Lucidchart

RESEARCH GUIDE

Lucidchart Security

Abstract

Lucidchart is a leading collaborative online diagramming application provided by Lucid Software, Inc. It provides an intuitive interface for building flow charts, mind maps, org charts, architecture diagrams, and more. The power, simplicity, affordability, and security of Lucidchart have driven its adoption by hundreds of thousands of individuals and teams from numerous businesses and educational institutions.

The following paper introduces Lucidchart's security policies, practices, and procedures. Review it to gain an understanding of how Lucidchart employees, service providers, and partners safeguard customer data.

This paper outlines:

- The architecture security for our software-as-a-service product
- The controls directly available to end users and account administrators
- The internal controls and external reviews that are employed to cover both application development and live site operations
- The security procedures and safeguards for our integrations with other products, such as Google Drive

Use the table of contents below to navigate this document and find content relevant to your needs.

Visit www.lucidchart.com/users/registerLevel to try Lucidchart free, or contact our sales team at sales@lucidchart.com or 1-844 (GO) LUCID for more information.

January 2015

About Lucidchart

Lucidchart is delivered through a software-as-a-service model that avoids upfront costs and IT operational burden. It is designed to be seamlessly compatible with several productivity platforms. The tables below outlines some of the services with which Lucidchart is either integrated or compatible.

Lucidchart Integrations	
Google Apps	✓
Google Drive	✓
Box	✓
Confluence	✓
JIRA	✓
Jive	✓
Gemini	✓

Lucidchart Import and Export Options	
Visio Import	✓
Visio Export	✓
OmniGraffle Import	✓
Gliffy Import	✓

Secure Architecture, Controls, and Partners

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

Our unique architecture ensures that our customers' names, emails, documents, images, and other intellectual property are available and protected at all times. Industry-standard encryption, multiple physically separate data centers, and dedicated engineers make Lucidchart the de facto charting application for corporations and individuals worldwide.
-Matthew Barlocker, Chief Architect, Lucid Software, Inc.

Architecture

Secure infrastructure

Lucidchart is powered by Amazon Web Services (AWS), the industry's leading provider of secure computing infrastructure. AWS meets stringent security measures that include 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. The table below outlines the certifications and third-party attestations that AWS has achieved:

AWS Certifications	
SAS70 Type II audits	✓
Level 1 service provider under the Payment Card Industry (PCI) Data	✓
ISO 27001 certification	✓
U.S. General Services Administration FISMA Moderate level operation	✓

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, communication, and personally identifiable information. To ensure the privacy of this information, all data is transferred between user devices and Lucidchart servers using a 256-bit encrypted connection via TLS 1.1 and a world-class certificate provider.

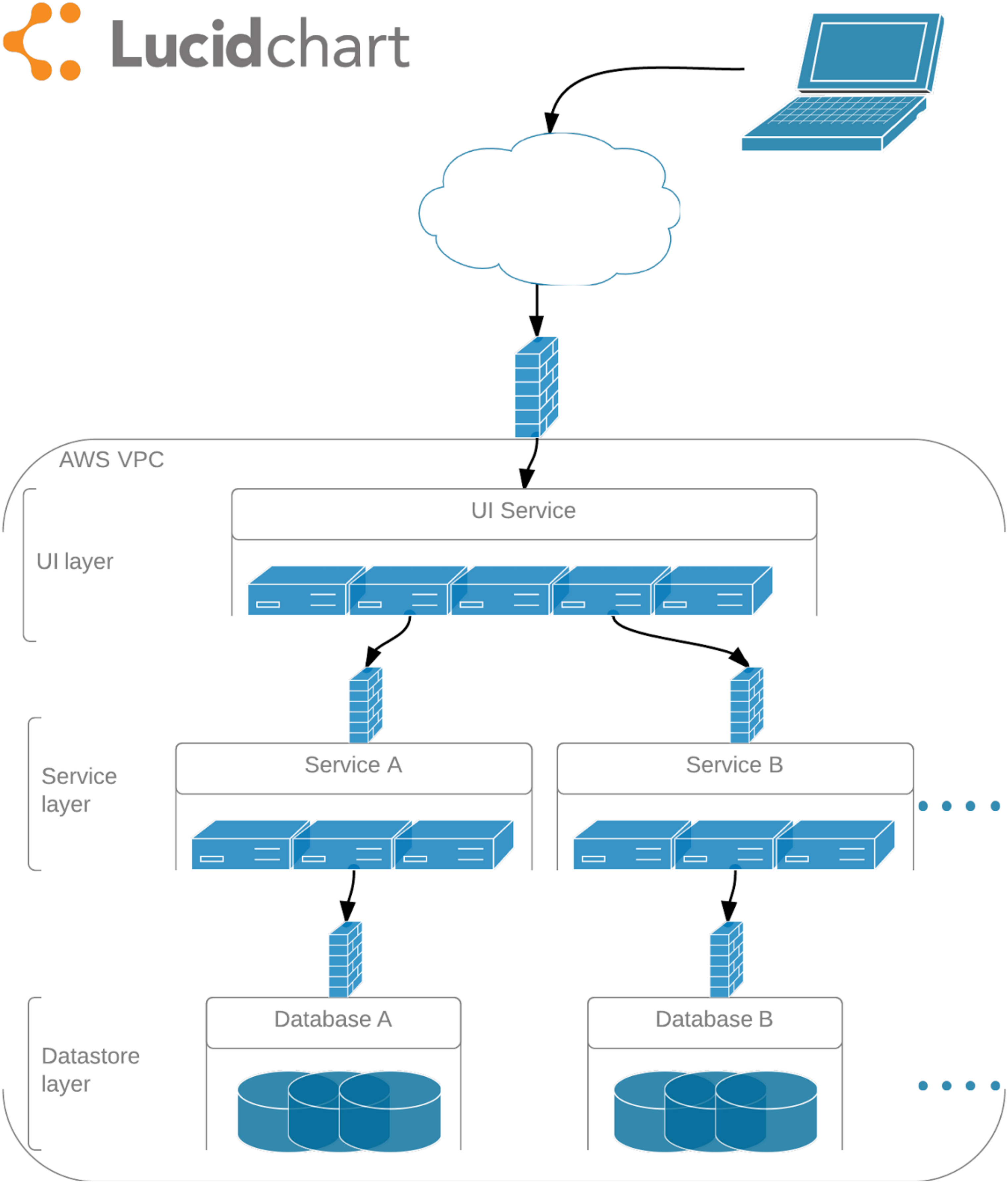
Lucidchart also employs encryption at rest to protect the secrecy of all data persisted by the application. All databases, database-backed caches, and other components with persisted data have their disks initialized with random data using a high-entropy, random data source. During use, the disks encrypt 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

Lucidchart runs 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 OpenVPN server that is locked down to a strict set of clients. SSH connections to the VPC servers use Diffie-Hellman 1024 for key exchange and encrypt the entire session with industry-standard Blowfish cipher and 1024-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).


AWS VPC
UI layer
UI Service
Service layer
Service A
Service B
Datastore layer
Database A
Database B

Availability

An integral part of the Lucidchart service is the ability to securely access the tool at any time and from any device or location. Lucidchart is architected from the ground up to be highly available. 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 needed.

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 Lucidchart, and our biweekly upgrades are done with no downtime. This means users will never receive a “down for scheduled maintenance” page when finalizing 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

Closely related to uptime is 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

Lucidchart gives 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 to reset their passwords.

Passwords are never transmitted in plain text. Only salted one-way hashes of passwords are ever stored by Lucidchart servers, and 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 is available to Lucidchart user administrators. 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. Table 4 lists the features that each role may access.

Permission	Account Admin	Team Admin	User	Billing Admin
List team members	✓	✓	✓	✓
Manage group	✓	✓		
Manage account users	✓	✓		
Set (not view) user	✓	✓		
Manage team settings	✓	✓		
Manage integrations with	✓	✓		
Manage team admins	✓	✓		
Manage subscription level	✓			✓
Manage payments	✓			✓

The account management tools allow account admins and team admins to both 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.

Admins may enable or disable the following features through the team settings page:
- Sharing of diagrams on social networks
- Publishing of diagrams as web pages, exportable documents, and images
- Generation of public links to diagrams
- Restriction of sharing to users with email addresses under certain domains.

In relation to Lucidchart documents, there are four roles: owner, editor, viewer, and commentor. The creator of the document automatically occupies the role of owner, though this can be changed. Documents are private by default, i.e. no other user has any level of access to the document. Table 5 lists the features that each role may access.

Permission	Owner	Editor	Viewer	Commentator
View document	✓	✓	✓	✓
Edit document	✓	✓		
Comment on document	✓	✓		✓
Delete document	✓			
Share document	✓			

Data ownership

Lucidchart 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 multi-dimensional 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 Lucidchart 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 team members with 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 several Lucid Software team members, including the CTO, Chief Architect, VP of Engineering, and others. 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 Lucidchart for OWASP Top 10 threats and all 26 WASC threat classes. These analyses are performed semi-annually using industry-leading automated tools and extensive manual testing.

Partners

Many users are attracted to Lucidchart because of its easy integration with a variety of popular business applications. These 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 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 are Google and Yahoo.

Lucidchart 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 a 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 which 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

Lucidchart integrates with Google Apps, Google Drive, 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.

Conclusion

Lucidchart employs powerful defense procedures to keep its customers' documentation secure. It provides secure diagramming to business users through a secure architecture, effective administrative tools, and a selection of partners respected by enterprises for their security.

The architecture implements secrecy through encrypted transmissions and storage of data. That data is made highly available and reliable through modern replication, backup, failover, and monitoring techniques. Authentication and authorization are foundational features of the service, with administrative controls to tune the system to meet different corporate guidelines and policies. In its integrations with several popular business tools, Lucidchart applies the same rigorous security standards.

Lucid Software is also committed to following information systems best practices of internal controls and external reviews.

Contact us

To explore Lucidchart's features, including a range of collaboration options and shape libraries, join our sales team for a live demo of the software. We're happy to demonstrate its ease of use, as well as answer any questions you might have.

Contact Lucidchart sales at sales@lucidchart.com or 1-844 (GO) LUCID to discuss service options.

Sources

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