imprivata

DATASHEET

Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access)

Secure and efficient remote vendor access for state and local governments

With regulations becoming stricter and the constant threat of cyberattacks or data breaches always present, cities, counties, and law enforcement need to make sure they secure and audit the remote access of all their vendors.

Without a vendor privileged access management (VPAM) solution in place, IT and security teams often spend too much time on manual management processes. This drains valuable and limited resources while also leaving uncertainty about whether they've fully minimized the risks associated with vendor access.

"It's a force multiplier. We no longer have to sit there and handhold vendors and watch them because the engagement is recorded. So, we're almost doubling the effectiveness of our workforce."

– Tony Bryson, Chief Information Security Officer for the Town of Gilbert, AZ

How Imprivata Vendor Privileged Access Management (VPAM) helps

Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access) provides state and local governments with a secure, standardized remote access platform specifically designed for third parties. It manages vendor identities and controls and audits vendor access – while also reducing the amount of time spent on vendor access – to increase their teams' capacity.

Manage vendor identities and enforce least privilege access policies

- Enforce the use of individual accounts verified with multifactor authentication (MFA)
- Verify current employment status
- Automate vendor onboarding with self-registration workflows and offboarding with automatic deprovisioning
- Define granular permissions to enforce least privilege access

Provide secure, controlled remote access to applications and systems

- Support broad connectivity requirements with access via any TCP or UDP-based protocol
- Configure granular access controls for each application, including enforcing access approvals and receiving connection notifications
- Secure credentials in the vault and eliminate sharing usernames and passwords with vendors
- Eliminate network-based access, defining access at the host and port level so that users can only access what they need and nothing else

"I was able to show the minimal cost of VPAM 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

Demonstrate compliance and cybersecurity best practices with audited, logged access

- Capture and record all required information in detailed audit logs, including the "who, how, when, why, and what" of each session
- Easily investigate and resolve any incidents with HD video and text-based recordings of session activity
- Meet relevant security standards such as CJIS, PCI, HIPAA, NERC, and others with granular audit trails, documentation of all access, and in-product compliance checklists

Faster time-to-value with a simple deployment on an easy-to-manage platform

- Keep your investment simple, with support, cloud implementation, onboarding enablement, and training included in your license cost
- Take advantage of the Nexus for your vendors who already own Imprivata Customer Privileged Access Management (formerly SecureLink Customer Connect). Shift the identity management to the vendor and retain full control over when and what a vendor has access to within your environment
- Deploy in the Imprivata cloud to get up and running in a matter of days
- Consider vendor onboarding services to facilitate vendor adoption and a smooth rollout with some or all your vendors

Benefits for government agencies

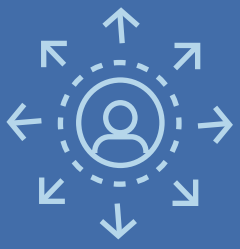
80% reduction
in time spent managing and tracking vendor access

70% reduction
reduction in time spent on audits and security investigations

90% reduction
in time spent troubleshooting and supporting vendor access

50% reduction
reduction in downtime of vendor applications

Leverage the Imprivata network



With 41,000+ enterprises, vendors and manufacturers using Imprivata for secure remote connectivity, you likely have one already connecting into your environment today! This existing connectivity sets you up for additional productivity benefits from day one.

Third-party access to your network is one of the most significant security and compliance risks your organization faces. Address these risks and enhance your team's efficiency with the leading vendor privileged remote access platform, designed to comprehensively secure third-party access.

To learn more about Imprivata Vendor Privileged Access Management, **visit our website.**

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:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0)208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

2800-2025_VPAM-DS-governments