imprivata®

Imprivata Product Roadmap: Recent Releases and Upcoming Innovation

Publish Date: February 28, 2025

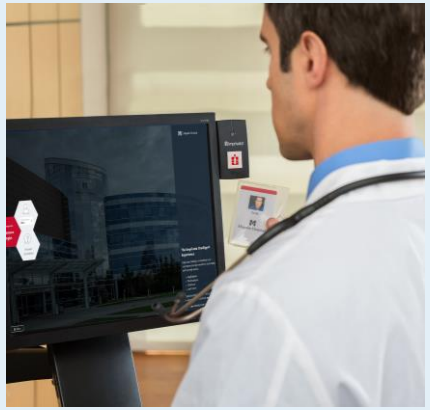
A Note Regarding Forward-Looking Statements

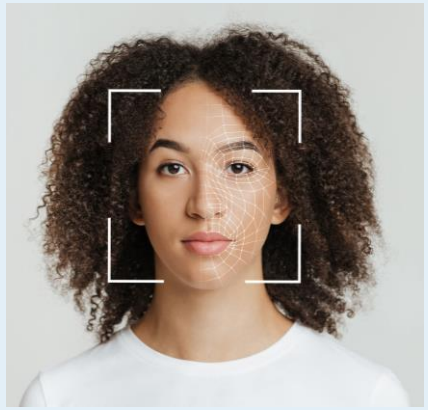
The following includes statements regarding planned or future development efforts for our existing or new products or services. These statements are not intended to be a promise or guarantee of future availability of products, services, or features and are not intended to indicate when or how particular features will be priced or packaged. These planned and future development efforts are based on factors known to us at the time of publication and may change without notice. Purchasing decisions should not be made based on reliance on these statements. We assume no obligation to update these forward-looking statements.”

Table of Contents

Using digital identity to maximize productivity, security, and ROI

Imprivata Access Management





Clinician Access Management

Enterprise Access Management
Simple, secure access to workstations, applications, and clinical workflows

Enterprise Access Management Analytics *[NEW]*
SSO and user access workflow analytics to drive actionable insights

Mobile Access Management
Security, optimization, and management of shared mobile devices at scale

Mobile Device Access
Secure, real-time access to shared devices and apps

Medical Device Access
Fast, convenient access to connected medical devices

Patient Access

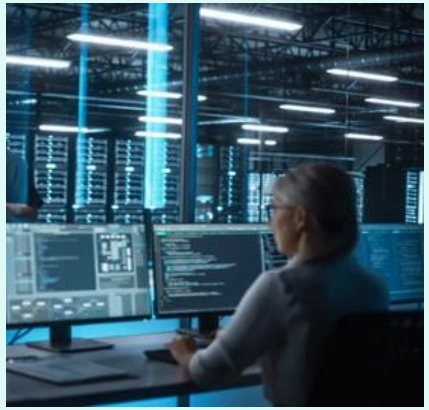
Patient Access
Touchless **facial *[NEW]*** and **palm vein** recognition to improve patient safety and experience

Access Compliance

Patient Privacy Intelligence
Patient privacy monitoring that detects and creates alerts for suspicious behavior

Drug Diversion Intelligence
Proactive drug anomaly detection to protect patients and staff

Imprivata Privileged Access Security



Privileged Access Security

Privileged Access Management
Enterprise credential vaulting and session management of privileged users and activities

Vendor Privileged Access Management
Secure and connect inbound remote access to critical assets

Customer Privileged Access Management
Enterprise remote support for service providers and technology vendors

imprivata®

Roadmap Update

Enterprise Access Management

(formerly OneSign and Confirm ID)

Overview

Imprivata Enterprise Access Management (EAM) offers SSO and user authentication to enable fast, secure access to the devices, applications, and workflows that clinicians and frontline workers need to care for patients and boost productivity. Capabilities include:

- **SSO into legacy and standards-based applications**
- **Badge-tap access to shared workstations, connected medical devices, and virtual desktops**
- **Re-authentication for in-app workflows**
- **Fast user switching on shared workstations**
- **Complete EPCS compliance**
- **Flexible authentication methods**
- **Comprehensive access workflow analytics**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Android support for Mobile EPCS (December 2024)
Extends the use of facial biometrics for EPCS signing from a mobile device (via Epic Haiku and Canto) to Android devices, giving providers more flexibility when prescribing controlled substances from a mobile device.

Azure Virtual Desktops for user access (November 2024)
EAM integrates with AVD on Windows for both single-user desktops and shared workstations (kiosks), enabling seamless badge-tap access to roaming AVD desktops.

Support for Entra ID-only customers (August 2024)
Allows customers who use only Microsoft Entra ID (but not AD) for their directory to use that as the stand-alone directory for EAM.

Enhanced self-service password reset (August 2024)
The Imprivata ID MFA mobile app is integrated as a second factor of authentication for self-service password reset, providing a higher level of security.

Windows Hello for Business supported for EAM SSO (July 2024)
Imprivata's application single sign-on can be used with Windows Hello for Business on single-user computers to support a passwordless Windows login experience.

Enterprise Access Management Analytics (May 2024)
Visibility into SSO and user access workflows across your organization to identify and remediate potential security gaps, reduce operational burden and IT overhead, and more.

COMING INNOVATION

Tap and go and EPCS on shared Mac computers
Imprivata agent for tap and go, and EPCS signing, on shared macOS computers. Will leverage native macOS account management for reduced overhead and will add passwordless SSO to Epic and Citrix Storefront apps.

Passwordless MFA login to single-user Windows computers
Secure and frictionless access to Windows login using facial biometrics and a device-bound passkey leveraging the trusted platform module (TPM) in Windows 10 and Windows 11 devices.

Integration with Epic Monitor (Pending Epic GA)
Enable clinicians to tap their badge on a digital monitor in the patient room, presenting a user specific Epic dashboard, often replacing the in-room whiteboard.

NHS England Care Identity Service 2 modern authentication support
Native EAM integration with the new NHS Care Identity Service 2 (CIS2), delivering simplified NHS Spine access and streamlined clinical workflows on the new, replacement Spine service.

Entra ID only joined devices for hybrid directory architectures
EAM will be available to customers using both Entra ID (formerly Azure AD) and on-prem AD directories. Endpoints will connect via Entra ID only, thus maximizing the benefits of Entra ID.

Enhanced self-service password reset
Will implement SMS passcodes and PINs as authentication factors for self-service password resets. This will enhance security around user credentials and reduce reliance on security questions.

Compliance with new PHI security policy in France
High assurance level authentication and SSO for applications integrated with Pro Santé Connect, a French centralizing authority for identity providers.

Appliance in AWS and Google Cloud
Enables hosting Imprivata appliances on AWS and Google Compute Engine, offering customers enhanced selection and adaptability in their infrastructure options.

imprivata®

Roadmap Update

Mobile Access Management

(formerly GroundControl)

Overview

Imprivata Mobile Access Management is a comprehensive, end-to-end mobility solution that helps organizations optimize their use of shared iOS and Android devices by delivering

- **Secure device checkout**
- **Simple access to mobile applications**
- **Personalized device experiences**
- **Visibility into device status and assignment**
- **Automated device managem ent workflows**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Simplify Launchpad management and configurations (January 2025)
Develop organization specific, pre-configured Launchpad installations to remove the need for manual configuration.

Faster Check Out experience for iOS devices (January 2025)
Improve the time it takes to check out a device for end users

Streamlined MFA workflow for checked out iPhones (August 2024)
Users are now prompted for their password or Imprivata PIN immediately when checking out a device to avoid additional steps when accessing applications

Support for additional Android Devices (August 2024)
Recent highlights include Samsung A15 and Samsung xCover 6 Pro

Simplified device refreshes, at scale (August 2024)
Support the bulk erasure and retiring of devices for faster time to value with device refreshes.

Native Epic Rover Logout (May 2024)
Update a user's presence status in Epic when devices are checked in to eliminate irrelevant alerts sent to checked in devices.

Simplified device Check Out with Smart Hub LEDs configuration (May 2024)
Admins can now disable the blue (deployment in progress) LED in the check out workflow action.

Indicators for network connectivity loss (May 2024)
Monitors network connectivity on checked in devices with visual indication if the phone loses network connectivity.

Automatically launch an Android application at check out (May 2024)
Admins can now configure an app (ex. Microsoft Teams) to launch automatically after checkout to improve the user experience.

COMING INNOVATION

Comprehensive analytics
Improve reporting and analytics for with more data, customizable dashboards and proactive issue detection.

Improved visibility of device status for department managers
Device management application to provide direct views into device check out status in real-time including who has been assigned each device and where it's been returned.

Simplify deployment of new Launchpads and Smarthubs
Automatically configure badge readers with Enterprise Access Management to quickly enable check out workflows.

Improved admin permissions for large organizations
Admins can have unique user roles and permissions at different levels of an organization

Improve Usability of the Dashboard
Improvements to help MAM administrators understand where issues are that need their attention as well as recommendations for manual interactions.

More intuitive display for Check In and Check Out
Introducing a Launchpad display for our clinical users to improve end user satisfaction and success rates while checking in and out mobile devices.

Passwordless device check out
'Tap and Smile' with facial biometrics for passwordless multi-factor authentication when checking out a device.

Passwordless authentication to mobile apps supporting OIDC
Login to apps like Epic Rover using facial biometrics for passwordless multi-factor authentication through the Locker App.

imprivata®

Roadmap Update

Mobile Device Access

Overview

Imprivata Mobile Device Access delivers on the promise of uncompromised security and efficiency by removing barriers to access share shared Android devices with

- **Secure, personalized access to Android devices**
- **Single sign-on for mobile applications**
- **Fast user switching with badge-tap on the device**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Deliver consistent workflows regardless of connectivity (December 2024)
Support for "offline mode" to enable device access when there is no network connectivity.

Support for new Android devices and applications (December 2024)
Recent highlights include integration with Zebra HC20 devices as well as support for Navenio and British National Formulary applications.

Support for new Android devices and applications (August 2024)
Recent device highlights include integration with Samsung A15, Samsung xCover Pro, various Google Pixel model, and Honeywell CT60. We've also introduced support for new applications such as Zebra Workcloud Connect, Manhattan Active, Diktamen, Nordic Health Group, and more.

Enable secure access for more environments and use cases (May 2024)
Support for Android workstations and devices with external badge readers.

Mobile Device Access Analytics through EAM Analytics Platform (May 2024)
Robust analytics capabilities provide unparalleled visibility into user access workflows across your shared mobile devices environments to drive actionable insights, remediate security gaps, and reduce operational burden and IT overhead.

Faster care team collaboration with support for native dialer applications (March 2024)
Mobile Device Access now supports the use of Samsung and Zebra dialer applications to enable fast, secure access to phone calls and notifications on shared devices.

Improved diagnostics and troubleshooting (March 2024)
Users can quickly check Mobile Device Access app configuration and connectivity right from the lock screen and submit logs from the tool for troubleshooting.

COMING INNOVATION

Understand application usage with enhanced analytics
Customers can report on user authentications to applications.

Configure device status based on charging
Admins can configure whether devices lock and/or logout when charging to streamline workflow and promote security.

Passwordless device check out
Customers can use facial biometrics for passwordless multifactor authentication when assigning out a device.

Passwordless device unlock
Customers can unlock an assigned device with facial biometrics.

imprivata®

Roadmap Update

Patient Access

(formerly Imprivata Biometric Patient Identity)

Overview

Designed with privacy in mind, Imprivata Patient Access is a facial recognition solution that enhances patient safety and experience by streamlining check-ins and accurately linking patients to their medical records with a single photo, helping to ensure efficient and error-free healthcare delivery.

- **Improved patient identification accuracy**
- **Enhanced patient safety and experience**
- **Streamlined registrar workflows**
- **Flexible hardware**
- **Seamlessly integrated with Epic**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Data Retention Controls (February 2025)
Introducing the ability for customers to set data retention controls to help support compliance with pertinent biometric privacy regulations.

Duplicate Proofing (December 2024)
As an extra safeguard to help prevent misidentification errors, Imprivata Patient Access will help ensure that each face is enrolled only once. (Allows for the enrollment of identical twins.) This critical feature helps maintain a one-to-one match between a patient and their medical record.

Configurable Enrollment Age (October 2024)
Tailor the patient enrollment experience by setting a minimum age for eligibility in healthcare facilities, helping ensure alignment with compliance and patient care standards.

Two-Factor Authentication with Imprivata ID for Patient Access Admin UI (October 2024)
Added ability to require Imprivata ID as a second factor of authentication when logging into the Patient Access Admin Console to further protect PHI.

Image Refinement for Patient Privacy (June 2024)
Improve how images are displayed by cropping backgrounds, focusing solely on the patient to protect privacy and improve the clarity of identification photos.

Enhanced Photo Retake Capability (May 2024)
Easily retake patient enrollment photos if the initial photo has issues, such as closed eyes. This flexibility helps improve the appearance of the patient photo.

Smart Workflow Management (April 2024)
Intelligently prompts the registrar with the appropriate action—either enroll or verify—based on the patient's status. This streamlines the enrollment and check-in processes.

COMING INNOVATION

Self-Service Enrollment into Patient Access
This feature enables patients to enroll in Patient Access (without a registrar) so that when they return for future visits, they can streamline their check-ins by checking in via Patient Access at a kiosk or registrar.

Self-Service Identification
With integration into Epic Welcome kiosks, patients can identify themselves, significantly easing the workload on registrars and speeding up the check-in process.

ID Proofing for Self-Service Enrollment into Patient Access
For a patient self-enrolling in Patient Access (without a registrar), ID proofing verifies the patient's identity to offer increased confidence that the patient enrolling is who they say they are.

Advanced Fraud Detection with Liveness Checks
Strengthen security measures with enhanced liveness and spoof detection capabilities, helping to ensure that the system is interacting with a real person and not a fraudulent representation.

Reporting By Location
Patient Access reports will be organized by location which will help admins and managers understand usage at a more granular level. Activity data by location will be available to view in a new informative dashboard.

Patient Access Integration with Imprivata Access Management Portal
Customers will be able to access their Imprivata products through a single portal, streamlining the log in experience for users.

Enrollment Photo Updates at Authentication
This will allow registrars to update enrollment photos if they notice significant appearance changes or elapsed time since enrollment. This will help maintain accuracy.

Support for Multiple Patient Identifiers
Allows healthcare organizations to display various patient identifiers, ensuring registrars can use the ones they are most familiar with for their tasks.

imprivata®

Roadmap Update

PatientSecure

Overview

Imprivata PatientSecure uses palm vein biometric identification to accurately and securely identify patients, reducing identity errors, preventing fraud, and improving workflow efficiency across healthcare systems. This touchless authentication solution ensures positive patient identification at any point of care, enhancing patient safety and satisfaction.

- **Accurate Patient Identification**
- **Enhanced Patient Safety**
- **Fraud Prevention**
- **Workflow Optimization**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Improve Admin Console Experience (January 2025)
Admin console will display frequently performed actions front and center for quick access and streamlined workflows.

System Health Dashboard Enhancements (January 2025)
System Health Dashboard now provides status and/or alerts about additional system components to help keep PatientSecure running smoothly.

Epic Welcome Kiosk Integration Language and Date Enhancements (September 2024)
Language support additions - Our customers serve diverse patient populations who speak many languages. PatientSecure's integration with Epic kiosk gives patients a better check-in experience by expanding language support to include French, Arabic, Korean, Chinese, Haitian Creole and Bengali.

Location date format setting - PatientSecure presents date formats according to the language selected at the kiosk. Now customers have the option for the PatientSecure date format to remain consistent with Epic.

Parallel PatientSecure and Imprivata Patient Access (September 2024)
Epic customers will be able to run either PatientSecure (Palm Vein) or Imprivata Patient Access (Facial) at each point of registration.

Display Patient's Preferred Name for Improved Patient Experience (May 2024)
Allows for a more personal patient check-in experience.

Scheduled Reporting Enhancements (May 2024)
We have added an option to email a notification regarding the outcome of a scheduled report. When a scheduled report fails, PatientSecure provides the option to re-run the report using the original parameters.

COMING INNOVATION

Notification when Left Palm is Detected
While the palm vein scanner will work well with either hand, consistent presentation of the same hand is required to authenticate patients. For consistency and patient comfort, the best practice guideline is to enroll and authenticate the right hand unless the right hand is permanently unavailable. This feature notifies the registrar when a left hand is being scanned to minimize the chance of left-hand scans.

Registrar Control to Start Scan Option
Adding the option for registrars to control the start of the enrollment scan capture to allow time to instruct the patient on hand placement.

Enrollment Quality Visibility and Reporting
PatientSecure will now provide an enrollment quality score to help troubleshoot issues like inconsistent authentication.

Opt-Out Workflow Enhancements Streamlines Workflows with:
- Consistent language
- Understanding of patient-driven versus registrar-driven causes
- More opt-out reasons allowed
- More prominent last opt-out information at verification and enrollment

Collect Product Analytics for Key Product Functions
This feature will time key product functions to help customers understand performance.

imprivata®

Roadmap Update

Patient Privacy Intelligence

(formerly FairWarning)

Overview

Imprivata Patient Privacy Intelligence (PPI) helps protect patient privacy and deliver actionable insights for investigations, documentation, and reporting of privacy breaches. Equipped with artificial intelligence (AI), machine learning, and behavioral analytics, PPI provides healthcare organizations with the tools they need to comply with confidence, protect patient data, and prevent violations

- **Proactive & reactive auditing**
- **Robust reporting**
- **Efficient investigations**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Dashboard Library (December 2024)
Enhance user and analyst workflows with the ability to install best practice dashboards for application monitoring with a single click.

Imprivata Cloud Portal (ICP) Integration (December 2024)
Streamline user experience by providing a holistic Imprivata Cloud Platform.

Internationalization of Machine Learning Closing Model (August 2024)
Availability of our full-feature set of machine learning to our international customers for optimized internal access auditing.

First Access Reporting (July 2024)
Allows customers to build custom reports on First Access data with scores and explanations for enhanced auditing functionality.

Auto-Disabled End User Accounts (May 2024)
Application users accounts that have not been logged into within the previous 180 days will now be automatically disabled for extra security. User accounts will not be deleted, and audit history will not be affected. User accounts can be re-enabled at any time and timeframes for auto-disabling can be customized.

Custom Investigation Memorandums (April 2024)
Allows users to quickly document investigations and manager outreach within the platform. This new functionality also allow users to document investigations that are initiated outside the application for a streamlined investigation process.

2015 Edition Cures Update Certification (March 2024)
Certification of Imprivata PPI Version 24 to the 2015 Edition Cures Update to make it easier to leverage PPI for modular certification under set criteria. Find certification information at Imprivata ONC Certification Disclosures.

COMING INNOVATION

Unified Patient Privacy Intelligence Model
Optimize risk identification, advancing anomalous workflow model and establishing a foundation for UEBA model expansion.

SailPoint Integration
Leverage an API integration with SailPoint to launch a workflow upon the creation of an alert in PPI.

User Notifier/First Time Offender workflows
Expand upon the current "Delegated Incident Review" workflow to include auto-provisioning of users (managers, end users, etc.), use of updated memo templates, identification of first-time and repeat offenders, and enhanced governance reporting.

Investigation List
New Bulk Actions and customizable Views on "Investigation List" page, replacing all functionality on classic screens.

Report Results – Details & Access Reports
Updated report results screens for Detailed and Access report types to improve performance and expand functionality.

Redesigned Report Builder
All new user interface for the application's report builder, improving performance and enhancing ease of use.

VIP / Watchlist
Create user and patient lists to flag VIP patients or suspicious users for more targeted monitoring in dashboards and reports.

imprivata®

Roadmap Update

Drug Diversion Intelligence

(formerly FairWarning)

Overview

Imprivata Drug Diversion Intelligence (DDI) helps organizations manage drug diversion to protect their patients, workforce, and organization while satisfying key regulatory requirements for managing controlled substances.

- **Medication lifecycle auditing**
- **Use Case Monitoring**
- **Investigation management**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Dashboard Library (December 2024)
Enhance user and analyst workflows with the ability to install best practice dashboards for application monitoring with a single click.

Imprivata Cloud Portal (ICP) Integration (December 2024)
Streamline user experience by providing a holistic Imprivata Cloud Platform.

User-Based Risk Model & AI Configuration (August 2024)
Streamline users and analyst workflows with the power of AI, providing the ability to rank users with peer clustering to determine which users present the most risk.

Device Cluster Management (June 2024)
Discover trends within users and potential anomalies for diversion mitigation through the ability to set defined peer groups.

Auto-Disabled End User Accounts (May 2024)
Application users accounts that have not been logged into within the previous 180 days will now be automatically disabled for extra security. User accounts will not be deleted, and audit history will not be affected. User accounts can be re-enabled at any time and timeframes for auto-disabling can be customized.

Custom Investigation Memorandums (April 2024)
Allows users to quickly document investigations and manager outreach within the platform. This new functionality also allow users to document investigations that are initiated outside the application for a streamlined investigation process.

COMING INNOVATION

High Risk User Monitoring
Leveraging One ID technology and our UEBA anomaly detection, monitor your high-risk users on your dashboard and immediately investigate.

SailPoint Integration
Leverage an API integration with SailPoint to launch a workflow upon the creation of an alert in DII.

User Notifier/First Time Offender workflows
Expand upon the current "Delegated Incident Review" workflow to include auto-provisioning of users (managers, end users, etc.), use of updated memo templates, identification of first-time and repeat offenders, and enhanced governance reporting.

Investigation List
New Bulk Actions and customizable Views on "Investigation List" page, replacing all functionality on classic screens.

Report Results – Details & Access Reports
Updated report results screens for Detailed and Access report types to improve performance and expand functionality.

Redesigned Report Builder
All new user interface for the application's report builder, improving performance and enhancing ease of use.

VIP / Watchlist
Create user and patient lists to flag VIP patients or suspicious users for more targeted monitoring in dashboards and reports.

User Risk Dashboard Workflow
Monitor high risk users, drill into access details, and open an investigation from a configurable dashboard widget.

imprivata®

Roadmap Update

Privileged Access Security

Vendor Privileged Access Management | Customer Privileged Access Management | Privileged Access Management

Overview

Imprivata's Privileged Access Security suite enables organizations to holistically and seamlessly manage and secure all privileged access – whether remote access from vendors, internal users, or outbound to customers.

- **Comprehensive, enterprise-grade remote access**
- **Third-party identity management & onboarding**
- **Credential management**
- **Session monitoring**
- **Least privilege**
- **Privileged account management**

Click here for more information

Return to Portfolio slide

RECENTLY RELEASED

Full, New User Interface (January 2025)
Experience a beautiful, modern UI and improved workflows that streamline navigation, processes and ensure information is easily and clearly available within Vendor Privileged Access Management.

Next-Gen Connection Manager (September 2024)
The next generation of the Connection Manager provides a more reliable and faster connection experience for users.

Containerized Network (September 2024)
Enable easy and streamlined access to users connecting to devices and thick clients with strict port requirements, such as PLCs, common in OT environments.

Improved Upgrade Process (September 2024)
Experience a faster and streamlined upgrade process that minimizes downtime and provides quicker access to new functionality and features.

Pre-Connection Notifications (May 2024)
Provide timely notifications during the connection process with application-specific information that vendor users need to know before connecting to an application.

Custom Application Access Request Forms (April 2024)
Capture custom information about access that your administrators need to make an informed decision when granting or denying access; common examples include case number or who approved access.

Access Request Reminder Notifications for Gatekeeper Admins (May 2024)
Automatically remind Gatekeeper Admins of pending requests on a configurable basis to reduce the need to reach out to remind customers and to facilitate quicker access approvals.

Beta for New VPAM UI (April 2024)
Experience and familiarize yourself with the brand-new UI in your sandbox environment; help shape future development with direct feedback to our Product Management team.

COMING INNOVATION

Credential Rotation & Job Engine
Improve the security around privileged credentials by automating password rotation based on certain events or time-based triggers, powered by a new job engine.

Access Request Workflows for Internal Users
Improve control over access to privileged assets by internal users by requiring users to request approval before access is granted.

Secret Unlock
Provide users with the permission to check-out and unlock credentials to view passwords for use cases where necessary – and ensure they are rotated after use to maintain credential security and peace of mind.

Full, New User Interface
Experience a beautiful, modern UI and improved workflows that streamline navigation, processes and ensure information is easily and clearly available within Customer Privileged Access Management.

HTML5 Client
Provide seamless and faster connectivity for users for RDP and SSH sessions directly in the browser, without the need to launch the Connection Manager.

Self-Managed Nexus Connections & Directory
Independently find, set up, enable and manage Nexus connections for vendors using Imprivata Customer Privileged Access Management for even faster connectivity.


imprivata®