EBOOK

Imprivata access management solutions

imprivata®

Automate the user access lifecycle and secure all privileged access in your enterprise

The lines continue to blur between who's inside the enterprise and who's outside it. There are external contractors, remote workers, privileged users, joiners, movers, leavers, and control over all access points is diminishing, making it increasingly challenging for IT and security to deliver secure access to applications and their network.

As enterprise IT adopts more cloud systems while maintaining legacy on-prem solutions, having access controls in place to monitor machine identities, administrative privileges – and who is granted access to which applications – becomes increasingly imperative to avoid a security breach due to access vulnerabilities and gaps in controls.

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

- Lack of visibility into application usage and 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 provide limited control over access
- No password rotation, and shared credentials for privileged 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- Inappropriate, excessive, and outdated access/permissions for the joiners, movers, leavers, and external users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 up 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 struggling to maintain 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?

What the analysts are saying

Gartner has named a new security discipline called Identity Threat Detection and Response (ITDR) that can be a helpful addition to an organization's identity and access management (IAM) infrastructure. ITDR incorporates detection mechanisms that then investigate suspicious posture changes and activities and respond to attacks to restore the integrity of the identity infrastructure.

ITDR incorporates strong Software as a Service (SaaS) security identity access management (IAM) governance methodologies and best practices that are found in SaaS security posture management solutions (SSPM), enabling security teams to gain continuous and consolidated visibility of user accounts, permissions, and privileged activities across the SaaS stack, such as:

- Identifying who is accessing what and when, and with the right levels of privileges
- Forensics related to user actions, focusing on privileged users and third-party vendors
- Roles' continuous and automated discovery and consolidation
- Role rightsizing by revoking unnecessary or unwanted access

It's time for organizations to reevaluate identity and access and to work with a trusted vendor that can address the significant access security problems and challenges enterprises face today.

An access management suite of solutions from a single, trusted vendor

By leveraging a suite of integrated solutions, experience the benefits of working with a single trusted vendor to manage and secure all user access and provisioning within your organization.

Imprivata access management solutions

Our access management solution suite enables organizations to manage the user access lifecycle of both employees and third parties securely and efficiently, and secure 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 access suite enables centralized policy definition and enforcement for all identity and access management forms. Privileged access needs can be managed within the identity policies of the organization's 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.

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

- **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-1 access

Accelerate secure role-based and least privileged access to systems and applications

Organizations employing thousands of people have ever-changing access needs to 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 their role-based policies. User permissions and privileges regarding what applications and systems a user can access in your environment must consistently match their job role in your business.

With Imprivata Identity Governance and Administration (formerly Imprivata Identity Governance), organizations gain this efficient and secure process to automate the management of the user access lifecycle. It 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 the Imprivata Identity Governance (IGA) solution, meaning the system can determine who has access to which information, device, and/or 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 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 their usage. It's a common problem in user access setup that IGA solves. It ensures that access permissions are granted solely based on the user's role or job title in the organization.

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

– SecurityIntelligence

IGA 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 role-based access controls when those roles are undefined, transient, and opaque. Imprivata Vendor Privileged Access Management (formerly 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 ensuring timely offboarding when access is no longer necessary.

What are your third-party vendors doing on your network?

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

Manage and control the critical access your 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/hybrid working environments for third parties and employees 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.

The 2019 Cost of a Data Breach Report from Ponemon Institute and IBM found that third-party involvement was one of the five biggest cost amplifiers, increasing the average cost by more than $370,000 to $4.29 million.

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

Imprivata Vendor Privileged Access Management (VPAM) secures these third-party remote access risks to your organization's critical systems and information. Designed specifically to address the unique challenges of external users, VPAM is a complete, all-in-one third-party remote access platform that:

- 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

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

Eliminate password fatigue

Managing access for privileged users

Password fatigue – also referred to as password chaos – occurs more frequently nowadays since 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, and uppercase letters, etc.

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

Imprivata Privileged Access Management (PAM) enables organizations to prove compliance by centrally collecting, securely storing, and indexing account access, keystroke logs, session recordings, and other privileged events. It secures privileged credentials to critical systems, minimizing the risk of credential theft and attack. It 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

Whereas a few years ago cyber insurance was a simple line item added to your organization's insurance policy, 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%. Coverage providers now require baseline security measures to be in place, including multifactor authentication (MFA), defined access provisioning processes, and privileged access management.

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, and/or 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 bad actors from gaining access, should they have compromised or stolen a user's credentials.

Imprivata Enterprise Access Management with multifactor authentication provides organizations with a holistic platform for multifactor authentication for their users. Whether users are remotely

accessing the network via a VPN, 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.

VPAM enables organizations to enforce MFA 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 to your environment, 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

IGA 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.

PAM integrated with IGA ensures user access to privileged accounts is appropriate and governed effectively. It secures the most important and critical access an organization's internal users have.

Managing access for remote workers and vendors

VPAM ensures that remote access is granted to authorized users only with layer 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 by automatically de-provisioning vendor access when appropriate.

PAM

Access controls are crucial to have in place when it comes to your 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.

PAM 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 your privileged access, including access to directory services, network backup environments, infrastructure and endpoints/servers.

Better together: Key capabilities

IMPRIVATA PRIVILEGED ACCESS MANAGEMENT

- Discover and lock down privileged accounts
- Automatic rotation of privileged credentials
- Monitor and record session activity
- Enforce strong passwords
- Compliance and audit reporting
- Multifactor authentication
- Delegate execution of privileged commands

IMPRIVATA IDENTITY GOVERNANCE AND ADMINISTRATION

- 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

Better together: Key capabilities

IMPRIVATA VENDOR PRIVILEGED ACCESS MANAGEMENT

- Manage and verify third-party identities with employment verification and MFA
- 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 ENTERPRISE ACCESS MANAGEMENT WITH MULTIFACTOR AUTHENTICATION

- Verify user identities with MFA
- Layered multifactor authentication for remote access:
  - Via VPN
  - Cloud applications
  - Windows servers and desktops
- Push token notifications (plus SMS and temporary codes)
- Self-service device management

The time is now – secure access for all users, applications, and data today

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

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

1972-2024_ebook-security-access-suite