EBOOK

Secure digital identities for all users, applications, and data

Provide “day one” automated access to an ever-growing number of technology assets while managing potential security and compliance risks with Imprivata Identity Governance

imprivata®

Introduction

As the enterprise business landscape continues to dramatically change, malicious hackers continue to look for increasingly vulnerable business systems, often starting with enterprises with poorly structured or monitored identity and access management (IAM) systems. Organizations often overlook critical vulnerabilities like inappropriate and outdated access and the risk it presents. Many organizations are still using manual processes for provisioning, de-provisioning, and conducting access certification that is extremely labor-intensive, time-consuming, inefficient, and unsecure.

Poor management of provisioning, role transition monitoring, and de-provisioning access for the joiners, movers, and leavers in an organization, can lead to:

01 **Employees accumulating permissions** beyond their normal functions. A single account that keeps acquiring privileges, could lead to “access creep,” creating a bloated account that makes an ideal target for hackers and insider threats.

02 **Poor offboarding**, which may allow former employees to keep permissions within an organization’s network for days and even months.

03 **Having users with the wrong permissions** constitutes a severe security risk, especially concerning unnecessary permissions.

04 **Delays in access** due to manual processes can lead to loss of user productivity and security risks.

05 **Audit fails**, by not having a system that documents and demonstrates access policy compliance to auditors.

Right now, IT, HR, and security teams are working in multiple systems to manage access requests, access reviews, and juggle help desk tickets. But what if there were a better way to manage the user lifecycle – from onboarding to job changes to offboarding – all while integrating with your workflow?

Avoid permission sprawl with day one provisioning and de-provisioning

On average, it takes **13 business days** for a new employee to be given access.	The process requires an average of **6.3 hrs** to create each account and provide access to the 16 common applications.*

- SecurityIntelligence

Automation of processes like employee onboarding and off-boarding can help IT save time and improve compliance. The absence of a proper user provisioning process may cause unnecessary confusion when new users come in as they would be blindsided by the end-user objects that are crucial for their role. On the flip side, allocating these access rights manually would give rise to redundancies in an IT administrator's work, as they are swamped with a variety of other tasks. It would impact the efficiency of both sides – admins and new users.

From streamlining the access management process to enhancing employee productivity and improving operational velocity, user provisioning will become a game-changer in your organization.

Imprivata Identity Governance increases user and staff productivity with automated, role-based access on day one as well as self-service account management. The solution provides same-day access to legacy and modern systems and applications – both on-prem and in the cloud – giving users the right resources to do their job at the right time. Imprivata Identity Governance leverages integrations with tools such as single sign-on software equipped with functionalities like multifactor authentication and more, allowing users to maintain productivity regardless of how quickly or how much their responsibilities change. With Imprivata Identity Governance, you can:

01 **Streamline provisioning** | Provision or de-provision access at any stage of the employee's identity lifecycle

02 **Improve approval workflows** | Validate key access assignment prior to automatic provisioning

03 **Certify active users** | Ensure appropriate access is verified on a regular basis

04 **Improve auditing and compliance** | Gain visibility to ensure the right people have access to the right things at the right times

"You can't protect what you can't see"

With new regulations and stricter protocols, organizations feel the strain of ensuring and proving compliance – so how can organizations make auditors love them?

All cybersecurity and identity management begins with visibility. Enterprises need a consistent framework to operationally manage and govern their rapidly expanding digital ecosystem and identity governance and administration is the critical piece to accomplish it.

Imprivata Identity Governance allows enterprises to embrace the benefits of hyper-connectivity while ensuring that only the right people have access to the right things at the right times, resulting in improved security and valuable insights about employee activity and needs that can help improve decision-making.

Create wonderful reports for auditors with one click

Applications, devices, data, and stakeholders are all linked through Imprivata Identity Governance. Consequently, the system can determine who has access to which information, device, and/or application, thus helping it in making access reports that are relevant to the questions that come up during regulatory auditing.

Ensure employees access only information they need to do their jobs and prevent them from accessing information that doesn't pertain to them.

Govern user access with policy-based controls

Role-based access control (RBAC) has become one of the most advanced methods for access control. It's difficult to predict which systems a user may access without having an individual monitor the usage. It's a common problem in user access setup that user provisioning solutions like Imprivata Identity Governance solve. The right solution ensures that access permissions are granted solely based on the user's role or job title in the organization.

Imprivata Identity Governance allows organizations to restrict network access based on an employee's role and provides them with only the access necessary to effectively perform their job duties. As a result, lower-level employees will not have access to sensitive data if they do not need it to fulfill their responsibilities. This is especially helpful for organizations that have a large volume of third parties and contractors that make it difficult to monitor network access closely.

ROLE-BASED ACCESS CONTROL WILL ALLOW ORGANIZATIONS TO SECURE SENSITIVE DATA AND ACCESS IMPORTANT APPLICATIONS.

"It was [the growth in users] that exposed some gaps in our IAM solution and other systems that led us to turn to Imprivata Identity Governance. We have around 40 or 50 employees who spend many hours each week entering new employees and setting up access to over 300 applications, dealing with changing roles and changes in access, including roles on the Epic side, PACS system, and imaging systems, all with different system administrators."

– Midwestern Health System

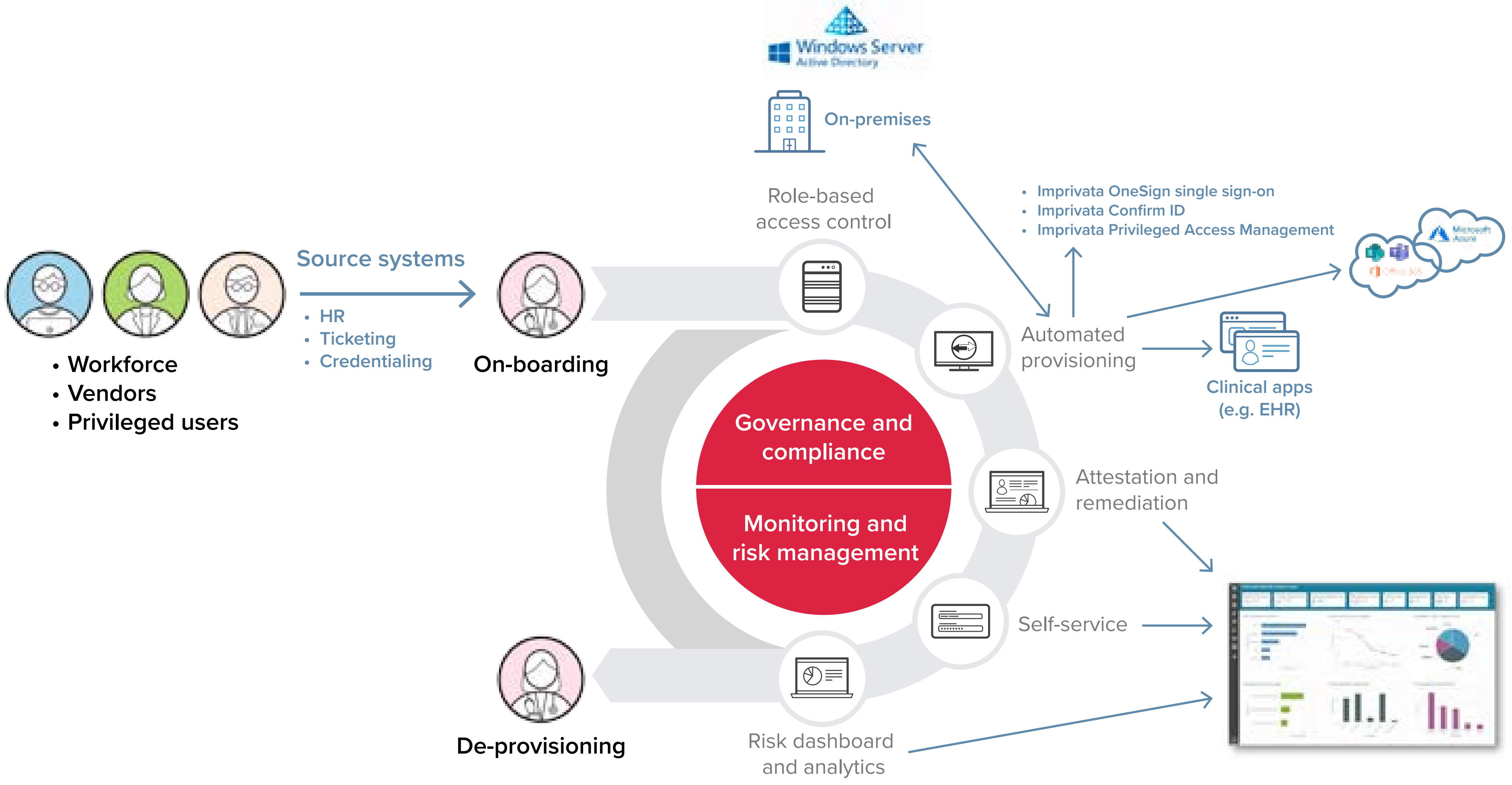
A plan driven by the experts, so you can get up and running fast

We not only understand the technology better than anyone, but we also understand your business and your industry. Our industry experts are your indispensable partners in achieving your organization's identity governance and administration goals.

Lasting value from technology investments can only be realized when capacity, consumption, cost, and performance are optimized. To help you keep your technology investment operating at peak performance, Imprivata Managed Services offers flexible and cost-effective subscription-based managed service solutions.

Our team of experts will provide insights and strategies to address your security and identity priorities and put emphasis on solving your most pressing challenges from day one. Our subscription-based managed services are delivered by a team of architects, engineers, and program managers that is not only highly skilled but has years of experience implementing our Imprivata Identity Governance solution in multiple facilities, environments, and continually changing technology stacks. You can feel confident in our ability to implement and scale our own identity technology to secure and protect your business.

Imprivata Managed Services eases the strain of managing mission-critical solutions at the enterprise scale, enabling you to focus on your core business. We work every day to continually be the first choice for safeguarding our customer's digital identity investments, while our industry experts serve as indispensable partners in reducing complexity and sustaining value.



How it works: The Imprivata Identity Governance architecture

Imprivata Identity Governance provides fast, secure role-based access to systems and offers capabilities such as automated provisioning and de-provisioning, standards-based integrations, custom integrations, access request management, entitlement management, password management, and detailed event logging, in the most efficient and secure way possible.

The time is now: Secure digital identities for all users, applications, and data

Identity governance should be viewed as an ongoing initiative, with focused, achievable goals along the way. This enables enterprises to become more secure, do more with less, and prepare for growth and change – no matter what form it takes. All while maintaining security and compliance.

And every journey starts somewhere. Request a demonstration today.

Identity governance should be viewed as an ongoing initiative, with focused, achievable goals along the way.

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com