Imprivata product security in the age of AI-enabled threats

How Imprivata is using AI-assisted analysis to strengthen product security, accelerate remediation, and support customer resilience

What is changing

AI introduces a new operating reality for identity security. Organizations must now account for faster vulnerability discovery and potential exploitation, more autonomous digital activity across systems and workflows, new non-human identities (including AI agents), increased need for real-time visibility and response, and the need to preserve human oversight for sensitive or high-risk actions.

Organizations need to know not only who is accessing systems, but also what autonomous processes or agents are acting, what permissions they have, whether their behavior is appropriate, and how quickly access can be limited or revoked when risk changes.

Imprivata helps customers address the shifting threat landscape by strengthening the security of the identity products they rely on, and by extending identity security to the AI agents operating in their environments.

An AI-ready approach to Imprivata product development

As a trusted component of customers' identity security infrastructure, Imprivata is evolving our own product security practices to address an AI-accelerated threat landscape.

We are incorporating AI-assisted security analysis into our standard product security and development workflows to help identify potential issues earlier, prioritize remediation faster, and strengthen release readiness before software is deployed in customer environments.

Our approach includes:

- **Earlier identification of potential vulnerabilities –** using AI-assisted analysis to help identify potential security issues across products and services more quickly
- **Broader product security review –** expanding assessment across code, application behavior, infrastructure, exposure, and release readiness
- **Risk-based prioritization –** prioritizing findings based on potential impact, exploitability, customer exposure, and operational considerations
- **Faster remediation workflows –** aligning product security and engineering teams to accelerate fixes and reduce time to remediation
- **Improved customer guidance –** providing clearer, more practical guidance to help customers evaluate risk, plan updates, and maintain secure deployments

Securing AI in customer environments

Imprivata also helps customers govern AI-driven access. As AI agents become more integrated into enterprise and clinical workflows, organizations need identity-first controls that extend to these new digital actors.

Imprivata helps organizations apply identity security principles to AI-driven access, including:

- Establishing trusted identities for AI agents
- Governing which systems, applications, and data AI agents can access
- Enforcing least-privilege access based on role, context, and risk
- Monitoring AI agent activity for unusual or inappropriate behavior
- Maintaining clear audit trails for investigation and compliance
- Preserving human oversight for sensitive or high-risk actions
- Limiting or revoking access when risk changes

This helps organizations unlock the productivity benefits of AI while maintaining the visibility, control, and accountability required in mission-critical environments.

Why it matters

With Imprivata, organizations can pursue AI innovation with greater confidence. Customers gain greater trust in the products they rely on as Imprivata evolves product security practices to account for AI-enabled vulnerability discovery and faster-moving threat conditions. Customers should expect continued security updates, patches, cloud service enhancements, and practical recommendations to help them make informed, risk-based decisions.

Imprivata also helps customers strengthen their governance of AI-driven access by extending access controls, monitoring, and auditability to AI agents and other non-human identities.

By securing both the identity infrastructure customers depend on and the AI-driven access emerging in their environments, Imprivata helps organizations adapt to the AI era without sacrificing security, compliance, or operational continuity.

Customer role

Customers play a critical role in maintaining a secure deployment posture for Imprivata products, while staying vigilant in the AI-enabled security space.

Recommended actions include:

- Stay current on supported product versions
- Review and apply security updates in a timely manner
- Follow Imprivata secure deployment and configuration guidance
- Identify where AI agents may need access to systems, applications, or data
- Establish governance requirements for AI-driven access
- Ensure AI agents can be monitored, audited, limited, and revoked
- Preserve human oversight for sensitive or high-risk workflows

The bottom line

Organizations can adopt AI with greater confidence by securing the identity infrastructure they rely on and governing the AI agents entering their environments.

Imprivata helps customers do both.

We are strengthening the security of the products customers depend on and extending identity-first controls to help organizations manage AI-driven access with trust, visibility, control, and accountability.

For more information, please contact us at **+1 877 663 7446** or visit us online at **www.imprivata.com**