DATASHEET

imprivata®

Enterprise Access: The solution for third-party access control

Reduce risk, increase visibility, and get back control of your vendors' access

With trust-based remote access solutions like VPNs or desktop sharing, organizations struggle to control and limit what their third parties and vendors have access to and when. This creates the potential for lateral movement, network scanning, and accessing assets they shouldn't at best, or at worst, nefarious activity like stealing sensitive data or compromising critical systems. With third parties as a primary, all-too-frequent target for bad actors to gain access to an organization, implementing stronger third-party access control and providing secure connectivity for third-party access has never been more critical.

Enterprise Access provides a secure, controlled connection for your vendors to your assets based on Zero Trust - minimizing the vulnerabilities associated with other trust-based methods and securing your organization against third-party access risks.

56% of organizations have experienced a data breach caused by a third party. 70% resulted from giving too much privileged access to those third parties

53% of organizations are not revoking credentials when appropriate

38% of organizations know the type of network access that their third parties have

57% of organizations say they are not able to provide third parties with just enough access to perform their designated responsibilities and nothing more

FINE-GRAINED ACCESS CONTROLS

- **Access Notifications:** Know exactly when vendors connect and disconnect with email notifications as well as an included summary of session activity
- **Access Approvals:** Require approval to be granted before a user can access a specific application. Approval can be granted for a certain amount of time or until a set date and time
- **Time-Based Access:** Grant access to users for a certain amount of time, or until a set date and time to ensure access is automatically deprovisioned when no longer needed
- **Access Schedules:** Grant a user access on a predetermined, custom schedule, like typical business hours, Monday through Friday from 9am - 5pm, and ensure access is disabled outside of that schedule

MULTI-FACTOR AUTHENTICATION

- Minimize the risk of unauthorized access by verifying the identity of the individual with MFA via any TOTP application, email, or SMS

ZERO TRUST NETWORK ACCESS

- Define access at the host and port level to prevent lateral movement, remove users as a node on the network, and ensure vendors only have access to what they need, when they need it

PRIVILEGED CREDENTIAL MANAGEMENT

- Manage credentials in SecureLink's credential vault or in your PAM solution. Credentials are obfuscated and injected into the session, minimizing the risk of compromised credentials and ensuring reps never see or know usernames and passwords.

Learn about how Enterprise Access fully secures third-party access, with third-party identity management and and session monitoring for total visibility

LEARN MORE

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

DS-EA-Solutions-2023