imprivata

DATASHEET

Adaptive and Risk-based Authentication

Zero Trust access that adapts to risk without slowing users down

Adaptive authentication for all users and use cases

Imprivata provides Adaptive and Risk-Based Authentication that continuously evaluates risk and user behavior to strengthen security without disrupting productivity. By leveraging a wide range of real-time signals, Imprivata dynamically identifies and challenges high-risk access events while allowing low-risk activity to proceed seamlessly.

At-a-glance benefits

- Stronger Zero Trust security
- Improved user experience
- Greater visibility and control
- Operational efficiency

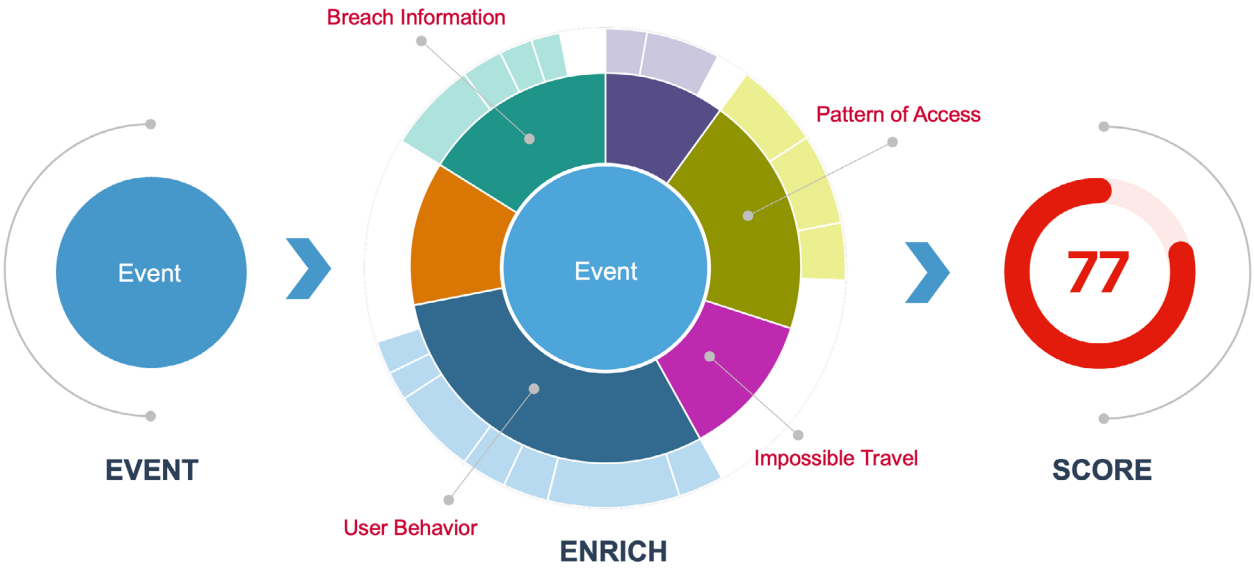
This set of capabilities is available with the **Imprivata Enterprise Access Management (EAM) – Advanced and Passwordless Access module** for employee access, and also with the **Imprivata Privileged Access – Identity Assurance and Threat Detection module** for managing internal privileged access and third-party vendor access.

How it works

Imprivata continuously scores access events using behavioral, device, and environmental signals. When risk is elevated, users are automatically challenged with step-up authentication, while low-risk activity proceeds seamlessly without MFA prompts.

Security is further strengthened with Imprivata SignalPrint™, a patented technology that creates a digital fingerprint for online identities by analyzing user interaction signals and enriching them with Open Source Intelligence (OSINT) to detect and prevent account fraud in real time, without requiring browser-based code.

Risk scoring process



Signals evaluated include:

- User, account, and credential context
- Device, IP, and geolocation attributes (e.g., impossible travel)
- Session behavior and event anomalies
- Time-of-day and contextual patterns

Addressing the most pressing access management challenges

Challenge	Solution
Credential-based attacks	Continuous risk and anomaly scoring to reduce account compromise
Excessive authentication friction	Adaptive step-up authentication for improved user experience
Limited visibility into access risk	Real-time risk scoring and reporting for stronger security insights
One-size-fits-all MFA policies	Context-aware authentication decisions for better balance of security and productivity
Unknown third-party identities	Enriched data signaling for external identities for stronger risk profiling for third-party users
Exploitation of privileged accounts	Block privileged access when risk surpasses set threshold to minimize breach likelihood and protect critical systems

Key use cases

Adaptive access dynamically adjusts grace periods based on real-time risk — balancing frontline worker efficiency with security — and adds additional authentication layers for privileged users based on their individual risk score at the time of access.

Risk profiling using a variety of signals differentiates access policies based on network location, behavior, and risk context.

Application-based MFA policies use the policy engine to set rules such as always enforcing MFA for sensitive apps or triggering it only when risk increases.

Phishing-resistant authentication requires stronger authentication methods when risk, location, or policy demands it.

Enriched data signaling for third-party identities pulls external data sources into risk profiling to provide strong first-time risk assessments of previously unknown external identities.

Risk-based privileged access enforcement blocks access when risk-based authentication determines elevated risk on a privileged or third-party account.

Delivering outcomes without compromise

This approach delivers clear business value by strengthening Zero Trust security while keeping day-to-day operations running smoothly. Continuous risk evaluation helps prevent credential-based attacks before they cause disruption or financial impact, protecting sensitive systems without slowing the business down.

At the same time, it improves productivity and efficiency. Low-risk users face fewer unnecessary MFA challenges, reducing friction and support tickets, while IT teams gain real-time visibility into access risk across the organization. Automated, policy-driven authentication decisions lower administrative overhead, allowing security teams to focus on higher-value initiatives instead of manual access management.

Why Imprivata

Imprivata delivers adaptive, risk-based authentication purpose-built for complex, mission-critical environments. With decades of experience securing frontline and enterprise workflows, Imprivata helps organizations reduce risk, improve productivity, and simplify Zero Trust access at scale.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

3850-2026_EAM-DS-aa-rb-auth