DATASHEET

imprivata®

Meet cyber insurance requirements with security controls that don't create barriers for your users

As organizations continue to endure an onslaught of ransomware and other cyber attacks, they now have another concern: rising costs of cyber insurance.

In response to the increasing volume, sophistication, and ferocity of attacks, insurance companies are now requiring organizations to have more comprehensive security controls in place that span a wider variety of attack vectors. Without these controls, insurance providers are significantly raising premiums, increasing deductibles, or in some cases, outright denying coverage.

Specifically, many insurance companies are now requiring:

- Multifactor authentication for a greater number of workflows, systems, and users
- Security and management of privileged users and accounts, including for vendor and other third-party access
- Enforcement of password complexity and rotation, including for nonhuman accounts
- Identity lifecycle management, including timely removal of user access when they leave the organization

Evolving cyber security insurance requirements

Imprivata offers a portfolio of digital identity solutions that help you meet these increasingly stringent requirements so you can maintain your coverage and keep your rates down. And importantly, we deliver this added security without creating barriers for your workforce. With Imprivata, you can balance the need for increased security with workflow efficiency for your users.

Requirement	Solution	The Imprivata advantage
Enforcing multifactor authentication for all users	Imprivata delivers a variety of solutions to satisfy multifactor authentication requirements across a broad set of workflows and systems, including: • Access to email through Web apps and/or cloud services • Remote network access via VPN • Remote access for contractors and third-party service providers	Imprivata offers the flexibility to deliver the authentication options that will best meet your users' different workflow requirements. For example: • Proximity badge for shared workstations and other endpoints • Phone-based token for remote network access through a personal laptop • Bluetooth-enabled proximity-based authentication for walkaway security Moreover, the Imprivata ID mobile app can be used across many multifactor authentication workflows, including remote access, cloud access, privileged access, and even electronic prescribing of controlled substances (EPCS), giving your users a single, convenient option and avoiding the need to purchase and implement multiple solutions.
Managing privileged accounts via a privileged access management (PAM) solution **Actively monitor all administrator access for unusual behavior patterns** **Enforce multifactor authentication for privileged access** **Segregation of administrator and user accounts** **Logging of privileged account use**	Imprivata offers identity governance and comprehensive privileged access management (PAM) capabilities to enforce the concept of least privilege and protect privileged accounts from unauthorized access. This includes password management, monitoring and auditing privileged sessions (including session recordings and keystrokes), and password rotation. This also includes enabling multifactor authentication for your privileged access, including: • Internal and remote admin access to directory services (AD, LDAP, etc.) • Internal and remote admin access to network backup environments • Internal and remote admin access to network infrastructure (firewalls, routers, switches) • Internal and remote access to endpoints/servers	Imprivata offers a complete, lightweight PAM solution that integrates with Imprivata multifactor authentication solutions to deliver added security from a single, comprehensive solution. Imprivata offers identity governance solutions to create and manage access for privileged users, which helps segregate admin accounts from user accounts based on defined roles. Imprivata leverages modern architecture and an easy-to-implement solution to deliver a much faster time to value for enterprise PAM than legacy vendors.
Enforce password complexity requirements **Regular password rotation** **Nonhuman ID password management and rotation**	Imprivata offers enterprise single sign-on (SSO), allowing you to meet more stringent password requirements (including both increasing password complexity as well as the frequency with which passwords should change) Imprivata also offers enterprise password vaulting to rotate passwords based on time, use, and/or other events. This includes password management and rotation for nonhuman IDs.	The Imprivata single sign-on solution supports both on-premises and cloud applications, enabling you to enforce complex passwords across a much more comprehensive set of applications to minimize risk. And, simple badge-tap access and a robust SSO capability make it easy for end users, who can focus on their job and not on remembering complex passwords.
Timely removal of user access when they leave the organization	Imprivata offers an enterprise identity management solution to quickly provision and deprovision users (including privileged users), allowing you to terminate user access rights as part of the employee exit process	Imprivata offers integrated identity governance with enterprise single sign-on and access management to instantly disable a user's credentials when they leave the organization. By automating the deprovisioning process, you can ensure that a user will no longer have access to your network, applications, or information as soon as they exit. And by simultaneously removing their access through your enterprise access management system, you add an additional layer of security to make sure all access is removed.

Meeting requirements without taxing your team

The requirements for cyber insurance laid out above are also security best practices that can help your organization stay safe. But they can also be resource-intensive to set-up and maintain. Imprivata understands this and has created purpose-built professional and managed services packages to help you implement these solutions and system quickly and cost-effectively. Imprivata experts become an extension of your team, helping you ensure security – and meet cyber insurance requirements – while not overtaxing your internal teams.

For existing Imprivata customers, the infrastructure to support all of the above solutions is already in place, meaning that you are able to meet these requirements right now, with a comprehensive platform from a single, trusted partner. The Imprivata digital identity portfolio can help your organization stay secure and meet cyber insurance requirements.

imprivata®

Imprivata, the digital identity company for healthcare, provides identity, authentication, and access management solutions that are purpose-built to solve healthcare's unique workflow, security, and compliance challenges.

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

PAM-DS-cyber-insurance-requirements-0522