LMS & CORPORATE UNIVERSITIES

Technical Documentation

Version 6.3 (February 2024)

👉 At **360Learning**, we don't make promises about technical solutions, we make commitments.
Your Data Is Yours.
Your Data Is and Will Stay Available To You.
You, and You Only.

360LEARNING IS A LEADING EUROPEAN CLOUD SOLUTION PROVIDER

" As a leading Cloud Solution Provider, we are strongly committed to providing our clients with high levels of security, SLAs and privacy, both in the contractual engagements we make and the technical infrastructure we build. We comply with French legal requirements, which are the most restrictive in terms of Data, Security & Privacy."

Nicolas Hernandez
CEO, 360Learning

👉 For more information, please contact us:

product@360learning.com ｜ www.360learning.com

Table of contents👇

360learning

Your Data is Yours

→ It really is

The client retains ownership of the data hosted on 360Learning.

At the end of the contract, clients may request 360Learning to retrieve their catalog of courses in its entirety in a standard format.

→ Our rights

360Learning employees only have access to the client's data in certain specific instances:

- → Client questions about their data
- → Problem resolution
- → Client requests to change the data

→ Confidentiality

360Learning warrants that no personal data to which it has access as data processor to deliver contracted services is sold, transferred or disclosed for commercial purposes to third parties.

→ Pseudonymisation

360Learning guarantees that personal data is isolated in a unique collection of our databases, and that all other business data (training content, training statistics, groups, courses ...) use a random identifier to reference each user, guaranteeing a pseudonymisation of personal data in accordance with the GDPR.

→ Availability

1. Minimum configuration

PLATFORM

A minimum configuration is required in order to fully benefit from the 360Learning application:

1. Verify the following workstation prerequisites: minimum display resolution of 1024x600 pixels and 256 MB of RAM.

2. Ensure all computers have a compatible browser: Microsoft Edge, Mozilla Firefox, Google Chrome or Apple Safari in a vendor-supported version.

3. Conduct network bandwidth tests in order to determine the available bandwidth for trainers and learners, and optimize the network configuration according to the type of teaching formats offered, for optimal delivery and consumption of teaching materials.

   Minimum bandwidth required for Internet connection: 512kbps per workstation for all usage including video streaming (under conditions specified in the "Video" paragraph below) and except SCORM courses.

4. Authenticate the mail servers to ensure that emails sent by the platform are not blocked by the client's IT department. The email address no-reply@360learning.com must be whitelisted in the "from" field (and not the SMTP server address field) in the mail client's settings, the mail server settings, and the anti-spam software settings. If you later customize the email address for platform notifications, you should also whitelist it in those locations. If you can not filter on the "from" field , you can whitelist the following IP addresses:
   Pre-production environment IPs:
   - 20.40.143.206
   - 20.74.25.131

   Production environment IPs:
   - 51.138.202.254
   - 20.74.1.94
   - 20.74.25.229
   - 52.252.128.38
   - 52.252.135.139
   - 20.88.12.20
   - 54.240.50.244

- 54.240.50.243

5. Whitelist *.360learning.com or the personalized domain name to ensure that members can access the platform.

6. Whitelist the domains below to access the Unsplash and Pixabay image banks
https://unsplash.com/*
https://pixabay.com/*

7. Optional: If you plan to use SCORM courses, make sure that pop-ups are authorized.

8. Optional: Whitelist api.amplitude.com and cdn.amplitude.com so that the 360Learning R&D Department has the necessary analytics tools to detect errors, fix bugs as quickly as possible and improve the user experience continuously.

To help you verify all the technical prerequisites and test your platform before its deployment, use the checklists available in our guide:

→ 360Learning - Technical Guide - Validation Procedure

MOBILE SUPPORT

Supported versions:

→ iOS 14 and higher
→ Android 5.0 and higher

On mobile devices, we only provide support for our native mobile applications. Although our platform employs responsive design, we do not support mobile web browsers.
Any custom application release or mobile application upgrades/updates are subject to the delays of the relevant application marketplace (Google Play store, Apple App store…) which remain beyond our control.

Our mobile applications support only Learner use cases. They support a wide range of course artifacts and file formats, including:

→ Course cheat sheets and 360Learning native questions
→ Images (gif, jpg, png, bmp, ico)
→ Videos (3gp, avi, flv, m2ts, m4v, mkv, mov, mp4, mpeg, mpg, mts, vob, webm, wmv)
→ PDF files
→ Microsoft Office documents (docx, xlsx, pptx)

→ Shareable content from the web (direct link, embed code or iframe code ; requires an internet connection)

VIDEO

360Learning supports uploading of HD videos and automatically creates SD versions on average 5 times smaller than the original files. A HD/SD selector is available in the bottom right-hand corner of the player so that the users can set the desired streaming quality. Please note that the player automatically adapts the video quality to the available bandwidth and that users clicking on HD consume more network bandwidth.

In order to manage bandwidth usage, please ensure the bitrate of your video files is less than or equal to the expected throughput of the target network. For example, if the desired SD and HD bandwidth usage should be lower than 512 kbps, please upload source files with a bitrate lower than 512 kbps.

2. Contents

The 360Learning platform supports the creation of cheat sheets and several types of questions, such as true / false, multiple choice, reordering, linking, sensitive areas, open questions, among others.

You can also import various types of documents:

→ Audio : .mp3, .m4a, .wav, .ogg, .aac, .opus
→ AutoCAD : .dwg
→ Archives : .zip, .rar, .7z, .rbz, .a
→ CAO : .stl
→ Calendar: .ics
→ Barcode: .btw
→ Ebook: .azw3, .epub
→ Excel: .xlsx, .xls, .xlsm, .ods, .csv, numbers, .xlsb, .gsheet, .xlt, .xltx
→ Flash: .swf, .f4v
→ Illustrations: .ai, .svg, .skp, .odg, .emf, .wmf, .vsdx, .jpe, .ps, .mcd, .psd, .xcf
→ Images: .jpg, .png, .heic, .gif, .jfif, .webp, .ico, .jpeg, .tif, .tiff, .bmp, .wdp, .jxr, .pdn, .jp2
→ JSON: .json
→ Keynote license: .key
→ Mail: .msg, .eml
→ Mathematica: .mm
→ Microsoft Power BI Report: .pbix
→ Mindmap: .xmind, .mvdx
→ Modeling: .rfa, .ifc
→ Music: .enc

- → Network report: .pkt
- → One Note: .one
- → PDF: .pdf, .xps
- → Project: .gan
- → Publisher: .pub
- → Question: .quiz
- → Table: .twb
- → Text: .log
- → Plain text: .txt, .md
- → Slideshow: .pptx, .ppt, .ppsx, .odp; .pptm, .ppsm, .pps, gslides, flipchart, .ppta
- → Vault: .dvs
- → Video: .wmv, .vob, .mts.mpg, .mpeg, .mkv, .m2ts, .flv, .3gp, .mp4, .webm, .mov, .m4v, .3gpp, .m2t, .avi
- → Word: .docx, .doc, .odt, .pages, .rtf, .story, .dotx, .dot, .wps, .sdoc
- → SCORM modules, version 1.2 or 2004

Shareable content from the web (direct link, embed code or iframe code) can also be imported, including content from services such as YouTube, Slideshare or Prezi.

3. Accessibility

360Learning employs user experience (UX) design best practices. Our Product and design teams keep stay current with the latest UX/UI trends. We optimize our platform usability thanks to continuous improvements based on data and user feedback.

At 360Learning, design is behavior and emotion as much as it is utility and facility. That is why user-friendliness and design are one of the main pillars of 360Learning's LMS, authoring tool and social and collaborative features.

360Learning draws inspiration from the standards and recommendations of the W3C (World Wide Web Consortium), the consortium responsible for promoting the compatibility of Web-based technologies, and from the RGAA (Référentiel général d'accessibilité pour les administrations) standard. The purpose of RGAA is to define the technical modalities of accessibility of the state's online services in France, as well as those of the territories and public institutions within the auspices of the state, for the three channels of the internet, television and telephony.

We are carrying out an accessibility audit this year, with the aim of achieving AA standard. To this end, we work with Level Access to monitor the changes that need to be made.

These are the elements of conformity on the 360Learning platform:

LEGIBILITY

→ The font used is Open Sans. A clear, simple font to improve legibility.
→ The use of capital letters is kept to a strict minimum.
→ Automatically generated subtitles available on course videos (standard video usage stops at 2,5 hours/user/year)
→ 360Learning favors high-contrast color combinations that facilitate optimal legibility. For example: white/black - dark blue/white. We ensure that the combination of text and background color does not fall below the recommended ratio of 4.5:1 for standard text (< 19px) and 3:1 for larger text (=> 19px).

A BALANCED STRUCTURE

To simplify content organization on the platform, our architecture enforces the following constraints:

→ A maximum of 4 sections width-wise, instead of the recommended 7
→ A maximum of 3 sections depth-wise, instead of the recommended 4

NAVIGATION BAR

The navigation system consisting of a "vertical bar" is compliant with the RGAA standard and optimizes platform navigation.

ZONING & COGNITIVE READABILITY

Navigation on 360Learning is semi-guided.
Each zone is distinctly separated and corresponds to an activity.
The structure of each course is the same, allowing the user to simplify and memorize the navigation path.

USER ORIENTATION ELEMENT

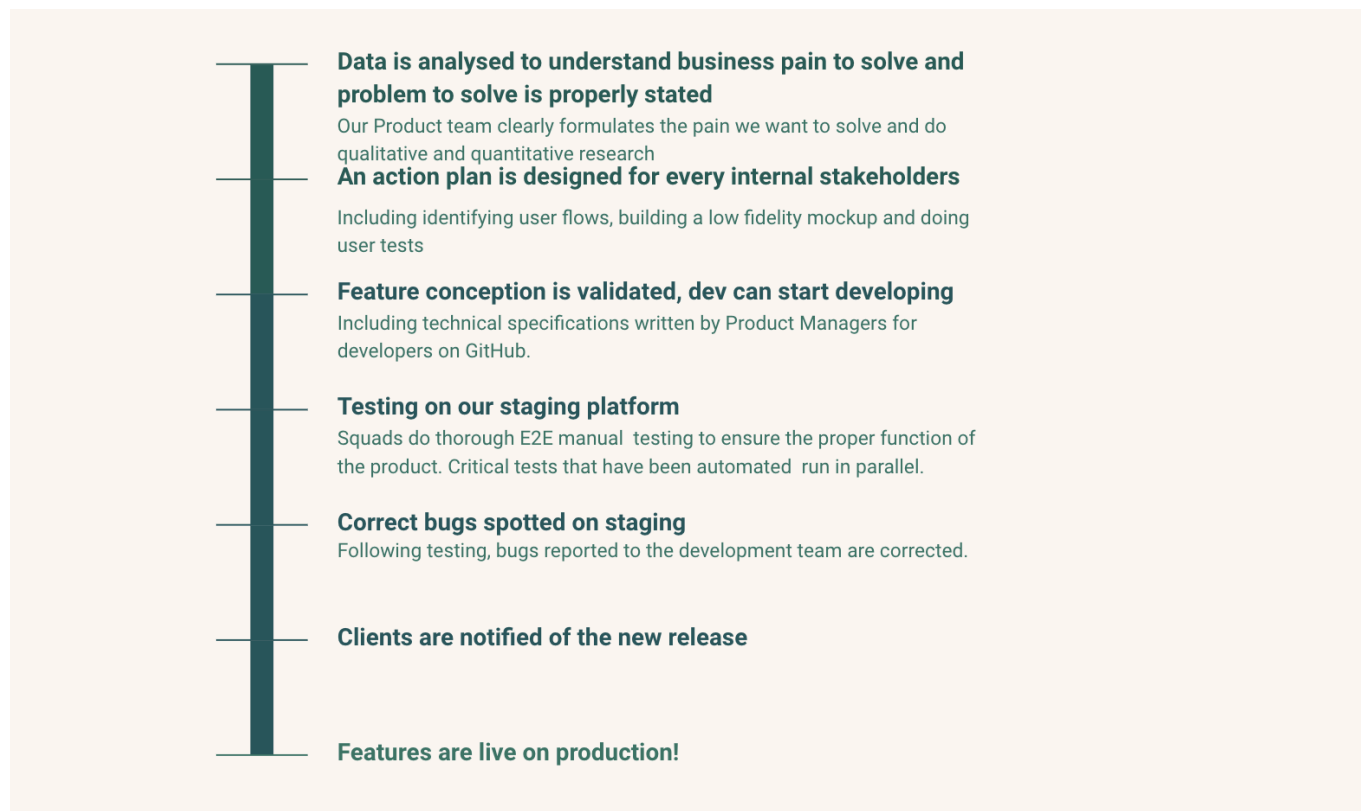The platform makes it easy for the learner to discern the displayed page from amongst the site's pages at any time. In particular, the UI provides an element that helps to learner to determine:

→ Where they are: The corresponding menu is displayed in bold and is brighter
→ Where they came from: The learner can locate himself within the program at any time
→ Where they can go next: The learner can project himself in his course
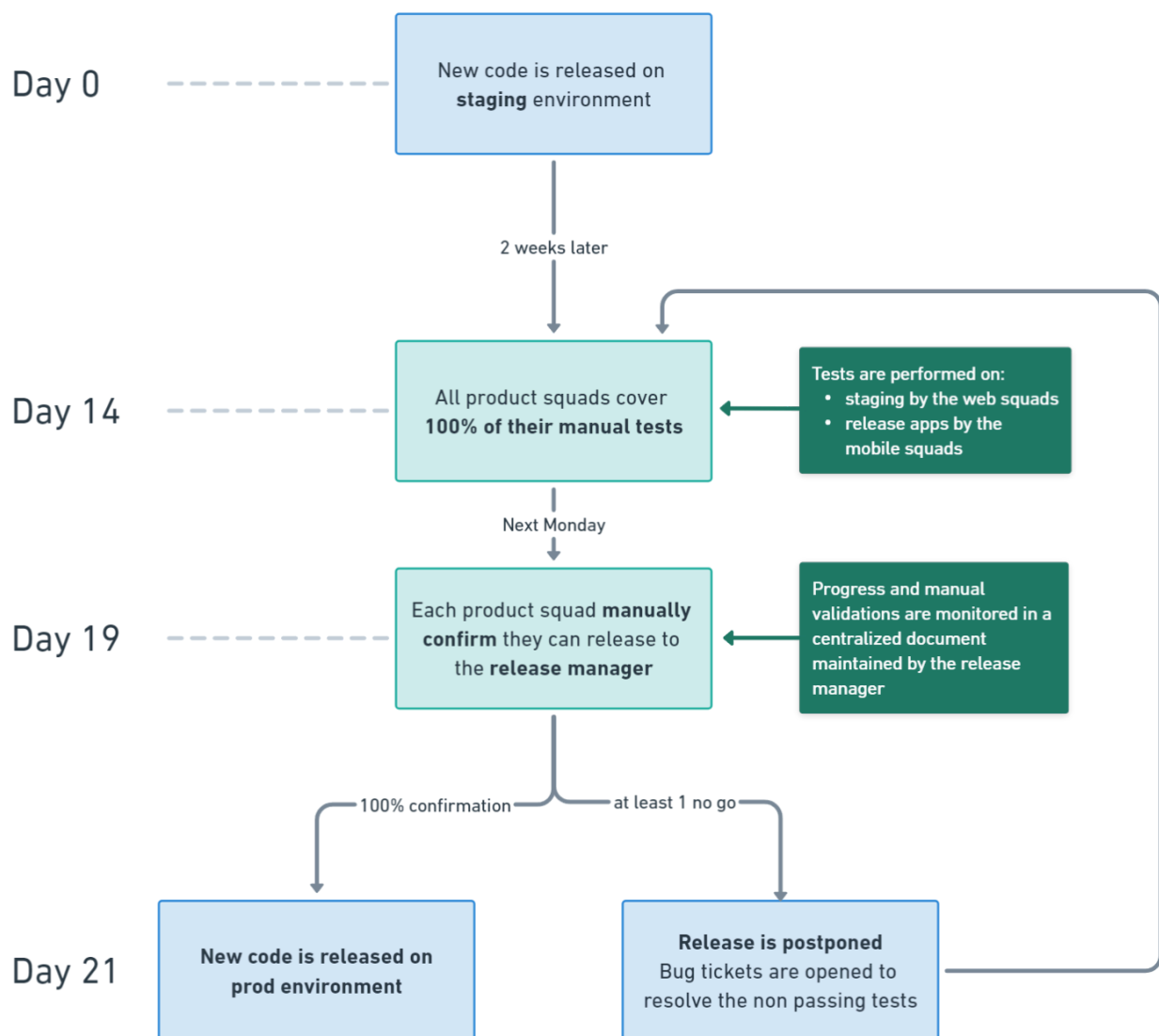
360learning

4. Development

NEW FEATURES

Every new feature is developed following a very specific plan, detailed below.👇

Data is analysed to understand business pain to solve and problem to solve is properly stated
Our Product team clearly formulates the pain we want to solve and do qualitative and quantitative research

An action plan is designed for every internal stakeholders

Including identifying user flows, building a low fidelity mockup and doing user tests

Feature conception is validated, dev can start developing
Including technical specifications written by Product Managers for developers on GitHub.

Testing on our staging platform
Squads do thorough E2E manual testing to ensure the proper function of the product. Critical tests that have been automated run in parallel.

Correct bugs spotted on staging
Following testing, bugs reported to the development team are corrected.

Clients are notified of the new release

Features are live on production!

QUALITY ASSURANCE

Every feature is tested on a **staging environment** before its deployment to the **production environment**, following the process detailed below.👇

To ensure we ship features at the expected level of quality, without breaking the other features of the platform, we're running manual end-to-end tests for each Milestone. A release manager is chosen and must ensure this process is followed, mainly by communicating with Tech Leads during the MS.

Day 0 ----- New code is released on **staging** environment

2 weeks later

Day 14 ----- All product squads cover **100% of their manual tests**

Tests are performed on:
- staging by the web squads
- release apps by the mobile squads

Next Monday

Day 19 ----- Each product squad **manually confirm** they can release to the **release manager**

Progress and manual validations are monitored in a centralized document maintained by the release manager

100% confirmation

at least 1 no go

Day 21

New code is released on prod environment

Release is postponed
Bug tickets are opened to resolve the non passing tests

Staging environment

A nearly exact replica of our production environment for software testing. We use the staging environment to test builds under a production-like environment before application deployment.

Production environment

Where the latest version of our platform is live for users. It is the environment where end users can see, experience, and interact with the product.

→ Security

1. Encryption

By default, access to the application is systematically forced to use HTTPS TLS 1.2 minimum with a compatible set of strong ciphers.

Please ensure the compatibility of your information system with this set of ciphers:

#TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1)

#TLS 1.3
TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256

N.B: We keep this list updated for maximum compatibility with recent web browsers but with a maximum level of security. The compatibility should not be an issue unless you have an old web browser or old http client library tools.

PASSWORD-PROTECTED ACCESS

Access to the application is protected by a password, which can be defined in a number of ways:

- → By the user upon first connection.
- → By an administrator upon creation of the account.
- → By the SSO mechanism, in which case 360Learning stores a random 32 characters string as a placeholder for the password in its database.

Once this password is defined, it is impossible for a 3rd party to obtain knowledge of this password by querying our database, as all passwords are irreversibly hashed using BCRYPT 10 rounds. In the event that we detect an attack, we would notify all affected clients in a timely manner.

ACCESS CONTROL BY IP ADDRESS

It is possible to filter the IP address to constrain access to the application: users can then only log in from a set location.

2. Physical security

HIGHLY SECURE DATA CENTERS

360Learning's main infrastructure is hosted on our partner Microsoft Azure. Microsoft Azure offers the highest level of security to guarantee the availability, integrity, and confidentiality of the hosted data.

CHARACTERISTICS OF THE DATA CENTERS – OVH

Security and Fire

→ Physical access to the computer servers is restricted to accredited employees
→ RFID Badge-controlled access, facilities guarded by professional security 24/7
→ Video surveillance and motion detection systems
→ Rooms equipped with smoke and heat detection systems
→ OVH builds upon the ISO 27002 and ISO 27005 standards for security management, the evaluation of risks and relevant mitigation measures.

Power Supply

→ Systematic double power supply
→ 250 KVA inverters
→ Generators with an initial autonomy of 48 hours
→ A minimum of 2 incoming network feeds to the data center; inside, 2 twin networks (rooms capable of taking over from each other)

Climate Control

→ Watercooling disperses 70% of the heat emitted by the processor
→ Aircooling disperses the remaining 30%
→ PUE between 1 and 1.2: energy consumption of the data centers constantly being reduced.

Facilities

→ OVH designs and builds its own data center since 2003
→ OVH's data centers are located outside of geographical areas subject to the Patriot Act
→ Facilities are located at least 125 miles from each other in order to ensure redundancy and continuity of service

Maintenance and technical management of the facilities

→ Technical personnel present on-site 24/7

360learning

CHARACTERISTICS OF THE DATA CENTERS – Microsoft Azure

Security and Fire

- → Autonomous access control by badge without RFID contact, and biometric through finger vein network recognition
- → Armored double-door entrance compliant with EN1627 anti-intrusion standards
- → Outdoor and indoor networks of digital cameras
- → Anti-intrusion devices on all points of access (APSAD R81) and APSAD R81 (intrusion detection)
- → Fire safety officer with SSIAP 2 specialization, on-site 24/7
- → VESDA LASER multi-point detection systems
- → SEMCO water mist fire-extinguishing systems compliant with APSAD R1/D2 and NFPA 750 standards
- → Additional RIA fire-fighting means and portable CO_2 extinguishers compliant with APSAD R4 standards
- → Fire compartment between each computer room capable of resisting fire over two hours

Power Supply

- → Input from EDF power grid via 2 two-way T-outputs of 9 MVA each
- → 7 low-voltage master distribution boards I of 2.5 MVA each, equipped with an automatic switch to generator redundancy apparatus
- → 6 gas oil generators for an installed capacity of 11.85 MVA
- → 48,800 litres of fuel oil, 50 hours of autonomy at full load
- → Area N+1: 3 independent UPS circuits
- → Area 2(N+1): 2 independent UPS circuits
- → Battery autonomy: 10 minutes at the end of battery life

Climate Control

- → 5 MW of cooling capacity in N+1 configuration
- → Redundant ice water network via looped (distribution circuits)
- → 90 kW climatic cabinets
- → Temperature maintained at 20°C +/-2°C in cold aisle
- → Systematic confined cold aisle layout
- → Independent climate control for each client room

Facilities

- → Design and construction specifically for use as a data center

Maintenance and technical management of the facilities

- → Maintenance compliant with AFNOR NF EN 13-306 and FD X60-000 standards
- → Remote monitoring of equipment by manufacturers
- → Infrastructure management by GTC Sima©

360learning

CHARACTERISTICS OF THE DATA CENTERS – AWS

Security and Fire

→ Physical access to the computer servers is restricted to accredited employees
→ Multi factor controlled access, facilities guarded by professional security 24/7
→ Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.
→ Rooms equipped with smoke and heat detection systems
→ Third-party testing of AWS data centers, as documented in our third-party reports, ensures AWS has appropriately implemented security measures aligned to established rules needed to obtain security certifications.

Power Supply

→ AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Climate Control

→ AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Facilities

→ AWS designs and builds its own data centers
→ AWS's data centers process data centers in EU which we rely on.
→ Facilities are located at least 125 miles from each other in order to ensure redundancy and continuity of service

Maintenance and technical management of the facilities

→ Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit.

360learning

3. Logical security

<div style="border:1px solid black;padding:10px;">
This is a quick summary of our security elements. For more details, please consult our Security Assurance Plan v3.1
</div>

PREVENTION OF DENIAL OF SERVICE ATTACKS (DDOS)

A DDoS attack aims to render your site unavailable by overloading the server's bandwidth or by occupying its resources until they are exhausted. The cases encountered are generally level 7 attacks (the highest level), based on the execution of a high number of requests in order to saturate the system.

Guaranteeing the online security of its clients and the availability of its service are among 360Learning's primary concerns. In order to counter these attacks, our host Microsoft Azure is adopting as standard a mitigation solution based on VAC technology. It consists of an exclusive combination of techniques that analyze your traffic in real-time and at high speed. They automatically detect and intercept attacks whilst letting legitimate requests through.

DETECTION AND PREVENTION OF OWASP ATTACKS

A Web Application Firewall Next Generation placed on our front servers filters every request to identify any potential threat. It embeds classic OWASP detection and business-specific rules to alert and block malicious attempts.
Alerts are sent to the DevOPS and the security team to launch if necessary a security incident.
All attacks are logged and kept at least 6 months to ensure proper security audits.

ANTI-VIRUS

Our solution of choice is the latest version of the ClamAV suite of tools. It is updated every 60 minutes automatically to ensure that the latest database is always used for threat detection and prevention. A scan is performed on all uploaded files and archives to ensure that no executables are stored.

If a virus is detected, the user who tried to import it is notified with this message: "Your document looks suspicious to our antivirus. Your file has not been imported." And the file is never imported.

THREAT DETECTION AND REMEDIATION

We have deployed:

360learning

- an Endpoint Detection and Response (EDR/XDR) solution Crowdstrike on each server to ensure high protection and an ability to identify any threats on our platform (ransomware, malware, rootkits, remote shell, …). Every agent is connected to a central platform which is externally managed 24/7 by the CrowdStrike teams and which escalate to the internal 360 Learning security team in case of emergency.
- a Web Application Firewall Next Generation which filters every request for all our external applications and endpoints.
- a SIEM which correlates logs from all our corporate and platform. This comes with an external 24/7 SOC which alerts the security team in case of abnormal behavior (non conformity, attack, unusual behavior such as a successful authentication from an unknown source).

ROLES WITHIN THE APPLICATION

The platform supports multiple roles and granular permission sets, enabling us to enforce a well-tuned access control policy according to the role of each user.

Roles determine what users can see and do in 360Learning. Main roles are designed to set the level of access users have to manage accounts, training content, and settings in 360Learning (admin access). Specific roles give users access to more collaborative features in 360Learning.

MAIN ROLES

Learner
Learners have access to their groups' homepages, can play training content shared by Authors, Coaches and Admins and can use the platform's social features.
Learners have no admin access.

Learner rights include:
→ Access to training content
→ Ability to post messages in groups, and forums of training content
→ Access to their personal learning analytics

Author
Authors can create training content, and share content to their group's library.

Author rights include:
→ Ability to create training content (courses, program templates, program sessions, paths and path sessions.
→ Ability to add courses, program templates and paths to the group's library.
→ Ability to create skills.
→ Ability to access the statistics of their training content.

Coach

Coaches can view and export their group statistics and share training content with their group.

Coach rights include:
→ Ability to watch any training from their group's library
→ Ability to create sessions from program templates in the group's library
→ Access to the group's training statistics from the Dashboard menu
→ Ability to add the group to a new session
→ Ability to send reminders

User Administrator

User Administrators can add and remove users from their group and perform other user management actions.

User administrator rights include:
→ Ability to invite and set up learners in their group
→ Cancel pending invitations for their group
→ Can validate registrations that have been sent by group coaches (if the validation option is activated)

Group Administrator

Administrators have full admin access to their groups. They also have all the permissions that Authors and Coaches have.

Administrator rights include:
→ Ability to set up the group settings
→ Ability to set up the Public Channel (if appointed as Admin of the company-wide group)
→ Access to the Advanced Settings of the platform (if appointed as Admin of the company-wide group)
→ Access to badge creation (if appointed as Admin of the company-wide group)
→ Can validate registrations that have been sent by group coaches (if the validation option is activated)

Platform Administrator

Platform administrators have full admin access to all groups and full admin access to the platform.

Owner

Platforms have a single Owner. They have the same permission level as Platform Admins and are the only ones who can access the billing menu.

360learning

Owner rights include:
→ All Platform administrator permissions
→ Access to Billing information
→ Download all platform data in JSON format

SPECIFIC ROLES

Main author

The main author of a course or path can edit it and access its statistics page. Only one user may be the main author; you can change it, and their permissions are transferred when they are deleted from the platform.

Main author rights include:
→ Ability to edit the training content.
→ Ability to access the statistics of the training content

Instructor

Instructors are in charge of program sessions and path sessions.

Instructor rights include:
→ Access the statistics of their path and program sessions.
→ Reception of program-related notifications (login information, comments, posts, program completed)
→ Correction of open questions
→ Correction of assessment steps
→ Management of participants in the session (add/remove participants in the session)
→ Possibility to send reminders from the session statistics

Manager

Managers can access the statistics of a user (even on courses or sessions they can't access themselves).

Managers can:
→ Access their managers' statistics from the Dashboard menu
→ Receive a weekly email featuring their managers' progress (they can disable this option for their settings)
→ Correct assessment steps

Co-Author (course or path)

Course and path co-authors have the same permissions as a main author, but their permissions are not transferred when they are deleted from the platform.

Co-authors can:
→ Edit courses and paths

Reviewer
Reviewers can review courses, and publish internal comments in the forum of those courses. This role is only available with the Champion solution.

Reviewers can:
→ Publish internal comments in a course

FIREWALL AND PORT FILTERING

Firewalls on 360Learning's servers provide an additional level of security with regard to flow control. All ports that are not necessary to the functioning and administration of the platform are closed. We use a Cloud Security Posture Management tool to alert in case a port is opened and not compliant with our security policy.

4. Internal Policies

SECURITY PASSWORD POLICY

1. **Overview**
All employees and personnel that have access to organizational computer systems must adhere to our IT charter and the password policies defined below in order to protect the security of the network, data integrity, and computer systems.

2. **Purpose**
This policy is designed to safeguard the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

3. **Scope**
This policy applies to any and all personnel who have any form of computer account requiring a password on the organizational network, including but not limited to a domain account and e-mail account.

4. **Password Protection**
→ Never write passwords down
→ Never send a password through email
→ Never include a password in a non-encrypted stored document
→ Never tell anyone your password

→ Never reveal your password over the telephone
→ Never hint at the format of your password
→ Never reveal or hint at your password on a form on the internet
→ Never use the "Remember Password" feature of application programs such as your email program, or any other program
→ Never use your corporate or network password on an account over the Internet which does not have a secure login where the web browser address starts with https:// rather than http://
→ Always use our official password manager
→ Report any suspicion of your password being compromised to your IT computer security office
→ If anyone asks for your password, refer them to your IT computer security office
→ Be careful about letting someone see you type your password
→ Use MFA whenever possible

5. Enforcement

Since password security is critical to the security of the organization and everyone, employees that do not adhere to this policy may be subject to disciplinary action up to and including dismissal.
To ensure the level of awareness of our employees, we conduct regular fake phishing campaigns, training and quizzes.

6. Other Considerations

Password protected screen savers should be enabled and should protect the computer within 10 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked.

Administrator passwords shall be protected very carefully. Administrator accounts shall have the minimum access to perform their function. Administrator accounts shall never be shared.

7. Use of a Password Wallet

The use of a Password manager, 1Password in our case, eases the aforementioned points.

What does it bring?

→ There is only one master password to remember.
→ It allows sharing access to an account in a secure way without giving the password.
→ It allows the generation of secured passwords.

How does it work?

→ AES 256-bit encryption with routinely-increased PBKDF2 iterations
→ All sensitive data is encrypted and decrypted locally before syncing with 1Password. The key never leaves the device and is never shared with 1Password. Our data stays accessible only to us.

5. Mobile application security

→ Our application uses the same servers as our web client and also connects using HTTPS with TLS 1.2 (TLS 1.3 and as such benefits from the same levels of security. As such logs are held and treated in the same manner whether generated using the mobile application or the web application.

→ Similarly, if you enforce acceptance of a Privacy Policy, users will have to agree to it on their first connection, regardless of the client used (mobile or web).

→ Geolocation data is pseudonymised upon collection for product analytics so no personal data is recorded when using our application.

→ Whether on iOS or Android offline data is not accessible in any way by another application or directly with the operating system.

→ Our mobile applications are pen-tested once a year.

6. Independent Audits

HDWSEC, HACKERONE, NeverHack: Security expert working alongside with 360Learning

HDWsec, a French security independent auditor and expert, works alongside 360Learning on the security management of its software and network infrastructure, as well as on the implementation of its security policy.

HackerOne is a famous US independent pentesting specialist which ensures deeper vulnerability tests and detailed programs to ensure maximum security and compliance.

In order to evaluate and strengthen 360Learning's security, HDWsec carries out:

→ 1 security audit per year, following the OWASP methodology with greybox and blackbox tests, including comprehensive audit of the configuration of 360Learning's architecture and simulated attacks (hacking attempts)

→ Continuous security training of 360Learning developers

→ Consultancy in the implementation of 360Learning's security policy

**In order to maximize the vulnerability and compliance knowledge of the 360Learning's security,
HackerOne carries out:**

→ 1 deep programmed security pentest audit per year with specifically chosen hackers for their knowledge of our technologies.

→ Continuous compliance check

**In order to evaluate the global level of security of the company, NeverHack conduct Red Team
exercise on the hole company assets, trying to gather information over:**

→ fake emails

→ fake phone calls

→ our corporate tools

7. Standards

SUBPROCESSORS LEGAL NAME	ISO 27001	AICPA SOC 2	PCI-DSS COMPLIANCE	ISO/IEC 27701 / ISO 27018
MICROSOFT AZURE	✅	✅	🚫	✅
OVH	✅	✅	🚫	✅
AWS	✅	✅	🚫	✅
SCALEWAY	✅	✅	🚫	✅
AMPLITUDE	✅	✅	🚫	✅
PENDO INC.	❌	✅	🚫	❌
GAINSIGHT INC.	❌	✅	🚫	✅
DATADOG	✅	✅	🚫	✅
ZENDESK	✅	✅	🚫	✅
STRIPE (for Team offer payments)	✅	✅	✅	❌
SNOWFLAKE COMPUTING NETHERLANDS B.V.	✅	✅	🚫	✅
ELASTIC APP SEARCH	✅	✅	🚫	✅
WORKATO	❌	✅	🚫	❌

✅ : Yes
❌ : No
🚫 : N/A

Service continuity

1. Internal Policies

We guarantee a 99,5% yearly uptime and a 12-hour response time for the resolution of blocking bugs (server errors).

More information on our availability and SLA can be found at https://360learning.com/legal/sla/

2. Backups

Your personal data as well as your videos, images and documents uploaded on 360Learning are hosted by our partner Microsoft Azure, in one of the Data Centers shown in the table below.

Region	Azure Data Center	Physical Location	Availability Zones	Commercial Availability
France	France Central	Paris region	3	Available to all customers
United States	US-WEST-2	Washington State	3	General availability planned in 2024

For the other training content, third-party services such as Youtube, Prezi or Vimeo are hosted by their publishers.

Azure Availability Zones are physically separate locations within each Azure region that are tolerant to local failures. Failures can range from software and hardware failures to events such as earthquakes, floods, and fires. Tolerance to failures is achieved because of the redundancy and logical isolation of Azure services. To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions.

Logical backups (service version and client data) are carried out once a day on the backup cluster remotely. This guarantees a maximum RPO of 24 hours, and we keep a 90 days snapshot history.
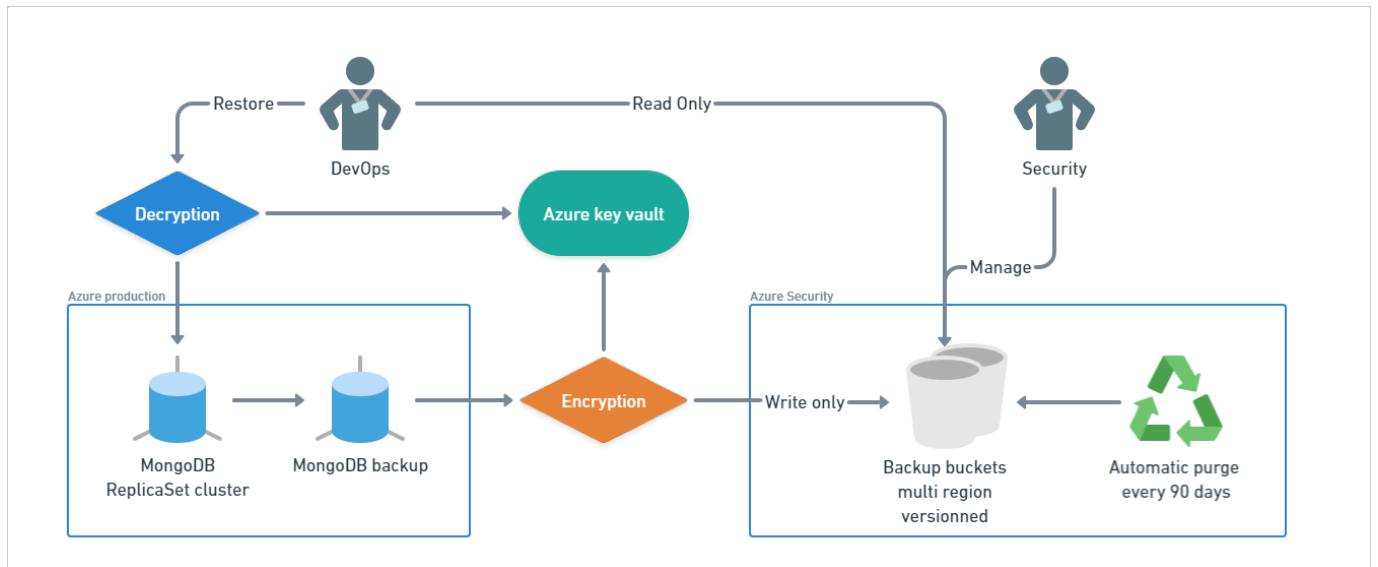
3. Redundancy

Servers are replicated. Data centers are powered by two independent current supplies and are equipped with inverters. Generators with 48 hours of autonomy ensure that power can still be generated in the event of a failure of the power supply network. Several security loops were thus established in order to avoid any potential unavailability. This multiplicity of links also enables your data to take the shortest route and therefore to be subject to the shortest lag times. Servers are also equipped with dual power supply and dual network cards for a fully redundant infrastructure.

4. Resumption of service

DISASTER RECOVERY PLAN

The DRP (Disaster Recovery Plan) is activated in the event of a disaster that impacts the integrity of the data:
→   Major logical fault
→   Physical destruction of the hosting facilities

In such a case, the client is immediately notified and the recovery procedure begins. New infrastructure is recreated in an available data center on Microsoft Azure. The data are restored from the latest version of the saved data. As mentioned previously, the complete backups (service version and client data) are carried out, stored, and encrypted four times a day on a remote storage; the data never physically leaves its storage location. This guarantees a maximum RPO (Recovery Point Objective) of 6 hours.

The maximum duration of the DRP is 12 hours. In the case of a change of data center, requiring modification of the IPs of the DNS entries, DNS caches worldwide take no more than 24 hours to update.

This guarantees an RTO (Recovery Time Objective) of less than 24 hours.

RESPONSE IN THE EVENT OF AN INCIDENT

At 360Learning's hosts

Alarms are configured to notify operational teams automatically when the first signs of alerts reach predefined thresholds. Once a threshold is reached, DevOps incident response is activated.

Microsoft Azure puts in place real-time logging and reporting systems in order to record and report security-related events.

Any events are documented and recorded for a period of 90 days after they have been observed.

On our network

360Learning uses a unique token system attached to the IP address to guarantee that no intruder can intercept exchanges and communicate with the API in place of the user ("man-in-the-middle" type attacks). Any connection attempts of this type are denied and recorded. In the event of an attack being detected, all clients affected are warned within 24 hours.

TECHNICAL SUPPORT

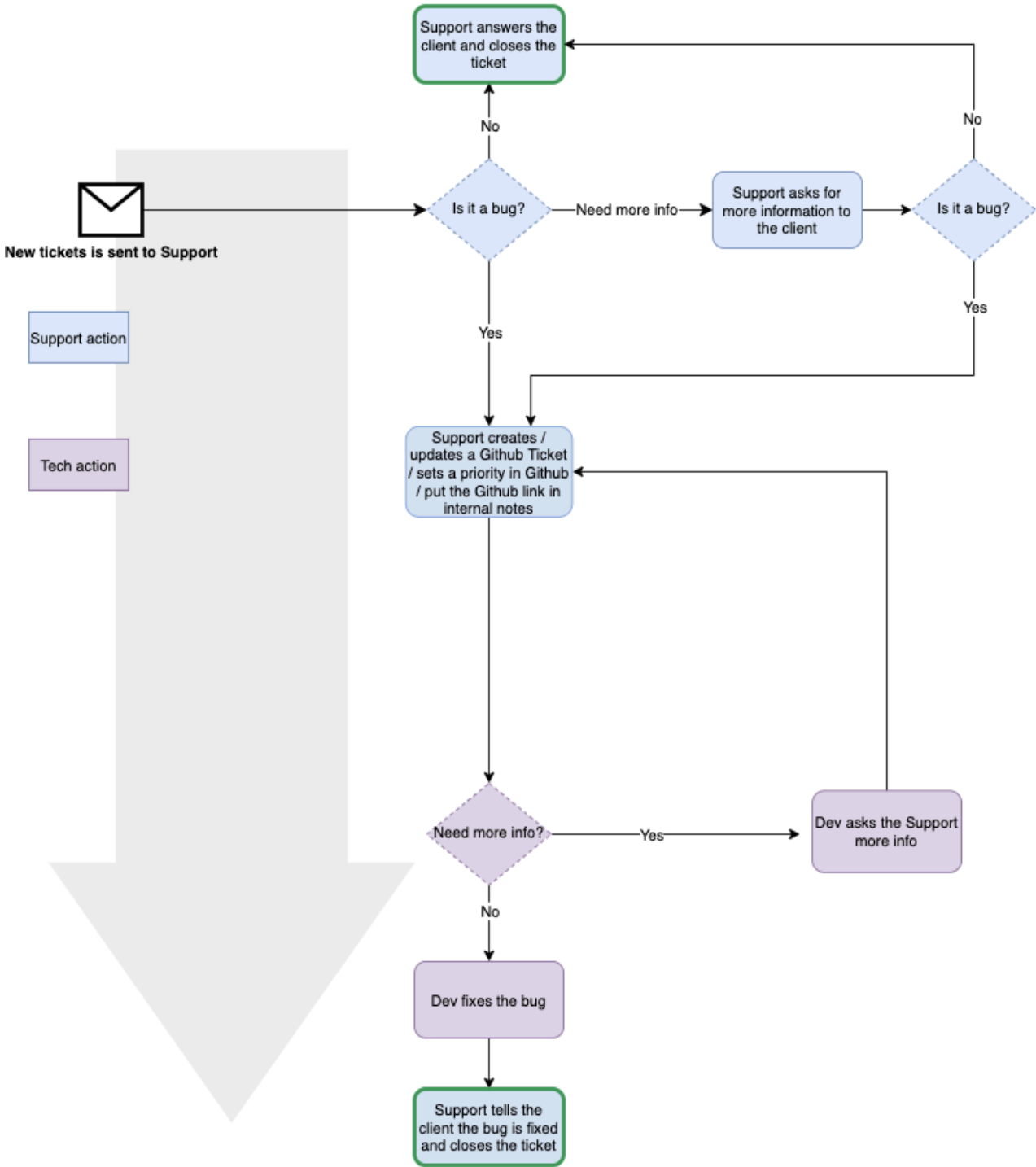360Learning offers an online technical support service, accessible in French and English during operating hours: from 9:00 am to 6:00 pm (Central European Time), Monday to Friday.

→   Technical and functional support via Zendesk
→   Provision of contextual online help
→   Support in the use of the documented API
→   Support for SSO integrations
→   Review and carrying out of functional development

SUPPORT PROCESS

Ticket funnel

New tickets is sent to Support

Support action

Tech action

Is it a bug? — No → Support answers the client and closes the ticket

Is it a bug? — Need more info → Support asks for more information to the client → Is it a bug? — No → Support answers the client and closes the ticket

Is it a bug? — Yes → Support creates / updates a Github Ticket / sets a priority in Github / put the Github link in internal notes

Is it a bug? — Yes → Support creates / updates a Github Ticket / sets a priority in Github / put the Github link in internal notes

Need more info? — Yes → Dev asks the Support more info → Support creates / updates a Github Ticket ...

Need more info? — No → Dev fixes the bug → Support tells the client the bug is fixed and closes the ticket

→ Scalability

1. System Occupation

SAAS (SOFTWARE AS A SERVICE)

360Learning offers a SaaS-type software (Software as a Service). The basis of the SaaS model is that the software is installed on servers rather than on the user's workstation.

Therefore, it requires no installation and can be accessed from any computer connected to the Internet.

The SaaS model offers great flexibility and makes frequent updates possible, allowing 360Learning's clients to benefit at all times from the latest technological advances.

SOFTWARE ARCHITECTURE

Our architecture is made up of three layers :

→   The interface, in JavaScript, is executed on the client's side. It contains a few workflows and business logic. This element scales naturally: each client receives it as soon as he connects to the site, and executes it himself.

   To obtain data to display, and send new data to the platform, this part sends AJAX requests to a REST API.

→   The REST API, exposed by a Node.js Web server. This API is made up of elementary micro-units (for instance, a "route" independent of all others within the API to add a user to a program) that the client code can call up. These routes contain perfectly optimized business layers and currently use up to only 30% of CPU resources and 10% of RAM resources (at a record high).

→   Node.js then sends requests to a MongoDB database to store data. A single replica is currently sufficient to respond to all read and write requests, using up around 10% of its resources. Once 40% of resources will be used, a migration process will be launched to host this MongoDB database on the cloud, using one of MongoDB's 3 standard sharding methods (the choice will be made based on our load profile at the time when migration is decided upon). This is a standard step that only requires a few lines of configuration.

MONITORING

360Learning follows the performance of its servers in real time in order to ensure the availability of the architecture. As soon as performance decreases and falls below a critical threshold, an email alert system notifies executive management and the R&D department.

System performance indicators monitored by 360Learning are CPU, RAM, Disk usage, IO, network, number of requests, latency by services, and other standards metrics. In addition to these low level metrics, 360Learning also monitors high-level, business-oriented indicators, such as the amount of courses played, the number of resources created (courses, users, groups, paths, etc.), and more. It is not anticipated that clients will have access to them. 360Learning does, however, provide real-time statistics concerning user activity on its clients' platforms via the application's dashboard, which can be exported.

360Learning collects and stores access and request logs as well as errors and incidents. These are stored, signed and aggregated for our whole infrastructure for all our customers. The retention period is fixed to a minimum of 3 months and a maximum of 6.

TECHNOLOGIES AND TOOLS

360Learning makes use of state-of-the-art technologies, which the Web's most prominent agents also adopt. Amongst these:

JavaScript & TypeScript
The 360Learning platform is developed in full JavaScript. There are many benefits:
→ Development time is significantly reduced: the R&D team must only master one technique.
→ Loading times are optimized: the load is shifted to the user's workstation, which requests data only when it is necessary.
For an even better reliability, the code is currently being migrated to TypeScript, a superset of JavaScript that aims at detecting errors and inconsistencies in the code more accurately and offers a easier maintenance (more than 80% of the source code files are in TypeScript at the date of writing).

Vue.js
360Learning web client application uses Vue.js, a front-end JavaScript library for building user interfaces. Thanks to declarative rendering and component composition, Vue.js based applications are much more modular, extensible and easy to maintain.

Node.js
360Learning uses Node.js, an event-driven, open-source software platform designed for network applications that require scalability. Node.js allows the creation of very fast applications.

Express.js

Express.js is a Node.js framework that makes it possible to expose an API safely.

MongoDB

360Learning uses a document-oriented database management system, MongoDB, state-of-the-art technology adapted to scalability. It is one of the most widely used DBMSs today, amongst others by Facebook, LinkedIn, Google, or Amazon.

More specialized database systems

For specific features, 360Learning leverages the power of more adapted state-of-the-art data management systems including ElasticSearch, Redis, and Snowflake. They support features such as dashboards, LiveLearners, Recommendations For You, Search, and more.
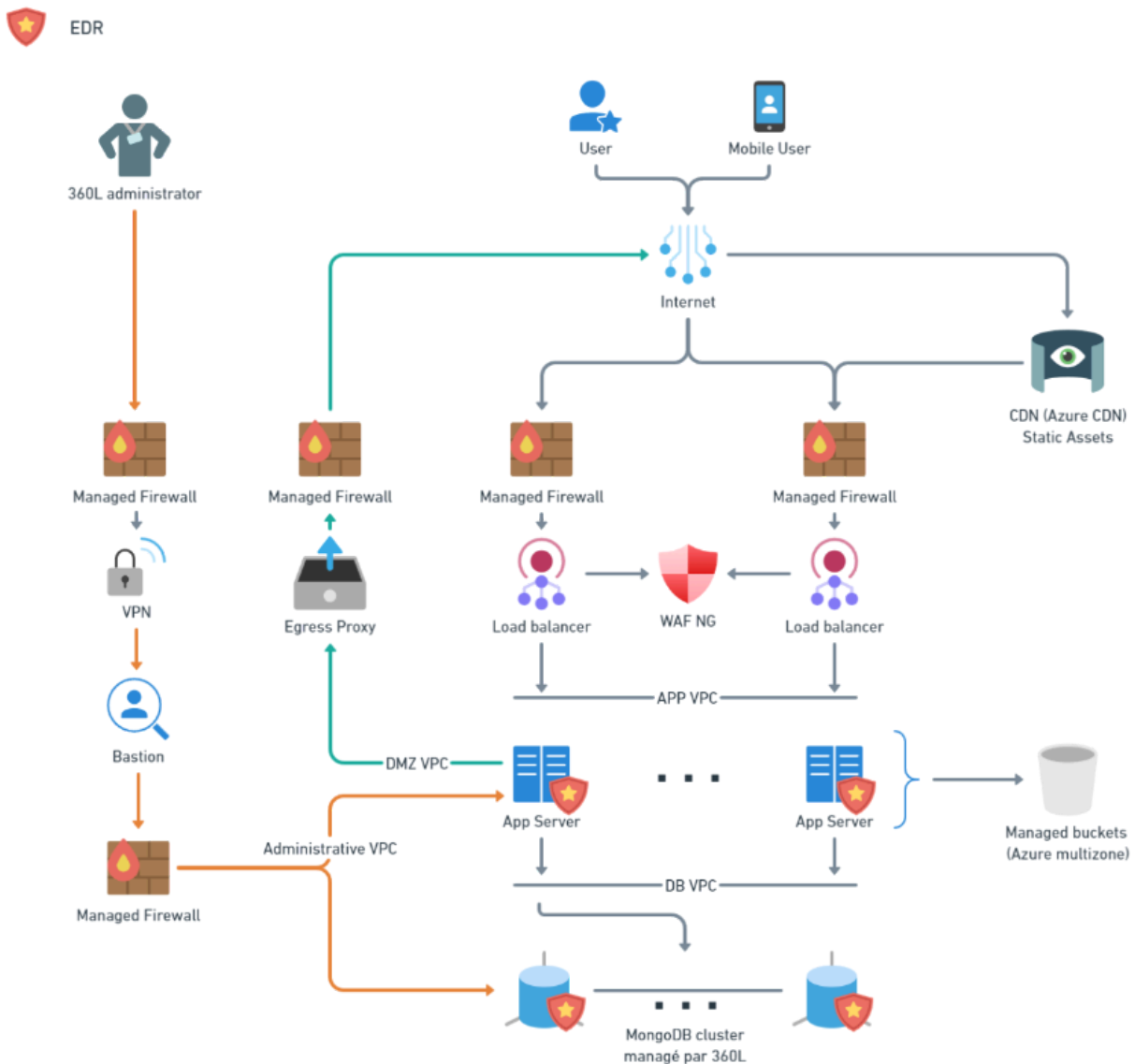
SERVERS

Our servers' operating system is Linux Ubuntu 22 LTS.

MANAGEMENT POLICY FOR NEW VERSIONS OF BROWSERS

When a significant new version of a browser is released, 360Learning makes sure its platform is compatible.

NETWORK

All the data is replicated on a pre-production server, which is comprehensively tested every 3 weeks. The cloud's response times are regularly tested with five predefined requests. Response times from France must be less than 50ms.

2. Client Volume

In order to guarantee a fair use for all users, 360Learning documents and optionally implements limits to some features. If the client needs more than 200k users to their platform, the R&D team must be informed one month in advance, so it can begin a rescaling process. A platform cannot exceed 30k groups. We also apply rate limits to the 360Learning API. Besides, limits on specific features are documented in the 360Learning Knowledge Base.

🠖 Integrations

1. SSO

GOALS

Single Sign-On (SSO) is an authentication mechanism that allows users to access several applications with only one set of login credentials.

By enabling SSO for your 360Learning application, you become responsible for the authentication of your users: they get authenticated through your own login portal and do not need an additional set of login/password anymore.
The benefits of using this SSO include:
→ Improved user experience
→ Improved security
→ Seamless navigation

TECHNOLOGIES

360Learning currently supports three SSO implementations: JWT (JSON Web Token), SAML (Secure Assertion Markup Language) and OIDC (OpenID Connect).

- SAML is an older format, based on XML. It is supported by many services and can be easily integrated with your corporate authentication system, for example, Windows Active Directory.

- JWT is a fairly recent standard based on JSON used in the latest authentication protocols. It offers great flexibility.

- OpenID Connect is built on the OAuth 2.0 protocol and uses an additional JSON Web Token (JWT) to standardize areas that OAuth 2.0 leaves up to choice, such as scopes and endpoint discovery.

DOCUMENTATION

Technical guides are available for both technologies to help you integrate SSO:
→ 360Learning - Technical Guide – SSO JWT
→ 360Learning - Technical Guide – SSO SAML
→ 360Learning - Technical Guide – SSO OIDC

2. API

GOALS

The 360Learning API supports bi-directional sync of a user directory with 360Learning users' directory. You can easily add or remove users, as well as define their name, password, and main profile characteristics. You can add users to groups, for instance, to maintain 360Learning groups up to date with changes in your organization.

DOCUMENTATION

API documentation is available online at https://api.360learning.com/
A technical guide is also available to help you to integrate:

→   [360Learning - Technical Guide – API](#)

Some limitations on API usage to be aware of are indicated in this page
https://support.360learning.com/hc/en-us/articles/210620943-Technical-guide-API,

If you need to run a higher number of requests, we suggest you pace the calls by batch or by setting a timer on the scripts.

360learning

→ Authorized Sub-processors *(for your information)* - Use of the platform

SUBPROCESSOR LEGAL NAME	LOCATION WHERE CUSTOMER DATA IS HOSTED	DESCRIPTION OF SERVICES PROVIDED	IF APPLICABLE: TRANSFER MECHANISM IN PLACE TO ENSURE ADEQUATE LEVEL OF PROTECTION FOR PERSONAL DATA TRANSFERRED TO A THIRD COUNTRY A	PERSONAL DATA PROCESSED
MICROSOFT	France	Hosting of 360Learning's infrastructure Generative AI Services	N/A	Last Name, First Name, Email, Employment, Photo, Login, Usage Stats, and in general, all data processed in the context of the services.
SCALEWAY	France	Hosting test environment , for customers who requested it for their own needs	N/A	Last Name, First Name, Email, Employment, Photo, Login, Usage Stats and in general all data processed in the context of the tests
OVH	France	Domain name Hosting	N/A	Media files (upload)
AMAZON SES	EU (Ireland)	Sending notification mails	N/A	Email, Email Content and Email Opt-in
AMPLITUDE	US	Usage statistics for reporting	-Signed DPA with Standard Contractual Clauses (SCC) - Certified compliant under the EU-U.S. Data Privacy Framework	ID (pseudonymisation)
PENDO	EU	Platform notifications, guides, and other in-app communication.	N/A	ID (pseudonymisation)
GAINSIGHT	EU (Germany)	Usage statistics for reporting	N/A	ID (pseudonymisation)

DATADOG	EU	Observability	N/A	ID (pseudonymisation)
SNOWFLAKE COMPUTING NETHERLANDS B.V.	EU	Usage statistics for reporting, Ship data-processing features (e.g: platform search)	N/A	Last Name, First Name, Email (*to make them available in the Search - Not used for statistics*) - For statistics : ID (pseudonymisation)
ELASTIC APP SEARCH	EU	Search engine to power platform search; usage analytics for recommendations	N/A	Last Name, First Name, Email
WORKATO	EU for EMEA customers - US for US customers	iPaaS provider for automations and 3rd party integrations	N/A	Only for workato's connectors: personal data uploaded to the service, which may include but is not limited to: Last Name, First Name, Email.
The following authorized subprocessorsmay only have access to a limited number of authorized users having a specific role: Author, Administrator, Owner				
ZENDESK	US and EU	Managing customer support requests	- Signed DPA with Standard Contractual Clauses (SCC) - Certified compliant under the EU-U.S. Data Privacy Framework	Last Name, First Name, Email, Photo (if added)

In order to provide the best service to our customers, this list may change

For more information on the processing of personal data, we invite you to consult our privacy policy accessible from the following link: https://360learning.com/privacy-policy

Legal Information

Cookies and Statistics

Accessing the 360Learning platform requires the usage of cookies. These cookies are essential and/or functional, which means they are necessary in order for the services to be provided, and do not require specific consent.

As a Data Controller, 360Learning collects and processes personal data for commercial and administrative management purposes from customers and their employees. Pseudonymized usage statistics are also collected to enable the analysis and improvement of our services. 360Learning may be required, for the sole purpose of this administration and management, to share such personal data to its service providers and/or with its affiliates.

360Learning takes all necessary precautions when collecting and processing customer's personal data to comply with applicable law. For any requests for access, opposition, rectification, portability, limitation, or data management in case of death: Customers may send an e-mail to the following address: data-protection@360Learning.com.

Use and Moderation of the Discussion Forum

The 360Learning platform allows users to communicate on a discussion forum to promote collaborative learning. 360Learning recommends that customers adopt a moderation charter containing best practices for using the discussion forum.