

EBOOK

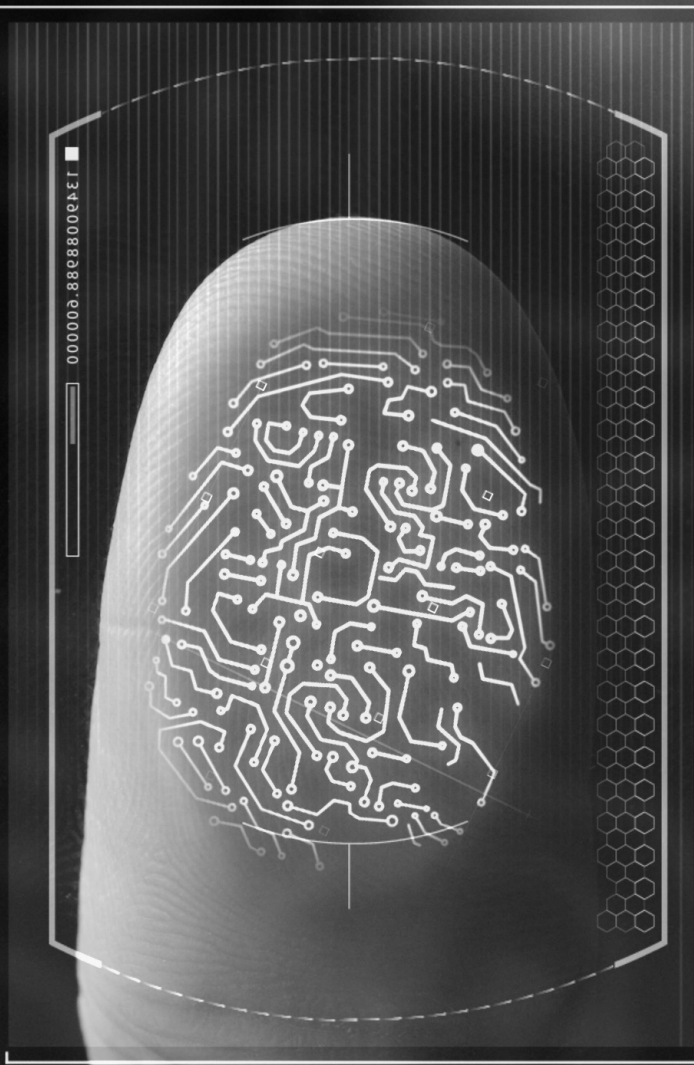
Automate Identity and Access Management Processes

Automate the user access lifecycle and secure all privileged access for internal and external identities.

 **imprivata**[®]



ΕΠΙΣΤΗΜΗ ΤΗΣ ΟΙΚΟΝΟΜΙΑΣ



Introduction

The lines continue to blur between who is inside the enterprise and who's outside it. There are now numerous roles – external contractors, remote workers, privileged users, joiners, movers, leavers, and more – which leads to diminished control over all access points. This makes it increasingly challenging for IT and security teams to deliver secure access to applications and their network.

As enterprise IT adopts more cloud systems while continuing to maintain legacy on-premises solutions, having access controls in place to monitor machine identities, administrative privileges, and who is granted access to which applications, becomes critical for avoiding a security breach due to access vulnerabilities and gaps in controls.

Just a few of the access security concerns organizations are confronting today – especially when relying on traditional access approaches – include:

- Lack of visibility into what privileged users or third-party vendors are doing in their network – and for how long
- Relying on less secure traditional access methods like VPN that provides limited control over access
- Inappropriate, excessive, and outdated access/permissions for the joiners, movers, leavers, and external users
- Manual processes for provisioning and de-provisioning access that cause delays in productivity and open security vulnerabilities
- Relying on spreadsheets and manual processes to manage all types of privileged credentials
- Cumbersome access reviews to answer who has access, when, and why
- Failing audits and maintaining compliance requirements
- Failing to meet cyber insurance security control requirements

How can organizations adopt a comprehensive method to gain control and visibility over who has access to what, why, how, and for how long – all while maintaining productivity and achieving the highest standards of security?

Identity and access management solutions from a single, trusted vendor

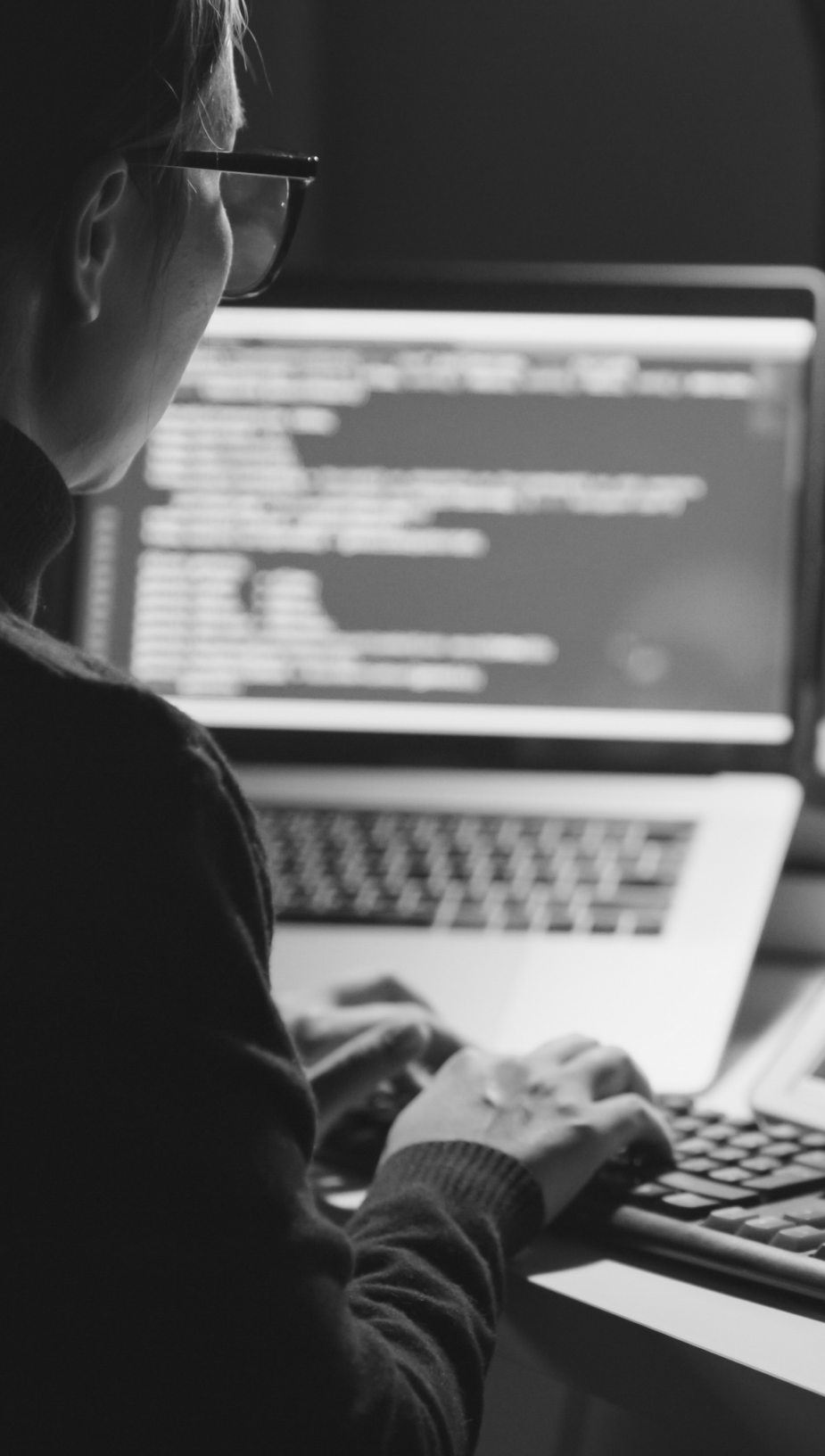
With a set of solutions that work together, experience the benefits of working with a single trusted vendor to manage and secure all user access and provisioning within the organization.

IMPRIVATA ACCESS MANAGEMENT SOLUTIONS

- Create a 1:1 association between a device and a user, even if that device changes hands
- Make authentication secure but simple, even on small form factors
- Achieve visibility into user interactions with devices to build a comprehensive audit trail of activity

The Imprivata identity and access solutions enable organizations to manage the user access lifecycle of both employees and third parties securely and efficiently. It also secures all privileged access to critical assets, mitigating the risks of a cyberattack or breach via over-privileged access rights, privileged credentials, or unsecured third-party access.

The combined solutions enable centralized policy definition and enforcement for all identity and access management forms. Privileged access needs can be managed within the parameters of the organization's identity policies managed within Imprivata Identity Governance. Together, these access solutions facilitate automated workflows to provide role-based access control for all users, including privileged access for vendors and internal users.



Benefits worth the challenges

Automate the management of the user lifecycle, including privileged users and third-party vendors, for greater efficiency and with a comparatively lower total cost of ownership, working with a single vendor.

IMPRIVATA ACCESS MANAGEMENT SOLUTIONS

- ✓ Provide fast, efficient, and secure access
- ✓ Secure privileged access and passwords for all identities
- ✓ Gain total visibility
- ✓ Meet compliance and security requirements
- ✓ Reduce IT burden and costs
- ✓ Reduce operational complexity

Provide consistent “day one” access

ACCELERATE SECURE ROLE-BASED AND LEAST PRIVILEGED ACCESS TO SYSTEMS AND APPLICATIONS

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

Organizations employing thousands of people have ever-changing access needs for applications, devices, and information. These access requirements must be driven by an individual’s role and responsibilities, which could change over time due to attrition, role changes, or promotions. Organizations need a fast and secure way to provision and de-provision this access based on role-based policies. User permissions and privileges regarding what applications and systems a user can access in an organization’s environment must consistently match their job role.

With Imprivata Identity Governance[®], organizations gain this efficient and secure process to automate the management of the user access lifecycle. The solution provides a holistic view of access risk vulnerabilities, including orphaned or inactive accounts, and unusual access rights, to ensure a high standard of security through efficient, effective automation of identity creation and termination including self-service account management. The solution provides detailed logging and analytics on all identity events to ensure compliance, detect potential over-privileges, and troubleshoot access issues.

CREATE DETAILED REPORTS FOR AUDITORS WITH ONE CLICK

Applications, devices, data, and stakeholders are all linked through Imprivata Identity Governance, meaning the system can determine who has access to what information, device, and application. This informs and creates access reports that provide answers to the questions that come up during regulatory auditing.

Govern user access with policy-based controls

ENSURE USERS HAVE ACCESS TO ONLY INFORMATION THEY NEED TO DO THEIR JOBS AND PREVENT THEM FROM ACCESSING INFORMATION THAT DOESN'T PERTAIN TO THEM.

Role-based access control (RBAC) has become one of the most advanced methods for access control. A common problem in user access setup is that it's difficult to predict which systems a user may access without having an individual monitor their usage, but it's a problem that Imprivata Identity Governance solves. The 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. Third parties and vendors pose a unique challenge when it comes to governing identities and access policies. As these users are outside of the control of the organization, it can be difficult to enforce RBAC when those roles are undefined, transient, and opaque. SecureLink Enterprise Access equips organizations to manage their third-party users, functioning as a single source of truth for external user identities. Granular access permissions

enable organizations to define and enforce least privileged access for their third parties – ensuring they have access to only what they need, when they need it – and ensures timely offboarding when access is no longer necessary. This is especially helpful for organizations that have a large volume of third parties and contractors that make it difficult to manage and monitor network access closely.

“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


You can't protect what you can't see: What are third-party vendors doing?

MANAGE AND CONTROL THE CRITICAL ACCESS THIRD PARTIES NEED TO SYSTEMS, SERVERS, AND DATABASES, WITHOUT SACRIFICING EFFICIENCY OR SECURITY.

The number of cyberattacks continues to increase and too many incidents over the years have shown that firewalls and VPNs alone cannot secure an organization – especially when it comes to third-party access. As trends like digital transformation and remote or hybrid working environments drive increases in the number of human and machine identities, the need to validate these identities and ensure access control to sensitive data is more critical than ever before.

According to research completed by the Ponemon Institute, third parties are involved in over half of the data breaches in the US, and a third-party data breach cost, on average, twice that of a normal breach. Considering the impact to brand reputation, loss in business, and possible decreases in share value, the overall cost of failing to effectively vet and evaluate third parties is about \$13 million.

Third parties and contractors aren't under organizations' control and it's unlikely that they provide complete transparency in their information security controls. Some vendors can have robust security standards and good risk management practices, while others may not. With their remote access and connectivity to organizations' networks, each vendor, whether directly or indirectly, impacts security posture.



SecureLink Enterprise Access secures these third-party remote access risks to organizations' critical systems and information. Designed specifically to address the unique challenges of external users, Enterprise Access is a complete, all-in-one third-party remote access platform

- Manages and verifies third-party identities and enforces least-privileged access
- Controls access with Zero Trust Network Access, fine-grained access controls, and secure credential management
- Records and audits all session activity for complete visibility and regulatory compliance
- Delivers fast time-to-value with vendor onboarding support and multiple deployment options

Eliminate password fatigue

MANAGING ACCESS FOR PRIVILEGED USERS

Password fatigue – also referred to as password chaos – is occurring more frequently because users are required to maintain good password hygiene, keep track of many passwords, not share credentials across accounts, and select difficult passwords containing a particular set of characters, numbers, symbols, uppercase letters, and more.

In today's environment, it is no longer a question of if, but when, an organization will be breached – likely due to a compromised credential. In 2021 alone, 212.4 million U.S. businesses were affected by a cyberattack.

As the majority of today's most damaging attacks stem from compromised credentials, password cybersecurity has become a major concern for business leaders. Organizations looking to prevent a breach, eliminate password fatigue, enhance security, and maintain cybersecurity coverage must adopt a security posture that starts with identity security. Privileged access management (PAM) is an information security mechanism that safeguards identities with special access or capabilities beyond regular users. A PAM solution can help organizations maintain security and compliance and increase IT administration efficiency and business agility.

Imprivata Privileged Access Management enables organizations to prove compliance by centrally collecting, securely storing, and indexing account access, keystroke logs, session recordings, and other privileged events. The solution secures privileged credentials to critical systems, minimizing the risk of credential theft and attack, and enables organizations to adhere to the principle of least privilege and protect themselves from inappropriate access by providing just enough access at the right time to privileged users to complete a task, and nothing more.

Cyber insurance

A few years ago, cyber insurance was a simple line item added to an organization's insurance policy. But, in today's environment of constant cybersecurity threats and attacks, it's both necessary to have and a large undertaking to gain and renew coverage. Premiums have skyrocketed, and organizations that fail to implement standard security controls are seeing the highest rate increases – as high as 300%. Insurance providers now require baseline security measures to be in place, including multifactor authentication, defined access provisioning processes, and PAM.

One of the most significant areas that companies can improve upon is identity and access management. Solutions that stop attackers from getting onto the company network and accessing information inappropriately are of particular interest.

MULTIFACTOR AUTHENTICATION

Multifactor authentication is a common requirement to gain (and keep) cyber insurance coverage. Without it in place, organizations face difficulty in even receiving a quote, or receiving astronomical premium hikes. This baseline security measure verifies a user's identity using a second form of authentication before granting access to the application or network. It provides an additional security layer that can stop a bad actor from gaining access, should they have compromised or stolen a user's credentials.

Premiums have skyrocketed, and organizations that fail to implement standard security controls are seeing the highest rate increases – as high as



300%

Imprivata Confirm ID® provides organizations with a holistic platform for multifactor authentication for their users. Whether users are remotely accessing the network via a VPN, the cloud, or Windows applications, organizations can secure that access with a fast and convenient push token notification that verifies the user's identity and secures the organization against a credential-based attack.

SecureLink Enterprise Access enables organizations to enforce multifactor authentication specifically for their external, third-party users. It verifies their identity before granting access to the company's internal critical systems and data.

USER ACCESS PROVISIONING

Tracking user activity and access rights – ideally from a central source – is a key requirement for cyber insurance. Being able to quickly identify unusual access rights or activity is crucial in identifying possible points of vulnerability, or even a bad actor who has gained access – especially to privileged accounts. Insurers also want to see a defined, efficient, and timely process for de-provisioning access for users who have left the organization, as excessive or unneeded permissions can pose a large security risk to organizations and are the source of many data breaches.

MANAGING ACCESS FOR JOINERS, MOVERS, AND LEAVERS

Imprivata Identity Governance allows organizations to provision access based on an employee's role and provides them with only the access necessary to effectively perform their job duties, ensuring employees will not have access to sensitive data if they do not need it to fulfill their responsibilities. It ensures access is updated appropriately based on role changes, and that access is removed in a timely manner when a user leaves the organization.

Imprivata Privileged Access Management integrated with Identity Governance ensures that user access to privileged accounts is appropriate and governed effectively. It secures the most important and critical access an organization's internal user

MANAGING ACCESS FOR REMOTE WORKERS AND VENDORS

SecureLink Enterprise Access ensures that remote access is granted to authorized users only with layered multifactor authentication and that external users have only the least amount of access needed to do their job. It addresses the all-too-common security vulnerability of external users having access longer than they should be automatically de-provisioning vendor access when appropriate.

PRIVILEGED ACCESS MANAGEMENT

PAM controls are crucial to have in place when it comes to privileged, critical accounts and applications. Compromised privileged credentials are the most common source of data breaches, so securing these keys to the kingdom is of utmost importance.

Imprivata Privileged Access Management is a comprehensive solution that protects privileged accounts from unauthorized access. This includes password management, monitoring, and auditing privileged sessions, and password rotation. It also supports multifactor authentication for privileged access, including access to directory services, network backup environments, infrastructure, and endpoints and servers.



Seamless integration with Imprivata OneSign

The integration of Imprivata's Identity and Access Management solutions with Imprivata OneSign® provides a powerful solution to help enterprises gain a holistic view of access risk vulnerabilities, including excessive or abnormal access rights and un-provisioned access. The joint solutions enable organizations to authenticate user access with single sign-on and multifactor authentication, as well as to confirm that users have the right access, that authorization policies are enforced, and that the process is compliant. This allows organizations to balance secure access and meet complex compliance requirements.

The integration simplifies access and improves administrator productivity by allowing organizations to ensure that only authorized internal/external privileged users can access their accounts. The integration of these solutions significantly reduces an enterprise's attack surface, while improving visibility and accountability for its users. Users can increase productivity, improve user experience, and provide secure authentication to manage all access.

Imprivata Privileged Access Management

- Provide fast, same-day access to legacy and modern systems applications.
- Automate identity creation and termination, including self-service account management
- Govern the identity and access lifecycle by adding and removing access rights for joiners, movers, and leavers
- Gain a holistic view of access risk vulnerabilities, including orphaned or inactive accounts and unusual access rights
- Compliance and audit reporting
- Permission and entitlement management

- Execute certification campaigns
- Role-based access control (RBAC)

SecureLink Enterprise Access

- Manage and verify third-party identities with employment verification and multifactor authentication
- Vendor self-registration
- Credential management and injection
- Granular Zero Trust access to needed applications only
- Fine-grained access controls, including access approval workflows and just-in-time access
- Monitor and record session activity
- Compliance and audit reporting with detailed documentation

- **Imprivata ConfirmID – MFA**
- Secure and convenient two-factor authentication (2FA) for all users for remote network access, cloud applications, and other critical systems and workflows.
- Combats phishing and other attacks to improve security and safeguard against unauthorized access to patient records and other sensitive information.
- Makes security invisible to users with innovative and convenient authentication methods such as push token notifications.

The Time is Now: Secure and Automate Access for All Identities

Ready to reduce risk and improve security with granular control over the provisioning, control, and monitoring of user, third-party, and internal privileged access? Request a demo today.



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

Copyright © 2023 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.