



# Imprivata Produkt-Roadmap: Aktuelle Veröffentlichungen und geplante Innovationen

Stand: 28. Mai 2024

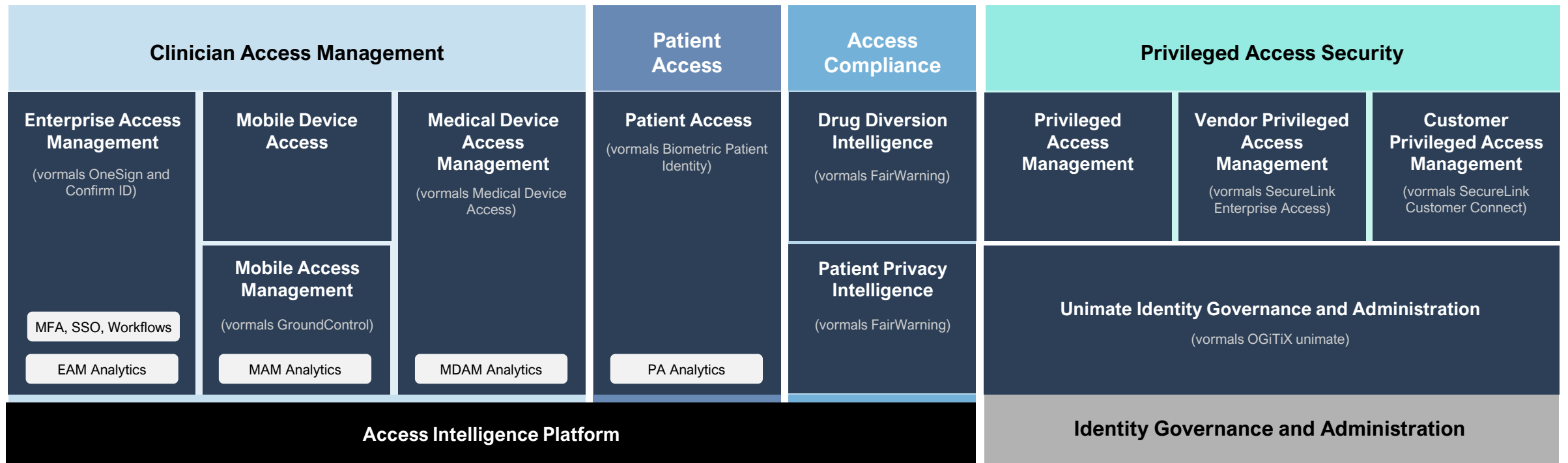




## **Ein Hinweis zu den zukunftsgerichteten Aussagen**

Die folgenden Aussagen beziehen sich auf geplante oder zukünftige Entwicklungsaktivitäten für unsere bestehenden oder neuen Produkte oder Services. Diese Aussagen sind nicht als Versprechen oder Garantie für die künftige Verfügbarkeit von Produkten, Services oder Funktionen zu verstehen und geben keine Auskunft darüber, wann oder wie bestimmte Funktionen preislich gestaltet oder gebündelt werden. Diese geplanten und zukünftigen Entwicklungsaktivitäten basieren auf Faktoren, die uns zum Zeitpunkt der Veröffentlichung bekannt sind, und können sich ohne vorherige Ankündigung ändern. Kaufentscheidungen sollten nicht im Vertrauen auf diese Aussagen getroffen werden. Wir übernehmen keine Verpflichtung, diese zukunftsgerichteten Aussagen zu aktualisieren.“

# Imprivata Access Management Portfolio



## Enterprise Access Management (vormals OneSign und Confirm ID)

### Übersicht

Imprivata Enterprise Access Management (EAM) bietet SSO und Benutzerauthentifizierung, um einen schnellen und sicheren Zugang zu den Geräten, Anwendungen und Arbeitsabläufen zu ermöglichen, die Kliniker und Mitarbeiter an vorderster Front benötigen, um Patienten zu versorgen und ihre Produktivität zu steigern. Die Funktionen umfassen:

- SSO an bestehende und standardbasierte Anwendungen
- Zugriff auf gemeinsam genutzte Workstations, angeschlossene medizinische Geräte und virtuelle Desktops per Badge-Tap
- Re-Authentifizierung für In-App-Arbeitsabläufe
- Sicherer und schneller Benutzerwechsel auf gemeinsam genutzten Workstations
- Vollständige EPCS-Konformität
- Flexible Authentifizierungsmethoden
- Umfassende Analyse der Zugriffsabläufe

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### Enterprise Access Management Analytics (Mai 2024)

Robuste Analysefunktionen bieten einen beispiellosen Einblick in SSO- und Benutzerzugriffsabläufe in Ihrem Unternehmen, was zu umsetzbaren Erkenntnissen führt, einschließlich der Identifizierung und Behebung potenzieller Sicherheitslücken sowie der Reduzierung des Betriebsaufwands und des IT-Overheads.

### Nummernabgleich zur Entschärfung von MFA-Fatigue-Angriffen (Oktober 2023)

Der Nummernabgleich für MFA ist für alle Imprivata EAM Remote-Zugriffs-Workflows verfügbar. Wenn diese Funktion aktiviert ist, müssen die Benutzer einen Code eingeben, der mit der Zufallszahl übereinstimmt, die in der aufgerufenen Anwendung angezeigt wird. Dies trägt dazu bei, MFA-Fatigue-Angriffe – eine häufige Phishing-Strategie – zu verhindern, indem das Risiko minimiert wird, dass Benutzer MFA-Push-Benachrichtigungen akzeptieren, die sie nicht initiiert haben.

### Mobiles EPCS mit Epic Haiku und Canto (Oktober 2023)

Imprivata Mobile EPCS ist branchenweit die einzige Lösung, die Gesichtsbioometrie zur Benutzerauthentifizierung unterstützt, um EPCS-Aufträge direkt vom mobilen iOS-Gerät eines Anbieters über Epic Haiku und Canto zu versenden. Dies ermöglicht ein einfacheres, effizienteres Verfahren für die Verschreibung kontrollierter Substanzen über ein mobiles Gerät und gewährleistet gleichzeitig die vollständige Einhaltung der DEA-Vorschriften.

### MFA-Integration mit Entra ID für bedingten Zugriff (Juli 2023)

Die Microsoft Entra ID-Richtlinien für den bedingten Zugriff können auf Imprivata MFA angewendet werden, um granulare Zugriffsrichtlinien zu unterstützen, MFA-Authentifikatoren zu konsolidieren, eine unkomplizierte und konsistentere Benutzererfahrung zu bieten und Sicherheitsrichtlinien weniger komplex zu gestalten.

### Erneuerung virtueller Smartcards per Self-Service (NHS England) (Juni 2023)

Kliniker können ihre auslaufenden virtuellen Smartcards selbst erneuern, um die zweijährige Verlängerungspflicht zu erfüllen, ohne sich an die Registrierungsadministratoren zu wenden. Dies spart Zeit und verringert den Aufwand.

## GEPLANTE INNOVATIONEN

### SSO-Integration mit Windows Hello for Business

Imprivatas Single Sign-On für Anwendungen kann mit Windows Hello for Business auf Einzelplatzrechnern verwendet werden, um eine passwortlose Windows-Anmeldung zu ermöglichen.

### Verbesserter Self-Service zum Zurücksetzen von Passwörtern

Die mobile App Imprivata ID MFA wird als zweiter Authentifizierungsfaktor für das Zurücksetzen von Passwörtern im Self-Service-Modus integriert und bietet so ein höheres Maß an Passwortsicherheit.

### Integration mit Epic Monitor für schnellen Zugriff auf digitale Whiteboards

Kliniker können das digitale Whiteboard mit ihrem Ausweis antippen, um ein Dashboard mit wichtigen Informationen für den Benutzer und seine Rolle anzuzeigen. Dies ermöglicht einen schnellen und sicheren Zugriff auf Patientendaten, ohne dass eine vollständige Anmeldung bei der Epic-Desktop-Anwendung erforderlich ist.

### Integration mit Microsoft Azure Virtual Desktops

Integrierter Badge-Tap-Zugriff auf gemeinsam genutzte und private virtuelle Azure-Desktops.

### Android-Unterstützung für Mobile EPCS für Epic Haiku und Canto

Erweitert die Nutzung der Gesichtsbioometrie für die EPCS-Signierung von einem mobilen Gerät (über Epic Haiku und Canto) auf Android-Geräte. Das bietet Dienstleitern mehr Flexibilität bei der Verschreibung von kontrollierten Substanzen von einem mobilen Gerät aus.

### Unterstützung virtueller Smartcards für Care Identity Service Passcode (NHS England)

Optionale Funktion, die es ermöglicht, alle neu erstellten virtuellen Smartcards mit dem vom Endnutzer bereitgestellten CIS-Passcode zu verschlüsseln. Sie unterstützt verbesserte Sicherheitsstandards für die landesweite Authentifizierung und den Zugriff innerhalb des NHS England.

### macOS-Unterstützung

Imprivata-Agent für Tap and Go und EPCS-Signierung auf privaten und gemeinsam genutzten macOS-Computern.

### Anmeldeunterstützung für Epic SAML

SAML-basierte integrierte Authentifizierung in Epic Hyperdrive für höhere Anwendungssicherheit.

### Automatisierte biometrische Freigabe für EPCS (Electronic Prescription of Controlled Substance)

Stellen Sie die Einhaltung staatlicher und bundesstaatlicher Vorschriften sicher, indem Sie die biometrische Freigabe in EPCS und andere Registrierungsabläufe einbinden.

# Mobile Device Access

## Übersicht

Imprivata Mobile Device Access löst das Versprechen von kompromissloser Sicherheit und Effizienz ein und beseitigt die Barrieren für den Zugriff auf gemeinsam genutzte Android-Geräte durch

- **sicheren, personalisierten Zugriff auf Android-Geräte**
- **Single Sign-On für mobile Anwendungen**
- **schnellen Benutzerwechsel mit Badge-Tap auf dem Gerät**

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### **Mobile Device Access Analytics über die EAM-Analyseplattform (Mai 2024)**

Robuste Analysefunktionen bieten einen beispiellosen Einblick in die Benutzerzugriffsabläufe in Umgebungen mit gemeinsam genutzten mobilen Geräten, um umsetzbare Erkenntnisse zu gewinnen, Sicherheitslücken zu beseitigen und den Betriebsaufwand sowie IT-Overheads zu verringern.

### **Schnellere Zusammenarbeit in Pflegeteams mit Unterstützung für native Dialer-Anwendungen (März 2024)**

Mobile Device Access unterstützt jetzt die Nutzung von Samsung- und Zebra-Dialer-Anwendungen, um einen schnellen und sicheren Zugriff auf Anrufe und Benachrichtigungen auf gemeinsam genutzten Geräten zu ermöglichen.

### **Verbesserte Diagnose und Fehlersuche (März 2024)**

Benutzer können die Konfiguration und Konnektivität der Mobile Device Access-App direkt vom Sperrbildschirm aus überprüfen und Protokolle zur Fehlerbehebung über das Tool übermitteln.

### **Unterstützung für neue Android-Anwendungen (März 2024)**

Zu den jüngsten Highlights gehört die Integration mit Tiger Connect, Dr. First, Microsoft Edge Browser und anderen.

### **Einfaches Anmelden in und Abmelden aus Cerner-Anwendungen (September 2023)**

Stellen Sie sicher, dass Klinikmitarbeiter schnell und sicher auf die benötigten Tools zugreifen können.

### **Unterstützung internationaler Sprachen (Februar 2023)**

Unterstützt Kunden, auf deren Geräten das Betriebssystem in der Landessprache läuft, und bietet Unterstützung für die Übersetzung von Zeichenketten in die Landessprache.

## GEPLANTE INNOVATIONEN

### **Sicherer Zugang zu weiteren Umgebungen und Anwendungsfällen**

Unterstützt Android-Workstations und Geräte mit externen Ausweislesern.

### **Konsistente Arbeitsabläufe unabhängig von der Konnektivität bereitstellen**

Unterstützung des „Offline-Modus“, um den Gerätezugriff zu ermöglichen, wenn keine Netzverbindung besteht.

# Mobile Access Management

(vormals GroundControl)

## Übersicht

Imprivata Mobile Access Management ist eine umfassende End-to-End-Mobilitätslösung, die Unternehmen hilft, den Einsatz gemeinsam genutzter iOS- und Android-Geräte zu optimieren. Dazu bietet sie

- **sicheres Abmelden von Geräten**
- **einfachen Zugriff auf mobile Anwendungen**
- **personalisierte Geräteerfahrungen**
- **Einblick in Gerätestatus und -zuweisung**
- **automatisierte Arbeitsabläufe für die Geräteverwaltung**

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### **Schnelle und einfache Ausweisregistrierung über mobile Geräte (Februar 2024)**

Nutzer können nun direkt in der Locker-App beim Check-out neue bzw. Ersatzausweise von Imprivata registrieren.

### **SAML-Einrichtung per Self-Service (Februar 2024)**

Administratoren können jetzt den Identitätsverbund mit ihrem Enterprise Identity Provider selbst konfigurieren.

### **Unterstützung für neue Android-Anwendungen, MDMs und MDM-Launcher (Februar 2024)**

Zu den jüngsten Highlights gehören die Anwendungen Tiger Connect und Voalte One, SOTI und Samsung Knox MDMs sowie Microsoft Intune Managed Home Screen und VMware Workspace ONE Launcher für Locker Android.

### **Überwachen Sie die Betriebsbereitschaft von Geräten und lösen Sie Probleme schnell mit Heartbeat (November 2023)**

Überwachen Sie die Betriebsbereitschaft der Locker-App und priorisieren Sie Geräte mit aktivem Heartbeat. Dashboard-Transparenz und **Bulk-Deployment** erleichtern Administratoren die schnelle Problembeseitigung aus der Cloud.

### **Einfaches Anmelden in und Abmelden aus Cerner-Anwendungen auf Android (August 2023)**

Sorgen Sie dafür, dass Klinikmitarbeiter schnell und sicher auf die benötigten Tools zugreifen können.

### **Zero-Touch-Bereitstellung und mehr Sicherheit auf Microsoft Intune (iOS) (August 2023)**

Überfällige Geräte können jetzt in den iOS-Modus „Verloren“ versetzt werden, um das Gerät mit Anweisungen zur Rückgabe zu sperren und den Standort an Intune zu übermitteln.

### **Unterstützung für Microsoft Shared Device Mode (August 2023)**

Automatisches An- und Abmelden unterstützter Apps auf Geräten, die für den Shared Device Mode konfiguriert sind, beispielsweise Teams.

### **Asset Management und Tracking für mobile Android-Geräte (Mai 2023)**

Nutzen Sie die Identitäts- und Asset-Management-Funktionen von Mobile Access Management auf ausgewählten Geräten von Zebra, Spectralink, Ascom, Honeywell und Samsung.

### **Proaktives Asset Management mit verbessertem Dashboard und Device-Home-Attributen. (Mai 2023)**

Administratoren erkennen schnell, wo sie handeln müssen, und ergreifen Maßnahmen, einschließlich Status auf Systemebene und Geräte nach Check-out-Status.

## GEPLANTE INNOVATIONEN

### **Native Epic Rover Logout**

Aktualisieren Sie den Anwesenheitsstatus eines Benutzers in Epic, wenn Geräte eingecheckt werden, damit keine irrelevanten Warnmeldungen an eingecheckte Geräte gesendet werden.

### **Vereinfachter Geräte-Check-out mit Konfiguration der Smart Hub LEDs**

Administratoren können jetzt die blaue LED (Bereitstellung läuft) in der Workflow-Aktion „Check-Out“ deaktivieren.

### **Indikatoren für den Verlust der Netzverbindung**

Überwachung der Netzwerkverbindung auf eingecheckten Geräten mit visueller Anzeige, wenn das Telefon die Netzwerkverbindung verliert.

### **Automatischer Start einer Android-Anwendung beim Check-out**

Administratoren haben nun die Möglichkeit, eine Anwendung wie Microsoft Teams so zu konfigurieren, dass sie nach dem Check-out automatisch startet, um so das Benutzererlebnis zu verbessern.

### **Geräteaktualisierungen in großem Umfang vereinfachen**

Unterstützen Sie die Massendehysterung und Stilllegung von Geräten für eine schnellere Time-to-Value durch Geräteaktualisierungen.

### **Optimierte und sichere Check-out-Workflows**

Stimmen Sie die Sicherheitsanforderungen zwischen Enterprise Access Management und Mobile Access Management ab, um den Check-out zu optimieren und die Sicherheit sowie das Sicherheitsmanagement zu verbessern.

### **Launchpad-Verwaltung und -Konfigurationen vereinfachen**

Entwickeln Sie organisationsspezifische, vorkonfigurierte Launchpad-Installationen, um eine manuelle Konfiguration überflüssig zu machen.

### **Umfassende Analysen**

Verbessern Sie Berichterstattung und Analysen mit mehr Daten, anpassbaren Dashboards und proaktiver Problemerkennung.

# Patient Access

(vormals Imprivata Biometric Patient Identity)

## Übersicht

Bei der Entwicklung von Imprivata Patient Access wurde größter Wert auf den Datenschutz gelegt. Die Gesichtserkennungslösung verbessert Patientensicherheit und -erlebnis, indem sie den Check-in optimiert und Patienten über ein einziges Foto exakt mit ihren Krankenakten verknüpft. So trägt sie zu einer effizienten und fehlerfreien Gesundheitsversorgung bei.

- **Höhere Genauigkeit bei der Patientenidentifizierung**
- **Verbesserte Patientensicherheit und optimiertes Patientenerlebnis**
- **Optimierte Arbeitsabläufe in der Patientenmeldung**
- **Flexible Hardware**
- **Nahtlose Integration mit Epic**

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

**Verbesserte Funktion zur wiederholten Aufnahme von Fotos (Mai 2024):** Wenn das erste Foto Probleme aufweist wie geschlossene Augen, können Sie die Fotos der Patientenmeldung problemlos wiederholen. Diese Flexibilität trägt dazu bei, das Patientenfoto zu verbessern.

**Smart Workflow Management (April 2024):** Fordert den Mitarbeiter in der Patientenmeldung je nach Status des Patienten auf intelligente Weise auf, die entsprechende Aktion durchzuführen – also anmelden oder verifizieren. Dadurch werden die Anmelde- und Check-in-Prozesse optimiert.

**Gesichtserkennung zur Patientenidentifizierung (Februar 2024):** Mit Imprivata Patient Access können Gesundheitseinrichtungen jetzt Sicherheit und Komfort für ihre Patienten verbessern, indem sie die Patienten über ein einfaches Gesichtsfoto mit ihrer Patientenakte verknüpfen. Durch Eins-zu-Eins-Zuordnung zwischen Patient und Patientenakte können Gesundheitsorganisationen eine optimale Versorgung sicherstellen und ihre betriebliche Effizienz steigern.

## GEPLANTE INNOVATIONEN

**Integration mit bestehenden Epic-Fotos:** Optimieren Sie den Anmeldeprozess, indem Sie bereits vorhandene Patientenfotos aus Epic nutzen. Diese Funktion macht eine persönliche Anmeldung überflüssig, ermöglicht sofortigen Zugriff und steigert die betriebliche Effizienz deutlich, wodurch die Time-to-Value beschleunigt wird.

**Self-Service-Identifizierung:** Durch die Integration in Epic Welcome Kiosks können sich Patienten selbst identifizieren, was die Arbeit der Mitarbeiter in der Patientenmeldung erheblich erleichtert und den Check-in-Prozess beschleunigt.

**Dublettenprüfung:** Als zusätzliche Sicherheit zur Vermeidung von Fehlern bei der Identitätsfeststellung hilft Imprivata Patient Access sicherzustellen, dass jedes Gesicht nur einmal erfasst wird. (Ermöglicht die Anmeldung von eineiigen Zwillingen.) Diese wichtige Funktion trägt dazu bei, eine Eins-zu-Eins-Übereinstimmung zwischen Patient und zugehöriger Krankenakte zu gewährleisten.

**Hochentwickelte Betrugserkennung mittels Liveness Checks:** Verstärken Sie die Sicherheitsmaßnahmen durch hochentwickelte Funktionen zur Liveness- und Spoofing-Erkennung, um sicherzustellen, dass das System mit einer echten Person und nicht mit einem betrügerischen Abbild interagiert.

**Konfigurierbares Anmeldealter:** Passen Sie das Anmeldeverfahren für Patienten an und legen Sie ein Mindestalter für die Anspruchsberechtigung in Gesundheitseinrichtungen fest, um Compliance und Standards in der Patientenversorgung zu gewährleisten.

**Berichterstattung nach Standort:** Erhalten Sie wertvolle Einblicke mithilfe von Berichtsfunktionen, die es Unternehmen ermöglichen, die Nutzungs- und Leistungskennzahlen für jeden Standort individuell zu analysieren.

**Bildoptimierung zum Schutz von Patientendaten:** Optimieren Sie die Bildpräsentation, indem Sie die Hintergründe zuschneiden und unscharf machen, um den Fokus ausschließlich auf den Patienten zu legen. Dies dient dem Schutz der Privatsphäre und verbessert die Klarheit der Identifikationsfotos.

# PatientSecure

## Übersicht

Imprivata PatientSecure nutzt biometrische Handvenenerkennung, um Patienten eindeutig und sicher zu identifizieren, Identitätsfehler zu reduzieren, Betrug zu verhindern und die Effizienz der Arbeitsabläufe in Gesundheitssystemen zu verbessern. Diese berührungslose Authentifizierungslösung gewährleistet eine eindeutige Patientenidentifizierung an jedem Punkt der Behandlung und erhöht die Patientensicherheit und -zufriedenheit.

- **Eindeutige Patientenidentifikation**
- **Erhöhte Patientensicherheit**
- **Betrugsbekämpfung**
- **Optimierung von Arbeitsabläufen**

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

**Single-User Session-Support für Azure Virtual Desktop (Mai 2024)** - Ermöglicht PatientSecure den Zugriff auf entfernte Maschinen über das Remote Desktop Protocol (RDP).

## GEPLANTE INNOVATIONEN

**Database Performance Enhancements** - Verringert die Anzahl von SQL-Sperren und Timeouts, Berichte werden deutlich schneller ausgeführt.

**Anzeige des bevorzugten Patientennamens zur Verbesserung des Patientenerlebnisses** - Ermöglicht ein persönlicheres Patientenerlebnis beim Check-in.

**Verbesserte Admin-Konsole** - In der Verwaltungskonsole werden häufig durchgeführte Aktionen im Vordergrund angezeigt, um einen schnellen Zugriff zu ermöglichen und Arbeitsabläufe zu optimieren.

**Parallele Nutzung von PatientSecure und Imprivata Patient Access** - Epic-Kunden können bei der Anmeldung jederzeit entweder PatientSecure (Handvenenerkennung) oder Imprivata Patient Access (Gesichtserkennung) nutzen.



# Patient Privacy Intelligence

(vormals FairWarning)

## Übersicht

Imprivata Patient Privacy Intelligence (PPI) trägt zum Schutz der Privatsphäre von Patienten bei und liefert verwertbare Erkenntnisse für die Untersuchung, Dokumentation und Meldung von Datenschutzverletzungen. Ausgestattet mit künstlicher Intelligenz (KI), maschinellem Lernen und Verhaltensanalysen bietet PPI Gesundheitsorganisationen die Tools, die sie benötigen, um Vorschriften zuverlässig einzuhalten, Patientendaten zu schützen und Verstöße zu verhindern

- **Proaktives und reaktives Auditing**
- **Zuverlässige Berichterstattung**
- **Effiziente Untersuchungen**

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### **Automatische Deaktivierung von Enduser-Konten (Mai 2024)**

Benutzerkonten von Anwendungsnutzern, die innerhalb der letzten 180 Tage nicht angemeldet wurden, werden jetzt automatisch deaktiviert, um die Sicherheit zu erhöhen. Die Benutzerkonten werden nicht gelöscht, und die Prüfhistorie bleibt davon unberührt. Benutzerkonten können jederzeit wieder aktiviert und die Zeitspannen für die automatische Deaktivierung individuell angepasst werden.

### **Kundenspezifische Untersuchungsberichte (April 2024)**

Ermöglicht Benutzern die schnelle Dokumentation von Untersuchungen und die Kontaktaufnahme mit Managern innerhalb der Plattform. Diese neue Funktion ermöglicht es den Nutzern auch solche Untersuchungen zu dokumentieren, die außerhalb der Anwendung initiiert werden, um den Untersuchungsprozess zu straffen.

### **2015 Edition Cures Update Zertifizierung (März 2024)**

Zertifizierung von Imprivata PPI Version 24 nach Update der Cures-Edition 2015, um es einfacher zu machen, PPI für die modulare Zertifizierung nach festgelegten Kriterien zu nutzen. Informationen zur Zertifizierung finden Sie unter Imprivata [ONC Certification Disclosures](#).

### **Erfahrungsberichte Task-Status (Februar 2024)**

Neue, aktualisierte Benutzeroberfläche für den Task-Status-Bildschirm mit verschiedenen Updates zur Verbesserung von Gesamtleistung und Navigation.

### **Verbesserte Anwendungsleistung (Januar 2024)**

Verbesserte Anwendungsnavigation senkt die Ladezeiten des Bildschirms um bis zu 60%. Beschleunigung der Arbeitsabläufe und Schaffung eines besseren Gesamterlebnisses.

### **Optionen für den Zeitrahmen des Governance-Berichts (September 2023)**

Neue Ergänzungen zum Governance Report Builder, um bei der Auswahl der Within Timeframe Comparators nach längeren Zeiträumen zu filtern.

### **Aktualisierungen der Benutzeroberfläche für ein besseres Benutzererlebnis (Juli & August 2023)**

Updates der Berichtsseite, um Massenaktionen durchzuführen, und Aktualisierungen des Governance-Seitenlayouts, um es an das Berichtsseitenlayout anzupassen. Aktualisierung auf einen einzigen Enforced Policies-Bildschirm (erzwungene Richtlinien) verbessert Benutzererlebnis und Leistung. Neuer Bildschirm in den Application Settings (Anwendungseinstellungen) zur Anzeige der Application Version History (Versionsverlauf der Anwendung) hinzugefügt und Dashboard „Alerts by“ (Alarmer nach) zur besseren Anzeige von „Alerts by Owner“ (Alarmer nach Eigentümern) aktualisiert.

## GEPLANTE INNOVATIONEN

**First Access Reporting** - ermöglicht Kunden die Erstellung von benutzerdefinierten Berichten über First Access-Daten mit Bewertungen und Erläuterungen für erweiterte Prüfungsfunktionen.

**Internationalisierung des Machine Learning Closing Model** - Bereitstellung des kompletten Funktionsumfangs des maschinellen Lernens für unsere internationalen Kunden zur Optimierung der internen Zugangsprüfung.

**Dashboard Filtering and Library** – Optimierung der Arbeitsabläufe von Benutzern und Analysten mit der Möglichkeit, Benutzer mittels Peer-Clustering einzustufen, um zu bestimmen, welche Benutzer das größte Risiko darstellen.

**Aktualisierung Multi-factor Authentication (MFA) und Password Reset** – Aktualisierungen der Arbeitsabläufe von MFA und Kennworrücksetzungen für ein besseres Benutzererlebnis und mehr Sicherheit. Dies ist auch ein erster Schritt, um den Kunden einen Single Point Login für Plattformintegrationen zu bieten.

**Imprivata Cloud Portal (ICP) Integration** – Optimierung des Benutzererlebnisses durch Bereitstellung einer ganzheitlichen Imprivata Cloud Plattform.

# Drug Diversion Intelligence

(vormals FairWarning)

## Übersicht

Imprivata Drug Diversion Intelligence (DDI) hilft Unternehmen, die Abzweigung von Arzneimitteln zu kontrollieren, um ihre Patienten, Mitarbeiter und ihr Unternehmen zu schützen und gleichzeitig die wichtigsten behördlichen Anforderungen für die Verwaltung kontrollierter Substanzen zu erfüllen.

- **Überwachung des Lebenszyklus von Arzneimitteln**
- **Überwachung von Anwendungsfällen**
- **Ermittlungsmanagement**

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### **Automatische Deaktivierung von Endbenutzerkonten (Mai 2024)**

Benutzerkonten von Anwendungsnutzern, die innerhalb der letzten 180 Tage nicht angemeldet wurden, werden jetzt automatisch deaktiviert, um die Sicherheit zu erhöhen. Die Benutzerkonten werden nicht gelöscht, und die Prüfhistorie bleibt davon unberührt. Benutzerkonten können jederzeit wieder aktiviert und die Zeitspannen für die automatische Deaktivierung individuell angepasst werden.

### **Kundenspezifische Untersuchungsberichte (April 2024)**

Ermöglicht Benutzern die schnelle Dokumentation von Untersuchungen und die Kontaktaufnahme mit Managern innerhalb der Plattform. Diese neue Funktion ermöglicht es den Nutzern auch solche Untersuchungen zu dokumentieren, die außerhalb der Anwendung initiiert werden, um den Untersuchungsprozess zu straffen.

### **Erfahrungsberichte Task-Status (Februar 2024)**

Neue, aktualisierte Benutzeroberfläche für den Task-Status-Bildschirm mit verschiedenen Aktualisierungen zur Verbesserung von Gesamtleistung und Navigation.

### **Verbesserte Anwendungsleistung (Januar 2024)**

Verbesserte Anwendungsnavigation senkt die Ladezeiten des Bildschirms um bis zu 60%. Beschleunigung der Arbeitsabläufe und Schaffung eines besseren Gesamterlebnisses.

### **Optionen für den Zeitrahmen des Governance-Berichts (September 2023)**

Neue Ergänzungen zum Governance Report Builder, um bei der Auswahl der Within Timeframe Comparators nach längeren Zeiträumen zu filtern.

### **Aktualisierungen der Benutzeroberfläche für ein besseres Benutzererlebnis (Juli & August 2023)**

Aktualisierungen der Berichtsseite, um Massenaktionen durchzuführen, und Aktualisierungen des Governance-Seitenlayouts, um es an das Berichtsseitenlayout anzupassen. Aktualisierung auf einen einzigen Enforced Policies-Bildschirm verbessert Benutzererlebnis und Leistung. Neuer Bildschirm in den Application Settings zur Anzeige der Application Version History hinzugefügt und Dashboard „Alerts by“ (Alarmer nach) zur besseren Anzeige von „Alerts by Owner“ (Alarmer nach Eigentümer) aktualisiert.

## GEPLANTE INNOVATIONEN

**Device Cluster Management** – Erkennen Sie Trends bei Benutzern sowie potenzielle Anomalien, um Medikamentenabzweigungen zu bekämpfen. Dabei ist es möglich, kundenspezifische Vergleichsgruppen zu definieren.

**Benutzerbasiertes Risikomodell und KI-Konfiguration** – Optimieren Sie Benutzer- und Analystenarbeitsabläufe mit der Leistungsfähigkeit von KI. Bieten Sie die Möglichkeit, Benutzer mit Peer-Clustering einzustufen, um zu bestimmen, welche Benutzer das größte Risiko darstellen.

**Dashboard Filtering and Library** - Optimieren Sie die Arbeitsabläufe von Anwendern und Analysten mit der Möglichkeit, Anwender mit Hilfe von Peer Clustering einzustufen, um zu bestimmen, welche Benutzer das größte Risiko darstellen.

**Aktualisierungen von Multifaktor-Authentifizierung (MFA) und Password Reset** – Aktualisierungen der Arbeitsabläufe von MFA und Kennworrücksetzungen für ein besseres Benutzererlebnis und mehr Sicherheit. Dies ist auch ein erster Schritt, um den Kunden einen Single Point Login für Plattformintegrationen zu bieten.

**Imprivata Cloud Portal (ICP) Integration** - Optimierung des Benutzererlebnisses durch Bereitstellung einer ganzheitlichen Imprivata Cloud Plattform.

# Privileged Access Management

## Übersicht

Imprivata Privileged Access Management (PAM) ist eine umfassende, einfach zu bedienende Lösung für das Managen privilegierter Zugriffe, die privilegierte Accounts vor unberechtigtem Zugriff schützt. Sie bietet Transparenz und Kontrolle über den privilegierten internen Zugriff und schützt privilegierte Anmeldeinformationen, um Datenschutzverletzungen oder Cyberangriffe zu verhindern.

- Sichere privilegierte Konten
- Privilegierte Passwörter verwalten
- Sitzungsaktivität überwachen
- Einhaltung der Vorschriften nachweisen
- Privilegierte Identitäten überprüfen
- Moderne Architektur

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### **Dynamische und Pass-Through-Anmeldedaten mit PAM-Web-Erweiterung (März 2024)**

Benutzer können sich schnell bei einer Website anmelden, indem sie über die PAM-Web-Erweiterung Tresor-geschützte Anmeldeinformationen dynamisch einfügen.

### **Neues Modul für Verbundanmeldungen (Februar 2024)**

Das neue Modul für Verbundanmeldungen bietet eine verbesserte Anmeldeseite, ist leistungsfähiger und verbessert die Backend-Sicherheit.

### **Sofortige Videowiedergabe mit Einblendung von Sitzungsereignissen (Dezember 2023)**

Verstehen Sie schnell und einfach, was ein Benutzer in einer Sitzung getan hat, ohne durch mehrere Berichte navigieren zu müssen. Eine Ereigniszeitleiste wird über die sofortige Videowiedergabe gelegt und zeigt die Aktivitäten des Benutzers an.

### **MFA-Karenzzeit (September 2023)**

Definieren Sie eine konfigurierbare Karenzzeit für die MFA-Durchsetzung, um Benutzern ein optimiertes Erlebnis bei der Verwendung des Produkts zu bieten und gleichzeitig die Sicherheit zu gewährleisten.

### **Tresor-basierte Datensatztypen (September 2023)**

Datensatztypen können bestimmten Tresoren zugewiesen werden. So haben Administratoren eine bessere Kontrolle darüber, durch wen, wo und wie Datensätze erstellt werden können. Dies erleichtert den Benutzern die Auswahl des Datensatztyps.

### **Unterstützung für Microsoft Entra ID (Azure) Konten (August 2023)**

Verwalten Sie gemeinsam genutzte oder privilegierte Entra ID-Konten innerhalb von Imprivata PAM. Führen Sie die Passwortrotation automatisch nach Bedarf oder nach einem definierten Zeitplan durch und eliminieren Sie so den manuellen Rotationsaufwand für diese Konten.

### **Session Relay Node mit zusätzlicher Unterstützung für RDP und SSH-Proxy (Mai 2023)**

Benutzer können über ihren ausgewählten Relay-Knoten von ihrer nativen RDP- oder SSH-Proxy-Sitzung aus eine Verbindung herstellen. Dies reduziert die Latenzzeit bei Zugriffen in mehreren Regionen.

### **Verfügbarkeit Deutsch (März 2023)**

Die Benutzer können das Imprivata PAM-Webportal jetzt auf Deutsch einstellen, um das Benutzererlebnis zu verbessern.

## GEPLANTE INNOVATIONEN

**Azure-Token-Authentifizierung für MSI-Konten** – Ermöglicht mit MSI-Konten verknüpfte Azure-Token, die sich über API-Aufrufe bei PAM authentifizieren und so eine nahtlose Authentifizierung für den Benutzer ermöglichen.

**Updates der SSH-Komponente** – Updates der zugrundeliegenden SSH-Komponente ermöglichen eine schnellere Verbindung zu Sitzungen und das Zurücksetzen von Passwörtern und Schlüsseln sowie den Zugriff auf moderne Schlüssel und Algorithmen. Zudem verbessern sie die Sicherheit.

**Multi-Account-Verwaltung** - Führt Hochverfügbarkeit für die Rotation von privilegierten Konten ein, um die Anforderungen von Systemen zu erfüllen, die für die Authentifizierung absolut ausfallsicher sein müssen.

**Virtuelle Azure-Desktop-Sitzungen** – Bieten Sitzungen sichere Verbindungen zu virtuellen Azure-Desktops, einschließlich Berechtigungs- und Workflow-Durchsetzung, Sitzungsaufzeichnung und zuverlässiger Überwachung.

# Vendor Privileged Access Management

(vormals SecureLink Enterprise Access)

## Übersicht

Imprivata Vendor Privileged Access Management (VPAM) ist eine Remote-Access-Plattform, die es Unternehmen ermöglicht, den privilegierten Zugriff durch Dritte und die Anbindung an ihre internen, kritischen Systeme zu verwalten und zu sichern.

- Third-Party-Identitätsmanagement
- Onboarding von Anbietern
- Unternehmensweiter Remote-Zugriff
- Berechtigungsmanagement
- Zero-Trust-Netzwerkzugriff
- Session-Monitoring

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### Pre-Connection Notifications (Mai 2024)

Rechtzeitige Benachrichtigung während des Verbindungsaufbaus mit anwendungsspezifischen Informationen, die die Benutzer des Anbieters kennen müssen, bevor sie eine Verbindung zu einer Anwendung herstellen.

### Benutzerdefinierte Antragsformulare für den Anwendungszugriff (April 2024)

Erfassen Sie benutzerdefinierte Informationen zum Zugriff, die Ihre Administratoren benötigen, um eine fundierte Entscheidung über die Gewährung oder Verweigerung des Zugriffs zu treffen. Häufige Beispiele sind die Fallnummer oder der Name der Person, die den Zugriff genehmigt hat.

### Neue UI, Beta-Version (April 2024)

Erleben Sie die brandneue Benutzeroberfläche in Ihrer eigenen Sandkastenumgebung und machen Sie sich mit ihr vertraut. Helfen Sie mit, die künftige Entwicklung durch direktes Feedback an unser Produktmanagementteam zu gestalten.

### Gateway Pool Management (Januar 2024)

Aktualisierung einer Instanz in einem Gateway-Pool, um die sicherste und aktuellste Version beizubehalten, ohne bestehende Benutzersitzungen oder Verbindungen zu beeinträchtigen.

### Export des Admin-Protokolls (November 2023)

Exportieren Sie schnell und einfach die spezifischen Informationen, die Sie aus dem Admin-Protokoll benötigen, um Berichte über bestimmte Aktivitäten oder Ereignisse zu erstellen.

### Verfügbarkeit Deutsch (Mai 2023)

Benutzer, deren Standard-Browsersprache auf Deutsch eingestellt ist, sehen die VPAM-Benutzeroberfläche automatisch auf Deutsch, um die Benutzerfreundlichkeit zu erhöhen.

## GEPLANTE INNOVATIONEN

**Vollständig neue Benutzeroberfläche** – Erleben Sie eine ansprechende, moderne Benutzeroberfläche und verbesserte Arbeitsabläufe, die die Navigation und die Prozesse vereinfachen und sicherstellen, dass Informationen einfach und klar dargestellt werden.

**Neuer Connection Manager** – Die nächste Generation des Connection Manager bietet ein zuverlässigeres und schnelleres Verbindungserlebnis.

**Containerized Network** – Ermöglichen Sie Benutzern einen einfachen und optimierten Zugriff auf Geräte und Thick Clients mit strengen Portanforderungen, wie z. B. PLCs, wie sie in OT-Umgebungen üblich sind.

**Passwortrotation** – Verbessern Sie die Sicherheit rund um privilegierte Anmeldeinformationen, indem Sie die Passwortrotation basierend auf bestimmten Ereignissen oder zeitbasierten Auslösern automatisieren.

**Anzeige der aktiven Benutzersitzungen** – Sorgen Sie für mehr Transparenz hinsichtlich der Benutzeraktivitäten, indem Sie aktive Sitzungen nach Benutzer und nicht nach Anwendung anzeigen.

# Customer Privileged Access Management

(vormals SecureLink Customer Connect)

## Übersicht

Imprivata Customer Privileged Access Management (CPAM) ist eine Remote-Support-Plattform, die es Dienstleistern und Technologieanbietern ermöglicht, sich sicher mit den Umgebungen ihrer Kunden zu verbinden.

- **Umfassender, jederzeitiger Zugriff**
- **Berechtigungsmanagement**
- **Sitzungsaufzeichnung**
- **Vereinfachter Zugriff**
- **Zugriffskontrollen für Kunden**
- **Least-Privileged-Zugriff**

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### **Erinnerungsbenachrichtigungen zu Zugriffsanfragen für Gatekeeper-Administratoren (Mai 2024)**

Automatisieren Sie die Benachrichtigung von Gatekeeper-Administratoren über offene Anfragen auf konfigurierbarer Basis, um Kunden weniger häufig kontaktieren zu müssen und eine schnellere Bearbeitung von Zugangsgenehmigungen zu gewährleisten.

### **Gateway Pool Management (Januar 2024)**

Aktualisieren Sie eine Instanz in einem Gateway-Pool, um die sicherste und aktuellste Version beizubehalten, ohne bestehende Benutzersitzungen oder Verbindungen zu beeinträchtigen.

### **Individuelle Geschäftsbedingungen für Quick Connect (Dezember 2023)**

Wenden Sie Ihre eigenen Allgemeinen Geschäftsbedingungen an, die von allen Kunden akzeptiert werden müssen, denen Sie Quick Connect bereitstellen.

### **Export des Admin-Protokolls (November 2023)**

Exportieren Sie schnell die spezifischen Informationen, die Sie aus dem Admin-Protokoll benötigen, um Berichte über bestimmte Aktivitäten oder Ereignisse zu erstellen.

### **Gatekeeper-Host-Informationen (Juli 2023)**

Finden Sie schnell benötigte Gatekeeper-Host-Informationen wie Versionsinformationen und Speicherplatz, ohne sich selbst mit dem Gatekeeper selbst verbinden zu müssen. Lassen Sie sich einfach die Liste der Hosts anzeigen, auf denen ein bestimmter Gatekeeper installiert sein kann, um Duplikate zu identifizieren.

### **Unterstützung SDK Credential Token (Juni 2023)**

Verbessern Sie die Sicherheit von SDK-Verbindungen, indem Sie die Offenlegung verschlüsselter Anmeldeinformationen mithilfe von Credential Tokens für die Eingabe von Benutzernamen und Passwörtern verhindern.

## GEPLANTE INNOVATIONEN

**Neuer Connection Manager** – Die nächste Generation des Connection Manager sorgt für ein zuverlässigeres und schnelleres Verbindungserlebnis.

**Nexus-Service- und Statusabfrage** – Überprüfen Sie spontan die an Nexus-Standorten verfügbaren Dienste und deren Verbindungsstatus, ohne eine Verbindung herstellen zu müssen, um diese Informationen zu erhalten.

**Containerized Network** - Ermöglichen Sie einen einfachen und reibungslosen Zugriff für Benutzer, die eine Verbindung zu Geräten und Thick Clients mit strengen Portanforderungen wie PLCs herstellen, wie sie in OT-Umgebungen üblich sind.

**Neue Benutzeroberfläche** – Erleben Sie eine ansprechende, moderne Benutzeroberfläche und verbesserte Arbeitsabläufe, die die Navigation und die Prozesse vereinfachen und sicherstellen, dass Informationen einfach und klar dargestellt werden.

# Unimate Identity Governance and Administration

(vormals OGiTiX unimate)

## Übersicht

Imprivata Unimate Identity Governance and Administration (UIGA) automatisiert das Identity Lifecycle Management, ermöglicht eine Least-Privileged-Umgebung und rollenbasierten Day-One Access.

- Lebenszyklus-Governance
- Rollenbasierte Zugriffskontrollen
- Same-Day Access
- Least-Privilege-Durchsetzung
- Zugriffskontrolle
- Zertifizierung aktiver Benutzer

Klicken Sie hier, um weitere Informationen zu erhalten.

Zurück zur Folie „Portfolio“

## KÜRZLICH VERÖFFENTLICHT

### Mehrsprachigkeit (Freigabe im April 2024)

Unsere Lösung unterstützt jetzt Mehrsprachigkeit für alle Formulare und E-Mails und passt sich den Benutzereinstellungen an. Die verfügbaren Sprachen sind Englisch, Deutsch, Französisch, Spanisch, Italienisch, Niederländisch und Portugiesisch. Dies sorgt für ein nahtloses und personalisiertes Erlebnis für die Nutzer rund um den Globus.

### Verbesserte Leistung (April 2024)

Diese Upgrades sorgen für kürzere Antwortzeiten, eine reibungslosere Navigation und eine effizientere Vorgangsbearbeitung.

### Bridge-Integration(April 2024)

Diese Erweiterung ermöglicht es Ihnen, bestehende Bridges wie EPIC direkt in IGA zu nutzen. Durch die nahtlose Anbindung an Ihre aktuellen Systeme optimiert diese Integration das Zugriffsmanagement und verbessert die Interoperabilität. Damit ist ein kohärenter und effizienter Identitätsmanagementprozess für Ihre Anwendungen im Gesundheitswesen und darüber hinaus gewährleistet.

### Verbesserte Identitäts- und BOB-Dashboard Reporting (November 2023)

Die Benutzer können einfach aus einer Vielzahl von vorgefertigten Berichten auswählen oder eigene Berichte erstellen, die auf ihre speziellen Bedürfnisse zugeschnitten sind. Mit dieser neuen Funktion erhalten Sie detailliertere Einblicke und behalten einen umfassenden Überblick, wodurch Ihre Identitätsmanagementprozesse effizienter und transparenter als je zuvor werden.

### Verbesserte SAP HCM-Schnittstelle (Dezember 2023)

Diese Integration stellt sicher, dass Ihr SAP Human Capital Management (HCM) System harmonisch mit unserer IGA-Lösung zusammenarbeitet. Durch die Anpassung an Ihre Organisationsstruktur werden das Onboarding von Mitarbeitern, Rollenzuweisungen und Zugriffskontrollen optimiert. Dabei wird die Einhaltung von Vorschriften gewährleistet und gleichzeitig die Effizienz gesteigert.

### Verbesserte SAP-Benutzerverwaltungsoberfläche (Dezember 2023)

Diese Funktion ermöglicht eine nahtlose und effiziente Verwaltung von Benutzerkonten in verschiedenen SAP-Umgebungen. Durch die Automatisierung von Provisioning, Rollenzuweisung und Zugriffskontrolle werden Konsistenz und Compliance über den gesamten Lebenszyklus der Benutzer sichergestellt.

## GEPLANTE INNOVATIONEN

### SAP Success Factors-Schnittstelle

Diese Integration stellt sicher, dass Ihre SAP SuccessFactors-Anwendung harmonisch mit unserer IGA-Lösung zusammenarbeitet. Durch die Anpassung an Ihre Organisationsstruktur werden das Onboarding von Mitarbeitern, Rollenzuweisungen und Zugriffskontrollen optimiert. Dabei wird die Einhaltung von Vorschriften gewährleistet und gleichzeitig die Effizienz gesteigert.

**HR Data Transformation Wizard** – Visuelles Tool zur Integration verschiedener HR-Quellen über SQL, ODBC, CSV, XML in IGA und deren Nutzung für den Life Cycle Service

**Abstimmung** – Bleiben Sie dank Echtzeitwarnungen und detaillierten Berichten auf dem Laufenden, wenn manuelle Änderungen vorgenommen werden, und sorgen Sie so für volle Transparenz und Kontrolle. Wird eine unbefugte oder fehlerhafte Änderung festgestellt, können Sie schnell und einfach den vorherigen Stand wiederherstellen und so die Integrität Ihres Systems wahren.

**Neues Serviceportal** – Vollständig neu entwickeltes Serviceportal mit responsivem Design und Sicherheitsfunktionen, das als öffentliches Portal genutzt werden kann.

**IGA Cloud Service** – Wir stellen Ihnen die Möglichkeit vor, unsere IGA-Lösung als Cloud-Service zu nutzen und gleichzeitig Ihre lokale Infrastruktur zu verwalten. Dieser hybride Ansatz bietet die Flexibilität und Skalierbarkeit der Cloud und kombiniert sie mit der Kontrolle und Sicherheit von On-Premise-Systemen

**Multi-Contract-Support** – Native Unterstützung für mehrere Mitarbeiterverträge für eine Identität.

**Imprivata PAM Integration** - Verwaltung administrativer Konten innerhalb von Imprivata PAM

**Verwaltung von NIS-2 Terminen**– Nutzen Sie den IGA-Workflow zur Verwaltung einer NIS 2-Terminen, um sicherzustellen, dass die gesetzlichen Fristen eingehalten werden

**KI-gesteuerte Peer-Analyse** - KI-gesteuerte Peer-Analyse in Echtzeit für die Zugriffsvergabe. Wenn Ihre Rollen für eine neue Anwendung oder eine neue Benutzergruppe noch nicht vollständig entwickelt sind, kann es Zugriffskoordinatoren und Führungskräfte gestattet werden, die Zugriffsrechte ihrer Kollegen zu überprüfen, um in Echtzeit fundierte Entscheidungen darüber zu treffen, welche Zugriffe der jeweilige Benutzer benötigt.

 **imprivata**<sup>®</sup>

