PRODUCT OVERVIEW

Enterprise Access: The Solution for Third-Party Identity Management

imprivata®

Security and Efficiency in a Single Solution

Managing third-party identities is — quite simply — complex. They typically only need short-term, temporary access, and are often transient and opaque; organizations have little-to-no visibility into employee hiring and firing, and struggle to verify identities and define access through traditional, HR-led methods.

- Over 50% of organizations do not have a comprehensive inventory of all third parties with access to their network
- On average, an organization shares data with 583 third parties
- Companies spend an average of 2,000 hours per year managing third-party accounts and access
- 59% of organizations are ineffective in preventing third parties from sharing usernames and passwords

Without a purpose-built solution, organizations often try to manage vendors in their Active Directory or utilize their identity governance solution. Using solutions designed for the employee lifecycle result in gaps and challenges: inefficiencies at best, and security vulnerabilities at worst.

Enterprise Access is specifically designed to be the single source for third-party identities, solving the security issues of employment status verification, shared credentials and unverified users, broad access permissions, and accounts that are mistakenly left active.

Customers see on average an

80%

reduction in time spent managing third-party accounts

Customers see on average an

90%

reduction in time spent troubleshooting account issues

FEATURES TO MANAGE THE INDIVIDUAL IDENTITIES AND ACCESS POLICIES OF THIRD-PARTY USERS:

Individual accounts

- Manage and enforce the use of individual accounts for each third-party user, with usernames tied to their work email account

Multi-factor authentication

- Minimize the risk of a compromised account by verifying the identity of the individual with MFA via any TOTP application, email, or SMS

Passwordless authentication

- Remove the need for users to enter another password with passwordless authentication; users can authenticate with hardware or biometrics on an existing device

Self-registration and onboarding

- Enable individuals to self-register for their own user accounts, and send the account creation approval request directly to the third-party owner without needing IT involvement

Employment verification

- Verify that the individual requesting access to your network is currently employed by the vendor with a valid reason for access

Time-based account provisioning and deprovisioning

- Provision access for only when needed, whether a few hours or weeks, and set parameters for automatic account deprovisioning

Access policies

- Granularly define what applications a user can access and with what permissions, based on the principle of least privilege

Learn about how Enterprise Access fully solves third-party access security, with zero trust network access and session monitoring for total visibility

LEARN MORE