DATASHEET

Monitor third-party access with Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access)

Gain total visibility into your vendors' access and easily investigate incidents

Having to wonder what your vendors are up to in your environment is an uneasy feeling at best, and a security nightmare at worst. Without a solution that monitors activity, organizations are left in the dark as to what their vendors are doing in their network – from not working productively, to inappropriately accessing sensitive or critical systems, to stealing information.

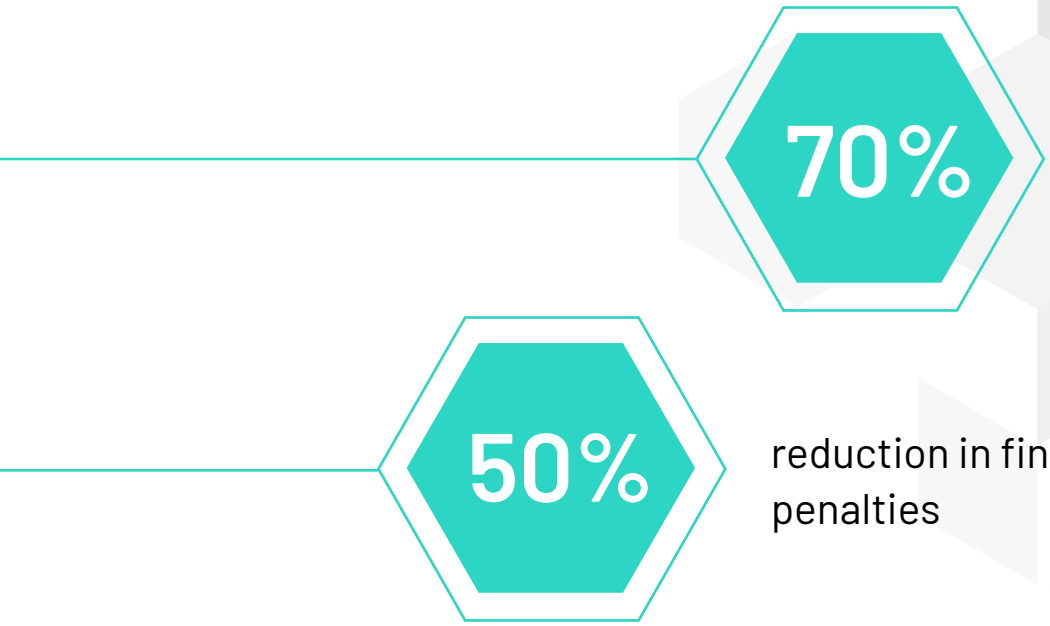
Lacking any evidence to review, a vendor-caused security incident or issue can be incredibly time consuming and difficult to uncover and resolve. Traditional access solutions like VPNs don't provide the visibility, recording functionality, and detailed audit logs needed to keep vendors accountable, to review (or investigate) activity, and to bring peace of mind.

Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access) is specifically designed to monitor and capture all third-party activity with detailed audit recordings. It provides organizations with complete visibility for peace of mind, incident investigation, accountability for vendor work, and proof of regulatory compliance.

The challenges with limited visibility into vendor activity:

- 51% of organizations don't monitor access to network resources and critical data
- The average time to detect a breach is 212 days
- Only 30% of organizations believe they are highly effective at responding to a third-party incident
- Only 41% of organizations believe they are effective in mitigating remote access third- party risks

Imprivata Vendor Privileged Access Management customers on average experience:



Monitor third-party user access with these features:

Audit logs

- Gain context for each access session with audit logs that capture the "who, how, when, why, and what" of each session; this includes who the individual was, who approved access and/or which credentials were used, when the session occurred, their reason for access, and what files were transferred or what services were accessed

HD video audit

- Capture video recordings of activity for graphical protocols for replay and to review exactly what a vendor did in a session

Text-based audit

- Capture commands run and the responses received for text-based protocols for review of all activity

Demonstration of compliance

- Use the detailed audit trails and workflows to demonstrate compliance with regulatory requirements such as HIPAA, CJIS, and PCI, with documentation of login attempts, multifactor authentication (MFA) used, and logs of each access session

Learn more about how Imprivata Vendor Privileged Access Management fully secures third-party access, along with third-party identity management, Zero Trust network access, and access controls.

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**

DS-EA+Monitoring-0401