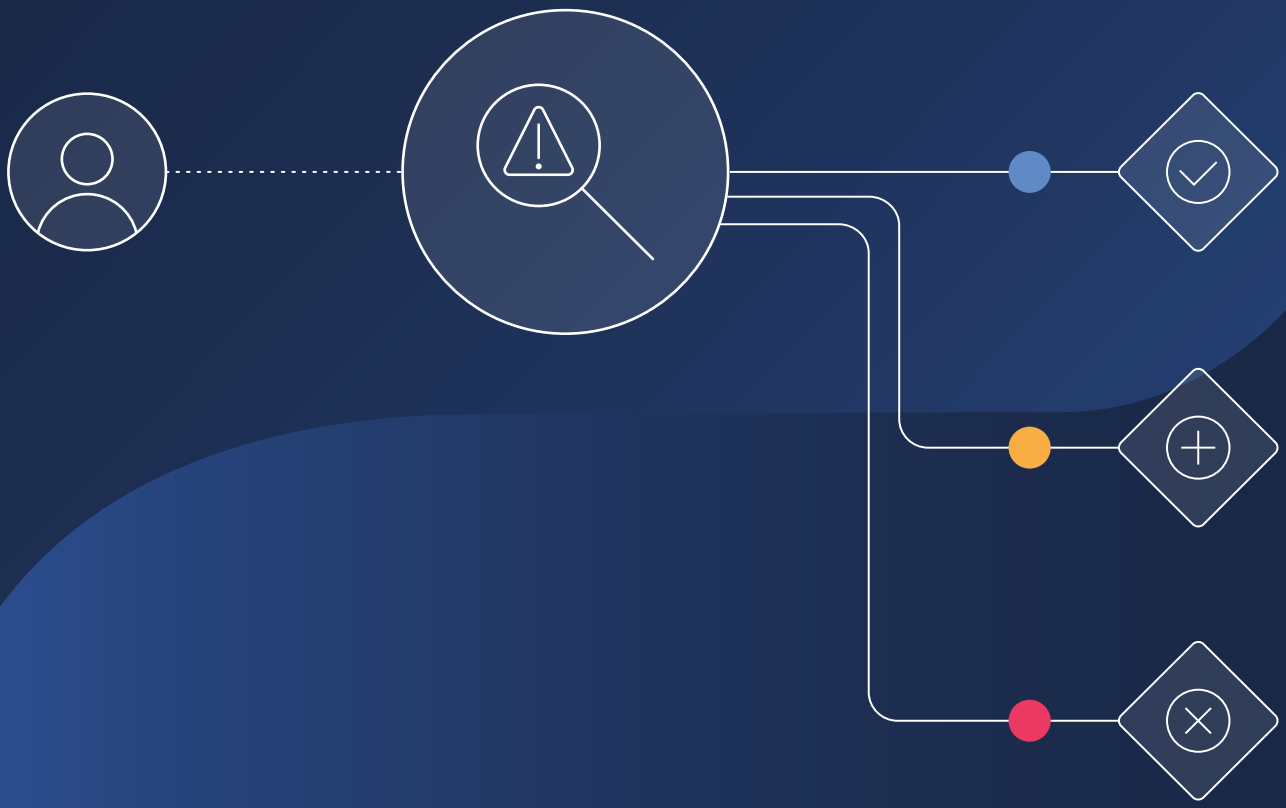
transmit security

USE CASE



Risk-Based Authentication

Blunt security measures degrade the customer experience

To secure access and stem the tide of account takeovers (ATO), customers are required to log in with multi-factor authentication (MFA). But it doesn't stop there. They must re-authenticate to recover an account, use a new device, transact, call support, change account details and more. Companies use costly and complicated measures, like one-time passcodes (OTP), made worse if a customer is in a hurry or has technical issues that require support. It all leads to drop-offs and lost revenue.

Moreover, repeatedly challenging users with a second factor does nothing to prevent ATO fraud during active sessions in the time between each authentication event. After all, authenticating the user only establishes trust at a single point in time. Today's fraud tools take advantage of this, making it easy for low-skill fraudsters to hijack active sessions, spoof user devices and play other tricks. Plus, hackers continually innovate (and sell) new tactics to evade detection. To plug the gaps, security teams add multiple anti-fraud tools, creating more complexity and friction for little gain.

This use case covers these challenges and how Transmit Security's risk-based authentication (RBA) delivers accurate risk-trust ratings to then add, adapt or remove authentication in real time — optimizing security and the user experience (UX) at all times.

How risk-based authentication solves these challenges

To mitigate these complex, conflicting challenges, organizations are adopting various forms of RBA. This method of dynamic authentication assesses the level of risk associated with a user's access request and adjusts the authentication requirements in real time. A high risk score can trigger stronger authentication methods, while a high level of trust can remove friction, giving customers access without having to reauthenticate.

The effectiveness of RBA relies on the strength of anomaly detection, data analysis and the algorithms used to determine risk scores. For the most accurate results, RBA should include a full range of authentication methods and identity orchestration plus real-time fraud prevention that provides continuous monitoring, behavioral biometrics, device recognition and other advanced capabilities. Anything less will fall short of optimal outcomes.

Challenges of risk-based authentication

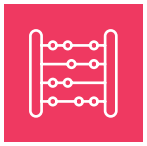
To prevent account fraud without frustrating customers, RBA risk ratings must be highly accurate. This is difficult to achieve as companies face a broad set of challenges:

Detection errors: By evolving their tactics and mimicking user behavior, fraudsters are able to slip past most defenses. Even machine learning (ML) algorithms require continuous fine-tuning to maintain accuracy. Comparing a few anomalies to known customer behavior is clouded by the fact that customers occasionally deviate from their norm, logging in from a new location or device, for example. In this environment, analyzing a narrow set of signals leads to mistakes. False positives disrupt customers with unnecessary step-ups, and false negatives result in fraud.

Siloed detection engines: In an attempt to detect more fraud, companies layer multi-vendor cyber and identity solutions. It's especially problematic when adding disparate anti-fraud tools with limited detection methods, incapable of assessing the full context of a user's access request. Security teams are left with data silos, blind spots and risk scores based on proprietary algorithms and methodologies. Solving these issues requires teams of experts to normalize risk scores, leading to more errors and slower response times.

Passkey vulnerabilities: To fortify and simplify RBA, companies can add passkeys, a new form of FIDO-based authentication. But passkeys are not without vulnerabilities, particularly during registration, account recovery, step-ups and cross-device enrollment. In cases when the user must fall back on legacy authentication methods (OTPs, passwords, etc.), accounts are vulnerable to phishing, credential stuffing and other common ATO tactics. Without additional security layers, there's little to stop fraudsters from registering a passkey on a new device or recovering access to a passkey on a compromised or stolen device. Passkey leakage is also a risk when syncing to a new, unregistered device.

Fragmented authentication experiences: Adding passkeys or another form of passwordless MFA to your identity framework allows customers to effortlessly authenticate with a higher level of assurance. But piecing this together with different solutions for OTPs, email magic links and social logins introduces complexity and challenges that impact RBA. After all, RBA adapts authentication based on the level of trust, including the strength of the login method itself.



Overhead complexity and cost: Stitching together multi-vendor cyber and identity solutions for RBA requires complex integrations, decision-making structures, coding and tuning cycles. Data correlation is further complicated by black box AI models. Complexity and costs continue to rise as you build and maintain layers of heuristic rules to detect new MOs. It's a never-ending process with suboptimal results.

Poor customer experiences: A cumbersome MFA process can create more friction than customers will tolerate. As you invoke more authentication challenges or limit session length, you're adding barriers and complexity that lead customers to call support or drop off entirely. Detection errors that result in fraud further degrade UX.

Risk-based authentication with Transmit Security

Transmit Security offers the only risk-native authentication solution on the market, giving you the most accurate and seamless risk-based authentication with the contextual intelligence to detect risk or trust and adapt security in real time. You'll prevent more fraud and improve UX.

Context-aware RBA prevents highly deceptive ATO fraud and removes friction from the trusted customer's path by providing a complete, leading-edge solution:

Highly-accurate detection: Transmit Security delivers the most accurate risk scores, reducing false positives and false negatives by 90% when tested against other solutions. End-to-end protection throughout the identity lifecycle includes three core components:

- **Multi-method detection:** Our state-of-the-art risk engine examines hundreds of telemetry streams to ensure the most accurate results — based on advanced behavioral biometrics, privacy-age device fingerprinting, bot detection, application and network evaluation, authentication analysis, transaction signing and other detections, which passively run in the background at all times.
- **Risk telemetry consolidation with machine learning (ML) and AI:** Our RBA solution continually analyzes the full context of all that's happening in real time by collecting and correlating telemetry across the identity lifecycle. ML and AI evaluate data in light of known or suspected fraud patterns, bot behavior and the customer's typical behavior, devices and IP addresses as well as the use case and application flows. All anomalies, even subtle deviations, are weighed as part of a holistic, contextual analysis. The outcome: smart, accurate risk scores.

- **Immediate threat response:** ML and AI automatically detect zero-day threats by analyzing a broader range of signals, greatly improving our ability to identify new attack patterns. In parallel, Transmit Security threat researchers continually add new detection mechanisms and tune algorithms, so you don't have to. High risk scores trigger MFA to challenge new and evolving fraud tactics as they emerge.

Phishing-resistant credentials: With Transmit Security's true passwordless MFA, customers simply log in with a fingerprint or face ID, never using a password, OTP or other vulnerable authentication method again. For enterprises adopting passkeys, we offer an added security layer that ensures passkeys only sync across devices and ecosystems with a deliberate transfer of trust. Plus, our risk engine offers device fingerprinting and behavioral biometrics to provide and maintain a high level of assurance throughout the user lifecycle.

Simplify security and reduce costs: With a single, unified platform, there's no need to cross-correlate data from multi-vendor solutions and standardize risk scores. One centrally-managed platform provides:

- **Identity orchestration:** Out-of-the-box decisioning rules eliminate the cost and complexity of building and maintaining layers of decision logic, and a visual drag-and-drop journey builder simplifies the creation of orchestrated user flows that adapt to risk and trust. The orchestration engine pulls it all together, consolidating and correlating data from all sources as ML and AI evaluate signals within the full context of user behavior, threat intelligence, the application and RBA use case.

- **All authentication methods in one:** For optimal efficiency and flexibility, Transmit Security provides the most complete set of authentication methods in a single platform, including best-in-class passwordless MFA and passkeys with our added security layer. In moments of risk, you can achieve the highest level of assurance by authenticating customers with fingerprint or face ID. You can also use SMS OTPs, email magic links, social logins or passwords. When passwords are at play, you can downgrade the level of trust extended to the customer. Having all authentication methods in one RBA solution ensures a seamless UX while minimizing IT complexity and costs.

- **Visibility and control:** A single, centrally-managed solution provides visibility of each users' authenticators, devices, risk scores and applications in one intuitive management console. An extensible, dynamic user store consolidates identity profiles across your brands and channels — providing a single source of truth with graphical displays of real-time data, attack patterns and trends.

Improved customer experience: With accurate risk and trust ratings, you can confidently remove second factor authentication or step-ups for customers who've achieved a high level of trust. Consolidated user data and powerful analytics make it easy to progressively build rich customer profiles as a strong foundation for privacy-age behavioral biometrics and device fingerprinting. These and other forms of passive authentication run at all times — to optimize fraud prevention and UX. You'll gain customer trust, loyalty and revenue.

Preventing fraud and delighting customers with RBA

Frequently challenging customers with one-size-fits-all authentication spoils the user experience and does nothing to mitigate risk in the time between authentication challenges. These gaps in security give fraudsters ample opportunity to take over accounts. Adding disparate anti-fraud solutions to improve protection has only created more challenges. A unified, purpose-built RBA solution is the key to resolving these problems.

Transmit Security RBA detects and mitigates risk while removing friction for trusted customers — throughout the identity lifecycle. Continuous fraud detection, identity orchestration, a full range of authentication methods and centralized management provide a complete RBA solution.

Behavioral biometrics, device fingerprinting, ML and AI assess hundreds of signals at all times — to distinguish between good and bad activity. A high risk score invokes authentication challenges, and a high trust score adapts by removing authentication or reducing friction — based on the full context of all that's happening in the moment and across time.

Transmit Security RBA delivers better outcomes while solving the challenges of detection errors, complexity, costs and friction:

Reduces false positives and false negatives by **90%**

Reduces bots by **98%**

Improves the accuracy of device fingerprinting to **99.7% or better**

Reduces friction, CAPTCHA and MFA challenges by **80%**

Reduces complexity & costs with a RBA unified solution

Discover how Transmit Security RBA stops fraud and rewards customers with easy access to all that your business offers.

Explore our platform