imprivata®

DATASHEET

Imprivata Vendor Privileged Access Management (VPAM)

Securing vendor access to your operational technology (OT) environment

Industrial and critical infrastructure organizations face the complex challenge of securing access to their operational technology (OT) environment against attackers who are increasingly targeting these often more vulnerable, older systems – particularly through their vendors and third parties. In fact, there was **a 140% increase in cyber-attacks** against industrial systems last year. In many cases, this resulted in physical consequences and an inability to operate.

Not only does this access need to be secure to minimize risks, but it also needs to be efficient for vendors to connect. Delays can increase costly downtime of equipment and systems.

Imprivata Vendor Privileged Access Management (VPAM, formerly SecureLink Enterprise Access) is an enterprise-grade remote access platform designed specifically to provide third parties and vendors with secure and efficient access to your most critical assets. Supportive of both IT and OT environments, it provides a secure connection for third parties to systems, servers, data, industrial control systems (ICS), programmable logic controls (PLC) and applications and supports connectivity via standard and custom protocols. It ensures each user has minimal, controlled access – providing you with control, visibility, and peace of mind over your third-parties' access.

Challenges organizations face:

- Only **24% of organizations** have completed OT security projects and upgrades
- 73% of OT devices are unmanaged
- Nearly 50% of OT and industrial organizations lack sufficient cybersecurity expertise

> **"... We also had a lot of people out at the plants using TeamViewer, or LogMeIn, or one of many other VPN or screen-sharing type solutions. That's why we brought in Imprivata VPAM, to try and get a handle on them."**
>
> – Dan Ward, Oldcastle Infrastructure

How Vendor Privileged Access Management secures your network and manages access

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

- Enforce the use of individual accounts and eliminate shared credentials
- Delegate the burden of account creation to the vendor with vendor self-registration
- Verify current employment status and identities with multifactor authentication (MFA)
- Define and manage granular permissions to your assets based on least-privileged access

Provide secure, controlled remote access to IT assets and OT systems, including legacy PLCs

- Support broad connectivity requirements via any TCP or UDP-based protocol and minimize infrastructure requirements by granting direct access to OT components at a port-by-port level
- Configure granular access controls for each asset, such as connection notifications, access approvals, time-based access, or repeating access schedules
- Eliminate network-based access; define access at the host and port level so that users can only access what they need and nothing else
- Manage credentials in the native vault or in your PAM solution, eliminating the need to share passwords to minimize the risk of compromised or stolen credentials

Monitor session activity for total visibility and vendor accountability

- Gain context and visibility into access with comprehensive 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
- Facilitate ad-hoc real-time collaboration and support with vendors with desktop sharing capabilities when needed
- Meet relevant security standards with granular audit trails and documentation of all access

Faster time to value with everything included that you need to be successful

- Keep your investment simple, with all services, support, implementation, onboarding and training are included in your license cost
- Use our vendor onboarding services to ensure a smooth adoption, helping to minimize the burden on your team to roll the solution out to your vendors
- Take advantage of the Nexus – for your vendors who already own Imprivata Customer Privileged Access Management (formerly SecureLink Customer Connect), shift the management of individual rep accounts to the vendor, while retaining 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, or in your own environment

> **"We can lose revenue and incur penalties if our systems are down, even if it's for routine maintenance, so it's crucial to be efficient with maintenance and to be able to respond immediately when there is an issue... Imprivata VPAM has improved both maintenance and response rates."**
>
> – VP of Security, $10B Energy Company

Third-parties are some of the greatest access risks within your organization. Mitigate these risks with the market-leading vendor privileged remote access platform designed to fully secure third-party access to your critical systems, data and IT/OT network.

To learn more about Imprivata VPAM and see it in action, **contact our team.**

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