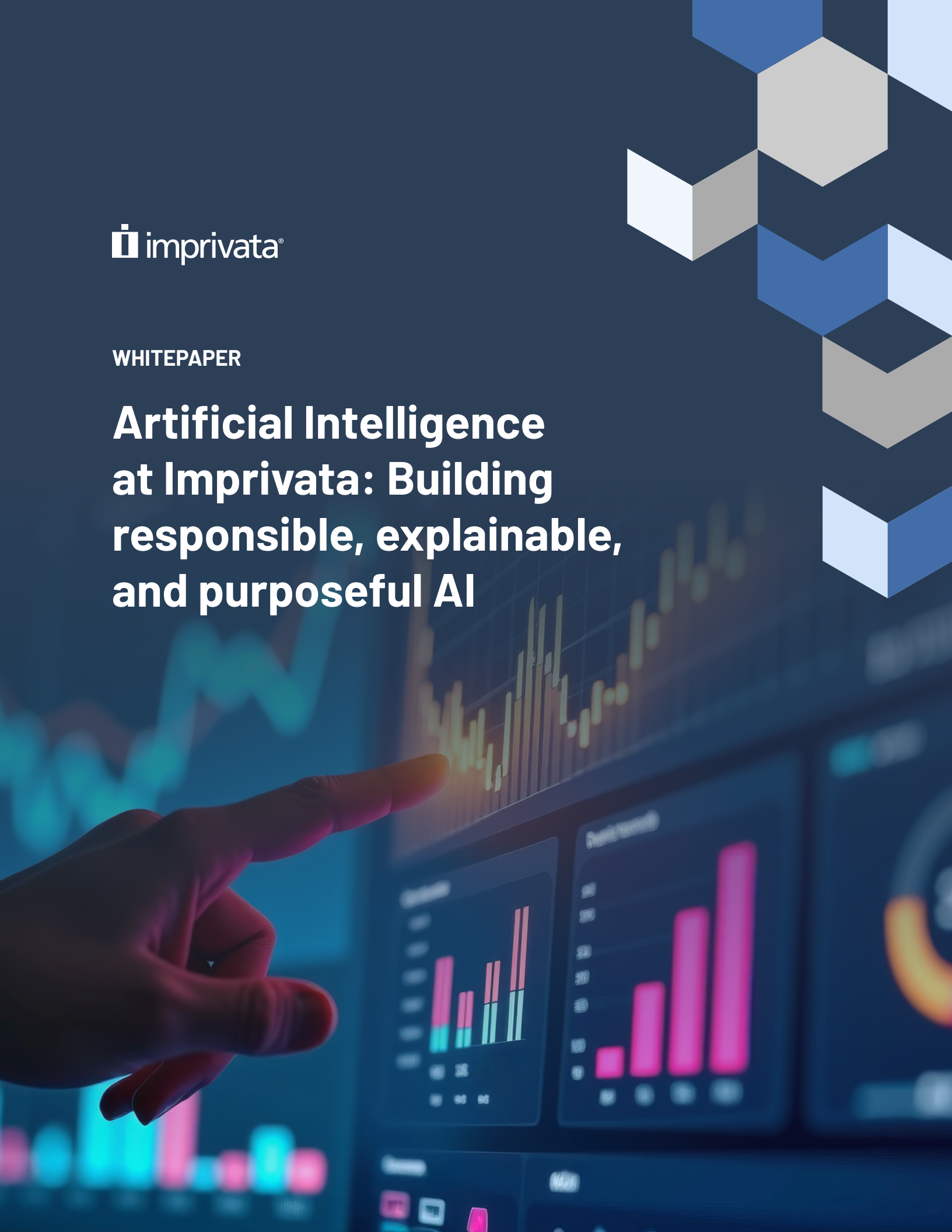
imprivata®

WHITEPAPER

Artificial Intelligence at Imprivata: Building responsible, explainable, and purposeful AI



Imprivata is a global leader in digital identity and access management, serving over 4,000 healthcare and commercial organizations worldwide. We're dedicated to simplifying and securing access to critical systems. This commitment naturally extends to our work in artificial intelligence (AI), where we innovate to deliver actionable insights and reinforce trust.

AI is reshaping how organizations manage their digital environments. At Imprivata, we're embedding AI analytics into access management and developing it to be responsible, transparent, and powerful. We believe our technology should not only protect sensitive data, but also deliver measurable value through precise, automated insights. Our AI-driven platform, Imprivata Access Intelligence, has been recognized as the IoT Security Analytics Solution of the Year in the 2025 Cybersecurity Breakthrough Awards, highlighting our commitment to developing industry-leading AI analytics.

Our AI capabilities are already enabling organizations to solve complex access and compliance challenges: from detecting inappropriate access to patient data (privacy monitoring) and identifying controlled substance diversion in healthcare (drug diversion detection) to analyzing access behaviors across connected systems and devices for greater operational insights. These are just a few examples of how Imprivata AI delivers real-world results that reduce risk and enhance efficiency.

While our expertise is deeply rooted in healthcare, the same principles apply across industries that rely on identity intelligence and access management, including finance, government, energy, and manufacturing to name a few. Imprivata's AI is built to bring clarity and trust to any environment where identity and access intersect.

This document explores how Imprivata approaches AI: grounded in responsibility but driven by innovation, as we empower our customers to achieve success safely and effectively.

The new imperative: Responsible AI for access management

Responsible AI means developing technology that empowers human judgement with data-driven insights, while preserving accountability and integrity.

Our responsible AI standards

Imprivata's approach to AI is guided by five key standards of ethical AI, as outlined in our Responsible AI Transparency Report:

- **Transparency:** AI decisions are designed to be explainable and interpretable by humans, with clear context around how models reach conclusions and how data is used, so organizations can act with confidence
- **Privacy by design:** We build privacy into every phase of design and development, ensuring data collection is limited to only what's necessary and customer data remains safe
- **Bias mitigation:** We work to promote fairness and reliable outcomes by actively identifying and eliminating sources of bias in our data and models
- **Accountability:** We maintain clear accountability protocols for model performance and AI use, addressing issues quickly and transparently
- **Configurability:** We design AI to require human oversight, feedback, and configuration, to ensure decisions remain human-directed

Together, these principles reflect our commitment to developing AI that's trustworthy and secure.

Privacy, opt-in, and data control

Data protection is central to how Imprivata designs and delivers AI. Our AI capabilities are developed with privacy and security as core principles, giving customers clear control over how their data is used.

Participation is strictly opt-in, and we follow strict privacy-by-design practices that align with global data protection standards. Customer data is processed only for agreed-upon purposes, protected with rigorous safeguards, and never shared outside the scope of a customer relationship. These measures ensure customers gain the full value of AI-driven insights, while maintaining confidence that their information remains secure.

High-quality data: The foundation of explainable AI

An AI model is only as reliable as the data that informs it. Imprivata AI leverages a wide range of healthcare and enterprise data sources, including electronic health records, HR systems, user access logs, patient and device data, and real-time behavioral signals. It uses this data to build a comprehensive picture of identity and access activity. By continuously correlating these sources, our models create a single, dynamic view of each user identity, connecting context across systems to explain not just who accessed a record or asset, or when they did so, but also why and how, through learned collaboration and workflow patterns.

This depth of insight transforms raw data into rich, actionable intelligence. Without this level of contextual understanding, even the most sophisticated AI models risk producing incomplete or biased outcomes. Additionally, our AI models are continuously refined over time to maintain accuracy and reflect evolving workflows.

Techniques that bring context to AI

Imprivata applies multiple AI and machine learning techniques to deliver actionable insights with clarity and accountability. Key examples include:

1. Behavioral communities: Context for peer comparison

Traditional anomaly detection treats all users alike, which limits accuracy. The Imprivata Access Intelligence Platform groups users and entities into behavioral communities, comparing individuals to peers with similar responsibilities and access patterns. This context improves sensitivity and specificity, while minimizing false positives.

Imprivata maps users and devices as nodes in a graph, connected by weighted edges that represent shared usage patterns. This approach ensures meaningful peer comparisons and a more precise understanding of behavior to more accurately flag suspicious activity.

2. Probabilistic record linkage: Connecting the dots across systems

Access activity rarely happens in one place. Users move between mobile devices, desktops, and applications, often within seconds. Imprivata uses probabilistic record linkage to join fragmented sessions into a single, coherent workflow. This approach bridges gaps that traditional identifiers miss, revealing workflow transitions and context that static logs cannot.

By tracking the complete user journey across devices and systems, organizations can form more accurate behavioral baselines and detect true anomalies more effectively.

3. Anomaly detection: Identifying meaningful deviations

Imprivata anomaly detection capabilities analyze dozens of behavioral signals – from frequency metrics to workflow variance – to identify access events that deviate from expected patterns. Each event receives a risk score accompanied by an explanation of why it was flagged, helping investigators understand and act faster.

These insights help investigators distinguish between technical issues, legitimate anomalies, and truly suspicious behavior, supporting faster and more confident decisions.

4. Agentic AI: From insight to actionable understanding

We've also begun introducing agentic AI capabilities within the Imprivata Access Intelligence Platform. These opt-in AI agents act as investigative assistants, autonomously gathering relevant data, reasoning through complex alert scenarios, and returning structured, evidence-based alert summaries to analysts.

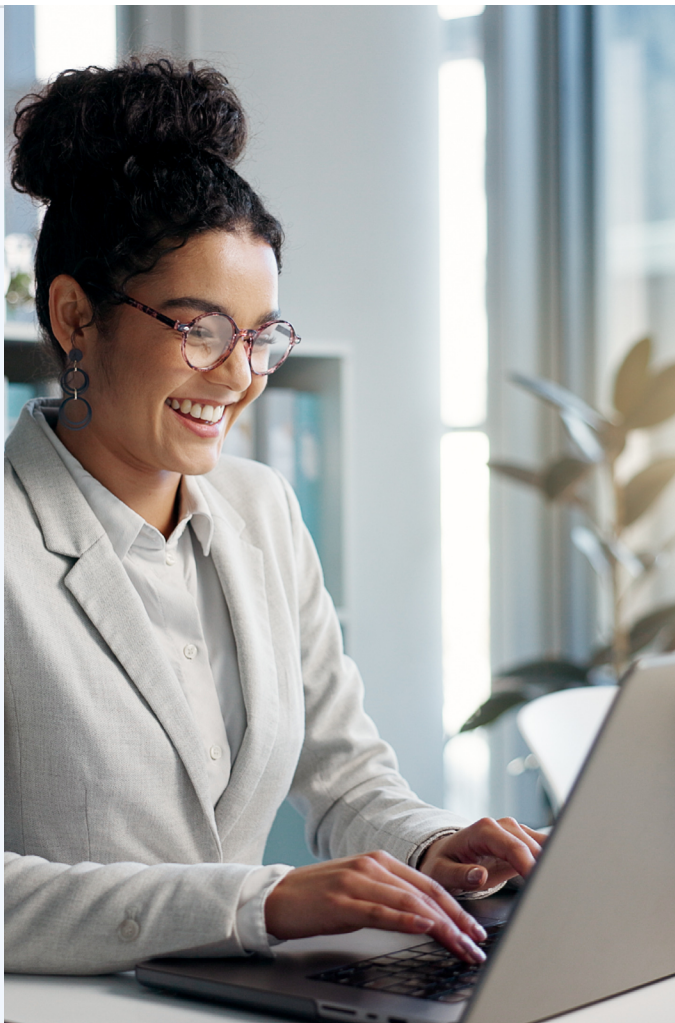
These agents operate within predefined guardrails, using approved tools and institutional knowledge to surface transparent explanations and recommendations. This approach enables teams to more quickly digest and act on critical information, reducing manual effort while preserving human oversight.

Real-world outcomes: Efficiency, accuracy, and trust

When built with intelligence and care, AI delivers impressive results:

- **Efficiency:** AI-driven insights help organizations reduce investigation workloads by focusing on the highest-risk access events
- **Accuracy:** Contextual modeling reduces false positives and strengthens the reliability of alerts
- **Trust:** Explainable, auditable insights build confidence in monitoring and compliance programs

Responsible AI also strengthens culture. When staff understand how AI is designed and governed, they are more likely to engage openly with compliance and security initiatives.



Looking forward: Our ongoing investment in AI

Imprivata's approach to AI is ongoing. We continue to invest in advancing our analytics and intelligence capabilities to help organizations better understand their access environments and make decisions with confidence. This investment is reflected in the continued evolution of risk-based authentication orchestration within our Zero Trust-driven access management platform, and the expansion of AI-powered Identity Threat Detection and Response (ITDR) to continuously validate identity and adapt in real time. We also support facial biometric authentication and AI-enhanced match accuracy for high-assurance liveness detection. We invite you to explore our latest roadmap updates to learn more.

Learn more and join the conversation

AI in access management is evolving rapidly, bringing new opportunities to strengthen security and productivity.

At Imprivata, AI is not a buzzword. It's a long-term commitment to empowering our customers with intelligent, explainable technology. We're building systems designed to be trusted and used with confidence.

We invite leaders and innovators to help shape the next chapter of AI in access management:

- **Listen to the Access Point podcast** for expert discussions on the future of access and analytics
- **Stay engaged** with our ongoing AI blogs and deep dive resources, and join the conversation

AI in access management is evolving, and we look forward to shaping what comes next.

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

3905-2026_WP-AI-at-imprivata