DATASHEET

Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access)

A secure third-party remote access solution built for enterprises

Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access) is an enterprise-grade remote access platform designed specifically to secure third-party access and connectivity to an organization's critical assets. Vendor Privileged Access Management (VPAM) provides a secure connection for third parties to systems, servers, data, and applications. It ensures that each user has minimal, controlled access, lessening the chance of a third-party breach, and provides you with control, visibility, and peace of mind over your third-parties' access.

How Vendor Privileged Access Management secures your network and manages user access

Manage third-party identities and enforce least-privileged access policy.

Vendor Privileged Access Management ensures that every individual has their own account to connect to your systems (no more shared accounts), verifies each user's identity, and allows you to define third-party user access policies. With VPAM, you can:

- Delegate the burden of account creation to the vendor with vendor self- registration.
- Verify the identity of the individual with multi-factor authentication (MFA), as well as their current employment status.
- Define and manage access policies to your assets with granular permissions, customizable at the group, vendor, or individual level.

Control access with zero trust network access, fine-grained access controls and credential management.

Vendor Privileged Access Management provides a secure, controlled connection to your assets based on Zero Trust, minimizing the vulnerabilities associated with other trust-based remote access methods. With VPAM, you can:

- Configure access controls for each asset, such as connection notifications, access approvals, time-based access, or repeating access schedules.
- Define access at the host and port level so that users can only access what they need and nothing else.
- Manage credentials in Imprivata's vault (or your own PAM solution), eliminating the need to share passwords and minimizing the risk of compromised credentials or lateral movement within your network.

Monitor session activity for total visibility.
Vendor Privileged Access Management provides total visibility into all third-party activity in your environment—as well as vendor accountability—via HD session recordings and detailed audit logs. With VPAM, you can:

- Gain context for access with audit logs, including the "who, how, when, why, and what" of each session.
- Easily investigate and resolve any incidents with detailed video and text- based recordings.
- Demonstrate and meet compliance regulations with granular audit trails and documentation of all access.

Faster time to value.
Multiple deployment options and vendor onboarding services allow you to get up and running quickly and help facilitate vendor adoption and rollout. With Imprivata's implementation services, we:

- Work directly with your vendors to answer questions, provide training, and test connectivity—all to ensure smooth adoption and rollout.
- Provide you with quicker time-to-value, removing the burden from your IT team with project management, implementation, workflow customization, and admin/user training.

Features and capabilities:

- **Identity Management & Access Policies:** Enforce individual accounts for every third-party user and assign the appropriate access policy based on assets and permissions.
- **Employment Verification:** Ensure that vendor reps are still employed by the third-party upon every login attempt.
- **Vendor Self-Registration:** Delegate account creation to vendors while maintaining control with your approval before creation is confirmed and finalized.
- **Multi-Factor Authentication:** Verify the identity of the individual requesting access to eliminate the risk of a bad actor gaining access to your assets.
- **Passwordless Authentication:** Enable users to login without having to enter a password using device-based authentication.
- **Zero Trust Network Access:** Define access at the host and port level to prevent lateral movement and ensure vendors only have access to what they need, when they need it.
- **Support for Vendor Connectivity Requirements:** Support access via any TCP or UDP-based protocols, including RDP, SSH, VNC and Telnet, from any OS, as well as the use of any native or proprietary support tools.
- **Fine-Grained Access Controls:** Implement access controls to critical assets, including access schedules, just-in-time access, and access approvals.
- **Credential Management:** Manage credentials in Imprivata's credential vault or in your own PAM solution. Credentials are obfuscated and injected into the session, so reps never see or know usernames and passwords.
- **Session Monitoring:** Gain total visibility into what vendors are doing with contextual audits of all sessions and detailed text and video session recordings, allowing for proactive monitoring as well as reactive investigations as needed.
- **Ad-hoc Attended Support:** Facilitate ad-hoc real-time collaboration and support with vendors via the Quick Connect module.
- **Security and Compliance Checklist:** In-product checklist ensures VPAM is configured appropriately to meet any relevant compliance requirements and security best practices.
- **Imprivata Nexus (formerly SecureLink):** For vendors who already own Imprivata Customer Privileged Access Management (formerly SecureLink Customer Connect), the Nexus allows you to shift the management of individual vendor rep accounts to the vendor, while retaining full control over when and what a vendor has access to within your network.
- **Deployment:** Choose from a physical, virtual, or Imprivata cloud deployment model.

> “From the start, [Imprivata] focused on our problem and not on other potential interests of the solution. They engaged us with our interests in mind and wanted to partner with us in finding a solution to our specific problem of secure vendor access to our environment.”
>
> – UMass Memorial Health

> “ Security and convenience are typically mutually exclusive. So before [Imprivata], we could create secure connections for our vendors with named accounts via VPN, but all work had to be monitored by a person watching their session, which was very inefficient. Even with that person monitoring, there was no logged audit beyond the time of connection. I was able to show the minimal cost of [Imprivata] was well worth it, with an ROI return in 6 months just in productivity, with the added benefit of audit of all activity. ”
>
> – Charlotte County, FL

With Vendor Privileged Access Management, organizations experience a:

80%	reduction in time spent managing and tracking vendor access accounts
90%	reduction in time spent supporting and troubleshooting vendor access
70%	reduction in time spent on security investigations and audit
50%	reduction in fines and penalties
50%	reduction in downtime of vendor applications

Third parties are the greatest access risk within your organization. The only solution is a third party privileged access management platform with the governance, control, and monitoring capabilities to fully secure third-party access to your critical systems, data, and network.

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

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