imprivata

The access landscape has changed. The traditional perimeters are dissolving, and as organizations move to a decentralized workforce and network architecture (including servers, data centers, access points, and more), what was previously safe behind a network wall is no longer protected. Credentials, critical assets, and access points are all vulnerable to a breach. It's time for organizations to innovate their cybersecurity the same way they've innovated their other systems and change their access management structures.

The data tells an alarming story

Both internal and third-party access creates risk for an organization, and the numbers highlight how much work organizations still have to do to secure their critical access points.

INTERNAL ACCESS ISSUES

- 80% of breaches involved privileged credentials.
- Privilege abuse was the most common form of misuse among breaches, most often caused by internal actors.
- 54% of organizations have experienced credential theft.

THIRD-PARTY ACCESS ISSUES

- 70% of organizations attribute a third party breach to too much privileged access.
- 67% of organizations feel drained and overwhelmed by managing third-party access.
- 43% of organizations feel their organization is effective in mitigating third-party remote access threats.

OVERALL ACCESS ISSUES

- 64% of organizations don't have visibility into the level of access and permissions both internal and external users have.
- 52% of organizations feel cyberattacks have increased.

When third-party and internal privileged access aren't properly managed, organizations are more prone to cyberattacks

SECURING CRITICAL AND PRIVILEGED ACCESS

Securing privileged access doesn't have to be complicated. But, before organizations can properly build out access management systems, they need to understand where the gaps are and why there are issues in the first place.

Third-party remote access

Organizations know they need a secure, efficient way to manage the connectivity between their environments and third-party vendors who access their systems and data. However, traditional methods like VPNs and desktop sharing leave major gaps in security and prevent organizations from being able to implement fine-grained access controls, credential vaulting, or even a zero trust approach to access. Organizations also need to inventory and keep track of the individual third-party users accessing their system (for both security and compliance), which can be time-consuming and difficult given the opaque, transient nature of those users.

Internal privileged access

Privileged credentials are called "privileged" for a reason — it takes a special use case for them to be accessed. But those unique use cases have been taken advantage of and compromised countless times. Too many passwords have been left on sticky notes, and too many cyberattackers have hacked login credentials. Without a privileged access management (PAM) solution, privileged credentials have to be shared among users who need it, or an employee will have access with just their personal username, which can cause a major breach if that username is compromised.

It's far too often that organizations don't secure those credentials properly, leading to major attacks, and loss of sensitive data, due to stolen credentials.

In this modern, decentralized world, organizations need high levels of security around their privileged credentials. The days of trusting employees with privileged credentials are over, and privileged credentials need to be securely vaulted and out of the hands of users.

ALL ACCESS. ALL IDENTITIES. ALL MANAGED.

Currently, most organizations, at best, have to work with both a third-party remote access platform and a privileged access management system, each of which comes from a different vendor and technology provider. This isn't ideal, and cybersecurity strategies are promoting the integration and interoperability of security technologies. In fact, by 2025, Gartner predicts that more than 70% of new access management, governance, administration, and privileged access deployments will be converged identity and access management platforms.

An integrated platform from a single vendor is possible, with Imprivata Vendor Privileged Access Management (formerly SecureLink Enterprise Access) and Imprivata PAM.

Vendor Privileged Access Management is a third-party remote access platform that secures the connectivity between an enterprise and its vendor.

- Third-party vendor identity management
- Zero Trust network access
- Access policies for third parties based on least privilege
- Multifactor authentication and vendor employment verification
- Access controls such as notifications, approvals, and time-based access
- Audit logs of vendor activity with HD video recordings and text-based recordings
- Documentation and reporting features for regulatory compliance requirements
- Compatible with RDP, SSH, VNC, HTTP(S), Telnet, or any TCP or UDP-based protocol
- Cloud or on-premise deployment option

Imprivata Privileged Access Management is a comprehensive, easy-to-use privileged access management (PAM) solution that secures privileged, critical accounts from unauthorized access.

- Advanced management of all privileged credentials
- Time-based access, password rotation, account discovery, credential workflows, and one-time-use generation
- Complete visibility with monitoring and audit of privileged sessions
- Ability to manage and inject credentials without disclosing password
- Multifactor authentication

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

PAM-WP-VPAM-integration-0124