

DATASHEET

Imprivata's access platform for CJIS compliance

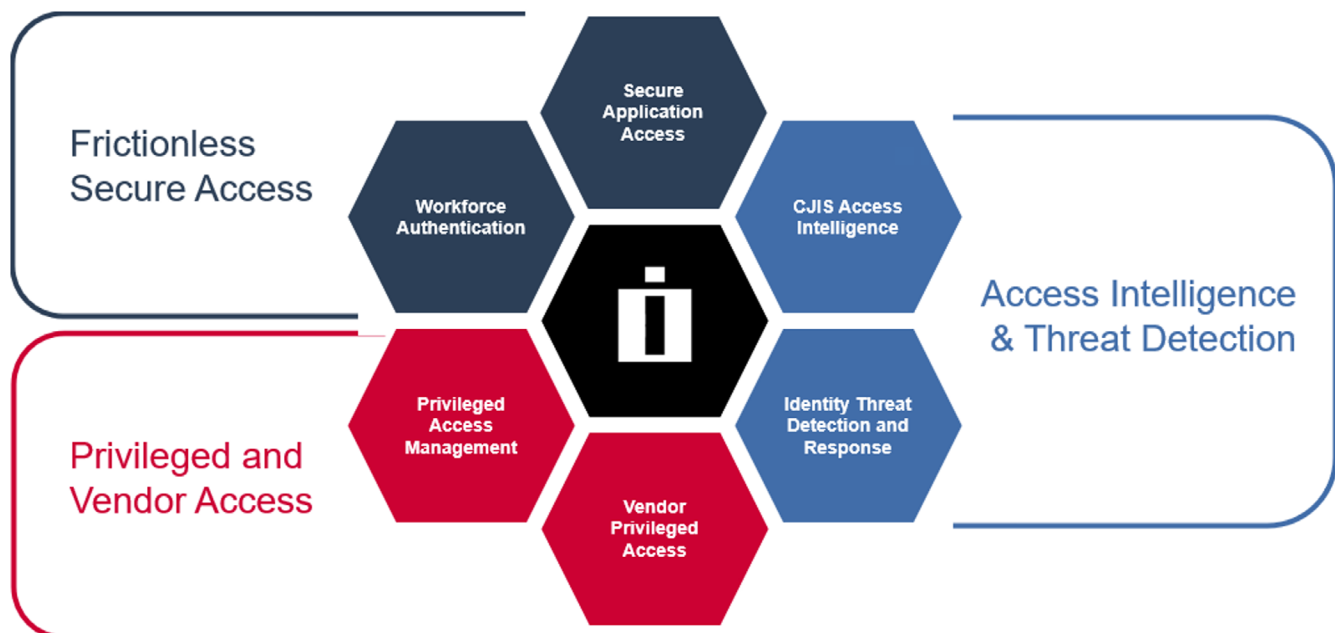
Secure every identity, session, and device without slowing mission-critical work

CJIS compliance has evolved.

The FBI's CJIS Security Policy is broad and complex, with hundreds of controls spanning more than 460 pages. Its technology requirements go well beyond multifactor authentication, covering identification and authentication, access control, privileged and third-party access, audit and accountability, and monitoring.

Meeting these requirements can be challenging in criminal justice environments, where officers and staff need immediate access across shared workstations, mobile environments, and legacy applications. Vendors need remote access, while IT teams must secure and manage it all with limited resources.

Imprivata's platform helps agencies address CJIS requirements across officers and staff, privileged users, and third parties, while supporting the realities of criminal justice operations.



How Imprivata supports CJIS compliance



ENTERPRISE ACCESS MANAGEMENT (EAM)

Deliver fast, secure authentication and access for officers and staff

EAM gives officers, dispatchers, and staff fast, secure access to the applications they need with single sign-on and passwordless MFA. It supports legacy and modern applications across shared workstations, patrol vehicles, laptops, mobile devices, and remote environments.

Key capabilities

- Passwordless multi-factor authentication
- Single sign-on to all applications
- Fast user switching
- Shared workstation support
- Identity verification

Supporting CJIS control families:

- Identity and Authentication
- Access Control
- Audit and Accountability



PRIVILEGED ACCESS MANAGEMENT (PAM)

Secure privileged access for your staff

Privileged Access Management helps agencies control privileged credentials and access, enforce least privilege, and maintain a record of privileged activity, reducing risk while strengthening accountability.

Key capabilities

- Credential management
- Least privilege access
- Privileged session management
- Account discovery
- Just in time access

Supporting CJIS control families:

- Access Control
- Identification and Authentication
- Audit and Accountability



VENDOR PRIVILEGED ACCESS MANAGEMENT (VPAM)

Secure third-party remote access

Vendor Privileged Access Management helps agencies securely manage remote access for vendors and contractors. Agencies can verify third party identities, control when and how vendors connect, monitor sessions, and audit all activity for better control and visibility with a lower operational burden.

Key capabilities

- Secure remote access
- Vendor identity management
- Session monitoring
- Zero Trust access
- Comprehensive audit records

Supporting CJIS control families:

- Identity and Authentication
- Access Control
- Audit and Accountability
- Supply Chain Risk Management



CJIS INTELLIGENCE

Understand how CJI is being accessed

Audit logs show activity but often don't provide enough context to determine whether access was appropriate. CJIS Intelligence brings together identity, access activity, and operational context across CJIS connected systems to help agencies identify potential misuse earlier, investigate suspicious activity, and strengthen accountability.

Key capabilities

- Access analytics
- Behavioral analysis
- Proactive alerts
- Investigation workflows
- Search and reporting

Supporting CJIS control families:

- Audit and Accountability
- Incident Response

CJIS access by different users

Imprivata helps agencies manage access and accountability for the different people who access CJL.

User Type	Imprivata solution
Officers and employees	EAM
IT administrators	PAM
Vendors and contractors	VPAM
Security, Compliance, Internal Affairs	CJIS Intelligence

Why agencies choose Imprivata

Public safety agencies need technology that fits the way their teams work. Imprivata supports complex agency environments without adding unnecessary burden for users or IT teams.

- ✔ **Built for criminal justice workflows:** shared workstations, mobile devices, and legacy applications
- ✔ **Supports all users:** officers, employees, administrators, vendors, and contractors
- ✔ **Addresses access and accountability together:** control who can access systems and understand how that access is used

[Learn how Imprivata can partner with you on your CJIS compliance journey.](#)



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.