



DATASHEET

Imprivata Privileged Access: Four powerful solutions. One platform.

A comprehensive, unified solution suite delivering advanced security, enhanced efficiency, and improved ROI



Securing access to privileged accounts for internal users, external users, and non-human users can be a daunting task. And today's expanded attack surface – along with the complexities of negotiating multiple platforms and solution vendors – make it even more challenging.

Now, Imprivata Privileged Access unifies and simplifies the management of all privileged identities on a single platform. The result: organizations benefit from the enhanced convenience and efficiency of just one consolidated platform for managing employee, third-party vendor, and agentic AI identities. Plus, it features real-time threat detection and adaptive authentication capabilities to reduce risk and support timely response.

The Imprivata Privileged Access platform

Imprivata Privileged
Access Management

Imprivata Vendor Privileged
Access Management

Imprivata Agentic
Identity Management

Imprivata Identity Assurance and Threat Detection

Here's a closer look at the platform's four solutions:



Imprivata Privileged Access Management

Privileged access management is crucial to improving an organization's security posture and implementing an effective Zero Trust approach. Stolen or misused credentials associated with internal users' privileged and shared accounts, poor authentication, and/or lack of control over privileged access can lead to devastating security breaches.

That puts organizations and their most sensitive information at risk. In fact, reports show that more than 80% of data breaches involve compromised or otherwise abused privileged credentials.

We help organizations address security risks involving their most privileged users, credentials, and assets with Imprivata Privileged Access Management. The solution does that by enabling strong visibility and control over privileged credentials and providing least privilege access to the most critical assets and information – all without impacting productivity.

KEY FEATURES INCLUDE:

- An enterprise password vault to securely store credentials
- A robust job engine to rotate passwords and discover privileged accounts
- A session manager to broker and monitor access to-and-from privileged systems and records

To learn more about Imprivata Privileged Access Management, [visit our website](#) or [contact us](#).



Imprivata Vendor Privileged Access Management

As organizations outsource more critical operations – IT support, software development, revenue cycle management, facilities, and managed security – third-party access has become one of the most common pathways into their environments.

When attackers obtain valid credentials (through phishing, password reuse, credential stuffing, or malware), missing or weak MFA turns a vendor account into a front door. As a result, nearly half of organizations have experienced a breach or attack involving a third-party vendor. And beyond direct costs of the initial intrusion, the impact includes lost trust, churn, plus time-consuming vendor relationship re-evaluation.

Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access) is a robust remote access platform designed to manage third-party identities and secure remote access to critical assets. It provides organizations with enhanced control, visibility, and peace of mind regarding third-party access while decreasing the operational burden on IT and security teams.

KEY BENEFITS INCLUDE:

- Third-party identity management and enforcement of least-privileged access policies
- Secure, controlled, remote access to applications and systems
- Monitored and audited session activity for total visibility and vendor accountability
- Faster time-to-value with a simple deployment

To learn more about Imprivata Vendor Privileged Access Management, [visit our website](#) or [contact us](#).



Imprivata Agentic Identity Management

AI agents can most effectively deliver productivity and efficiency gains when they're able to take action inside real enterprise environments. But giving them access safely is the challenge: without tight controls and oversight of their autonomous actions, they can create significant security risks.

Unfortunately, many organizations simply don't have a secure way to provide agents with access to their networks and apps – especially legacy systems.

Imprivata Agentic Identity Management provides a comprehensive new approach to securing agentic AI access by helping organizations bring AI agents under the same access controls as human users. The result: greater opportunity for accelerated AI adoption and increased productivity by ensuring the proper controls and security measures are in place.

KEY BENEFITS INCLUDE:

- AI agents treated as managed identities with governed access
- Reduced reliance on embedded credentials
- Greater visibility and control over agent activity
- Secure access extended to both modern and legacy systems

To learn more about Imprivata Agentic Identity Management, [visit our website](#) or [contact us](#).



Imprivata Identity Assurance and Threat Detection

Cybercriminals are targeting organizations with sophisticated identity-based attacks – including AI-driven tactics – and can now go undetected by mimicking typical user behavior. Compounding the problem is the fact that traditional authentication methods used by many organizations are static and cannot adapt quickly to changing identity risk.

Without strong visibility into suspicious privileged access activity, many organizations remain in a highly vulnerable state. To safeguard their privileged accounts, they need the ability to continuously assess identity trust and respond to threats in real time.

Imprivata Identity Assurance and Threat Detection helps organizations detect and respond to high-risk privileged access by adding real-time intelligence to privileged access workflows. It continuously scores identity risk, profiles unknown third-party identities, and adjusts authentication requirements based on context and behavior. When suspicious activity is detected, it triggers step-up authentication, alerts stakeholders, or disables access to help contain the compromise before it spreads.

KEY BENEFITS INCLUDE:

- Reduced risk of privileged account compromise
- Earlier detection of identity-based attacks
- Improved visibility into privileged identity risk
- Better protection of critical systems and sensitive resources without compromising productivity

To learn more about Imprivata Identity Assurance and Threat Detection, [visit our website](#) or [contact us](#).



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

Copyright © 2026 Imprivata, Inc. All rights reserved. Imprivata is a registered trademark of Imprivata, Inc. in the U.S. and other countries. All other trademarks are the property of their respective owners.