DATA SHEET

RSA® Risk AI

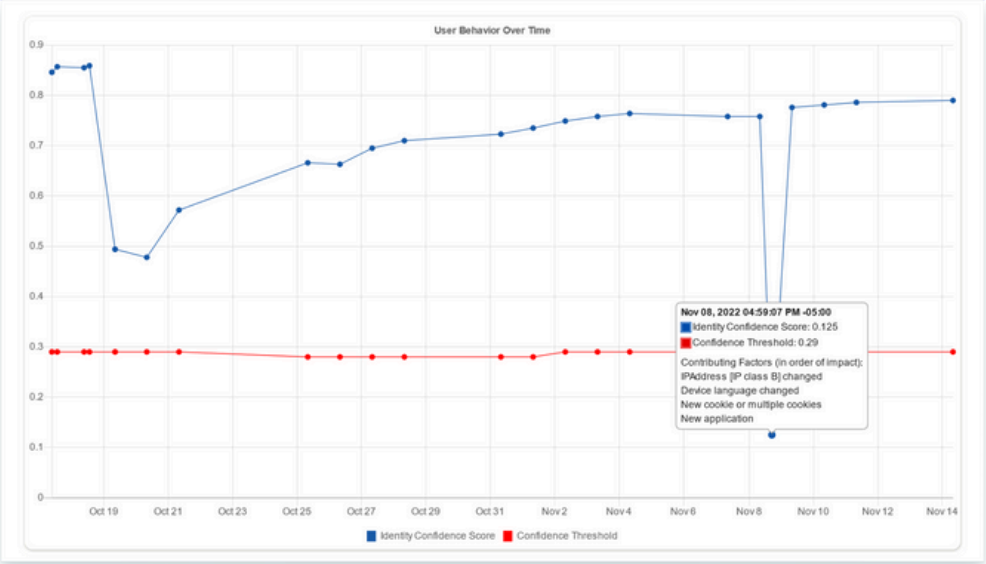
Risk-based access intelligence

Attackers keep inventing new ways to sneak past multi-factor authentication (MFA) with advanced AI-driven attacks, including session hijacking, help desk scams, and social engineering, or fraud. Traditional rules and static access policies can't keep up. RSA Risk AI is the intelligent layer of RSA ID Plus that spots these attacks in real time and stops them before they start. The solution uses machine learning and over 30 risk signals, like behavioral analytics and business context, for smarter access protection and easier user access.

- **Secure:** Detects anomalies that static rules miss and orchestrates policies to block risky activity or require step-up authentication.
- **Convenient:** Let trusted users sail through with fewer step-ups and re-auth prompts.
- **Intelligent:** Deterministic machine learning (ML) that self-tunes. No fraud analysts or data-science team required. Teams stay in control without complexity.
- **Manual tuning:** Admins can manually adjust identity confidence thresholds to prepare for planned changes and tuning the identity-scoring mechanism.

Access based on identity confidence

When a user requests access to an organization's resources, RSA Risk AI responds by instantly analyzing past and present user behavior, assessing the business context for the request, and performing real-time risk scoring. With this extensive intelligence, the technology establishes a level of confidence in the user's identity—and determines whether it should grant access.



RSA Risk AI uses identity confidence to assess user behavior in real time.

RSA Risk AI benefits:

- **Stop advanced identity attacks fast:** Real-time identity confidence scores block or step-up risky logins, stopping attacks before they start.
- **Let good users glide:** Fewer needless prompts mean happier users and lighter help-desk queues.
- **See risk, act quickly:** Clear High/Low scores and "why" details turn alerts into instant action.
- **Set-and-forget protection:** Self-tuning models and unified policy orchestration slash rule-maintenance work.
- **Continuous Zero Trust validation:** Enforce least-privilege access all day, every day, without blind spots or drift.
- **Anticipate—and learn from—anomalies:** Admins can manually adjust identity confidence thresholds to account for and learn from planned anomalies like travel, mergers, or significant numbers of new users
- **Your data, your model:** Each organization runs a private Risk AI instance that learns only from your organization's activity; nothing is shared with RSA.

Machine learning to inform future access

RSA Risk AI is a risk engine that uses deterministic machine learning to get smarter over time. In the process of gathering information for access decisions, Risk AI builds a store of knowledge to inform risk scoring for future access requests. It constantly recalibrates based on what it has learned in the past and what it observes in the present to make optimal access decisions.

Secure authentication that's easy for users and admins

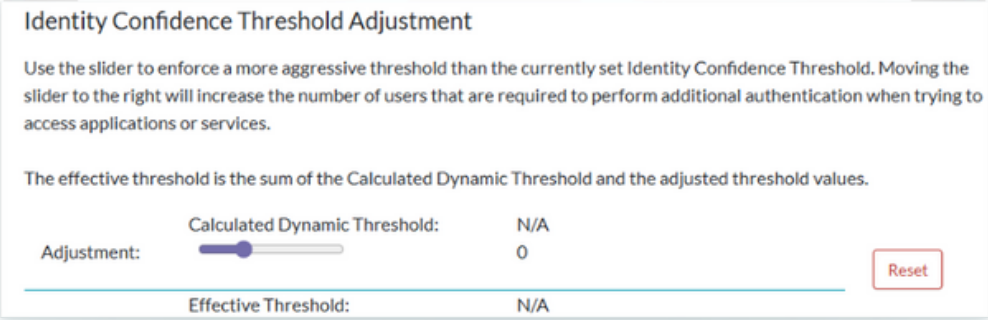
As Risk AI becomes increasingly familiar with users' behavior and the context for their access requests, the users themselves experience fewer authentication challenges. At the same time, security remains strong, with Risk AI detecting any anomalies and responding accordingly, either by requesting more information or denying the request if the level of risk warrants it.

Temporary tuning for planned changes

Admins can adjust the identity confidence threshold to account for expected anomalies. Risk AI continues to score each request in real time; access policies use that score plus the temporary adjustment to decide whether to allow, step up, or deny.

When it helps

- Planned events: office moves, travel, device rollouts, payroll cutovers, red-team exercises.
- Short-term changes in behavior that would otherwise trigger extra prompts.



Admins can create more lenient or aggressive identity confidence thresholds for expected anomalies.

Discover more

Contact us to learn more about Risk AI.

About RSA

RSA provides mission-critical cybersecurity solutions that protect the world's most security-sensitive organizations. The RSA Unified Identity Platform provides true passwordless identity security, risk-based access, automated identity intelligence, and comprehensive identity governance across cloud, hybrid, and on-premises environments. More than 9,000 high-security organizations trust RSA to manage more than 60 million identities, detect threats, secure access, and enable compliance. For additional information, visit our website to contact sales, find a partner, or learn more about RSA.

RSA

©2025 RSA Security LLC or its affiliates. All rights reserved. RSA and the RSA logo are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 12/25 Data Sheet