Pagefreezer Security

Pagefreezer

Application, Platform, and Organizational Security

Our customers place trust in Pagefreezer to secure data. Our application, platform, and organizational security is designed around the idea that no one should ever gain unauthorized access to electronic records. We want to do everything we can to help customers have secure archives. With this in mind, we offer a host of features to empower our customers with complete control over how archived data is accessed.

SOC 2 Type I & II Compliance

Pagefreezer is SOC 2 Type 1 and Type 2 compliant. Our independent auditor's report attests that Pagefreezer has put in place controls for information security and confidentiality that are suitably designed (according to the trust services criteria), and that after in-depth testing and examination, these controls operated effectively throughout the review period. The data centers that we use are also SOC compliant.

ISO 27001 Certification

Pagefreezer's management system is ISO 27001:2013 certified, meaning that we consistently meet the security goals outlined in ISO 27001. This includes limiting data access only to those who are authorized, protecting data integrity by preventing unauthorized alteration, and offering customers reliable access to the data that they need. Pagefreezer also makes use of data centers that are SSAE18 and ISO 27001 certified.

Single Sign-On (SSO)

Pagefreezer offers single sign-on (SSO) as a way of logging into the Pagefreezer dashboard. This means that customers making use of an identity and access management (IAM) solution—like ADFS, OpenAM, Okta, or Ping Identity—can use it to grant their platform users access to the Pagefreezer dashboard.

Two-Factor Authentication (2FA)

2FA can be deployed to require users to authenticate with a second factor when logging into the Pagefreezer platform. When activating 2FA, administrators can choose between a security code sent via email or verification through a third-party app such as Google Authenticator.

IP Whitelisting

IP whitelisting allows platform administrators to limit access to specific IP addresses (or an IP range). This is useful in a scenario where an organization wants to ensure that employees can only access records from company premises.

Timestamps and Digital Signatures

Pagefreezer stamps each archived page with an RFC 3136 compliant Time Stamp Authority (TSA) synchronized with the atomic clocks of a Stratum-1 Time Server. This non-refutable time cannot be altered without detection. Each archived page also boasts a SHA-256 digital signature, ensuring data integrity and authenticity.

User, Group, and Role Management

To ensure that organizations have control over who exactly has access to what electronic records, Pagefreezer offers advanced user, group, and role management that makes the appropriate provisioning of users simple and easy. The archive activities of all users are also logged to easily monitor actions.

Concurrent Login Management

To curb the sharing of credentials in the workplace and reduce the attack surface for a potential breach, platform administrators can control the number of concurrent logins for each user. For instance, should a second user log in with credentials already in use, the system will remove the original user from the platform.

Password Policy Management

Pagefreezer automatically enforces strong password policies for all accounts, but platform administrators can also set password policies that align specifically with an organization's internal security requirements.

Data Encryption

In order to reduce the risks that sensitive data is exposed to, Pagefreezer encrypts data both in transit and at rest.

Audit Logs

Audit logs give platform administrators detailed insight into all activities on the system, including what exactly was done, who did it, and when this activity took place.

Backup and Recovery

Disaster Recovery support is offered through data backup with fail-over, as well as the ability to recover content within 30 days of deletion.

Protect What Matters