Security Guide

Published: November 2020

Contents

Disclaimer: The content contained herein is correct as of November 2020 and represents the status quo as of the time it was written. Lumi.Media's security policies and systems may change going forward, as we continually improve protection for our customers.

Operational Security

Vulnerability Management

At Lumi.Media, we employ the following security practices to ensure your data remains safe:

- All developer code is peer reviewed.
- All developer code is checked through a comprehensive set of environments; from development to testing, quality assurance, staging and finally, production.
- All servers in all environments are protected by independent third party monitoring / deployment tools.

  These tools:

  - Monitor all configuration and deployment changes.
  - Monitor all access and report on administrator access.
  - Check external and internal attack vectors for vulnerabilities.
  - Harden all deployment containers whenever possible new vulnerabilities are discovered.
- All servers are fronted by CloudFlare.
- All communication between servers utilise SSL.
- All communication between servers and subscribers utilises SSL.

Operational Security

Malware / Ransomware Prevention

The term malware or ransomware refers to software that intentionally damages devices, steals data or causes chaos. This malicious software is usually embedded within an innocuous looking file that tries to trick you into clicking on it and running the software. For the damage to occur the software must be executed (run) on your device or your own servers.

Lumi and your data cannot be damaged in any way by any virus infected file. All files remain inert and harmless while in Lumi. But, an infected file can spread to other devices simply by being available for other users to download it. At all times you should ensure your devices have all the latest malware / virus protection software installed.

Lumi allows organisations to integrate with Microsoft Office Online where users can edit Word, Excel and PowerPoint documents within the browser. Editing documents within the browser gives an added layer of malware protection as the document is compartmentalised from your device.

Incident Management

Lumi.Media has incident response team and notification procedures to handle security incidents and mitigate risks. The team has clear procedures in place for communicating the incidents to any involved party and for handling escalations. The level of severity is a measure of its impact on, or threat to, the operation or integrity of the customer and its information.

Secure Technology

Location and Hosting

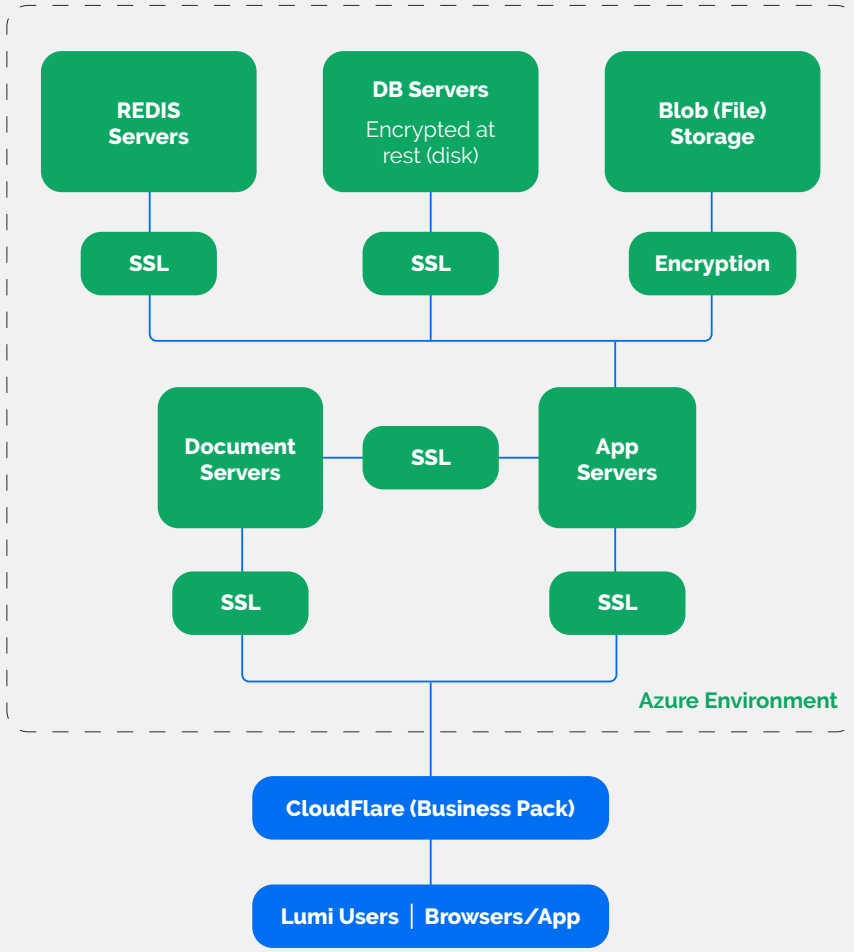
Lumi is deployed on Microsoft Azure's SaaS service.

The app and document servers are hosted in Microsoft Azure data centres in the "Australia East" region (in NSW, Australia).

All data in Lumi is kept safe in Azure's double encrypted, offsite redundant backup storage. All media (documents, images etc.) and the database data itself are encrypted in transit (SSL) and at rest.

Azure provides extremely secure facilities with world class back-up and security.

Our Azure servers are fronted by CloudFlare for DDoS protection, caching speed of delivery and web threat shielding. For more information see here.



Secure Technology

Location and Hosting [Continued]

Microsoft provides an incredibly high level of data security that far exceeds what most, even large, companies achieve when self hosting. You can find more information on Microsoft's security standards and procedures here.

By using the Microsoft Azure SaaS platform Lumi gains the backing of the Azure Security Center (ASC) that helps prevent and detect threats with tools that monitor traffic, collect logs, and analyze these data sources. Security Health Monitoring in ASC helps identify and solve potential vulnerabilities. Microsoft has a detailed Security Incident Response Management and notification process specific to Azure and maintains security certifications for Azure, including ISO 27001, SOC 1 & 2 Type 2, FedRAMP, and PCI Level 1.

Secure Technology

Data Safety

All data in Lumi is kept in Azure's double encrypted, offsite redundant backup storage. All media (documents, images etc.) and the database data itself are encrypted in transit (SSL) and at rest.

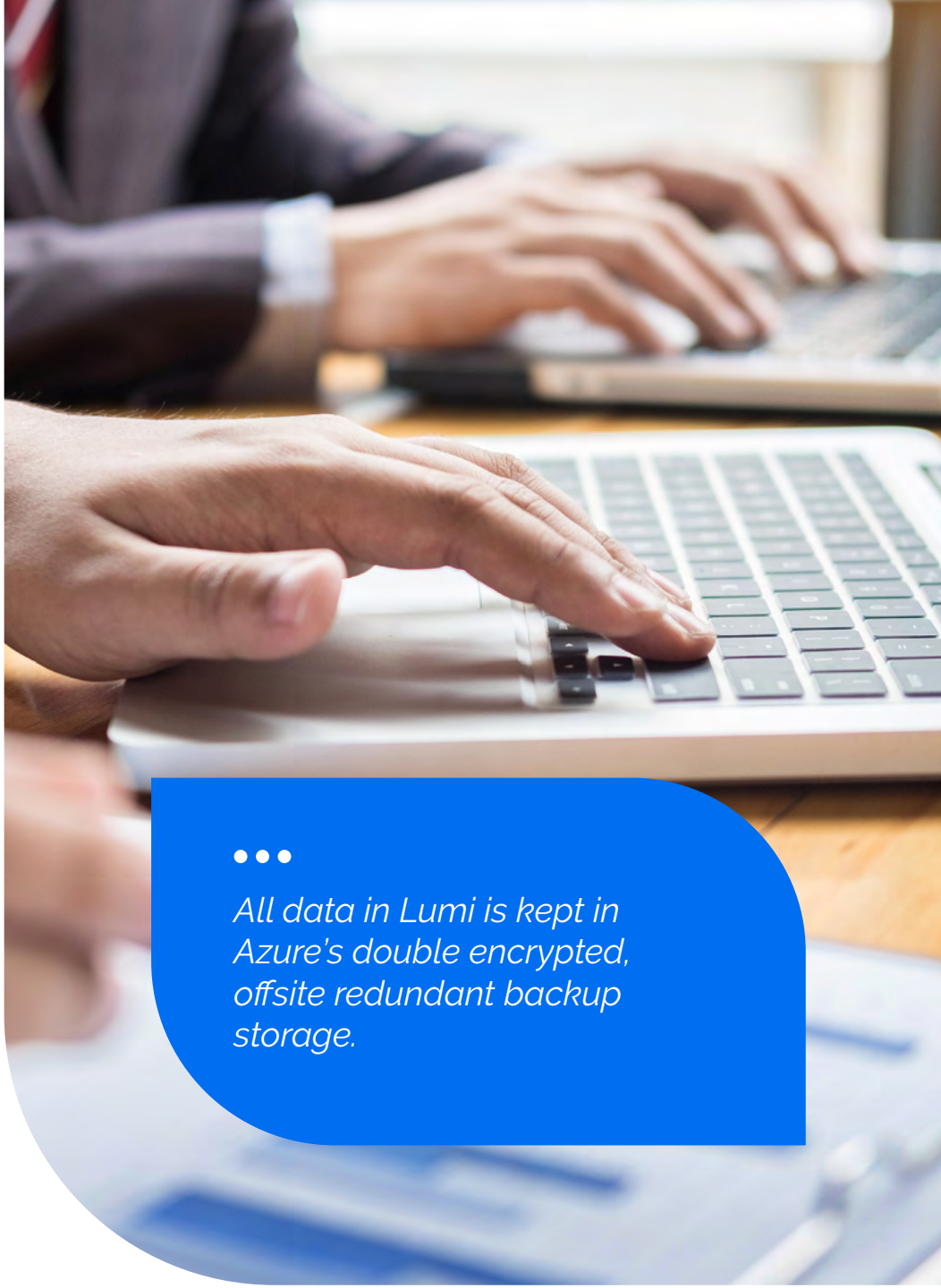
Service Availability

Our uptime historical average is 99.983%. We reserve the right to two hours per month maintenance outage window for upgrades to Lumi. However, generally an outage is not required for upgrades.

If required, Lumi.Media will enter a Service Level Agreement guaranteeing up time of 99.95%. Contact us if your organisation requires this.

Data Ownership

You own your data not us. Should you choose to stop using our services, upon request, Lumi.Media will return your data, without penalty or additional cost.



Data Access and Restrictions

Personnel Security

Lumi.Media knows that the malicious activities of an insider could have an impact on the confidentiality, integrity, and availability of all types of data and has therefore formulated policies and procedures concerning the hiring of IT administrators or others with access to production systems. Administrator permissions are continuously updated and adjusted so when a job no longer involves infrastructure management, the user's rights are immediately revoked.

Administrative Access

Only a small group of Lumi.Media employees have access to customer data. Their access rights and levels are based on their job function and role and are matched to defined responsibilities.

Customer Administrators

Within customer organizations, administrative roles and privileges for Lumi are configured and controlled by the customer. Integrated audit logs offer a detailed history of administrative actions, helping customers monitor internal access to data and adherence to their own policies.

Data Access and Restrictions

User Management

There are three levels of users within Lumi:

Account Administrators

- Able to set up new projects at the organisation, assign and deactivate Project Administrators and all other users to a project (we recommend only a select few key Senior Administrators or Executive Staff are Account Admins).

Project Administrators

- Able to invite users to a particular project, change the project and all other functions (great for senior members of the team).

Team

- Lumi users are assigned to projects.
- Cannot invite new users or deactivate etc.

For more detailed information on what each user can do, please refer to the Lumi User Management Help Guide.

Restricting Access to Information

Lumi uses Vaults to restrict access to items e.g.:

- Cards
- Boards
- Kanbans
- Lists
- Documents and Media

Every Lumi user has a personal vault and team vaults can be created to limit the access to specific items to a group within your Lumi project.

For more detailed information, please refer to the Lumi Vaults and Security Guide.

Empowering dynamic content production.

Lumi.Media are the creators of a revolutionary new approach to content making that empowers production teams to be their best, together.

Our dynamic hub brings real-time knowledge, clarity and unity to everyone, maximizing your ideas, resources and time.

Lumi connects the entire team to the whole story enabling you to reach new heights of creativity and productivity.

To learn more about Lumi.Media's dynamic content production hub, visit our website lumi.media.