
Exploiter un lieu de visite en toute sécurité

Pourquoi un musée, un centre de culture scientifique ou un centre d'expérience de marque doit être exploité comme un parc informatique bien gouverné, et comment taleor y parvient : chaque appareil identifié, chaque connexion chiffrée, chaque modification attribuée, chaque visiteur anonyme.

Livre blanc · octobre 2026 · Version 1.0

Pour les directions, les responsables techniques et informatiques, les intégrateurs audiovisuels, les consultants et les commissions d'appel d'offres des musées, centres de culture scientifique, centres d'expérience de marque, sites patrimoniaux et sites de loisirs.

taleor

Sommaire

1	Synthèse	3
2	Le problème : un lieu est désormais un parc informatique	3
3	Ce dont un lieu a réellement besoin	5
4	Comment fonctionne taleor	6
5	Sécurisé dès la conception	8
6	Configuré par un assistant	13
7	Statistiques : ce qu'un lieu apprend	14
8	Fonctionne partout, avec le matériel que vous avez	15
9	Modèles de déploiement et méthode d'évaluation	17
10	À propos de taleor	19
	Sources et vérification	19

1 Synthèse

Un lieu de visite était autrefois un bâtiment équipé de quelques écrans. C'est aujourd'hui un réseau : des centaines d'ordinateurs, d'afficheurs, de projecteurs, de haut-parleurs, d'éclairages et de capteurs d'une douzaine de fabricants, chacun avec son propre micrologiciel, une adresse et souvent un mot de passe, exploités par une petite équipe qui n'est pas une équipe informatique.

Ce livre blanc défend l'idée qu'un lieu doit être exploité comme un parc informatique bien gouverné : chaque appareil identifié, chaque connexion chiffrée, chaque modification attribuée, chaque mise à jour vérifiée, chaque visiteur laissé anonyme. La section 3 énonce sept principes, les sections 4 à 8 décrivent comment taleor les respecte, et la section 9 se termine par une liste de contrôle qu'une commission d'appel d'offres peut soumettre à n'importe quel fournisseur, nous compris.

taleor est une manière sûre et agentique d'exploiter un lieu de visite : ses contenus, ses applications interactives, ses lecteurs (le logiciel ou l'ordinateur qui fait fonctionner chaque écran) et son matériel, depuis une seule console. Il repose sur trois piliers : il est sécurisé dès la conception ; il est configuré par un assistant qui n'applique jamais une modification sans l'accord d'une personne nommément identifiée ; et ses statistiques affichent « non mesuré » plutôt que zéro. Il fonctionne comme application web, comme application de bureau pour Windows, macOS et Linux, et comme serveur local dans votre propre bâtiment, y compris entièrement isolé du réseau (air gap). Ses lecteurs fonctionnent sous Windows, macOS, Linux, Raspberry Pi et Android. Il pilote des équipements de toutes marques au moyen de standards ouverts.

2 Le problème : un lieu est désormais un parc informatique

2.1 Des centaines d'appareils, des dizaines de marques, une petite équipe

Comptez les ordinateurs dans les salles d'un musée contemporain : un derrière la plupart des installations, plus les afficheurs en réseau, les projecteurs, les processeurs audio, les contrôleurs d'éclairage, les capteurs, les lecteurs de badges et les boutons. Dans un lieu de taille modeste, on atteint vite quelques centaines. Les données de démonstration utilisées pour développer taleor, modélisées sur un musée régional type, comptent 69 installations et 342 appareils parlant 49 protocoles de commande. C'est un parc ordinaire.

Chaque fabricant apporte son propre protocole, son propre outil de gestion et sa propre conception des mises à jour. Les contenus changent à chaque saison. L'équipe compte généralement deux à cinq personnes dont les postes n'ont pas été conçus pour inclure la gestion d'un parc d'appareils et l'application des correctifs.

2.2 L'exposition aux risques de sécurité

Quatre points faibles s'aggravent mutuellement.

Les identifiants par défaut. Le matériel audiovisuel professionnel est livré avec une interface d'administration et un mot de passe d'usine rarement modifié, car le changer sur deux cents appareils représente une semaine de travail dont personne n'a la charge. Le botnet Mirai de 2016 a recruté des appareils en essayant une courte liste de mots de passe d'usine. L'audiovisuel des lieux de visite n'y échappe pas.

Les lecteurs non corrigés. L'ordinateur qui se trouve derrière une installation fonctionne souvent encore avec le système d'exploitation de sa mise en service, car le mettre à jour implique de fermer l'installation. Une machine non corrigée sur le même réseau que la billetterie et la gestion technique du bâtiment est une porte d'entrée. Les référentiels auxquels sont soumis les organismes publics en Allemagne, aux Pays-Bas et en Pologne (BSI IT-Grundschutz, la Baseline Informatiebeveiliging Overheid et les obligations découlant de NIS2) considèrent l'application rapide des correctifs et l'inventaire des actifs comme des mesures de base.

Les secrets partagés. De nombreux systèmes de commande authentifient un lecteur au moyen d'une clé stockée dans un fichier de configuration. Quiconque peut lire ce fichier peut se faire passer pour ce lecteur.

La dépendance au cloud. Un système qui s'arrête lorsque la connexion internet ou le cloud du fournisseur tombe a déplacé le point de défaillance unique là où le lieu ne peut pas intervenir. Pour une institution publique, c'est aussi une question d'achat public : qui détient les données, sous quel droit, et que se passe-t-il à la fin du contrat ?

2.3 Interruptions, angles morts et dépendance vis-à-vis d'un fournisseur

L'interruption de service est la défaillance la plus visible et la moins mesurée. Un écran se fige à dix heures, un visiteur le signale à midi, le technicien l'apprend à quatorze heures, et rien n'a enregistré les quatre heures perdues.

La plupart des lieux comptent les visiteurs à l'entrée et nulle part ailleurs. Ils ne peuvent pas dire devant quelle installation les gens se sont arrêtés, pendant combien de temps, ni si une vidéo a été regardée jusqu'au bout. Là où une mesure existe, il s'agit souvent d'un système distinct, trop souvent équipé de caméras qui identifient les personnes.

Chaque sous-système arrive avec son propre fournisseur et son propre contrat. Lorsqu'un fournisseur est racheté ou abandonne un produit, les contenus conçus pour un lecteur propriétaire ne peuvent pas être transférés, et le matériel qui ne dialogue qu'avec un seul contrôleur devient bon pour la casse. La question qu'une commission devrait poser n'est pas « ce fournisseur prend-il en charge notre matériel ? » mais « si ce fournisseur disparaissait, que posséderions-nous encore ? »

3 Ce dont un lieu a réellement besoin

Ces problèmes ont déjà été résolus, dans l'informatique généraliste. Ce qui manquait, c'était leur application à la forme particulière d'un lieu de visite : beaucoup de petits ordinateurs, beaucoup de marques, une petite équipe, un public, et un bâtiment qui doit ouvrir à dix heures. Nous proposons sept principes.

1. **Chaque appareil possède une identité impossible à copier.** Une clé générée sur son propre matériel et qui ne l'a jamais quitté. Pas un mot de passe. Pas un jeton dans un fichier.
2. **Chaque connexion est chiffrée et authentifiée dans les deux sens.** Toute protection moindre permet à un inconnu présent sur le réseau du lieu de mettre en place une imitation convaincante.
3. **Rien ne s'exécute sur un lecteur sans avoir été vérifié au préalable.** Les pilotes et les mises à jour sont contrôlés sur le lecteur lui-même au moyen d'une signature ou d'une somme de contrôle, et pas seulement à la source.
4. **Chaque modification porte un nom et une heure.** Un journal d'audit qu'un administrateur peut réduire à une journée, ou modifier, n'est pas un journal d'audit.
5. **Chacun dispose des droits dont son travail a besoin, et pas davantage.** Un responsable technique peut redémarrer un écran figé sans pouvoir le supprimer.
6. **Les visiteurs restent anonymes par construction, et non en vertu d'une politique.** C'est une propriété du schéma de la base de données, et elle est testée.

7. **7. Le lieu est propriétaire de son système.** Il peut tout faire fonctionner dans son propre bâtiment, sans internet, et peut changer de solution sans perdre ses contenus.

C'est ce qu'un service informatique compétent exigerait de n'importe quel parc de deux cents ordinateurs. La suite de ce livre blanc décrit comment taleor y répond.

4 Comment fonctionne taleor

4.1 Les composants

La console. Une application web dans laquelle le personnel voit chaque installation, chaque lecteur et chaque équipement, charge les contenus, définit les plannings et les déclencheurs, surveille l'état de fonctionnement et les alertes, et consulte les statistiques. Elle fonctionne dans tout navigateur récent, ou comme application de bureau pour Windows, macOS et Linux.

L'agent du lecteur. Un petit service d'arrière-plan sur l'ordinateur placé derrière chaque installation. Il maintient une connexion permanente et mutuellement authentifiée avec le serveur, diffuse ce qu'on lui demande, pilote les équipements reliés à cet ordinateur, lit ses capteurs, signale son état et se tient lui-même à jour. Par défaut, il conserve une copie locale de ses contenus de 4 Go et continue la diffusion lorsque le serveur est injoignable. Les agents fonctionnent sous Windows, macOS, Linux, Raspberry Pi et Android. Un écran sans ordinateur s'associe comme lecteur dans le navigateur, grâce à un code à six chiffres lu directement sur l'écran.

Les pilotes. Un paquet signé qui indique à taleor ce qu'un équipement sait faire et comment communiquer avec lui. La console demande une action, comme l'alimentation, la source ou le volume ; le pilote parle le protocole.

Le serveur. La base de données, les concentrateurs WebSocket qui transportent l'état en direct, l'autorité de certification de chaque lieu, le stockage des médias, le moteur de planification, la surveillance des alertes, le journal d'audit et les statistiques. C'est le même logiciel dans notre cloud ou sur une machine dans votre bâtiment, avec ou sans internet.

4.2 Un seul logiciel, trois façons de l'exploiter

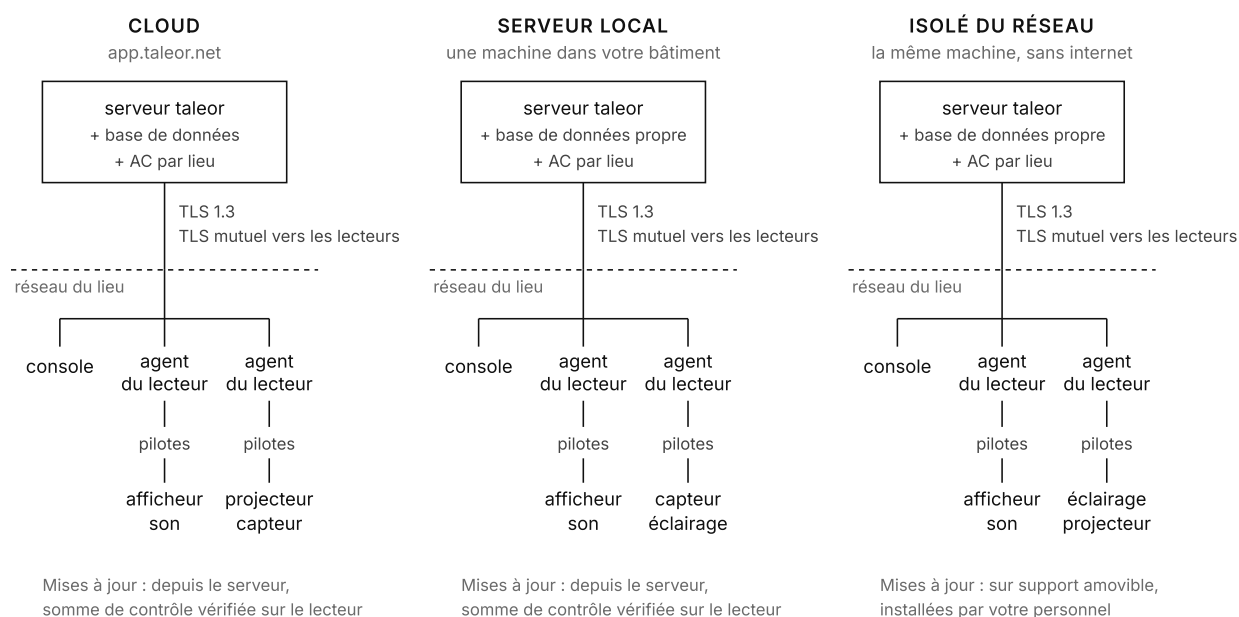


Figure 1. Un seul logiciel, trois façons de l'exploiter. Le même serveur, la même console et les mêmes agents de lecteur dans le cloud, sur un serveur local dans le bâtiment, ou isolés du réseau, sans internet.

En mode cloud, la console et le serveur se trouvent à l'adresse app.taleor.net et les agents s'y connectent de l'intérieur vers l'extérieur ; les équipements du réseau du lieu sont pilotés par les agents situés dans ce réseau. En mode serveur local, le même paquet s'installe sur une machine Windows, macOS ou Linux dans le bâtiment, avec sa propre base de données privée et sa propre autorité de certification, de sorte que la console, les lecteurs, les médias et le journal d'audit restent tous sur place. En mode isolé, ce serveur fonctionne sans aucun accès à internet : l'environnement d'exécution et la base de données sont inclus dans le paquet, rien n'est téléchargé lors de l'installation, et les mises à jour sont apportées sur un support amovible par votre propre personnel. Une seule base de code, une seule console ; un lieu qui démarre dans le cloud peut ensuite tout rapatrier sur place.

5 Sécurisé dès la conception

5.1 Identité : une clé qui ne quitte jamais la machine

taleur remplace le secret partagé par un certificat. Lors de son enregistrement, un lecteur génère une paire de clés asymétriques sur sa propre machine et n'envoie que la partie publique, dans une demande de signature de certificat, à l'autorité de certification du lieu, qui signe et renvoie un certificat. La clé privée ne circule jamais. Dès lors, le lecteur prouve son identité en produisant une signature, en direct, lors de chaque négociation TLS. Il n'y a rien à copier.

Une autorité de certification par lieu, ouverte depuis la console par un administrateur. Une compromission dans un lieu ne permet pas de fabriquer une identité dans un autre. La clé privée de l'autorité est chiffrée au repos sous un secret distinct des autres secrets du serveur.

La demande n'est pas considérée comme fiable. Seule la clé publique est reprise de la demande de signature ; le sujet, la durée de validité et toutes les extensions sont fixés par le serveur, de sorte qu'un lecteur ne peut ni demander à porter le nom d'un autre lecteur, ni devenir une autorité de certification. Les certificats des lecteurs sont émis uniquement pour l'authentification client : un certificat volé ne peut donc pas servir à monter un faux serveur.

Il n'existe pas de bouton « émettre un certificat ». Un certificat dont le serveur aurait un jour détenu la clé privée irait à l'encontre du but recherché.

5.2 Transport : chiffré et contrôlé, dans les deux sens

Chaque connexion entre un navigateur, un lecteur et la console passe par TLS 1.3 (la version 1.2 est acceptée pour les clients plus anciens). Les connexions des lecteurs utilisent le TLS mutuel (mTLS) : chaque partie présente son certificat à l'autre.

Un certificat valide est nécessaire, mais pas suffisant. À chaque connexion, le serveur vérifie également, dans la base de données et non dans une liste en cache, que le certificat n'est ni révoqué ni expiré, que l'appareil qu'il désigne existe toujours et que cet appareil appartient bien au lieu pour lequel le certificat a été émis.

Les certificats sont valables 398 jours, le plafond fixé par le CA/Browser Forum pour les certificats publiquement reconnus, et se renouvellent au cours de leurs 30 derniers jours par la propre connexion mTLS du lecteur : un parc renouvelle ainsi ses identifiants sans déplacement sur site. L'émission d'un nouveau certificat révoque le précédent.

L'activation du TLS mutuel se fait par étapes : un mode de transition accepte à la fois un certificat et l'ancien identifiant pendant que le parc migre salle par salle, puis un mode obligatoire est activé une fois que chaque point de terminaison dispose d'un certificat. Le serveur refuse ce basculement tant qu'un appareil qui se connecte en serait exclu, car l'alternative serait un musée plongé dans le noir. Le retour au mode désactivé annule immédiatement le changement.

5.3 Intégrité : rien ne s'exécute sans avoir été vérifié

Les pilotes sont signés. Un pilote est un paquet accompagné d'un manifeste et d'une signature Ed25519 détachée portant sur l'empreinte du paquet. Par défaut, un serveur de production refuse un paquet non signé, car un pilote est du code qui ouvre des sockets et communique avec du matériel. Les intégrateurs et les fabricants peuvent écrire et signer leurs propres pilotes avec le kit de développement de pilotes.

Les mises à jour des lecteurs sont vérifiées par somme de contrôle. Le serveur publie une version accompagnée de sa somme de contrôle SHA-256. Le lecteur vérifie la somme de contrôle avant toute autre opération, extrait la mise à jour dans un répertoire intermédiaire, la met en place et redémarre. Une vérification qui échoue entraîne le refus de la mise à jour.

Les mises à jour respectent le bâtiment. Une mise à jour ne s'installe qu'en dehors des heures d'ouverture. Une nouvelle version qui échoue à son contrôle de fonctionnement dans les dix minutes qui suivent est annulée, et toute nouvelle tentative est bloquée. Un lieu peut exclure un lecteur des mises à jour ; un lecteur exclu ou en retard est signalé « Pas à jour » dans la console, de sorte qu'il n'est jamais oublié sans que personne ne s'en aperçoive.

5.4 Accès et rôles

talor propose cinq rôles attribuables.

Rôle	À quoi il sert
Administrateur réseau	Tout, dans chaque lieu exploité par l'organisation
Administrateur du parc	Tous les droits à l'échelle d'un lieu, dans les lieux d'un parc
Administrateur du lieu	Tous les droits à l'échelle d'un lieu, dans un seul lieu
Gestionnaire de contenu	Contenus, Reels, plannings et modèles
Responsable technique	Exploitation des équipements : redémarrage, alimentation, source, volume

Les rôles sont volontairement peu nombreux et larges, car un modèle de droits que personne ne sait expliquer est un modèle que personne n'applique. Chaque route vérifie à la fois le rôle et le lieu : une personne disposant de droits dans un lieu ne voit rien d'un autre. La connexion est individuelle, jamais partagée ; un nouveau compte doit changer son mot de passe lors de sa première utilisation.

5.5 Le journal d'audit

Chaque écriture est consignée dans le journal d'audit avec la personne, l'action, l'heure et l'adresse réseau d'origine. Cela inclut les actions effectuées par l'assistant, enregistrées comme appliquées par l'assistant pour le compte d'une personne nommément identifiée. Le journal peut être filtré dans la console et exporté au format CSV avec les mêmes filtres, afin qu'un auditeur puisse l'emporter.

Deux propriétés protègent le journal contre les personnes qui ont le plus de pouvoir sur lui. La catégorie audit est soumise à une durée de conservation minimale imposée de 180 jours : un lieu peut conserver son journal plus longtemps, jamais moins. Et lorsqu'un membre du personnel exerce son droit à l'effacement, le compte devient une trace anonymisée (tombstone) : identité masquée, adresses réseau supprimées, actions conservées, de sorte que le journal indique toujours qu'une personne, depuis effacée, a publié une scène le 3 du mois. Un administrateur ne peut pas effacer son propre compte.

5.6 La vie privée des visiteurs, par construction

Les visiteurs d'un lieu sont des membres du public, dont beaucoup d'enfants. La bonne conception est celle dans laquelle le système est incapable d'enregistrer qui ils sont.

Les deux tables qui contiennent le comportement des visiteurs, les événements de présence et les événements d'interaction, comportent un lieu, un appareil, une zone, un mot d'état ou d'événement et un horodatage. Elles ne comportent aucun identifiant de la personne, de quelque nature que ce soit : ni adresse réseau, ni visage, ni cookie, ni session. C'est une propriété du schéma, et non une promesse inscrite dans une politique ; un test la vérifie sur les définitions réelles des tables et fait échouer la compilation si quelqu'un ajoute une telle colonne.

Derrière cela se trouve un registre des activités de traitement qui réside dans le code et qui est revu dans la même modification que le code qui crée les données : finalité, base légale, degré d'identification, destinataires et durée de conservation pour chaque catégorie. Une purge nocturne supprime les lignes dont la durée de conservation est dépassée, par lots afin de ne jamais bloquer un lieu ouvert, et enregistre une ligne pour chaque exécution, y compris les échecs. Ce registre est la première preuve que demande un auditeur.

Catégorie de données	Conservation par défaut	Minimum
Présence devant une installation	400 jours	1 jour
Touchers et choix	400 jours	1 jour
Ce qui a été diffusé, et quand	1 825 jours	365 jours
Journaux des lecteurs	30 jours	1 jour
Qui a fait quoi (audit)	730 jours	180 jours

Les mesures de contrôle sont conçues selon les exigences techniques de l'ISO/IEC 27701, l'extension relative à la vie privée de l'ISO/IEC 27001. Nous restons prudents sur cette affirmation : un produit ne peut pas être certifié 27701 ; une organisation le peut, après un audit. taleor met en œuvre les mesures que la norme rend techniques et produit les preuves dont un auditeur a besoin ; l'institution doit toujours désigner un responsable de la protection des données, réaliser son analyse d'impact, conclure ses contrats de sous-traitance et afficher les mentions d'information dans les salles.

5.7 Message d'urgence

Une seule commande déclenche un message d'urgence sur tout le lieu, un étage, une zone ou des lecteurs choisis. Le message occupe tout l'écran, une annonce défile en bas, et le son des installations se coupe. Un lecteur qui se reconnecte pendant une diffusion la reçoit malgré tout. Le message d'urgence peut être lancé et arrêté depuis un appareil portable du personnel, et il est consigné dans le

journal d'audit comme toute autre action. Nous disons « son des installations » à dessein : taleor fait taire ce qu'il contrôle, et ce n'est pas un système de sonorisation de sécurité.

5.8 Isolation et air gap

Le paquet du serveur local installe sa propre instance PostgreSQL privée, qui n'écoute que sur l'interface de bouclage et sur un port non standard, de sorte qu'elle n'entre jamais en conflit avec une base de données déjà présente sur la machine. Personne ne saisit le mot de passe de la base de données : un mot de passe aléatoire est généré à l'installation et ne réside que dans un fichier de configuration lisible par le système et ses administrateurs. Aucun environnement de conteneurs n'est nécessaire. Le mode isolé est le même paquet, sans internet (section 4.2).

Les équipements du réseau du lieu sont toujours pilotés depuis l'intérieur de ce réseau, par les agents des lecteurs ou par le serveur local. La console cloud n'a jamais besoin d'une route vers votre bâtiment ; ce sont les agents qui se connectent vers l'extérieur.

5.9 Des défaillances qui restent sûres

- Un lecteur qui perd le contact avec le serveur continue de diffuser sa dernière configuration valide depuis son cache local, y compris après des redémarrages, jusqu'au retour du serveur.
- Un lecteur qui décroche déclenche une alerte qui l'identifie et indique où il se trouve, ce qu'il devrait afficher et depuis quand. L'alerte disparaît d'elle-même lorsque le lecteur revient ; une panne répétée met à jour l'alerte existante.
- Le serveur sauvegarde sa base de données selon un planning, avec un historique glissant et une restauration possible à partir de n'importe quel point. Tout ce qui est supprimé de la bibliothèque de contenus reste récupérable pendant 30 jours.
- Le serveur refuse de verrouiller un lieu en TLS mutuel tant qu'un appareil en resterait exclu, refuse un plan de l'assistant devenu obsolète et refuse un pilote non signé. Entre deviner et s'arrêter, taleor s'arrête et explique pourquoi.

5.10 Comment nous vérifions notre propre travail

Avant le lancement, la console, le lecteur et le site web de taleor ont fait l'objet d'une revue de sécurité applicative : un modèle de menaces rédigé, des exploits de démonstration (proof of concept) pour chaque faiblesse suspectée, des outils d'analyse des dépendances et d'analyse statique, et une nouvelle analyse après

correction. Chaque constat porte un niveau de gravité, un responsable et une correction vérifiée ; une étape de validation n'est pas franchie tant qu'un constat bloquant reste ouvert. Exigez la même chose de tout fournisseur.

6 Configuré par un assistant

6.1 Ce qu'il fait

Configurer une installation interactive a toujours été un travail de spécialiste que seule une personne du lieu sait faire. taleor intègre dans la console un assistant appelé Oli. Vous tapez ce que vous voulez :

Quand quelqu'un s'approche à moins d'un mètre de l'écran du hall, passer à la vidéo d'accueil, puis revenir après trente secondes sans personne.

L'assistant lit la configuration du lieu (installations, lecteurs, Reels, entrées déclarées) et propose un plan qui liste les modifications exactes :

Lecture de l'écran du hall : capteur de présence déclaré, 2 Reels.

Proposition : à une distance de 100 cm ou moins, diffuser « vidéo d'accueil », revenir après 30 s.

En attente de votre vérification.

Vous le lisez. Vous appuyez sur Appliquer, ou sur Abandonner. Quand il manque quelque chose, l'assistant précise quoi : aucun Reel nommé « vidéo d'accueil », ou aucun capteur de présence sur ce lecteur. Il pose une seule question à la fois lorsqu'une demande est ambiguë, et il ne suppose jamais l'existence d'un matériel absent.

L'assistant propose des déclencheurs, des affectations de Reels et l'activation d'un déclencheur, et les applique une fois que vous avez donné votre accord. Toutes les commandes restent disponibles manuellement.

6.2 Le modèle de droits

L'assistant n'est pas un utilisateur privilégié. Il ne dispose d'aucun droit propre.

- **Lecture.** Ses outils de consultation du lieu sont en lecture seule et limités au lieu dans lequel travaille la personne.
- **Proposition.** Ses outils de planification ne font qu'enregistrer une étape proposée. Rien ne s'exécute. Ce point est testé.

- **Application.** Lorsque vous appuyez sur Appliquer, les étapes enregistrées passent par les mêmes fonctions de service, les mêmes validations et les mêmes contrôles de droits que si la personne avait effectué chaque modification à la main : une personne qui n'a pas le droit de modifier quelque chose ne peut pas le faire modifier par l'assistant. Le journal d'audit enregistre le résultat comme appliqué par l'assistant pour cette personne nommément identifiée.
- **Obsolescence.** Un plan devenu obsolète, parce qu'un Reel a été supprimé entre la proposition et la validation, est refusé : l'assistant ne cherche pas à deviner.
- **Confinement.** L'assistant est désactivé et masqué tant qu'il n'est pas configuré. Sa consommation est mesurée, avec un plafond mensuel strict pour l'ensemble du serveur. Les erreurs du service sous-jacent ne sont jamais affichées telles quelles.

6.3 Pourquoi vérifier avant d'appliquer

Un système qui modifie ce qui est diffusé sur deux cents écrans doit pouvoir répondre à la question « qui a modifié cela, et une personne l'a-t-elle validé ? » Posez cette question à tout produit qui vante une configuration automatisée.

7 Statistiques : ce qu'un lieu apprend

7.1 Des statistiques fondées sur ce que signalent réellement les lecteurs

Les statistiques de taleor (rubrique « Statistiques » de la console) sont construites à partir de ce que signalent les lecteurs et les capteurs, et non à partir d'un système de comptage distinct : le capteur qui lance une vidéo est celui-là même qui compte qui s'est arrêté et pendant combien de temps. Chaque indicateur peut porter sur le lieu entier, un étage, une zone ou un lecteur, pour aujourd'hui, cette semaine, ce mois-ci ou cette année, avec la période précédente à titre de comparaison.

7.2 Ce que vous voyez

Fréquentation et temps de présence. Visiteurs par heure, par jour ou par mois, d'après les capteurs et les interactions tactiles. Temps de présence moyen des visites avec interaction. Les zones et les heures les plus fréquentées, sous forme de carte de chaleur par zone et par heure.

Ce qui a le mieux fonctionné. Les installations classées par visites et par temps de présence, de sorte qu'un recoin délaissé apparaisse avant qu'un conservateur ne passe devant sans le remarquer. Les visiteurs et le temps de présence concernent l'installation ; la disponibilité et les diffusions concernent chaque lecteur.

Preuve de diffusion. Chaque élément, chaque diffusion, menée à son terme ou non, avec un export CSV qui respecte le même périmètre et la même période. Conservée cinq ans par défaut, elle survit ainsi à la durée d'une licence et à celle d'un contrat de mécénat.

État et disponibilité des lecteurs. La disponibilité de chaque lecteur sur la période, calculée à partir des relevés d'état. Une période sans relevé est considérée comme inconnue, et non comme en bon état.

7.3 Des chiffres honnêtes

Un indicateur qui ne peut pas être mesuré affiche « non mesuré », jamais zéro. Une zone sans capteur n'annonce pas zéro visiteur ; elle indique que les visiteurs n'y ont pas été mesurés.

7.4 La vie privée par construction, encore

Les événements qui sous-tendent chaque indicateur sont ceux de la section 5.6, sans aucun identifiant du visiteur : pas de caméras, pas de détection de visage, pas de suivi des appareils, pas de cookies.

8 Fonctionne partout, avec le matériel que vous avez

8.1 Plateformes

Composant	Fonctionne sur
Console (application web)	Tout navigateur récent, sur app.taleor.net ou sur votre serveur local
Console (application de bureau)	Windows, macOS, Linux
Serveur local, y compris isolé du réseau	Windows, macOS, Linux
Agent du lecteur	Windows, macOS, Linux, Raspberry Pi, Android
Lecteur dans le navigateur	Tout navigateur récent ; association par code à six chiffres

L'application de bureau ouvre la console dans sa propre fenêtre, peut diffuser l'installation sur le même ordinateur et conserve la dernière configuration valide après un redémarrage.

8.2 Le matériel, au moyen de standards ouverts

taleor pilote des équipements de toutes marques au moyen des standards qu'ils parlent déjà.

Famille	Exemples	Via
Afficheurs	Tout écran relié à un ordinateur qui exécute le lecteur taleor, ou qui affiche le lecteur dans le navigateur	lecteur taleor · lecteur dans le navigateur · HDMI
Projecteurs	Tout projecteur compatible PJLink ; protocoles série propres aux fabricants	PJLink · ESC/VP21 · RS-232 · TCP
Capteurs	Présence, distance (lidar, ultrasons), bouton sans contact, bouton-poussoir, RFID ; contrôleurs de capteurs derrière n'importe quel lecteur	Série · USB · TCP
Contrôleurs	OSC entrant depuis une console d'éclairage ou un contrôleur de spectacle, OSC sortant depuis un déclencheur, touches USB, pédales et cartes série, un appareil portable	OSC · USB · série
Son	Processeurs audio et haut-parleurs en réseau, du casque d'une seule installation à une grande salle	REST · TCP
Éclairage	Éclairage architectural et éclairage des installations	DALI

Liste complète des standards : PJLink · RS-232 · TCP · DALI · MQTT · OSC · REST · WebSocket · série · USB.

Des pilotes sont disponibles pour ces familles, et nous les testons avec vos équipements avant votre ouverture ; nous l'attestons par écrit plutôt que d'afficher une liste de logos. Si un appareil n'est pas couvert, le kit de développement de pilotes permet à un intégrateur d'en écrire un : un manifeste, un adaptateur, une signature. Les fabricants peuvent nous apporter un appareil et nous en réaliserons l'intégration.

8.3 Ce que cela signifie pour la dépendance vis-à-vis d'un fournisseur

La couche de commande parle des standards ouverts : le matériel n'est donc pas lié à taleor. Le serveur fonctionne sur votre propre machine avec sa propre base de données : les données ne sont donc pas liées à notre cloud. Les contenus sont des fichiers multimédias ordinaires et la configuration s'exporte sous forme

de données brutes : un lieu qui s'en va emporte donc ses contenus et son historique. Les médias peuvent aussi rester dans l'espace Google Drive du lieu : taleor ne lit que les fichiers sélectionnés, et les écrans en conservent une copie pour la diffusion hors ligne. Nous préférons qu'on nous garde parce que le produit est bon, et non parce qu'il serait impossible de partir.

9 Modèles de déploiement et méthode d'évaluation

9.1 Trois modèles

Cloud. Le démarrage le plus rapide : ouvrez app.taleor.net, créez le lieu, installez l'agent sur l'ordinateur de chaque installation. Les agents se connectent vers l'extérieur ; rien ne se connecte vers l'intérieur. Pour les lieux sans infrastructure de serveurs, et pour les intégrateurs qui gèrent plusieurs lieux.

Serveur local. Le paquet serveur sur une machine du bâtiment, avec ou sans internet. Pour les institutions qui disposent de leur propre service informatique, et pour tout lieu dont les règles d'achat exigent que les données restent sur place.

Isolé du réseau. Le serveur local sans aucun accès à internet ; les mises à jour sont apportées par le personnel. Pour les lieux soumis à des politiques réseau strictes ou dépourvus de connexion fiable, et pour quiconque a décidé que ses salles ne doivent pas dépendre d'une connexion qu'il ne maîtrise pas.

Les trois modèles exécutent le même logiciel et la même console, et le choix peut être modifié par la suite.

9.2 Une liste de contrôle pour les commissions d'appel d'offres

Posez ces questions à tout fournisseur. Voici nos réponses, avec la section correspondante :

Question	taleor	Section
Comment chaque lecteur prouve-t-il son identité ? Une clé ou un mot de passe partagé intervient-il ?	Certificat propre à chaque lecteur ; clé générée sur la machine, jamais copiée ; une autorité par lieu	5.1
La connexion du lecteur est-elle chiffrée et authentifiée dans les deux sens ? Les certificats peuvent-ils être renouvelés sans déplacement sur site ?	TLS 1.3 ; TLS mutuel ; certificats de 398 jours renouvelés par la propre connexion du lecteur	5.2

Question	taleor	Section
Les pilotes sont-ils signés ? Les mises à jour sont-elles vérifiées avant installation ?	Pilotes signés Ed25519, paquets non signés refusés ; somme de contrôle SHA-256 vérifiée sur le lecteur	5.3
Une mauvaise mise à jour peut-elle mettre une installation hors service ?	Installation en dehors des heures d'ouverture ; retour à la version précédente et blocage en cas d'échec du contrôle de fonctionnement	5.3
Un technicien peut-il redémarrer un écran sans pouvoir le supprimer ?	Cinq rôles ; oui	5.4
Chaque action est-elle associée à une personne, une heure et une adresse ? Un administrateur peut-il raccourcir ou effacer le journal ?	Oui ; export CSV ; durée de conservation minimale de 180 jours ; l'effacement laisse une trace anonymisée, pas une lacune	5.5
Qu'enregistre le système sur les visiteurs, et pendant combien de temps ?	Lieu, appareil, zone, état, heure ; aucun identifiant, garanti par un test du schéma ; conservation par catégorie, suppression attestée	5.6
Existe-t-il un message d'urgence, et jusqu'où porte-t-il ?	Lieu, étage, zone ou lecteurs choisis ; plein écran ; son des installations coupé	5.7
L'ensemble du système peut-il fonctionner sur place, sans internet ?	Oui ; serveur local et mode isolé	5.8, 9.1
Que deviennent les installations lorsque le serveur est indisponible ?	Les lecteurs continuent la diffusion depuis leur cache local, y compris après des redémarrages	5.9
Le produit a-t-il fait l'objet d'une revue de sécurité, et pouvons-nous en voir les constats ?	Oui ; modèle de menaces, preuves de concept, analyseurs, corrections vérifiées	5.10
Si la configuration est automatisée, une personne valide-t-elle chaque modification exacte, en son nom ?	Oui ; proposer, vérifier, appliquer ; consigné comme appliqué pour la personne nommément identifiée	6.2
Quelles plateformes et quels standards matériels ?	Lecteurs sous Windows, macOS, Linux, Raspberry Pi, Android et dans tout navigateur ; PJLink, RS-232, TCP, DALI, MQTT, OSC, REST, WebSocket, série, USB	8

Question	taleor	Section
Que possédons-nous si nous partons ?	Les contenus sous forme de fichiers ordinaires, la configuration sous forme de données brutes, la base de données sur votre machine	8.3

9.3 Ce qu'il faut demander lors d'un projet pilote

Un livre blanc n'est pas un produit. Demandez un projet pilote portant sur quelques installations et mettant à l'épreuve les mesures de sécurité : enregistrer un lecteur en TLS mutuel et examiner son certificat ; essayer une seconde machine avec une copie de sa configuration et vérifier qu'elle est refusée ; faire redémarrer un écran par un responsable technique, puis lui faire tenter de le supprimer ; faire proposer un déclencheur par l'assistant, abandonner la proposition, puis en valider une et lire le journal d'audit ; débrancher un câble réseau et constater que le lecteur continue la diffusion ; exporter le journal d'audit et la preuve de diffusion au format CSV ; demander le registre de la dernière purge liée aux durées de conservation. Chaque étape prend quelques minutes et en apprend davantage à une commission que n'importe quelle liste de fonctionnalités.

10 À propos de taleor

taleor est une manière sûre et agentique d'exploiter un lieu de visite : ses contenus, ses applications interactives, ses lecteurs et son matériel, depuis une seule console, dans le cloud, sur un serveur local ou entièrement isolé du réseau. Il s'adresse aux musées, centres de culture scientifique, centres d'expérience de marque, sites patrimoniaux et sites de loisirs, ainsi qu'aux personnes qui les exploitent et qui en assurent les achats.

taleor sera lancé en novembre 2026. Écrivez à hello@taleor.net pour organiser un projet pilote ou pour demander la fiche technique destinée aux appels d'offres, dans l'une de nos sept langues : anglais, allemand, néerlandais, polonais, français, espagnol ou italien.

Sources et vérification

Chaque affirmation technique de ce livre blanc repose sur une source identifiée dans le code, les documents de conception ou la revue de sécurité de taleor, consignée dans un registre des affirmations qui recense chaque affirmation, la

section où elle figure et le fichier dont elle est tirée. Écrivez à hello@taleor.net pour obtenir ce registre.

Références publiques utilisées dans la section 2, aucune ne comportant de chiffres : le botnet Mirai de 2016 (largement documenté, notamment par l'agence américaine Cybersecurity and Infrastructure Security Agency) ; BSI IT-Grundschutz (Allemagne) ; la Baseline Informatiebeveiliging Overheid (Pays-Bas) ; la directive (UE) 2022/2555, dite NIS2 ; et les exigences de base du CA/Browser Forum pour la durée de vie de 398 jours des certificats.

