Lucidscale

Security | White Paper

How Lucid protects your data

Nathan Cooper, Sr. Information Security Architect
David Torgerson, Sr. Director of Engineering

October 2021

lucidscale.com
1-844-GO-LUCID
sales@lucidscale.com

Lucidscale security practices

We know that cloud storage requires extra effort to protect your data. Lucidscale has processes in place to keep your data secure and accessible to the right people. We use best practices for security for all three cloud providers that integrate with Lucidscale—AWS, Azure, and GCP. Third-party access, permissions, user IDs, and storage practices are outlined here.

Imported AWS data is embedded as part of the Lucidscale document, so clients control access to the imported data using Lucidscale's standard sharing permissions. Lucidscale can securely store your AWS IAM credentials after performing the initial scan of your AWS infrastructure. Your credentials will be transferred to our servers using standard encryption methods.

Additionally, clients may negotiate encryption protocols up to AES-256 and we utilize "describe and list" permissions to access your environment.

Privacy

Lucidscale claims no ownership over any document data. You retain all intellectual property and other rights to your documents and the information they contain. Lucid constantly reviews controls to ensure that industry standards and best practices work together to prevent unauthorized access.

To ensure the privacy of your information, all data is transferred between user devices and Lucidscale servers using up to 256-bit encrypted connection via TLS 1.2 and a world-class certificate provider. Lucidscale also employs encryption at rest (AES-256) to protect the secrecy of all data persisted by the application. The cryptographic keys used to secure Lucidscale are protected by Amazon's Key Management Services, which is FIPS 140-2 validated.

While we do everything possible to prevent security incidents, we also build appropriate plans to handle such an occurrence and fulfill our responsibilities to our customers. If Lucid experiences a security incident that exposes customer data or access credentials, we will work with our customers to investigate the incident as outlined in our Security Incident Response Plan. Notification timeline and instructions are built into the contract with the customer, outlining how Lucid will notify users if an incident occurs.

We provide a backup and retention plan of six months that protects your data. If you choose to end your contract with Lucid, we support immediate deletion of customer data except for disaster recovery backups, which will be deleted after six months.

Compliance certifications

Lucidscale complies with applicable local and international requirements and maintains appropriate compliance certifications. Lucid currently maintains:

- PCI compliance
- SOC 2 Type II certification
- CCPA compliance
- GDPR compliance

Security and availability

Lucidscale is powered by Amazon Web Services (AWS), the industry's leading provider of secure computing infrastructure. AWS provides stringent security measures, which include the following certifications:

- SOC 2 audits
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)
- ISO 27001 certification
- U.S. General Services Administration FISMA-Moderate level operation authorization

To learn more about the security procedures employed by AWS, please **review their documentation.**

Visibility and control

Lucid Enterprise features allow you to maintain governance of your accounts so you can better adhere to compliance requirements. These features include document sharing restrictions, allowed IP restrictions, and allowed domains. We offer Key Management Service (KMS), which allows customers to control their own unique encryption keys to add an additional level of security.