Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access) vs. VPNs

imprivata®

Imprivata Vendor Privileged Access Management (VPAM) vs. VPNs – Competitive Considerations

- **Vendor Identity Management |** VPNs do not provide comprehensive and individual identity and access management for third-party users; using VPNs, organizations often struggle to have a comprehensive inventory of all vendor reps with access to their network, to know if access is still needed or not, and to verify the current employment status of the vendor user. They are not designed to deal with the transient and opaque nature of third-party identities, nor enable least privilege access.
- **Granular, Zero Trust Access |** VPNs are inherently trust based and make it difficult to granularly isolate what the vendor has access to. The vendor user becomes a node on the network, which allows for the possibility of lateral movement and network snooping. Should the VPN credentials become compromised, bad actors have a foothold on the network and often too much privileged access that enables them to move and escalate privileges.
- **Credential Management |** Organizations typically have to share VPN and system or applications credentials when providing remote access via VPN to their vendors. They can struggle to prevent credential sharing among users, making it difficult-to-impossible to know exactly who has access to their network.
- **Session Monitoring |** VPNs provide limited visibility at best into vendor rep activity on the organization's network. Organizations cannot review vendor sessions activity in detail, which limits vendor accountability and the ability to effectively investigate issues should an incident occur.

Features	VPN	Vendor Privileged Access Management
Individual Identity Management and Verification	With VPNs, logins and passwords are routinely shared, so organizations don't know the actual individual who is accessing the network, creating risk for both sides. Organizations also struggle to verify if a vendor rep is still employed by the vendor before granting access.	VPAM enforces individual accounts with least privilege access policies, integrates with existing authentication structures when present, uses unique multi-factor authentication schemes, and verifies the current employment status with the vendor.
Vendor Onboarding, Self-Registration and Deprovisioning	Providing access to vendors via a VPN is time-intensive on the IT team. It typically requires setting up an account in Active Directory, provisioning VPN access with credentials, and sharing those with the vendor. It also requires IT to remember to deprovision access, which is often left active longer than needed.	VPAM is designed to streamline the vendor onboarding and offboarding process, with self- registration and approval workflows available to remove the burden from the IT team. Vendor accounts can be automatically deprovisioned as soon as access is no longer needed.

Features	VPN	Vendor Privileged Access Management
Granular Access Controls	VPNs don't provide organizations with granular control over vendor access, such as access approvals, access schedules, just-in-time access or access notifications.	VPAM enables organizations to granularly control when and under what circumstances a vendor may have access, with access approvals, access schedules, just-in- time access and access notifications. Access policies are defined on the principle of least privilege, ensuring that only the right technicians have the correct level of access at the right time.
Credential Management	VPN and system or application credentials have to be provided to the vendor in order for them to have access. This means privileged credentials are outside of the control of the organization, and runs the risk of credential compromise and a third-party data breach.	VPAM allows organizations to manage privileged credentials within the solution vault (or their own PAM solution); credentials are obfuscated and injected directly into the session. Vendors never need to know or see usernames and passwords, reducing the risk of credential theft and attack.
Enterprise-grade, Zero Trust Network Access	While VPNs provide enterprise-grade connectivity, access is inherently based on trust; vendor users become a node on the network, which allows the possibility of lateral movement and network scanning by nefarious actors.	VPAM provides access based on the principle of Zero Trust; vendors are provisioned access to only the specific host, ports and applications they need and nothing else. It provides secure connectivity to any TCP or UDP-based protocol and supports the use of any native or proprietary tools, meeting your vendors connectivity requirements while increasing the security of access.
Imprivata Platform	VPNs are not an effective tool to secure internal or external privileged access to sensitive systems and data. They require the use of other tools from vendors to secure this access appropriately.	VPAM integrates with Imprivata Privileged Access Management to combine privileged password and session management to efficiently discover, manage, and audit all privileged credentials and access for employees and vendors - all from a single, trusted vendor.

With Imprivata, you gain a partner, not just a technology vendor. Imprivata solves complex workflow, security, and compliance challenges for mission- and life-critical industries with the industry's only platform to fully manage and secure all enterprise and third-party identities. The Imprivata digital identity platform delivers identity governance, multifactor authentication, enterprise single-sign-on, privileged access management, third party access management, customer access management, mobile access and control, and digital identity intelligence. This comprehensive, end-to-end identity and access management ensures all users have secure but seamless access to the applications and information they need, anytime and anywhere they need it, from any device and location.

Contact us about the next steps. We cannot wait to welcome you as a customer.

imprivata®

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