imprivata®

Stop ransomware before it happens: Save your reputation and millions of dollars with integrated access security solutions

Avoid the bad press while giving customers, employees, and vendors secure access to the data they need

Ransomware groups are targeting critical infrastructure including healthcare, manufacturing, and government, with no signs of slowing down. A typical ransomware attack can disable an organization, either by encrypting critical files and systems or threatening to disclose sensitive data unless you pay the ransom – or both. Once an attack has occurred, cyber insurance and monitoring won't be enough to repair a company's reputation and the trust of its customers and employees. Moreover, cyber insurance will rarely cover anywhere close to the full hard cost of an attack.

In this case, the best defense is a good offense: enterprises need to prevent ransomware from occurring at all.

Ransomware, at its core, is an identity and data access issue. To do what it's intended to do, ransomware must access data, and it will attempt to compromise accounts and user identities to gain access to that data. Hackers frequently use phishing to compromise credentials, and ransomware is no different – to even begin to run the software, privileges are needed. Therefore, employees with the highest privileges provide hackers with the best opportunity to cause more damage, due to their high levels of access to the organization's most valuable resources. In most cases, some users don't even need privileged access but still have it due to a lack of visibility into who has access to what and why, thus creating more vulnerable targets.

Enterprises need to protect employee and vendor credentials by making it harder for them to be stolen or compromised. Access security systems protect these credentials and ensure that everyone can do their jobs safely and effectively.

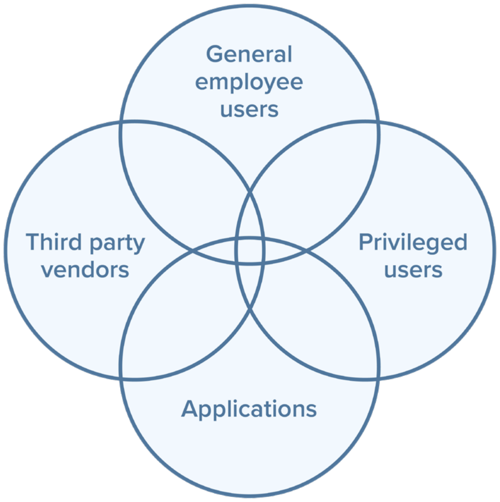
With the Imprivata Access Security Suite, the only integrated suite of solutions that solves all aspects of privileged security, organizations can secure privileged credentials and access rights, and:

- Secure and vault privileged credentials of employees and vendors
- Obfuscate privileged credentials from the end user to prevent phishing
- Enforce multifactor authentication before access and usage of privileged credentials
- Avoid human error in the provisioning and de-provisioning of access
- Enable just-in-time access Implement a least privileged access model
- Enforce granular access controls such as approvals, schedules, and notifications
- Enforce employment verification for third-party users

Can you verify that the files you consider the "crown jewels" of your organization are stored in locations with restricted access permissions?

Imprivata Access Security Suite

Solving access security for all user classes



25% of employees still have access to accounts from past jobs or roles

80% of breaches involved a stolen privileged credential

56% of organizations have experienced a third-party data breach

80% of organizations still store credentials in scripts and applications that when breached can be reused elsewhere

*2022 Ponemon Report
*Verizon 2020 Data Breach Investigations Report (DBIR)
*Identity Report 2022

Imprivata Access Security Suite

The Imprivata Access Security Suite is made up of three core Imprivata products which together can stop ransomware in its tracks, ensure appropriate and secure access to those who need it, and increase compliance and audit reporting.

IMPRIVATA PRIVILEGED ACCESS MANAGEMENT

- Discover and lock down privileged accounts
- Remove user-based privileges to reduce risk and blast radius
- Enable automatic rotation of privileged credentials, and enforce strong passwords
- Monitor and record session activity

SECURELINK VENDOR PRIVILEGED ACCESS

- Manage and verify third-party identities with employment verification and multifactor authentication
- Enable credential management and injection, as well as vendor self-registration
- Zero Trust Network Access technology to eliminate local network access
- Create fine-grained access controls, including access approval workflows and just-in-time access
- Monitor and record session activity

IMPRIVATA IDENTITY GOVERNANCE

- Automate identity creation and termination, including self-service account management
- Provide same-day access and govern the identity and access lifecycle by adding and removing access rights for joiners, movers, and leavers
- Gain a holistic view of access risk vulnerabilities, including orphaned or inactive accounts and unusual access rights
- Enable role-based access control (RBAC)

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com