Lucid

Security Information

How Lucid protects your data

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

October 2021

Lucid is the only visual collaboration suite that helps teams see and build the future from idea to reality. Its products, Lucidchart and Lucidspark, provide users with an end-to-end experience that helps teams truly see and build the future, by enabling collaboration and clear communication.

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

About Lucid Software

Lucid products are delivered through a software-as-a-service model that avoids upfront costs and IT operational burden. Lucid applications are designed to be seamlessly integrated with several collaboration platforms your organization is already using.

Integrations

Lucidchart ● Lucidspark ○ Lucidscale ●

- G Suite ●
- Confluence ● ●
- Jira ●
- Microsoft Office 365 ●
- Quip ●
- Salesforce ●
- Slack ● ○
- Jive ●
- Gemini ●
- AWS ● ●
- GCP ●
- Azure ●
- Zapier ●
- BambooHR ●
- LeanIX ●
- Lucidspark ●
- Lucidchart ● ○
- Zoom ○

Lucid import & export options:

- Visio import
- Visio export
- OmniGraffle import
- Gliffy import
- draw.io import

Information security governance

Securing customer data is a primary objective at the highest levels of management at Lucid Software. To this end, Lucid maintains a team dedicated to securing Lucid's systems, processes, and controls. This team develops and implements the overall security program at Lucid, including training sessions, internal audits, and evaluations of compliance.

The security team at Lucid assists operations in maintaining systems related to event reporting, identity management, and configuration management, ensuring that they are properly geared to accommodate the security requirements of the customer.

Secure architecture, controls, and partners

Lucid delivers secure visual collaboration through a defensive application architecture, a system of internal controls, and a set of policies governing partnerships and integrations. Lucid provides security across many dimensions, including data secrecy, authentication, authorization, and auditing.

Secure infrastructure

Lucid applications are powered by Amazon Web Services (AWS), the industry's leading provider of secure computing infrastructure. AWS meets stringent security requirements, including a variety of physical controls to the data centers, data privacy guarantees, and robust controls to its services. AWS has published white papers on risk and compliance and security processes. AWS has achieved the following certifications and third-party attestations:

AWS certifications

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

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

Data encryption

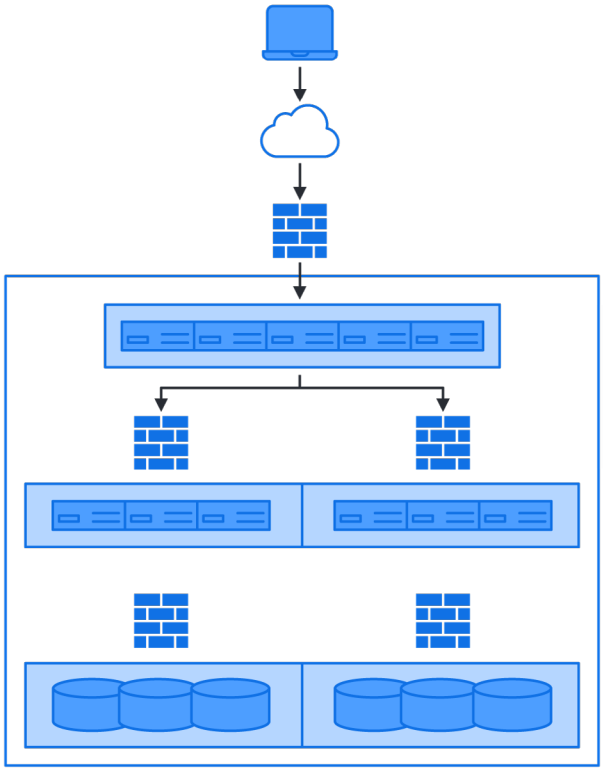
Lucid Software understands the sensitivity of private business documents, ideas, communication, and personally identifiable information. To ensure the privacy of this information, all data is transferred between user devices and Lucid servers using up to 256-bit encryption via TLS 1.2 and a world-class certificate provider. Lucid Software also employs encryption at rest to protect the secrecy of all data persisted by the application. All databases, database-backed caches, and other components with persisted data have their disks initialized with random data using a high-entropy, random data source. During use, the disks encrypt their contents with 256-bit AES with ESSIV. The cryptographic keys are protected by a pair of redundant passphrases stored in separate environments.

Network protection

Lucid applications run in an AWS Virtual Private Cloud (VPC) that is not accessible from the public Internet. All traffic to and from the public Internet must travel through specific gateways.

The Lucid Software operations team uses secure connections for working on VPC machines. Network access to the environment happens through an industry-standard VPN solution that is locked down to a strict set of clients. SSH connections to the VPC servers use Diffie-Hellman 2048 for key exchange and encrypt the entire session with industry-standard Blowfish cipher and 2048-bit unique keys. Keys are generated per user and can be shut off individually upon termination.

To provide rigorous access control, the various services and service tiers are segregated by network layer (IP) and transport layer (TCP & UDP) firewalls. The firewalls are implemented by AWS Security Groups and limit all inbound network connection attempts, except with strict sets of client machines for each service (see Figure 1 below).



Availability

An integral part of the Lucid Software service is the ability to securely access the applications at any time and from any device or location. Documents, account information, access control lists, and other persistent data is replicated across availability zones using industry-standard database management systems, replication, and failover solutions.

All services are clustered and served through AWS Elastic Load Balancers (ELBs), giving users access to their documents whenever they need it.

One of the benefits to software-as-a-service is that users always get the latest version of the software at no cost and without any work by IT. That is true for Lucid applications, plus our biweekly upgrades are done with no downtime. Users will never receive a “down for scheduled maintenance” page when they need to finalize critical documents for a meeting or deadline.

Because components may fail on occasion, the Lucid Software operations team maintains a robust automated live site monitoring system and a 24/7 on-call rotation to ensure that the redundancy, failover, and self-healing mechanisms work properly at all times.

Disaster recovery

Customer documents and related data are backed up hourly to multiple physical environments across availability zones in encrypted format. The Lucid Software operations team performs regular validations of these snapshots to ensure that they can be used for restoration in the event of an emergency.

Content controls

Application

Authentication

Lucid applications give team administrators the flexibility to set the password policy for their account. They can set the required password length, required character classes, and frequency of password changes. Admins may also manually force all team members or individuals to reset their passwords.

Passwords are never transmitted in plain text. Only salted one-way hashes of passwords are ever stored by Lucid servers, never the passwords themselves. Individual user identity is authenticated and re-verified with each transaction, using a secure token created at login.

Authorization

We follow security best practices and protect your data by using the principle of least privilege access. A simple role-based permissions system allows administrators to manage access to documents owned by the account. There are two primary sets of access controls: account controls and document controls. Four roles exist in regards to account management: account administrator, team administrator, user, and billing administrator. The following table lists the features that each role may access.

Permission	Account Admin	Team Admin	User	Billing Admin
List team members				
Manage group membership				
Set (not view) user passwords				
Manage team settings				
Manage integrations with other apps				
Manage team admins				
Manage subcription level				
Manage payments				

The account management tools allow account and team admins to remove users from their account, as well as delete users that are part of their account. In the latter case, the admin has the option to take ownership of any documents that the deleted user owns.

Through the team settings page, admins can:

- Restrict document sharing on social networks.
- Restrict publishing of documents as web pages, exportable documents, and images.
- Restrict the generation of public links to documents.
- Restrict sharing to users with email addresses under certain domains.
- Restrict user login to whitelisted IP addresses.

In relation to Lucidchart documents, there are four roles that users could have: owner, editor, commenter, and viewer. The creator of the document automatically occupies the role of owner, though this setting can be changed. Documents are private by default, i.e. no other user has any level of access to the document. The following table lists the features that each role may access.

Permission	Owner	Editor	Commenter	Viewer	Anonymous Contributors *only for Lucidspark
View document					
Edit document					
Comment on document					
Delete document					
Share document					

Data ownership

Lucid Software claims no ownership over any documents created through our services. Users retain copyright and any other rights, including all intellectual property rights, on created documents and all included content.

We respect your privacy and will never make your documents or other information publicly available without permission

Internal controls

Lucid Software uses a multidimensional control framework to ensure that security is maintained and continually improved. Company leaders support security and provide a positive control environment. Risk assessment is performed by both internal and external system reviews. Security information and objectives are openly shared among team members, and security measures are continually monitored and improved.

Operations

Administrative access to the production environment of Lucid applications is controlled. Only authorized members of the Lucid Software operations team have access to the AWS console that manages the environment. Least privilege access is designed so that team members with a legitimate need to access components, such as production logs, may do so without administrative access to critical processes and secure drives.

Internal reviews

Security reviews are performed at multiple stages in the development process. All critical architecture designs are reviewed by the relevant system maintainers. Code reviews of implemented designs include security reviews. These reviews verify secrecy, authentication, authorization, and other security needs of each feature or component.

External reviews

Lucid Software hires a third party to perform penetration testing. These security professionals analyze Lucid applications for vulnerabilities such as the OWASP Top 10 threats and WASC threat classes. These analyses are performed semi-annually using industry-leading automated tools and extensive manual testing.

Partners

Many users are attracted to Lucid applications because of their easy integration with a variety of popular business applications. These integrations include on-premise applications like local Confluence instances and Microsoft Word, as well as many cloud-based services like Google Drive and Confluence OnDemand. Lucidchart and Lucidspark integrations can be managed by account and team admins.

Single sign-on

Lucidchart supports single sign-on (SSO) using the popular OpenID technology. Supported OpenID providers include Google and Yahoo.

Lucid also supports single sign-on through Security Assertion Markup Language (SAML). SAML is an XML-based framework for communicating user authentication, entitlement, and attribution information. When a customer enables SAML integration, Lucidchart acts as the service provider and the customer's SAML service acts as the identity provider.

On-premise applications

Lucidchart's Microsoft Word integration uses a sandboxed browser built into Word. The browser opens up a version of the Lucidchart site on the lucidchart.com domain. Because the integration occurs through the browser, a user can access their diagrams using standard username and password. Those credentials are not shared with Word.

Admins for on-premise Confluence instances have the option to add the Lucidchart plugin

if desired. It is configured using an OAuth key and secret that are unique to that team and that only team and account admins can access on lucidchart.com. Confluence users are then able to insert Lucidchart diagrams using industry-standard OAuth.

Cloud-based applications

Lucid applications integrate with Google Apps, Google Drive, Slack, and Jive using OAuth. Because these applications use OAuth, user passwords are never entered into or stored by a third-party application. The integrations require minimal configuration by the admin.

Lucidchart integrates with Confluence Cloud using JSON Web Token (JWT) authentication. Like OAuth, user passwords are never entered into or stored by a third-party application, and the integrations require minimal configuration.

Visio viewers

Lucidchart supports the viewing of Microsoft Visio files on the web through its Visio API. Lucidchart plugins with Box.com and on-premise Confluence instances enable users of those apps to view Visio files.

Users access the viewer by manually selecting a single Visio file to view in Lucidchart. The file is sent over a secure HTTPS connection (see data encryption section) to the Lucidchart servers, and the plugin receives an HTTPS URL to a web page that allows the user to privately view the diagram. The web page is secured by a time-limited, secure token known only to that client.

The Visio files are not stored permanently by Lucidchart unless the user manually selects to import it into their Lucidchart account after viewing it. If the user does import the file, it is protected by all of the standard authentication and authorization mechanisms described above.

Summary

Lucid is the only visual collaboration suite that helps teams see and build the future from idea to reality. Its products, Lucidchart and Lucidspark, provide users with an end-to-end experience that helps teams truly see and build the future, by enabling collaboration and clear communication.

Lucidspark is a virtual whiteboard application for freeform ideation, group brainstorming and real-time collaboration across teams. Lucidchart is an intelligent diagramming application for understanding the people, processes and systems that drive business forward.

Lucid products are utilized in over 180 countries by more than 30 million users, including customers like Google, GE, NBC Universal and Johnson & Johnson and ninety-nine percent of the Fortune 500. Lucid's partners include industry leaders such as Google, Atlassian, Amazon Web Services, Salesforce and Microsoft. Since the Utah-based company's founding in 2010, it has received numerous awards for its product, business and workplace culture.

For more information, visit https://lucid.co.

Resources

https://aws.amazon.com/security/

http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

https://aws.amazon.com/security/
http://openid.net/

https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20

http://oauth.net/

http://self-issued.info/docs/draft-ietf-oauth-json-web-token.html