LMS & CORPORATE **UNIVERSITIES**

Documentation technique

version 6.4 (Septembre 2024)

👉 Chez **360Learning**, face à vos problématiques techniques, nous ne vous faisons pas de promesses, nous prenons des engagements.
Vos données vous appartiennent.
Vos données sont et resteront à votre disposition. À votre seule disposition.

360LEARNING UNE RÉFÉRENCE EUROPÉENNE DU LOGICIEL EN LIGNE.

> “En tant que Pionnier du Collaborative Learning, nous nous devons d’assurer à nos clients une sécurité, une confidentialité et une qualité de service irréprochables, tant au niveau de notre engagement contractuel que de notre infrastructure technologique. Nous respectons scrupuleusement la réglementation européenne et française qui sont parmi les plus restrictives en termes de protection des données, de sécurité et de confidentialité.”

Nicolas Hernandez
CEO, 360Learning

👉 Pour tout renseignement contactez-nous :

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

Table des matières👇

Vos données vous appartiennent

Elles vous appartiennent vraiment

Le client conserve la propriété des données hébergées sur 360Learning.

En fin de contrat, le client peut demander à 360Learning de récupérer l'ensemble de son catalogue de modules dans un format standard.

Nos droits

Les employés de 360Learning ont accès aux données du client uniquement dans certains cas précis :

- Questions du client relatives à ses données
- Résolution de problèmes
- Demande de changement dans les données

Confidentialité

360Learning garantit qu'aucune donnée personnelle à laquelle elle a accès en tant que responsable du traitement des données pour fournir des services contractuels n'est vendue, transférée ou divulguée à des fins commerciales à des tiers.

Pseudonymisation

360Learning garantit que les données personnelles sont isolées dans un ensemble unique de nos bases de données, et que toutes les autres données professionnelles (contenus de formation, statistiques de formation, groupes, cours...) utilisent un identifiant aléatoire pour référencer chaque utilisateur, garantissant ainsi une pseudonymisation des données personnelles en accord avec le RGPD.

Disponibilité

1. Configuration minimale

PLATFORME

Afin de profiter pleinement de l'application 360Learning, une configuration minimum est nécessaire :

1. S'assurer que les conditions préalables sur tous les postes sont satisfaites : écran ayant une résolution minimale de 1024 x 600 pixels et mémoire RAM de 256 Mo.

2. S'assurer de disposer sur tous les postes d'un navigateur compatible Microsoft Edge, Firefox, Chrome ou Safari dans l'une des versions supportées par leurs éditeurs respectifs.

3. Effectuer des tests de bande passante pour s'assurer que les utilisateurs pourront utiliser la plateforme dans les meilleures conditions et déduire des recommandations en termes de poids et de nature des formats pédagogiques utilisés pour une intégration et une consultation fluides.

   Bande passante minimale conseillée : 512 kbit/s par poste de travail pour l'ensemble des utilisations y compris streaming vidéo (sous conditions spécifiées dans le paragraphe "Vidéo" ci-dessous) et hors lecture de modules SCORM.

4. Authentifier les serveurs de mails afin de s'assurer que les messages en provenance de la plateforme ne soient pas bloqués par la DSI client. Il est nécessaire de whitelister l'adresse email no-reply@360learning.com à partir du champ "from" (et non à partir de l'adresse d'envoi du serveur smtp) dans les configurations du client mail, et dans les serveurs mail / logiciel anti-spam. S'il ne vous est pas possible de filtrer sur ce paramètre, vous pouvez autoriser les adresses IP dédiées que 360Learning utilisé pour l'envoi de mail:

IP de Pre-production:

- 20.40.143.206
- 20.74.25.131

IP de Production:

- 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

5. Whitelist *.360learning.com ou le nom de domaine personnalisé afin de s'assurer que les membres pourront accéder à la plateforme.

6. Whitelist les 2 domaines ci-dessous afin de pourvoir accéder aux banques d'images
   https://unsplash.com/*
   https://pixabay.com/*

7. Facultatif : Si utilisation de modules SCORM, vérifier que les pop-ups sont autorisées.

8. Facultatif : Si utilisation de modules SCORM au format Flash, vérifier que le plugin Flash est à jour dans les navigateurs.

   Pour vous aider à vérifier tous les pré-requis techniques préalables et tester votre plateforme avant son déploiement, utilisez les check-lists disponibles dans notre guide :

→ 360Learning - Guide Technique - Procédure de Validation

SUPPORT MOBILE

Les versions supportées sont susceptibles d'évoluer et sont actuellement :

→ iOS 14 et supérior
→ Android 5.0 et supérieur

Sur les appareils mobiles, nous ne fournissons une assistance que pour nos applications mobiles natives. Bien que notre plateforme utilise un design de type "responsive", nous ne prenons pas en charge les navigateurs web mobiles.
Toute version d'application personnalisée ou mise à jour d'application mobile est soumise aux délais de la place de marché d'application concernée (Google Play store, Apple App store...) qui échappent à notre contrôle.

Les fonctionnalités sur périphériques mobiles sont conçues pour une utilisation en tant qu'apprenant et prennent en charge un large choix de formats :

→ Fiches de cours et questions natives 360Learning
→ Images (gif, jpg, png, bmp, ico)
→ Vidéos (3gp, avi, flv, m2ts, m4v, mkv, mov, mp4, mpeg, mpg, mts, vob, webm, wmv)
→ Fichiers PDF
→ Documents Microsoft Office (docx, xlsx, pptx)
→ Contenu partagé en provenance du Web (lien direct, code d'incorporation ou code iframe ; nécessite une connexion internet pour être visionnée dans l'application)

VIDÉO

360Learning vous permet d'uploader des vidéos en HD et crée automatiquement un version SD de toutes les vidéos en moyenne 5 fois plus légère que l'originale. Un bouton HD/SD apparaît en bas à droite dans le player et permet aux utilisateurs de sélectionner la qualité souhaitée. Notez que sans action de l'utilisateur le player adapte la qualité de la vidéo à la bande passante disponible, et que si l'utilisateur clique sur HD cela demandera naturellement plus de débit.

Afin de bénéficier d'un débit SD inférieur à 512 kbit/s, veillez à contrôler la taille de vos fichiers sources. Si vous souhaitez que le débit des versions SD et HD de vos vidéos soit inférieur à 512 kbit/s, assurez-vous que le débit de vos fichiers sources soit inférieur à 512 kbit/s

2. Contenus

360Learning vous permet de créer des fiches de cours et plusieurs types de questions (Vrai / Faux, Choix multiple, Ordre, Association, Zones sensibles, Ouvertes...).

Vous pouvez également importer divers types de 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

Il est également possible d'importer du contenu partagé en provenance du Web (lien direct, code d'incorporation ou code iframe). Ceci inclut des services tels que YouTube, Slideshare ou Prezi.

3. Accessibilité

360Learning est construite sur les préceptes fondamentaux de l'UX design. Les équipes de product managers & designers se tiennent quotidiennement à la page des dernières tendances UI. Ils participent aux cercles de réflexion nationaux et internationaux sur l'expérience utilisateur : meetup "Get the swag on", UX Week, meetup "UX Souls", SXSW, Future of Web Design London...

Les usages et fonctionnalités sont perpétuellement analysés et optimisés grâce à des outils d'AB Testing ou des cartes de chaleur. Le design et l'ergonomie de 360Learning sont inspirés par les données et les grandes tendances du marché.

Chez 360Learning, le design est tout autant un comportement et une émotion qu'une utilité et une facilité. C'est pourquoi l'ergonomie et le design sont parmi les piliers fondamentaux du LMS, de l'outil-auteur et des fonctionnalités sociales et collaboratives de 360Learning.

360Learning s'inspire des règles du W3C (World Wide Web Consortium), organisme de normalisation chargé de promouvoir la compatibilité des technologies du web, et de la norme RGAA (Référentiel général d'accessibilité pour les administrations) qui est destiné à définir, en France, les modalités techniques d'accessibilité des services en ligne de l'État, des collectivités territoriales et des établissements publics qui en dépendent, pour les trois canaux du Web, de la télévision et de la téléphonie.

Voici les éléments de conformité sur la plateforme 360Learning :

LISIBILITÉ

- → La police utilisée est Open Sans. Une police claire et simple pour améliorer la lisibilité.
- → Les majuscules sont limitées au strict minimum.
- → Les sous-titres générés automatiquement sont disponibles pour les vidéos des modules.
- → Afin de simplifier la lisibilité, 360Learning utilise moins de 10 couleurs sur la plateforme.
- → 360Learning privilégie les combinaisons qui permettent une lisibilité maximale.
  Exemple : blanc/noir - bleu foncé/blanc

UNE ARCHITECTURE ÉQUILIBRÉE

Afin de faciliter l'assimilation de l'organisation des contenus par l'utilisateur, notre architecture est la suivante :

- → 4 rubriques maximum en largeurs au lieu des 7 recommandés
- → 3 rubriques maximum en profondeur au lieu des 4 recommandées

SYSTÈME DE NAVIGATION

Le système de navigation constitué d'une « barre verticale » est conforme à la norme RGAA et rassemble l'ensemble des possibilités de navigation.

ZONING ET LISIBILITÉ COGNITIVE

La navigation sur 360Learning est semi-guidée.
Chaque zone est séparée distinctement et correspond à une activité.
La structure de chaque module est la même, ce qui permet à l'utilisateur de simplifier et de mémoriser le chemin de navigation.

ÉLÉMENT D'ORIENTATION

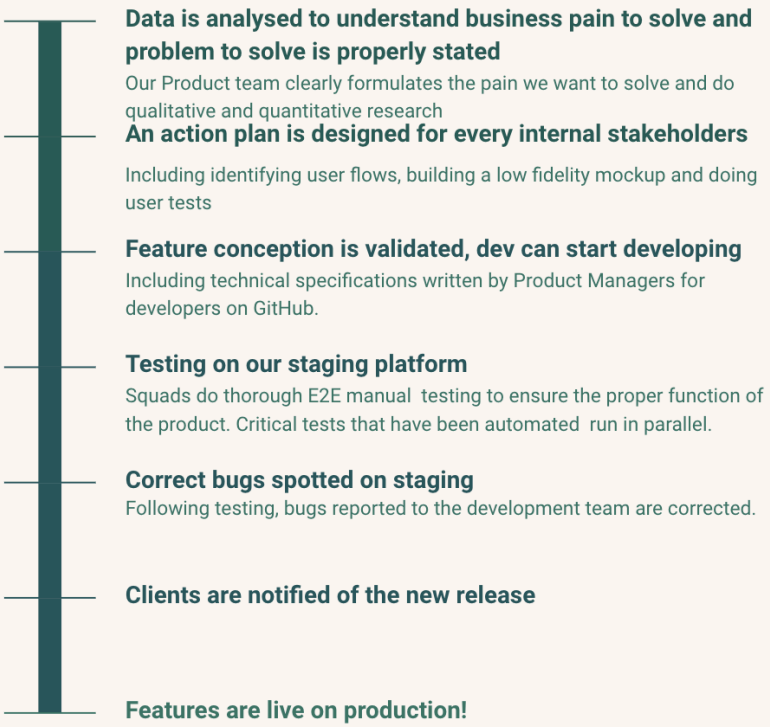
À tout moment sur la plateforme, l'apprenant peut localiser la page affichée parmi les pages du site.

- → Où il se situe : Le menu correspondant apparaît en gras et en plus lumineux
- → D'où il vient : L'apprenant peut à tout moment se situer dans le parcours
- → Où il peut aller : L'apprenant peut se projeter dans son module

4. Développement

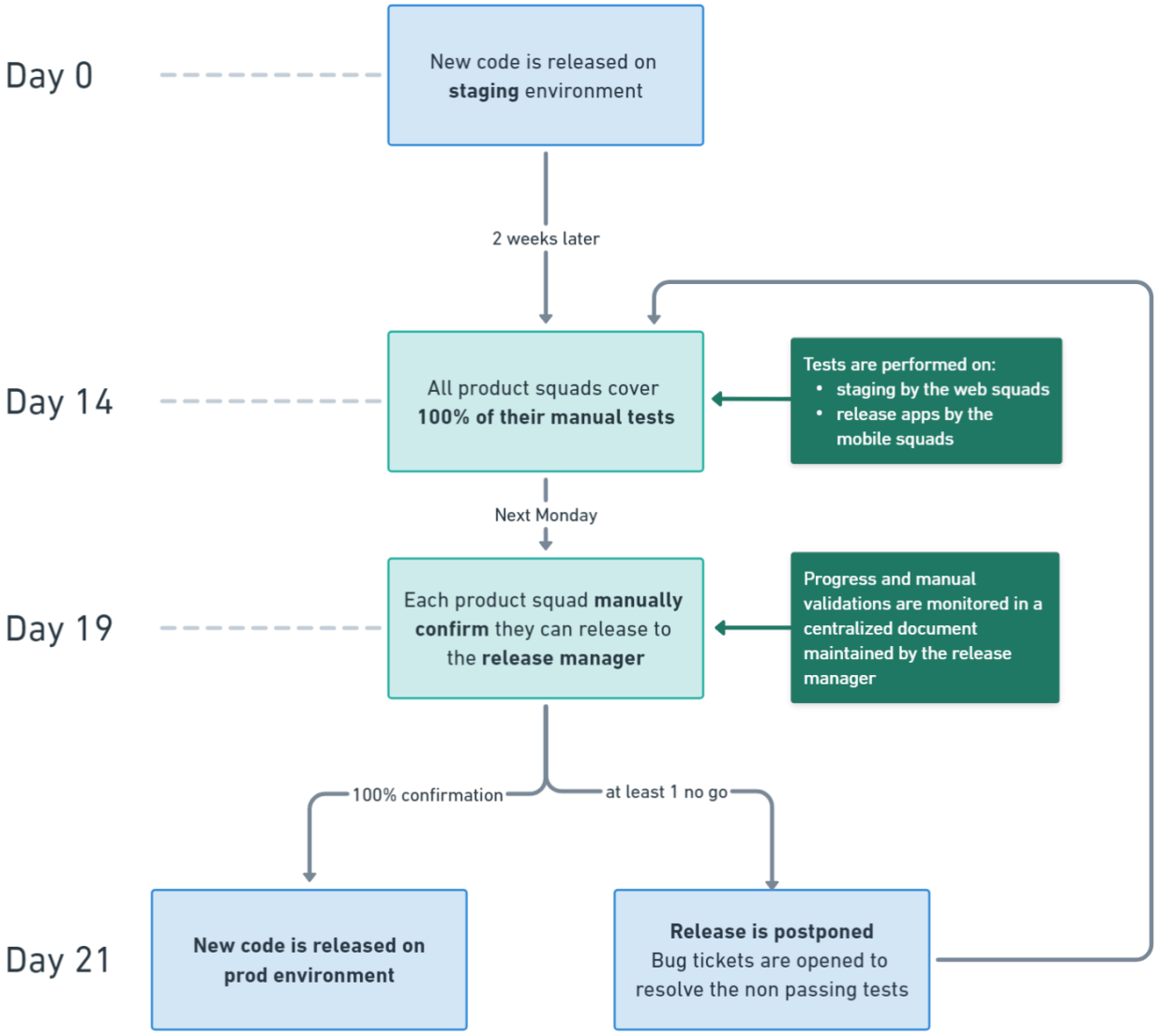
NOUVELLES FONCTIONNALITÉS

Chaque nouvelle fonctionnalité est développée selon un schéma très précis, détaillé ci-dessous.👇



Quality & Assurance

Chaque fonctionnalité est testée dans un environnement de test avant son déploiement vers l'environnement de production, suivant un processus détaillé ci-dessous.👇



Pour s'assurer que les fonctionnalités sont livrées au niveau de qualité attendu, sans casser les autres fonctionnalités de la plateforme, nous effectuons des tests manuels de bout en bout pour chaque jalon. Un responsable de version est choisi et doit s'assurer que ce processus est respecté, principalement en communiquant avec les responsables techniques pendant la phase de mise en œuvre.

Modifier l'apparence de la plateforme avec du CSS personnalisé

360Learning peut décider d'offrir, à titre commercial et gracieux, à un client qui en fait la demande la possibilité d'ajouter du CSS pour personnaliser l'apparence de la plateforme. Cette fonctionnalité optionnelle ne peut être activée que par le Account Manager du client et sous certaines conditions.

Les recommandations générales concernant les CSS personnalisés sont listées dans cet article sur la base de connaissances de 360Learning :
https://support.360learning.com/hc/fr/articles/4956106195732-Modifier-l-apparence-de-la-plateforme-avec-du-CSS-personnalis%C3%A9

Le client est responsable de toutes les modifications des paramètres de sa plateforme avec des CSS personnalisés. 360Learning ne fournit pas d'aide à la mise en place du code CSS, ni à sa maintenance, n'assure pas l'interopérabilité, et ne fournit pas de support pour le code personnalisé.

Par exemple, si un Client détermine que le CSS personnalisé lui convient, le Propriétaire de la plateforme doit être prêt à :

- Tester le code personnalisé à chaque montée de version, ce qui se produit toutes les trois semaines.
- Gérer, dépanner et prendre en charge tout problème lié au CSS personnalisé.

360Learning : (i) peut désactiver le CSS personnalisé du client à tout moment, en particulier si 360Learning identifie des problèmes de sécurité ou de performance; et (iii) ne prend aucune garantie expresse ou implicite de quelque nature que ce soit sur le CSS personnalisé.

Toute utilisation d'un CSS personnalisé par un client n'autorise par le client à créer des œuvres dérivées de la plateforme.

Sécurité

1. Chiffrement

Par défaut, l'accès à l'application est systématiquement forcé en HTTPS TLS 1.2 comme version minimale, avec des suites de chiffrement prises en charge.

Vérifiez la prise en charge des suites de chiffrement suivantes par votre système d'information :

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_CBC_SHA384 (secp256r1)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1)

N.B : nous maintenons cette liste à jour pour assurer une prise en charge maximale avec les navigateurs web récents tout en ayant un niveau de sécurité maximal. La prise en charge ne devrait pas poser problème, à moins que vous n'utilisiez un ancien navigateur ou des bibliothèques clientes HTTP anciennes.

ACCÈS PROTÉGÉ PAR MOT DE PASSE

L'accès à l'application est protégé par un mot de passe qui peut être défini de plusieurs manières :

- → Par l'utilisateur lors de sa première connexion.
- → Par l'administrateur lors de la création du compte
- → Par le mécanisme de SSO. Dans ce cas 360Learning garde un mot de passe de 32 caractères aléatoires en base de données.

Une fois ce mot de passe défini, il est impossible pour une personne tierce de connaître ce mot de passe en soumettant une requête à notre base de données, car l'ensemble des mots de passe sont cryptés de façon irréversible en BCRYPT 10 rounds. Si un utilisateur oublie son mot de passe, un mail lui est envoyé pour le réinitialiser. En cas de détection d'attaque, tous les clients concernés sont avertis dans les meilleurs délais.

CONTRÔLE D'ACCÈS PAR ADRESSE IP

Il est possible de filtrer l’adresse IP pour restreindre l'accès à l’application : les utilisateurs ne peuvent ainsi se connecter que depuis un site défini.

2. Sécurité physique

CENTRES DE DONNÉES SOUS HAUTE PROTECTION

L'infrastructure principale de 360Learning est hébergée chez notre partenaire Microsoft Azure. Le contenu multimédia est stocké au sein des centres de données de Microsoft Azure et OVH. OVH et Microsoft Azure fournissent tous deux le plus haut niveau de sécurité afin de garantir la disponibilité, l'intégrité et la confidentialité des données hébergées.

CARACTÉRISTIQUES DES CENTRES DE DONNÉES – OVH

Sécurité et Incendie

- → Seuls les salariés accrédités peuvent accéder physiquement aux serveurs informatiques
- → Accès contrôlés par badge RFID, gardiennage 24h/7
- → Systèmes de vidéo-surveillance et détection de mouvement
- → Salles équipées de systèmes de détection de chaleur et de fumée
- → OVH s'appuie sur les normes ISO 27002 et ISO 27005 pour la gestion de la sécurité et l'appréciation des risques et traitements associés.
- → OVH s'appuie sur les normes ISO 27002 et ISO 27005 pour la gestion de la sécurité et l'appréciation des risques et traitements associés.

Alimentation électrique

- → Double alimentation électrique systématique
- → Onduleurs de 250 KVA chacun
- → Groupes électrogènes d'une autonomie initiale de 48h
- → 2 arrivées réseau minimum jusqu'au centre de données; à l'intérieur, 2 salles réseau jumelles capables de prendre le relais l'une de l'autre

Climatisation

- → Le Watercooling permet de dissiper 70 % de la chaleur émise par le processeur
- → L'Aircooling évacue les 30 % restants PUE compris entre 1 et 1,2 : réduction constante de la consommation énergétique des centres de données

Bâtiments

- → OVH conçoit et construit ses propres centres de données depuis 2003
- → Les centres de données d'OVH sont situés en dehors des zones soumises au Patriot Act
- → Bâtiments géographiquement distants de plus de 200 km afin d'assurer redondance et continuité de service

Maintenance et gestion technique du bâtiment

- → Personnel technique présent 24h/7

CARACTÉRISTIQUES DES CENTRES DE DONNÉES – Microsoft Azure

Sécurité et Incendie

- → Contrôle d'accès autonome par badge sans contact RFID et biométrique par reconnaissance du réseau veineux des doigts
- → Sas d'entrée blindé conforme aux normes anti-intrusion EN 1627
- → Réseau de caméras numériques, extérieur et intérieur
- → Dispositif anti-intrusion sur tous les ouvrants (APSAD R81) et APSAD R81 (détection d'intrusion)
- → Agent de sécurité incendie avec spécialisation SSIAP 2, 24/7
- → Systèmes de détection multi-ponctuelle VESDA LASER
- → Systèmes d'extinction incendie par brouillard d'eau SEMCO conforme aux normes APSAD R1/D2 et NFPA 750
- → Moyens complémentaires de lutte contre le feu RIA et extincteurs portatifs CO2 conformes aux normes APSAD R4
- → Compartiment résistant au feu plus de deux heures entre chaque salle informatique

Alimentation électrique

- → Arrivées EDF via 2 doubles dérivations de 9 MVA chacune
- → 7 TGBT de 2,5 MVA équipés d'un dispositif redondant de permutation automatique sur groupe
- → 6 générateurs diesel pour une puissance installée de 11,85 MVA
- → 48800 litres de fioul, 50 heures d'autonomie à pleine charge
- → Zone N+1 : 3 chaînes ondulées indépendantes
- → Zone 2(N+1) : 2 chaînes ondulées indépendantes
- → Autonomie batterie : 10 minutes en fin de vie de batterie

Climatisation

- → 5 MW de puissance frigorifique en configuration N+1
- → Réseau d'eau glacée redondant par circuits de distribution bouclés
- → Armoires de climatisation de 90 kW
- → Température maintenue à 20°C +/-2°C en allée froide
- → Urbanisation systématique en couloir froid confiné
- → Climatisation indépendante pour chaque salle client

Bâtiments

- → Conception et construction spécifiques pour l'usage en centre de données

Maintenance et gestion technique du bâtiment

- → Maintenance conforme aux standards AFNOR NF EN 13-306 et FD X60-000
- → Télésurveillance des équipements par les constructeurs
- → Supervision de l'infrastructure via la GTC Sima©

CARACTÉRISTIQUES DES CENTRES DE DONNÉES – AWS

Sécurité et Incendie

- → Seuls les salariés accrédités peuvent accéder physiquement aux serveurs informatiques
- → Contrôle d'accès multifacteur, gardiennage par des professionnels de la sécurité des bâtiments 24h/7
- → Les points d'accès physique aux salles de serveurs sont filmés dans le système de télévision en circuit fermé (CCTV). Les images sont conservées selon les obligations légales et de conformité.
- → Salles équipées de systèmes de détection de chaleur et de fumée
- → Des tests tiers des centres de données AWS, comme documentés dans nos rapports tiers, garantissent qu'AWS a implémenté correctement des mesures de sécurité conformes aux règles établies pour obtenir des certifications de sécurité.

Alimentation électrique

- → Les systèmes d'alimentation électrique de nos centres de données sont conçus pour être totalement redondants et gérables sans que cela ait une quelconque incidence sur les opérations, 24h/24. AWS s'assure que les centres de données sont équipés d'une alimentation de secours fournissant du courant pour garantir le maintien du fonctionnement en cas de panne électrique pour les charges critiques et essentielles sur le site.

Climatisation

- → Les centres de données AWS utilisent des mécanismes pour contrôler les conditions climatiques et maintenir une température de fonctionnement appropriée pour les serveurs et autres matériels, afin de prévenir la surchauffe et de réduire les risques de pannes d'alimentation. La température et l'humidité sont surveillées et régulées à des niveaux appropriés par le personnel et divers systèmes.

Bâtiments

- → AWS conçoit et construit ses propres centres de données
- → AWS possède et exploite des centres de données au sein de l'Union Européenne sur lesquels nous nous appuyons.
- → Bâtiments géographiquement distants d'au moins 200 kms afin d'assurer redondance et continuité de service

Maintenance et gestion technique du bâtiment

- → Des systèmes électroniques de détection d'intrusion sont installés dans la couche des données pour surveiller, détecter et alerter automatiquement le personnel compétent en cas d'incidents de sécurité. Les points d'entrée et de sortie des salles de serveurs sont sécurisés avec des dispositifs qui obligent chacun à fournir une authentification multi-facteurs avant d'autoriser l'entrée ou la sortie.

3. Sécurité logique

Il s'agit d'un résumé rapide de nos éléments de sécurité. Pour plus de détails, veuillez consulter notre plan d'assurance sécurité v3.2.

PRÉVENTION CONTRE LES ATTAQUES PAR DÉNI DE SERVICE (DDOS)

Une attaque DDoS vise à rendre un site indisponible, en surchargeant la bande passante du serveur ou en accaparant ses ressources jusqu'à épuisement. Les cas rencontrés concernent généralement des attaques de niveau 7, le plus élevé, basées sur des requêtes exécutées en nombre visant à saturer le système.

Garantir la sécurité en ligne de ses clients est une des préoccupations majeures de 360Learning. Pour contrer ces attaques, notre hébergeur Microsoft Azure intègre en série une solution de mitigation basée sur la technologie VAC. Il s'agit d'une combinaison exclusive de techniques qui analysent en temps réel et à haute vitesse votre trafic. Elles détectent et interceptent automatiquement les attaques, tout en laissant passer les requêtes légitimes.

DÉTECTION ET PRÉVENTION DES ATTAQUES OWASP

Un pare-feu d'applications web (WAF) de nouvelle génération placé sur nos serveurs frontaux filtre chaque requête afin d'identifier toute menace potentielle. Il inclut les règles de détection de l'OWASP et des règles métier spécifiques afin d'alerter et bloquer les attaques malveillantes.
Des alertes sont envoyées à l'équipe DevOPS et à l'équipe sécurité afin de lancer, si nécessaire, un incident de sécurité.
Les attaques sont enregistrées et archivées pendant au moins 6 mois à des fins d'audit de sécurité.

ANTI-VIRUS

Nous disposons de la dernière version de la suite ClamAV (Version : 0.103.6/26545). Afin de nous assurer d'obtenir la dernière base de données et vous offrir la meilleure protection nous mettons à jour la base de données toutes les 60 minutes. Une analyse est effectuée sur tous les documents et archives chargés sur la plateforme pour s'assurer qu'aucun fichier exécutable n'est envoyé.

Si un virus est suspecté, l'utilisateur concerné recevra le message suivant : "Notre anti-virus trouve votre document suspect. Votre fichier n'a pas été importé." Et le fichier n'est jamais chargé sur nos serveurs.

THREAT DETECTION AND REMEDIATION

Nous avons déployé:

- une solution Endpoint Detection and Response (EDR/XDR) Crowdstrike sur chaque serveur afin de garantir une protection élevée et une capacité à identifier toute menace sur notre plateforme (ransomware, malware, rootkits, remote shell, ...). Chaque agent est connecté à une plateforme centrale qui est gérée en externe 24/7 par les équipes de CrowdStrike et qui escalade vers l'équipe de sécurité interne de 360Learning en cas d'urgence.
- un Web Application Firewall Next Generation qui filtre toutes les requêtes pour toutes nos applications externes et nos points d'accès.
- un SIEM qui met en corrélation les journaux de toutes nos entreprises et plateformes. Ceci est accompagné d'un SOC externe 24/7 qui alerte l'équipe de sécurité en cas de comportement anormal (non-conformité, attaque, comportement inhabituel tel qu'une authentification réussie à partir d'une source inconnue).

RÔLES DANS L'APPLICATION

La plateforme distingue plusieurs rôles et plusieurs niveaux de permission, instaurant une sécurité logique supplémentaire.

Les rôles et leurs autorisations sont détaillés dans la documentation en ligne de notre Base de connaissances : https://support.360learning.com/.

4. Politiques Internes

POLITIQUE DE SÉCURITÉ DE MOT DE PASSE

1. **Synthèse**

Tous les employés et membres du personnel ayant accès aux systèmes informatiques de l'organisation doivent adhérer à la politique définie ci-dessous afin d'assurer la sécurité du réseau, protéger l'intégrité des données et protéger les systèmes informatiques.

2. **Objet**

L'objet de cette politique est de protéger les ressources de l'organisation sur le réseau en requérant des mots de passe sécurisés ainsi que la protection de ces mots de passe, et en fixant un délai court entre les modifications des mots de passe.

3. **Portée**

Cette politique s'applique à tout membre du personnel possédant une forme de compte informatique sur le réseau de l'organisation requérant un mot de passe, incluant sans s'y limiter un compte de domaine et un compte e-mail.

4. **Protection de mot de passe**

- → N'écrivez jamais un mot de passe
- → N'envoyez jamais un mot de passe par e-mail
- → N'incluez jamais un mot de passe dans un document stocké non-crypté
- → Ne communiquez jamais votre mot de passe à qui que ce soit
- → Ne divulguez jamais votre mot de passe au téléphone
- → Ne donnez jamais d'indications concernant le format de votre mot de passe
- → Ne divulguez jamais et ne donnez jamais d'indications concernant votre mot de passe sur un forum sur Internet
- → N'utilisez jamais la fonctionnalité « Mémoriser le mot de passe » d'applications telles que votre programme de boîte e-mail ou tout autre programme.
- → N'utilisez jamais votre mot de passe d'entreprise ou de réseau sur un compte sur Internet qui n'est pas doté d'une connexion sécurisée, dont l'adresse dans le navigateur Web commence par https:// plutôt que par http://
- → Si vous avez la moindre raison de penser que votre mot de passe a été compromis, signalez-le à votre unité de sécurité informatique
- → Si quelqu'un vous demande votre mot de passe, renvoyez cette personne vers votre unité de sécurité informatique
- → Assurez-vous de ne pas être observé lorsque vous tapez votre mot de passe
- → Utilisez le MFA lorsque c'est possible

5. **Application**

Étant donné que la sécurité des mots de passe est essentielle à la sécurité de l'organisation et de tous, les employés qui n'adhèrent pas à cette politique sont passibles de mesures disciplinaires, jusqu'à et incluant le licenciement.

6. **Autres Considérations**

Des écrans de veille protégés par mot de passe doivent être activés et doivent protéger les ordinateurs au bout de 5 minutes d'inactivité de la part des utilisateurs. Les ordinateurs ne doivent pas être laissés sans surveillance si l'utilisateur a une session ouverte et qu'aucun écran de veille protégé par mot de passe n'est activé. Les utilisateurs doivent prendre l'habitude de ne pas laisser leurs ordinateurs déverrouillés.

Les mots de passe d'administrateur doivent faire l'objet d'un degré de protection particulièrement élevé. Les comptes d'administrateur doivent bénéficier de l'accès minimum nécessaire pour remplir leurs fonctions. Les comptes d'administrateur ne doivent pas être partagés.

7. **Utilisation d'un gestionnaire de mots de passe**

L'utilisation d'un gestionnaire de mots de passe, LastPass dans notre cas, facilite les points cités précédemment

Qu'apporte-t-il ?

- → Il n'y a qu'un seul mot de passe-maître à mémoriser.
- → Il permet de partager l'accès à un compte de manière sécurisée, sans communiquer le mot de passe.
- → Il permet de générer des mots de passe sécurisés.

Comment fonctionne-t-il ?

- → chiffrement 256-bit AES, avec itérations PBKDF2 systématiquement répétées.
- → Toutes les données sensibles sont cryptées et décryptées localement avant la synchronisation avec LastPass. La clé ne quitte jamais l'appareil, et n'est jamais transmise à LastPass. Nos données ne sont accessibles à personne d'autres que nous.

5. Sécurité de l’application mobile

- → Notre application utilise les mêmes serveurs que notre client web et se connecte également en utilisant le protocole HTTPS TLS 1.2 minimum (TLS 1.3 supporté). Ainsi, elle bénéficie du même niveau de sécurité. Les logs sont gardés et traités de la même manière qu’ils soient générés depuis l’application mobile ou la plateforme web.
- → De même, si vous mettez en place une politique de confidentialité, les utilisateurs devront l’accepter lors de leur première connexion quel que soit le mode d’accès (client web ou client mobile)
- → Les données de géolocalisation sont pseudonymisées lors de la collecte. Ces données sont uniquement utilisées pour des raisons d’analyse de l’utilisation du produit. Ainsi, aucune donnée personnelle n’est enregistrée lors de l’utilisation de notre application.
- → Que ce soit sur iOS ou Android, les données hors ligne ne sont en aucun cas accessibles ni pour une application tierce ni pour le système d’exploitation.

6. Audits Indépendants

Nous réalisons depuis 2022, deux audits par an afin de nous assurer de la sécurité de nos développements.

HDWSEC et HACKERONE, EXPERTS EN SÉCURITÉ AUX CÔTÉS DE 360LEARNING

HDWsec, auditeur indépendant et expert français en sécurité, accompagne 360Learning sur la gestion de la sécurité de son infrastructure logicielle et réseau ainsi que sur la mise en œuvre de sa politique de sécurité.
HackerOne, célèbre spécialiste des tests d'intrusion américain indépendant, réalise des tests de vulnérabilité plus poussés afin d'assurer une sécurité maximale et la mise en conformité.

Pour évaluer et renforcer le niveau de sécurité de 360Learning, HDWsec opère :

- → 1 audit de sécurité par an, selon la méthodologie OWASP, à l'aide de tests en boîte noire et de tests en boîte grise, y compris un audit complet de la configuration de l'architecture 360Learning et des simulations d'attaques (de type tentative de piratage)
- → La formation continue des développeurs 360Learning à la sécurité
- → Le conseil dans la mise en œuvre de la politique de sécurité de 360Learning

Pour acquérir le maximum de connaissances sur les vulnérabilités et la conformité de la sécurité de 360Learning, HackerOne opère :

- → 1 audit de sécurité programmé sous la forme d'un test d'intrusion par an, réalisé par des hackers sélectionnés pour leurs connaissances de nos technologies.
- → La vérification de la conformité continue à la norme ISO 27001

Afin d'évaluer le niveau global de sécurité de l'entreprise, NeverHack a mené un exercice Red Team sur l'ensemble des actifs de l'entreprise, en essayant de recueillir des informations sur :

- → email de phishing
- → faux appels téléphoniques
- → nos outils d'entreprise
- → notre infrastructure
- → nos applications

7. Normes

DÉNOMINATION SOCIALE DU SOUS-TRAITANT	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

Continuité du service

1. Service Level Agreement (SLA)

Nous vous garantissons un taux de disponibilité mensuel de 99,8%.

Vous trouverez de plus amples informations sur notre accord de niveau de service selon votre niveau d'accompagnement aux adresses suivantes:

- Pour les clients Essential & Advanced : [FR] SLA
- Pour les clients Ultimate: https://360learning.com/fr/legal/slafrultimate/

2. Backups

Vos données personnelles ainsi que vos vidéos, images et documents téléchargés sur 360Learning sont hébergés par notre partenaire Microsoft Azure, dans l'un des Data Centers indiqués dans le tableau ci-dessous.

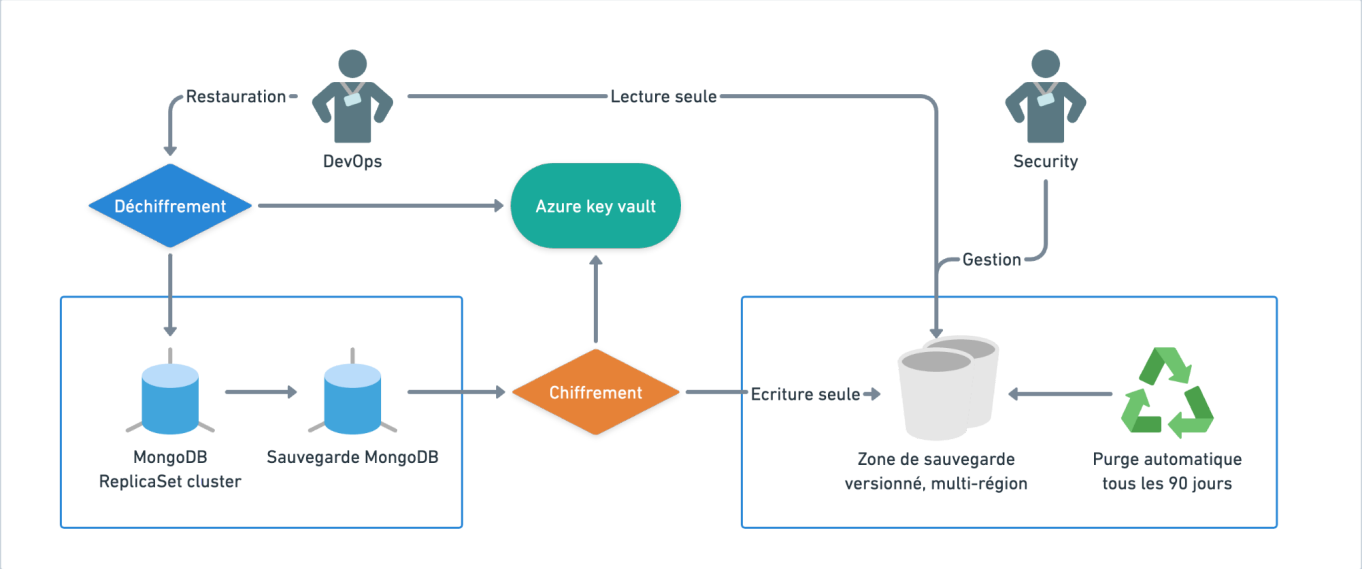
Region	Azure Data Center	Physical Location	Availability Zones	Commercial Availability
France	France Central	Paris region	3	Disponible pour tous les clients
United States	US-WEST-2	Washington State	3	Mise à disposition planifiée pour 2024

Pour les autres contenus de formation, des services tiers tels que Youtube, Prezi ou Vimeo sont hébergés par leurs éditeurs.

Les zones de disponibilité Azure sont des emplacements physiquement séparés au sein de chaque région Azure qui sont tolérants aux défaillances locales. Les défaillances peuvent aller de pannes logicielles et matérielles à des événements tels que des tremblements de terre, des inondations et des incendies. La tolérance aux pannes est obtenue grâce à la redondance et à l'isolation logique des services Azure. Pour

garantir la résilience, un minimum de trois zones de disponibilité distinctes sont présentes dans toutes les régions dotées d'une zone de disponibilité.

Les sauvegardes logiques (version du service et données du client) sont effectuées une fois par jour sur le cluster de sauvegarde à distance. Cela garantit un RPO maximum de 24 heures, et nous conservons un historique de 90 jours.



3. Redondance

Les serveurs sont répliqués, les centres de données sont alimentés par deux arrivées électriques indépendantes l'une de l'autre et sont également équipés d'onduleurs. Des groupes électrogènes d'une autonomie de 48 heures permettent de pallier une éventuelle panne du réseau de fourniture d'électricité. Plusieurs boucles de sécurisation ont ainsi été mises en place, afin d'éliminer tout risque d'indisponibilité. Cette multiplicité des liens permet également à vos données d'emprunter le chemin le plus court et donc d'afficher des temps de latence minimums. Les serveurs sont par ailleurs équipés d'une double alimentation et d'une double carte réseau : l'infrastructure est ainsi redondée de bout en bout.

4. Reprise de service

DISASTER RECOVERY PLAN (DRP)

Le DRP est activé en cas de désastre impactant l'intégrité des données :
→ faille logique majeure
→ destruction physique des infrastructures d'hébergement

Dans un tel cas, le client est prévenu instantanément et la procédure de reprise commence. Une nouvelle infrastructure est recréée dans l'un des centres de données disponibles sur Microsoft Azure.

Les données sont restaurées à partir de la dernière version des données sauvegardées. Comme mentionné précédemment, les sauvegardes complètes (version du service et données du client) s'effectuent automatiquement une fois par jour sur le cluster de secours et à distance, les données ne sortant jamais physiquement de leur lieu de stockage. Ceci garantit un RPO (Recovery Point Objective) maximum de 24 heures.

La durée du DRP est de 12 heures maximum. Et dans le cas d'un changement de centre de données obligeant à changer les IP des entrées DNS, les caches des DNS à travers le monde mettent 24h maximum à se mettre à jour.

Ceci garantit un RTO (Recovery Time Objective) de moins de 24 heures.

RÉACTION EN CAS D'INCIDENT

Chez les hébergeurs de 360Learning

Les alarmes sont configurées pour automatiquement notifier les équipes en charge des opérations lorsque les premiers signes d'alertes atteignent des seuils prédéfinis. Quand un seuil est dépassé, la réaction en cas d'incident de Microsoft Azure est déclenchée.

OVH met en place des logging et des systèmes de reporting en temps réel afin d'enregistrer et de rapporter les événements liés à la sécurité.

Tout événement est documenté et enregistré pendant une période de 90 jours après avoir été constaté.

Sur notre réseau

360Learning utilise un système de token unique attaché à une adresse IP pour garantir qu'un intrus ne puisse pas intercepter les échanges et communiquer avec l'API à la place de l'utilisateur (attaques type "man-in-the-middle"). Les tentatives de connexion de ce type sont rejetées et enregistrées. En cas de détection d'attaque, tous les clients concernés sont avertis sous 24h.

SUPPORT TECHNIQUE

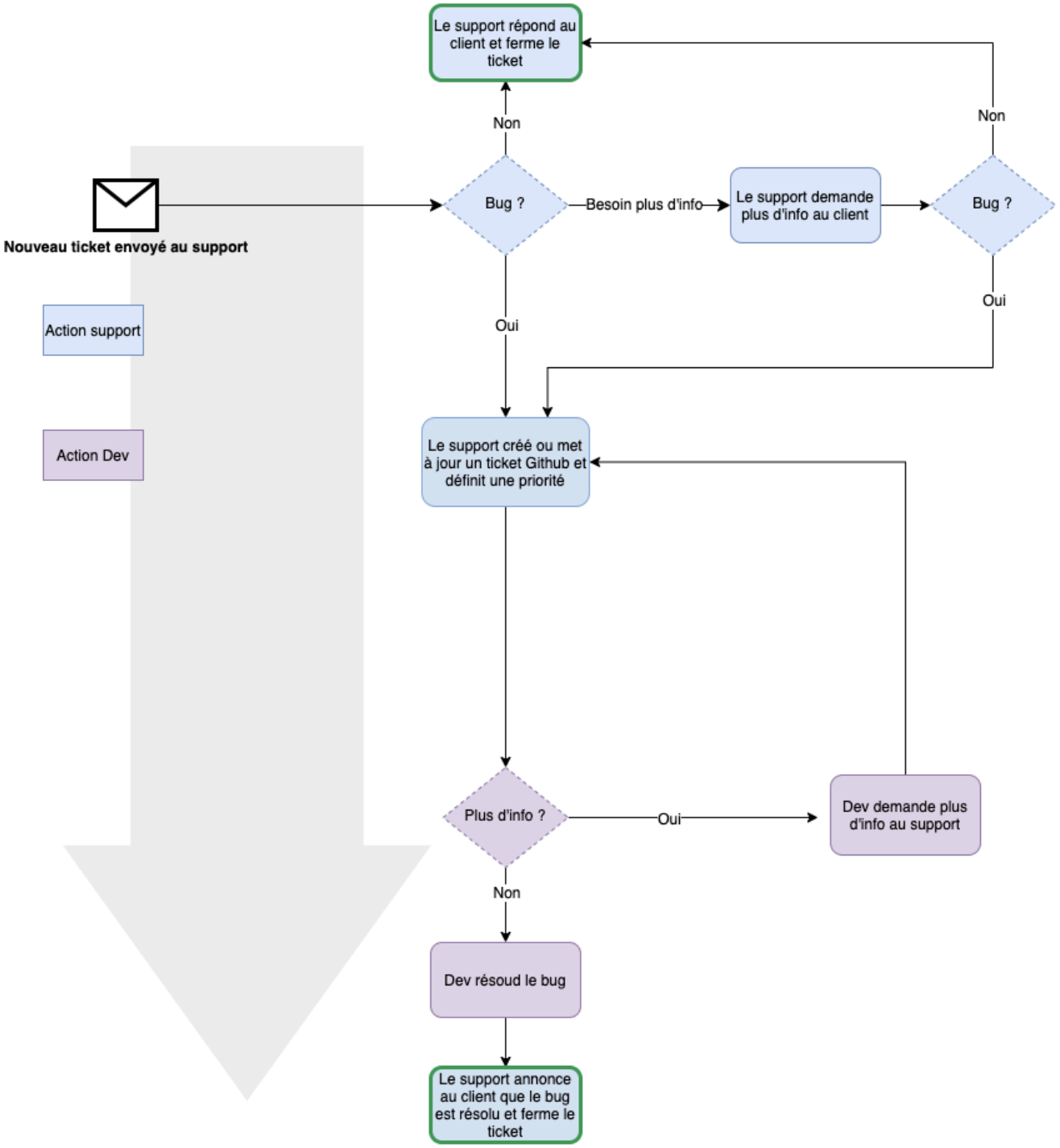
360Learning offre un service de support technique en ligne accessible en français et en anglais de 9:00 à 18:00 heure de Paris, du lundi au vendredi.

- → Support technique et fonctionnel par email
- → Mise à disposition d'une aide en ligne contextuelle
- → Accompagnement à l'utilisation de l'API documentée

→ Accompagnement pour les intégrations SSO
→ Étude et réalisation des demandes de développement

PROCESSUS DE PRISE EN CHARGE

Workflow Ticket



Architecture

1. Système

SAAS (SOFTWARE AS A SERVICE)

360Learning propose un logiciel de type SaaS (Software as a Service, Logiciel en tant que Service). Le modèle SaaS part du principe que le logiciel est installé sur des serveurs plutôt que sur la machine de l'utilisateur.

Il ne requiert donc aucune installation et permet un accès depuis n'importe quel ordinateur connecté à internet.

Le modèle SaaS offre une grande souplesse et permet de fréquentes mises à jour, permettant aux clients de 360Learning de bénéficier à chaque instant des dernières avancées technologiques proposées par 360Learning.

ARCHITECTURE LOGICIELLE

Notre architecture se découpe en trois couches (voir schéma) :

→ L'interface, en Javascript, qui s'exécute chez le client. Elle contient quelques workflows et des logiques métier. Cet élément passe naturellement à l'échelle : chaque client le recevant dès qu'il se connecte au site, et l'exécutant lui-même.
Pour obtenir les données à afficher, et envoyer de nouvelles données à la plate-forme, cette partie fait des requêtes AJAX à une API REST.

→ L'API REST, exposée par un serveur Web Node.js. Cette API est découpée en micro-blocs élémentaires (par exemple, une "route" indépendante de toutes les autres dans l'API pour ajouter un utilisateur à un parcours) que le code client peut appeler. Ces routes contiennent du code métier parfaitement optimisé, et ne consomment actuellement que 30% des ressources CPU et 10% des ressources RAM, ces niveaux correspondant à un pic de charge observé à un plus haut historique.

→ Node.js fait ensuite des requêtes à une base de données MongoDB pour stocker les données. Actuellement, un unique réplica suffit à répondre à toutes les requêtes de lecture et d'écriture, consommant environ 10 % de ses ressources. Quand 40 % des ressources seront atteintes, un processus de migration sera lancé, pour héberger cette base MongoDB dans le cloud, avec une des 3 méthodes de sharding standard de MongoDB (le choix sera fait selon notre profil de charge au

moment où la migration sera décidée). Cette étape est standard et ne demande que quelques lignes de configuration.

SUPERVISION

Pour garantir la disponibilité de cette architecture, 360Learning suit en temps réel les performances de ses serveurs. Dès que les performances se dégradent et passent en deçà d'un seuil critique, un système d'alerte (emails) notifie la direction et le département R&D.

Les indicateurs de performance des systèmes que 360Learning suit sont l'utilisation du CPU, de la RAM, utilisation du disque, I/O, la qualité du réseau, le nombre de requêtes, et la latence par service. Il n'est pas prévu qu'ils soient communiqués au client. En revanche, 360Learning fournit des statistiques de l'activité des utilisateurs sur les plateformes de ses clients en temps réel via les tableaux de bord de l'application, qui sont par ailleurs exportables.

360Learning collecte les logs d'accès et requêtes (ainsi que les erreurs et incidents). Ces logs sont stockés en étant signés de manière agrégée sur tous nos clients. La durée de rétention est fixée à minimum 3 mois.

TECHNOLOGIES ET OUTILS

360Learning utilise des technologies de pointe, utilisées par les plus grands acteurs du Web. Parmi lesquelles :

JavaScript & TypeScript

La plateforme 360Learning est développée en full Javascript, quasiment sans PHP. Les avantages sont nombreux :

- → Le temps de développement est considérablement réduit : une seule technique est à maîtriser par l'équipe R&D.
- → Les temps de chargement sont optimisés : la charge est déplacée vers le poste utilisateur qui fait une requête de données uniquement au moment où cela est nécessaire

Pour une fiabilité encore plus grande, le code est en cours de migration vers TypeScript, un surensemble de JavaScript qui vise à détecter les erreurs et les incohérences dans le code de manière plus précise et offre une maintenance plus facile (plus de 80 % des fichiers du code source sont en TypeScript à la date de rédaction).

Vue.js

L'application client web de 360Learning utilise Vue.js, une bibliothèque JavaScript frontale pour la construction d'interfaces utilisateur. Grâce au rendu déclaratif et à la composition de

composants, les applications basées sur Vue.js sont beaucoup plus modulaires, extensibles et faciles à maintenir.

Express.js
Express.js est un framework Node.js qui permet d'exposer une API en toute sécurité.

Node.js
360Learning utilise Node.js, plateforme logicielle libre et événementielle en JavaScript conçue pour les applications réseau qui doivent pouvoir monter en charge. Node.js permet de créer des applications extrêmement performantes.

MongoDB
360Learning utilise un système de gestion de base de données orientée documents, MongoDB, technologie de pointe adaptée à la montée en charge. Aujourd'hui c'est l'un des SGBD les plus utilisés, notamment par Facebook, Linkedin, Google ou Amazon. MongoDB est installé sur nos serveurs et géré à 100% par 360 Learning.

Bases de données spécialisées
Pour les fonctionnalités spécifiques, 360Learning exploite la puissance de systèmes de gestion de données de pointe plus adaptés, notamment ElasticSearch, Redis et Snowflake. Ils prennent en charge des fonctionnalités telles que les tableaux de bord, les LiveLearners, les recommandations personnalisées, la recherche, et bien plus encore.

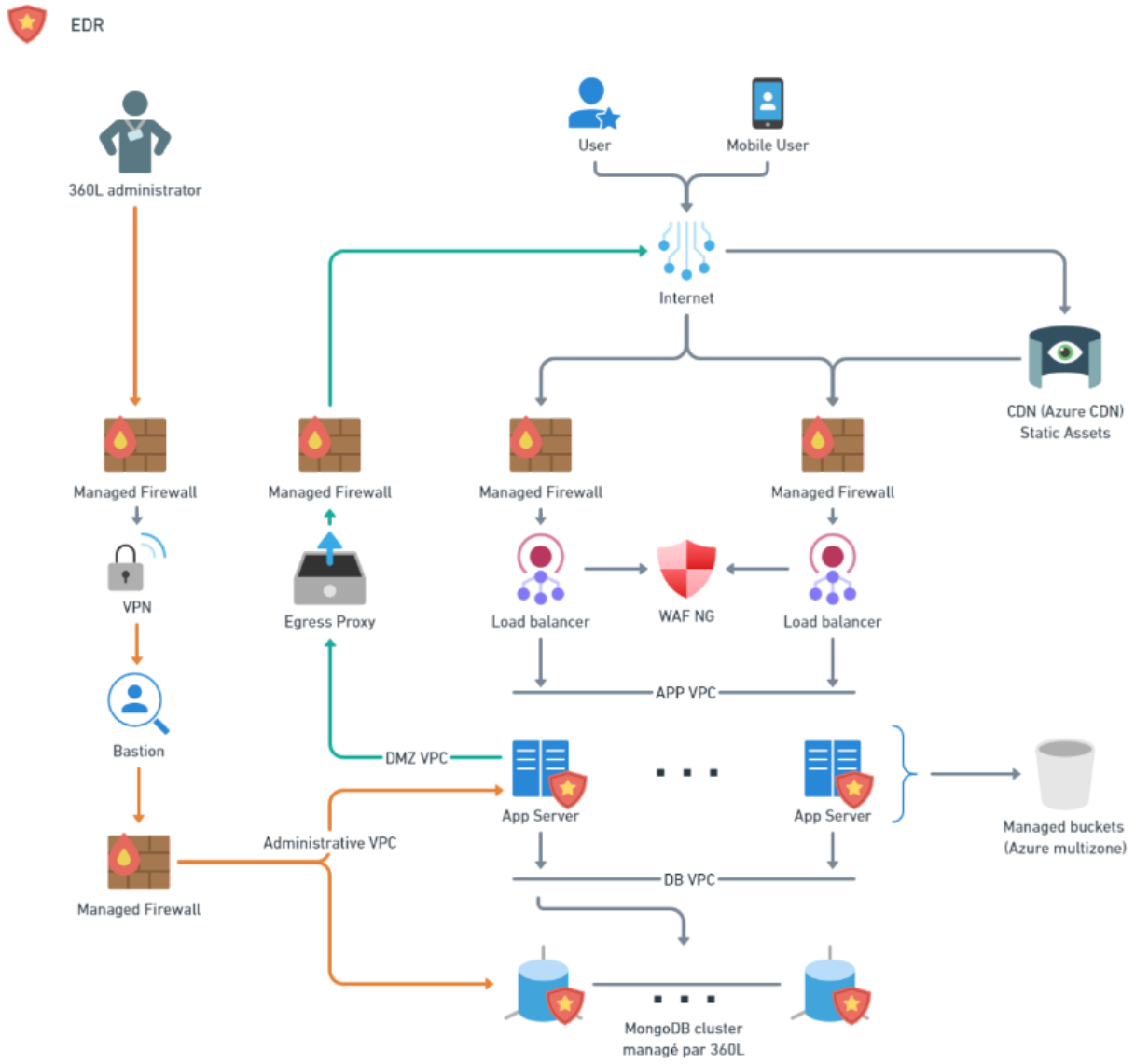
SERVEURS

Le système d'exploitation de nos serveurs est Linux Ubuntu LTS 22 LTS.

POLITIQUE DE GESTION DES NOUVELLES VERSIONS DES NAVIGATEURS

Quand une nouvelle version significative d'un navigateur fait son apparition, 360Learning s'assure de la compatibilité de sa plateforme.

RÉSEAU



L'intégralité des données est répliquée sur un serveur de préproduction qui est testé en profondeur toutes les 3 semaines. Les temps de réponse du cloud sont régulièrement testés sur cinq requêtes prédéfinies. Les temps de réponse depuis la France doivent avoir un temps de réponse inférieur à 50 ms.

2. Volume Clients

Afin de garantir une performance équitable pour tous les utilisateurs, 360Learning documente et implémente optionnellement des limites à certaines fonctionnalités. Si le client a besoin de plus de 200 000 utilisateurs sur sa plateforme, l'équipe R&D doit être informée un mois à l'avance, afin qu'elle puisse commencer un processus de redimensionnement. Une plateforme ne peut pas dépasser 30 000 groupes. Nous appliquons également des limites de taux à l'API 360Learning. De plus, des limites sur des fonctionnalités spécifiques sont documentées dans la base de connaissances de 360Learning.

Intégrations

1. SSO

OBJECTIFS

Le Single Sign-On (SSO) est un mécanisme d'authentification qui permet aux utilisateurs d'accéder à plusieurs applications en n'utilisant qu'un seul identifiant de connexion.

En activant le SSO sur votre plateforme 360Learning, vous devenez responsable de l'authentification de vos utilisateurs : ils sont authentifiés à travers votre propre portail de connexion et n'ont plus besoin d'un identifiant / mot de passe supplémentaire.

Parmi les avantages de l'utilisation de ce SSO :
→ Amélioration de l'expérience utilisateur
→ Renforcement de la sécurité
→ Navigation plus fluide

TECHNOLOGIES

360Learning prend actuellement en charge trois implémentations SSO : JWT (JSON Web Token) et SAML (Secure Assertion Markup Language) et OIDC (OpenId Connect.
→ SAML est un format plus ancien, basé sur le XML. Il est pris en charge par de nombreux services et peut facilement être intégré au sein de votre système d'authentification d'entreprise, comme Windows Active Directory.

→ JWT est un standard utilisant le format JSON, et est utilisé au sein des protocoles d'authentification les plus récents. Il offre une grande souplesse d'utilisation.360Learning prend actuellement en charge

deux solutions de SSO : JWT (JSON Web Token) et SAML (Secure Assertion Markup Language). JWT et SAML sont tous deux des formats de token de sécurité qui ne dépendent d'aucun langage de programmation.

→ OpenID Connect s'appuie sur le protocole OAuth 2.0 et utilise un jeton Web JSON (JWT) supplémentaire pour normaliser les domaines qu'OAuth 2.0 laisse au choix, tels que les champs d'application et la découverte des routes d'API.

DOCUMENTATION

Des guides techniques concernant les deux technologies sont disponibles afin de vous aider à intégrer le SSO :
→ 360Learning -Technical Guide – SSO JWT
→ 360Learning -Technical Guide – SSO SAML
→ 360Learning - Technical Guide – SSO OIDC

2. API

OBJECTIFS

L'API 360Learning vous permet de synchroniser votre annuaire utilisateur avec l'annuaire utilisateur 360Learning, et ce dans les deux sens. Vous pouvez facilement ajouter ou supprimer des utilisateurs, définir leur nom, mot de passe et leurs caractéristiques principales de profil. Vous pouvez ajouter des utilisateurs à des groupes, par exemple pour maintenir des groupes 360Learning à jour avec des changements au sein de votre organisation.

L'API vous permet également d'exporter les statistiques d'apprentissage relatives aux parcours.

Plus globalement, l'API désigne les interfaces logicielles de la plateforme 360Learning permettant l'échange de données entre la plateforme et votre système d'information, y compris tout logiciel édité par un tiers pour lequel vous disposez d'un droit d'utilisation

DOCUMENTATION

Une description complète de notre API est disponible en ligne https://api.360learning.com/ ou au sein de notre guide technique :
→ 360Learning -Technical Guide – API

CONDITIONS D'UTILISATION

L'accès et l'utilisation des API de la plateforme 360Learning sont soumis à l'acceptation et au respect des présentes Conditions d'Utilisation, définissant les conditions dans lesquelles 360Learning met à disposition l'API, ainsi que les droits et obligations liés à l'utilisation de l'API.

Les APIs font partie intégrante des Services et ne sont ouvertes en conséquence :

- qu'aux clients d'une entité du groupe 360Learning ayant un contrat en vigueur régissant les conditions contractuelles afférentes aux Services de la plateforme pour une durée minimum de douze mois et dans le respect de la politique de mise à disposition des API déterminées par 360Learning ;
- aux partenaires ayant conclu, avec 360Learning SA en tant que titulaire des droits sur la plateforme, un contrat définissant les modalités d'accès et d'utilisation des API.

Les Conditions d'Utilisation sont susceptibles d'être mises à jour. Les Conditions applicables sont celles en ligne dans la Documentation à la date de l'utilisation de l'API.

MODALITÉS ET CONDITIONS D'ACCÈS

Vous accédez et utilisez l'API en application du contrat signé avec 360Learning..
Les modalités d'accès et limites sont définies dans le Guide Technique API.

Il vous appartient, en qualité de responsable de traitement, d'utiliser l'API en vous assurant du respect des règles propres à la protection des données à caractère personnel. Vous garantissez à 360Learning que vous utilisez les API dans le respect des droits des titulaires des droits des systèmes avec lesquels vous mettez en œuvre l'API.

Dans le cas où un tiers accède et utilise l'API, cette utilisation s'exerce sous votre responsabilité au bénéfice exclusif de vos utilisateurs couverts par le contrat conclu entre vous et 360Learning (affiliées, prestataires de services de votre système d'information, éditeurs).
Dans ce cadre, l'API est mise à votre disposition uniquement pour un usage technique et pour votre usage interne. L'utilisation suppose de ne pas:

- détourner l'utilisation de l'API à des fins commerciales ;
- commettre un acte de contrefaçon, en particulier donner accès, en tout ou partie, à l'API à un tiers dans un objectif de décompilation ou d'études notamment de la plateforme ou dans un but de concurrence déloyale ;
- perturber le bon fonctionnement de l'API et, plus généralement, de la plateforme et des Services ;

Vous vous assurez de la compatibilité des équipements informatiques utilisés pour accéder à l'API, lesquels doivent respecter l'état de l'art en matière de sécurité. Vous respectez les procédures et règles de sécurité prescrites par 360Learning.

360Learning se réserve le droit de suspendre l'accès à l'API en cas de suspicion légitime du non-respect des conditions d'utilisation de l'API.

PROPRIÉTÉ DE L'API ET CONTINUITÉ DE DISPONIBILITÉ

360Learning est titulaire des droits sur l'API et intervient en qualité de gestionnaire de l'API.

360Learning pourra être amené à déprécier, modifier ou limiter l'accès aux API. Dans ce cas, il informera les clients, dans les meilleurs délais.

360Learning ne peut être tenu pour responsable des conséquences de ces modifications, 360Learning ne prenant aucun engagement de continuité des APIs. Dans le cas où une dépréciation, une modification ou une limitation d'accès entraînerait une dégradation significative des Services impactant les conditions déterminantes de contractualisation des Services par le client, celui-ci pourra résilier le Contrat, sous réserve d'un préavis de trente jours (30). Sauf dans le cas de contestation légitime de 360Learning, la résiliation prendra effet à la date de fin du préavis notifié par lettre recommandée explicitant et démontrant la dégradation significative sur les Services et le lien direct avec les conditions déterminantes de contractualisation.

Sous-Traitants ultérieurs autorisés (à titre d'information) – Utilisation de la plateforme

DÉNOMINATION SOCIALE DU SOUS-TRAITANT	JURISDICTION/ EMPLACEMENT GÉOGRAPHIQUE DES SERVICES FOURNIS	DESCRIPTION DES SERVICES FOURNIS	MÉCANISME DE TRANSFERT EN PLACE POUR ASSURER UN NIVEAU DE PROTECTION ADÉQUAT POUR LES DONNÉES À CARACTÈRE PERSONNEL DANS LE CAS OÙ LE TRANSFERT EST VERS UNE ENTITÉ À L'EXTÉRIEUR DE L'UE	DONNÉES PERSONNELLES TRAITÉES
MICROSOFT	France pour les clients EMEA - US pour les clients US	Hébergement de l'infrastructure 360Learning Service d'IA générative	N/A	Nom, Prénom, Email, Fonction, Photo, Login, Statistiques d'usage
SCALEWAY	France	Hébergement de l'infrastructure de test 360Learning pour les clients en ayant fait la demande	N/A	Nom, Prénom, Email, Fonction, Photo, Login, Statistiques d'usage
OVH	France	Hébergement de nom de domain	N/A	Fichiers multimédia (import)
AMAZON SES	UE (Irlande) US pour les clients US*	Envoi des mails de notification	N/A	Email, contenu et statut des emails de notification
AMPLITUDE (non-utilisé pour les clients Allemands**)	US	Statistiques d'usage pour la création de rapports	DPA Signé avec Clauses Contractuelles Type (CCT)	ID (Pseudo)
PENDO INC.	EU	Notifications de plateforme, guides et autres communications dans l'application.	N/A	ID (Pseudo)
GAINSIGHT INC.	EU (Allemagne)	Statistiques d'usage pour la création de rapports	N/A	ID (Pseudo)
DATADOG	EU	Observabilité	NA	ID (Pseudo)

SNOWFLAKE COMPUTING NETHERLANDS B.V.	EU US pour les clients US*	Statistiques d'usage pour la création de rapports, Fournir des fonctions de traitement des données (par exemple, la recherche sur la plateforme)	N/A	Nom, Prénom, Email (pour les rendre disponibles dans la recherche) - Non utilisé pour les statistiques. Pour les statistiques : ID (Pseudo)
ELASTIC APP SEARCH	EU US pour les clients US*	Moteur de recherche pour la recherche sur la plateforme ; analyse de l'utilisation pour les recommandations	N/A	Nom, Prénom, Email
WORKATO	EU pour les clients EMEA - US pour les clients US*	Fournisseur iPaaS pour les automatisations et les intégrations de tiers	N/A	Uniquement pour les connecteurs de Workato : les données personnelles téléchargées sur le service, qui peuvent inclure mais ne sont pas limitées à : Nom, prénom, courriel. .
Les sous-traitants autorisés suivants peuvent uniquement avoir accès à un nombre limité d'utilisateurs autorisés ayant un rôle spécifique : auteur, administrateur, propriétaire et non à tous les utilisateurs.				
ZENDESK	US and UE	Gestion des demandes de support client	DPA Signé avec Clauses Contractuelles Type (CCT) BCR Internes Zendesk	Nom, Prénom, Email, Photo (Si ajoutée)

*désigne tout Client ayant signé un contrat avec l'entité 360Learning INC et ayant demandé un hébergement de ses données dans une infrastructure située aux Etats-Unis.
**désigne tout Client ayant signé un contrat avec l'entité 360Learning GmbH.

Afin de fournir le meilleur service à nos clients, cette liste peut être amenée à évoluer.

Pour plus d'informations sur le traitement des données personnelles, nous vous invitons à consulter notre politique de confidentialité accessible depuis le lien suivant:
https://360learning.com/fr/politique-de-confidentialite

Informations Juridiques

Déclaration des contenus

Afin de répondre à nos obligations en tant qu'hébergeur de contenu dans le cadre de la loi pour la confiance dans l'économie numérique, n° 2004-575 du 21 juin 2004 ("LCEN"), 360Learning a mis en place une procédure de notification qui permet aux clients de signaler un contenu illégal sur la plateforme et de demander son retrait. Les clients peuvent envoyer cette notification par e-mail à l'adresse suivante : data-protection@360Learning.com

Cookies et Statistiques

L'accès à la plateforme 360Learning nécessite l'utilisation de cookies. Ces cookies sont essentiels et/ou fonctionnels, ce qui signifie qu'ils sont nécessaires pour que les services soient fournis. Leur traitement repose sur l'intérêt légitime, conformément au RGPD, et ne nécessite pas de consentement spécifique.

En tant que Responsable du Traitement, 360Learning collecte et traite les données personnelles à des fins de gestion commerciale et administrative des clients et de leurs employés.

Des statistiques d'utilisation pseudonymisées sont également collectées pour permettre l'analyse et l'amélioration de nos services. 360Learning peut être amené, aux seules fins de cette administration et de cette gestion, à partager ces données personnelles avec ses prestataires de services et/ou avec ses sociétés affiliées.

360Learning prend toutes les précautions nécessaires lors de la collecte et du traitement des données personnelles du client pour se conformer au droit applicable. Pour toute demande d'accès, d'opposition, de rectification, de portabilité, de limitation, ou de gestion des données en cas de décès : Les clients peuvent envoyer un courrier électronique à l'adresse suivante : **data-protection@360Learning.com.**

Les données personnelles du Client sont conservées pendant une durée conforme aux dispositions légales et proportionnelles aux finalités pour lesquelles elles ont été enregistrées. Lorsque leur conservation n'est plus justifiée par des exigences légales, commerciales ou liées à la gestion du compte client, ou si le Client fait usage d'un droit de modification ou d'effacement, nous les supprimerons de façon sécurisée.

Politique de Modération

Ces règles d'utilisation ont pour objectif de définir les principes et les modalités de modération des contenus publiés sur la plateforme 360Learning par les Client et leurs Bénéficiaires

Elles visent à garantir un environnement conforme aux exigences légales du règlement relatif au marché unique des services numériques du 19 octobre 2022 ("DSA") en vertu duquel 360Learning est qualifié de « fournisseur de service d'hébergement ». Les présentes dispositions n'exonèrent pas les Clients de leur

obligation d'insérer leur propre charte de modération sur la plateforme, à destination de leurs utilisateurs.

Principes généraux applicables à l'utilisation de la plateforme 360Learning :

Dans le cadre de l'utilisation de la plateforme 360Learning, les Clients et les Bénéficiaires doivent respecter les principes généraux suivants :

- respect de la loi : tous les contenus publiés sur la plateforme 360Learning doivent être conformes à la réglementation applicable, notamment les lois relatives à la diffamation, au harcèlement et aux droits d'auteur ;
- politesse et respect d'autrui : les utilisateurs doivent se traiter les uns les autres avec respect, même en cas de désaccord. Ils doivent s'abstenir de toute forme de langage haineux, discriminatoire ou offensant ;
- les commentaires sur le forum ne doivent porter que sur des échanges relatifs aux contenus dans le contexte du Collaborative Learning ;
- confidentialité et vie privée : le partage des informations personnelles d'autres utilisateurs sans leur consentement est formellement interdit ;
- authenticité et propriété intellectuelle : les utilisateurs doivent s'assurer que les contenus qu'ils publient sont authentiques et qu'ils détiennent les droits de propriété intellectuelle nécessaires ;
- véracité des informations : la diffusion de fausses informations ou de contenus trompeurs est strictement interdite.

Responsabilité des Parties concernant les contenus publiés sur la plateforme 360Learning par les les Clients et leurs Bénéficiaires :

Conformément au Contrat, les Services proposés par 360Learning ont pour finalité d'offrir l'accès et l'utilisation à une plateforme permettant aux clients de créer une expérience de formation engageante et collaborative grâce à la création et mise à jour des contenus de formation à visée pédagogique

Les clients, responsables des contenus publiés sur la plateforme, se doivent de diffuser leur propre politique de modération des contenus. 360Learning, en tant que fournisseur de service d'hébergement, pourra suspendre ou supprimer des contenus considérés comme illicites en vertu des lois applicables ou figurant sur la liste suivante :

Catégories de contenus illicites :

- contenus illicites : contenus contraires à la loi française et européenne, tels que les discours de haine, l'apologie du terrorisme, la pédopornographie, etc. ;
- contenus haineux ou discriminatoires : contenus qui incitent à la haine, à la violence ou expriment de la discrimination envers un individu ou un groupe de personnes en raison de leur origine, de leur religion, de leurs opinions politiques, etc. ;
- contenus portant atteinte à la vie privée : contenus qui divulguent des informations personnelles sans le consentement de la personne concernée ;
- contenus à caractère sexuel explicite : contenus pornographiques ou à caractère sexuel explicite, y compris la représentation de mineurs ;
- contenus faux ou trompeurs : contenus qui diffusent de fausses informations ou qui sont de nature à tromper les utilisateurs ;
- contenus plagiés : contenus sur lesquels l'utilisateur qui les publie n'a pas de droits de propriété intellectuelle.

Signalements auprès du Client :

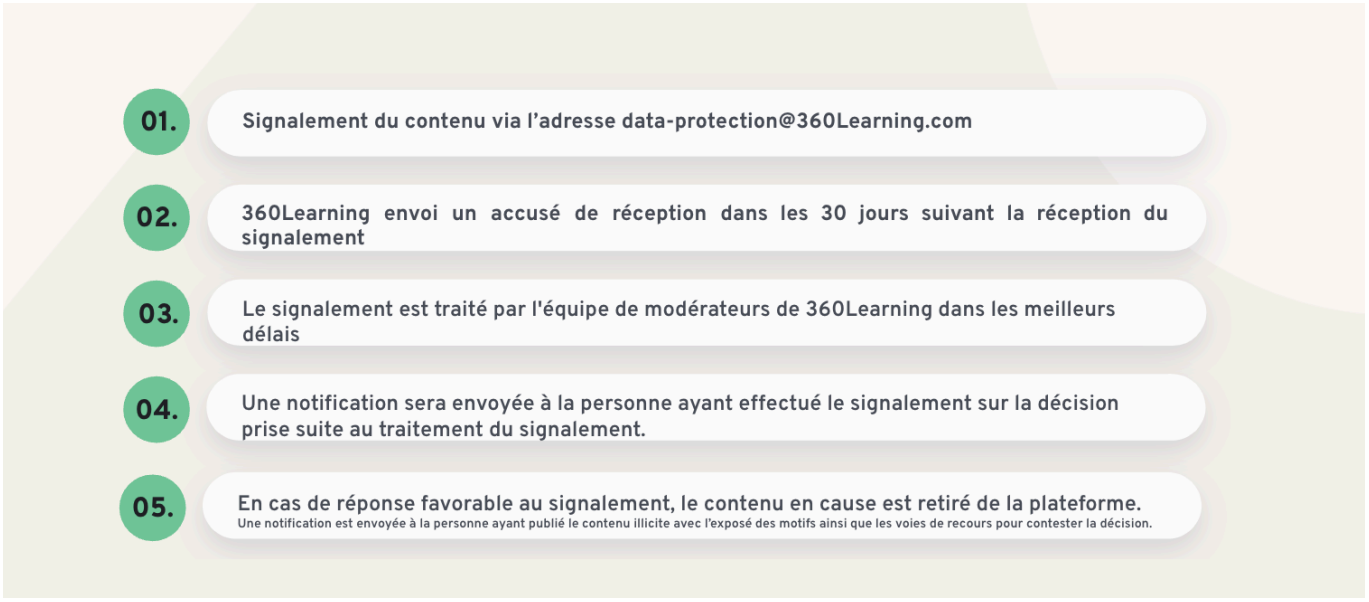
Il est rappelé que les clients sont responsables des contenus publiés sur la plateforme et qui leur appartient de les valider avant toute diffusion.

La plateforme permet d'inclure une charte de modération, ainsi qu'une procédure de modération et de signalement des contenus illicites ou contraire à la politique de modération déterminé par le client.

Pour plus de détails sur cette procédure veuillez consulter cet article : Charte de modération

Signalement des commentaires : La plateforme offre également la possibilité de signaler les commentaires illicites ou contraires à la politique de modération défini par le Client, en utilisant le bouton "Signaler" présent au niveau de chaque commentaire. Ce signalement sera traité par le Client selon ses propres procédures internes. Pour plus de détails sur cette procédure veuillez consulter cet article : Signaler des commentaires

Mécanisme de signalement de contenus illicites auprès 360Learning, fournisseur de services d'hébergement :



Tout contenu illicite ou contraire à la politique de modération de 360Learning peut-être signalé en l'envoyant par e-mail à l'adresse suivante : data-protection@360Learning.com

Pour être pris en compte, le signalement devra contenir, a minima :

- Les coordonnées de de la personne effectuant le signalement ;
- Les coordonnées de l'entité fournissant l'accès à la plateforme (le Client) ;
- Le lien URL et toute autre information sur l'emplacement du contenu ;
- Les raisons pour lesquelles le signalement du contenu est considéré comme illicite.

360Learning enverra un accusé de réception à la personne ayant effectué le signalement dans les 30 jours suivant la réception du signalement.

Les signalements de contenus faits auprès de 360Learning, seront traités par l'équipe de modérateurs de 360Learning dans les meilleurs délais.

Une notification sera envoyée à la personne ayant effectué le signalement sur la décision prise suite au traitement du signalement.

En cas de réponse favorable au signalement, le contenu en cause est retiré de la plateforme. Une notification sera également envoyée à l'utilisateur concerné ayant publié le contenu illicite et au Client

fournissant l'accès à la plateforme avec l'exposé des motifs ainsi que les voies de recours pour contester la décision de restriction suite au traitement du signalement.

Conformément aux obligations découlant du DSA, 360Learning a désigné data-protection@360Learning comme point de contact unique pour toute communication.