
Een belevingscentrum veilig beheren

Waarom een museum, wetenschapscentrum of merkbeleving beheerd moet worden als een goed bestuurd IT-landschap, en hoe taleor dat doet: elk apparaat geïdentificeerd, elke verbinding versleuteld, elke wijziging toegeschreven, elke bezoeker anoniem.

Whitepaper · oktober 2026 · Versie 1.0

Voor directeuren, technische en IT-verantwoordelijken, AV-integrators, adviseurs en aanbestedingscommissies van musea, wetenschapscentra, merkbelevingscentra, erfgoedlocaties en attracties.

taleor

Inhoud

1	Managementsamenvatting	3
2	Het probleem: een locatie is nu een IT-landschap	3
3	Wat een locatie werkelijk nodig heeft	5
4	Hoe taleor werkt	6
5	Veilig door ontwerp	8
6	Ingericht door een assistent	12
7	Analyse: wat een locatie te weten komt	14
8	Draait overal, werkt met wat u al hebt	15
9	Implementatiemodellen en hoe u ze beoordeelt	16
10	Over taleor	18
	Bronnen en verificatie	19

1 Managementsamenvatting

Een belevingslocatie was vroeger een gebouw met een paar schermen erin. Nu is het een netwerk: honderden computers, displays, projectoren, luidsprekers, lampen en sensoren van zo'n twaalf fabrikanten, elk met eigen firmware, een adres en vaak een wachtwoord, beheerd door een klein team dat geen IT-team is.

Deze paper betoogt dat een locatie beheerd moet worden zoals een goed bestuurd IT-landschap: elk apparaat geïdentificeerd, elke verbinding versleuteld, elke wijziging toe te schrijven aan een persoon, elke update geverifieerd, elke bezoeker anoniem. Sectie 3 zet zeven principes uiteen, de secties 4 tot en met 8 beschrijven hoe taleor daaraan voldoet, en sectie 9 sluit af met een checklist die een aanbestedingscommissie aan elke leverancier kan voorleggen, ook aan ons.

taleor is een veilige, agentische manier om een belevingslocatie te beheren: de content, interactieve toepassingen, players en hardware, vanuit één console. Het rust op drie pijlers: het is veilig door ontwerp; het wordt ingericht door een assistent die nooit een wijziging doorvoert zonder goedkeuring van een bij naam genoemde persoon; en de analyse zegt "niet gemeten" in plaats van nul. Het draait als web-app, als desktop-app voor Windows, macOS en Linux, en als lokale server in uw eigen gebouw, ook volledig air-gapped. De players draaien op Windows, macOS, Linux, Raspberry Pi en Android. Het stuurt apparatuur van elk merk aan via open standaarden.

2 Het probleem: een locatie is nu een IT-landschap

2.1 Honderden apparaten, tientallen merken, een klein team

Tel de computers in de zalen van een hedendaags museum: één achter de meeste exhibits, plus displays in het netwerk, projectoren, audioprocessors, lichtregelaars, sensoren, lezers en knoppen. In een locatie van bescheiden omvang loopt het aantal op tot een paar honderd. De voorbeelddata waarmee taleor is ontwikkeld, gemodelleerd naar een doorsnee regionaal museum, bevat 69 exhibits en 342 apparaten die 49 besturingsprotocollen spreken. Dat is een gewoon IT-landschap.

Elke fabrikant brengt een eigen protocol mee, een eigen beheertool en een eigen opvatting over hoe updates werken. De content verandert elk seizoen. Het team bestaat meestal uit twee tot vijf mensen van wie de functie nooit bedoeld was voor het beheer van een apparatenpark en het installeren van patches.

2.2 Blootstelling aan beveiligingsrisico's

Vier zwakke punten versterken elkaar.

Standaardwachtwoorden. Professionele AV-apparatuur wordt geleverd met een beheerinterface en een fabriekswachtwoord dat zelden wordt gewijzigd, omdat het wijzigen ervan op tweehonderd apparaten een week werk is waar niemand verantwoordelijk voor is. Het Mirai-botnet van 2016 lijfde apparaten in door een korte lijst fabriekswachtwoorden te proberen. AV-apparatuur in een locatie vormt daarop geen uitzondering.

Players zonder patches. De computer achter een exhibit draait vaak nog het besturingssysteem waarmee hij in gebruik is genomen, omdat bijwerken betekent dat het exhibit dicht moet. Een computer zonder patches op hetzelfde netwerk als ticketing en gebouwbeheer is een weg naar binnen. De kaders waaraan overheidsinstanties in Duitsland, Nederland en Polen worden getoetst (BSI IT-Grundschutz, de Baseline Informatiebeveiliging Overheid en de verplichtingen die voortvloeien uit NIS2) beschouwen tijdig patchen en een inventaris van alle apparaten als basismaatregelen.

Gedeelde geheimen. Veel besturingssystemen voor AV verifiëren een player met een sleutel in een configuratiebestand. Wie dat bestand kan lezen, kan zich voordoen als die player.

Afhankelijkheid van de cloud. Een systeem dat stopt wanneer het internet of de cloud van de leverancier uitvalt, heeft het enkele storingspunt verplaatst naar een plek waar de locatie het niet kan verhelpen. Voor een publieke instelling is het ook een aanbestedingsvraag: wie beheert de gegevens, onder welk recht, en wat gebeurt er als het contract afloopt?

2.3 Uitval, blinde vlekken en leveranciersafhankelijkheid

Uitval is de meest zichtbare storing en de minst gemeten. Om tien uur bevriest een scherm, om twaalf uur meldt een bezoeker het, om twee uur hoort de technicus ervan, en nergens zijn de vier verloren uren vastgelegd.

De meeste locaties tellen bezoekers bij de ingang en nergens anders. Ze kunnen niet zeggen bij welk exhibit mensen bleven staan, hoe lang, of een film tot het einde werd bekeken. Waar wel wordt gemeten, is dat vaak een apart systeem, en te vaak een met camera's die mensen identificeren.

Elk subsysteem komt met een eigen leverancier en een eigen contract. Wanneer een leverancier wordt overgenomen of een product schraapt, kan content die voor een gesloten player is gemaakt niet mee, en wordt hardware die maar met één

controller praat afval. De vraag die een commissie moet stellen is niet "ondersteunt deze leverancier onze hardware?" maar "als deze leverancier verdween, wat zouden we dan nog bezitten?"

3 Wat een locatie werkelijk nodig heeft

Deze problemen zijn al eerder opgelost, in de algemene IT. Wat ontbrak, is de toepassing ervan op de vorm van een belevingslocatie: veel kleine computers, veel merken, een klein team, een publiek en een gebouw dat om tien uur open moet. Wij stellen zeven principes voor.

1. **Elk apparaat heeft een identiteit die niet te kopiëren is.** Een sleutel die op de eigen hardware is gegenereerd en die nooit heeft verlaten. Geen wachtwoord. Geen token in een bestand.
2. **Elke verbinding is versleuteld en in beide richtingen geverifieerd.** Met minder kan een vreemde op het netwerk van de locatie een overtuigende vervalsing opzetten.
3. **Er draait niets op een player dat niet eerst is geverifieerd.** Drivers en updates worden op de player zelf gecontroleerd aan de hand van een handtekening of een controlesom, niet alleen bij de bron.
4. **Elke wijziging heeft een naam en een tijdstip.** Een audittrail die een beheerder kan inkorten tot één dag, of kan bewerken, is geen audittrail.
5. **Mensen krijgen de bevoegdheden die hun werk vraagt, en niet meer.** Een facilitair manager kan een bevroren scherm herstarten zonder het te kunnen verwijderen.
6. **Bezoekers blijven anoniem door het ontwerp, niet door beleid.** Een eigenschap van het databaseschema, en getest.
7. **De locatie is eigenaar van haar systeem.** Ze kan alles in haar eigen gebouw draaien, zonder internet, en kan overstappen zonder haar content te verliezen.

Dit is wat een competente IT-afdeling zou vragen van elk park van tweehonderd computers. De rest van deze paper beschrijft hoe taleor daaraan voldoet.

4 Hoe taleor werkt

4.1 De onderdelen

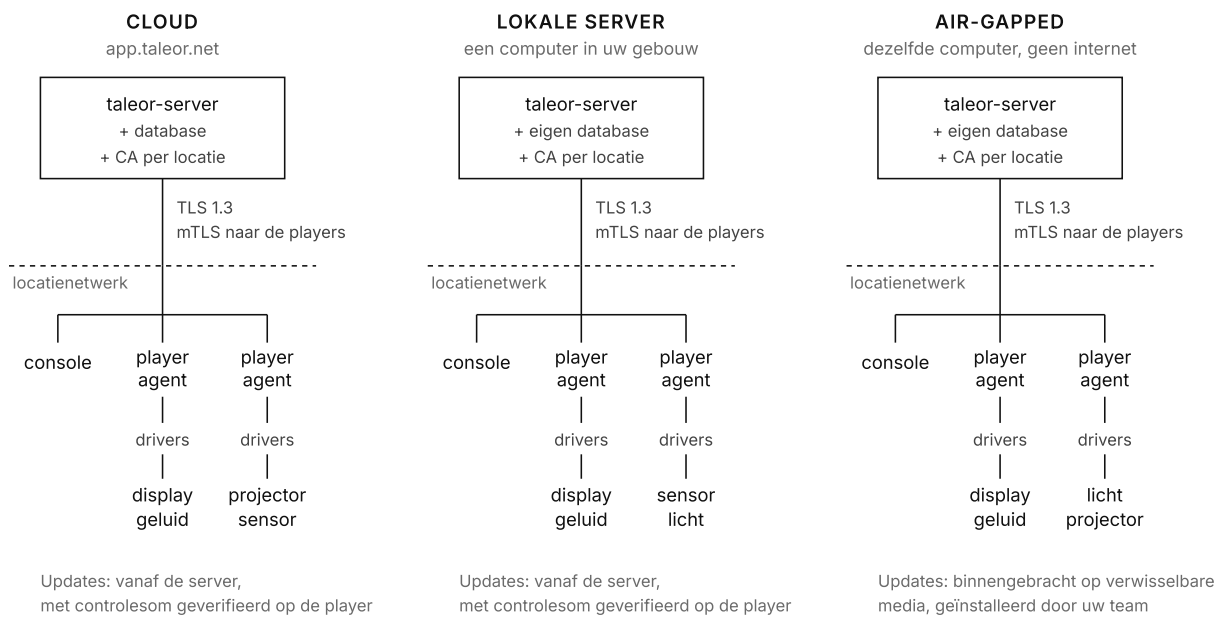
De console. Een webapplicatie waarin medewerkers elk exhibit, elke player en alle apparatuur zien, content laden, planningen en triggers instellen, de status en meldingen volgen en de analyse lezen. Ze draait in elke actuele browser, of als desktop-app voor Windows, macOS en Linux.

De playeragent. Een kleine achtergronddienst op de computer achter elk exhibit. Hij onderhoudt een blijvende, wederzijds geverifieerde verbinding met de server, speelt af wat hem wordt opgedragen, stuurt de apparatuur op die computer aan, leest de sensoren uit, rapporteert zijn status en houdt zichzelf bijgewerkt. Standaard bewaart hij een lokale kopie van 4 GB van zijn content en blijft hij afspelen wanneer de server onbereikbaar is. Agents draaien op Windows, macOS, Linux, Raspberry Pi en Android. Een scherm zonder computer wordt gekoppeld als browserplayer met een zescijferige code die op het scherm staat.

Drivers. Een ondertekend pakket dat taleor vertelt wat een apparaat kan en hoe ermee te communiceren. De console vraagt om een handeling zoals aan/uit, bron of volume; de driver spreekt het protocol.

De server. De database, de WebSocket-hubs die de livestatus doorgeven, de certificeringsinstantie voor elke locatie, de mediaopslag, de planningsengine, de meldingenmonitor, het auditlog en de analyse. Het is dezelfde software in onze cloud of op een computer in uw gebouw, met of zonder internet.

4.2 Eén build, drie manieren om die te draaien



Afbeelding 1. Eén build, drie manieren om die te draaien. Dezelfde server, console en playeragents in de cloud, op een lokale server in het gebouw, of air-gapped zonder internet.

In de cloudmodus staan de console en de server op app.taleor.net en maken de agents een uitgaande verbinding daarmee; apparatuur op het netwerk van de locatie wordt aangestuurd door de agents binnen dat netwerk. In de modus lokale server wordt hetzelfde pakket geïnstalleerd op een Windows-, macOS- of Linux-computer in het gebouw, met een eigen afgeschermd database en certificeringsinstantie, zodat console, players, media en auditlog allemaal binnen blijven. In de air-gapped modus draait die server volledig zonder internet: runtime en database zitten in het pakket, er wordt bij de installatie niets gedownload, en updates worden door uw eigen medewerkers op verwisselbare media binnengebracht. Eén codebase, één console; een locatie die in de cloud begint, kan later naar eigen beheer overstappen.

5 Veilig door ontwerp

5.1 Identiteit: een sleutel die de computer nooit verlaat

taleor vervangt het gedeelde geheim door een certificaat. Wanneer een player wordt aangemeld, genereert hij op zijn eigen computer een asymmetrisch sleutelpaar en stuurt hij alleen de publieke helft, in een certificaatondertekeningsverzoek, naar de certificeringsinstantie van de locatie, die een certificaat ondertekent en terugstuurt. De privésleutel reist nooit. Vanaf dan bewijst de player zijn identiteit door bij elke TLS-handshake live een handtekening te zetten. Er is niets te kopiëren.

Eén certificeringsinstantie per locatie, in de console geopend door een beheerder. Een inbreuk bij de ene locatie kan geen identiteit aanmaken bij een andere. De privésleutel van de instantie wordt versleuteld opgeslagen onder een geheim dat losstaat van de andere geheimen van de server.

Het verzoek wordt niet vertrouwd. Alleen de publieke sleutel wordt uit het ondertekeningsverzoek overgenomen; het onderwerp, de geldigheidsduur en elke extensie worden door de server bepaald, zodat een player niet kan vragen om de naam van een andere player te krijgen of om certificeringsinstantie te worden. Playercertificaten worden alleen uitgegeven voor clientauthenticatie, zodat met een gestolen certificaat geen nepserver kan worden opgezet.

Er is geen knop "certificaat uitgeven". Een certificaat waarvan de server ooit de privésleutel in handen had, zou het doel ondermijnen.

5.2 Transport: versleuteld en gecontroleerd, in beide richtingen

Elke verbinding tussen een browser, een player en de console loopt via TLS 1.3 (1.2 wordt geaccepteerd voor oudere clients). Playerverbindingen gebruiken mutual TLS: elke kant toont zijn certificaat aan de andere.

Een geldig certificaat is noodzakelijk, maar niet voldoende. Bij elke verbinding controleert de server bovendien, in de database en niet in een lijst in de cache, dat het certificaat niet is ingetrokken of verlopen, dat het apparaat dat erin staat nog bestaat, en dat het apparaat hoort bij de locatie waarvoor het certificaat is uitgegeven.

Certificaten zijn 398 dagen geldig, het maximum van het CA/Browser Forum voor publiek vertrouwde certificaten, en worden in hun laatste 30 dagen vernieuwd via de eigen mutual-TLS-verbinding van de player, zodat een park zijn inloggegevens vernieuwt zonder bezoek ter plaatse. Het uitgeven van een nieuw certificaat trekt het vorige in.

Mutual TLS wordt gefaseerd ingeschakeld: een roterende modus accepteert zowel een certificaat als de oudere inloggegevens terwijl het park zaal voor zaal overgaat, daarna volgt een verplichte modus zodra elk eindpunt gecertificeerd is. De server weigert die omschakeling zolang een apparaat dat verbinding maakt zou worden buitengesloten, omdat het alternatief een donker museum is. De modus terugzetten naar uit draait de wijziging direct terug.

5.3 Integriteit: er draait niets dat niet is geverifieerd

Drivers zijn ondertekend. Een driver is een pakket met een manifest en een losse Ed25519-handtekening over de hash van het pakket. Een productieserver weigert standaard een niet-ondertekend pakket, omdat een driver code is die sockets opent en met hardware communiceert. Integrators en fabrikanten kunnen met de driverkit hun eigen drivers schrijven en ondertekenen.

Playerupdates worden geverifieerd met een controlesom. De server publiceert een versie met de bijbehorende SHA-256-controlesom. De player verifieert eerst de controlesom, pakt de update uit in een tijdelijke map, wisselt die in en herstart. Een mislukte verificatie betekent een geweigerde update.

Updates houden rekening met het gebouw. Een update wordt alleen buiten de openingstijden geïnstalleerd. Een nieuwe versie die binnen tien minuten niet door de statuscontrole komt, wordt teruggedraaid en geblokkeerd voor een nieuwe poging. Een locatie kan een player uitsluiten van updates; een uitgesloten of achterlopende player wordt in de console gemarkeerd als "niet actueel", zodat hij nooit ongemerkt wordt vergeten.

5.4 Toegang en rollen

taleor heeft vijf toewijsbare rollen.

Rol	Waarvoor die dient
Netwerkbeheerder	Alles, voor elke locatie die de instelling beheert
Organisatiebeheerder	Elke locatiebrede bevoegdheid, voor de locaties binnen een organisatie
Locatiebeheerder	Elke locatiebrede bevoegdheid, binnen één locatie
Contentmanager	Content, reels, planningen en sjablonen
Facilitair manager	Bediening van apparatuur: herstarten, aan/uit, bron, volume

De rollen zijn bewust grof ingedeeld, omdat een bevoegdhedenmodel dat niemand kan uitleggen een model is dat niemand toepast. Elke route controleert zowel de rol als de locatie, zodat iemand met rechten in de ene locatie niets van een andere ziet. Inloggen gebeurt per persoon, nooit gedeeld; bij een nieuw account moet het wachtwoord bij het eerste gebruik worden gewijzigd.

5.5 De audittrail

Elke schrijfactie komt in het auditlog terecht, met de persoon, de handeling, het tijdstip en het netwerkadres waar ze vandaan kwam. Dat geldt ook voor handelingen van de assistent, die worden vastgelegd als doorgevoerd door de assistent namens een bij naam genoemde persoon. Het log kan in de console worden gefilterd en met dezelfde filters als CSV worden geëxporteerd, zodat een auditor het kan meenemen.

Twee eigenschappen beschermen het log tegen de mensen met de meeste macht erover. Voor de auditcategorie geldt een afgedwongen minimale bewaartermijn van 180 dagen: een locatie mag het log langer bewaren, nooit korter. En wanneer een medewerker het recht op gegevenswissing uitoefent, wordt het account een tombstone: identiteit onleesbaar gemaakt, netwerkadressen verwijderd, handelingen bewaard, zodat het log nog steeds zegt dat iemand, inmiddels gewist, op de derde van de maand een scène heeft gepubliceerd. Een beheerder kan zijn eigen account niet wissen.

5.6 Privacy van bezoekers, door het ontwerp

De bezoekers van een locatie zijn leden van het publiek, onder wie veel kinderen. Het juiste ontwerp is er een waarin het systeem niet kán vastleggen wie ze zijn.

De twee tabellen die bezoekersgedrag bevatten, aanwezigheidsgebeurtenissen en interactiegebeurtenissen, bevatten een locatie, een apparaat, een zone, een status- of gebeurteniswoord en een tijdstempel. Ze bevatten geen enkele identificatie van de persoon: geen netwerkadres, geen gezicht, geen cookie, geen sessie. Dit is een eigenschap van het schema, geen belofte in een beleidsstuk; een test toetst het aan de actuele tabeldefinities en laat de build mislukken als iemand zo'n kolom toevoegt.

Daarachter staat een register van verwerkingsactiviteiten dat in de code staat en in dezelfde wijziging wordt beoordeeld als de code die de gegevens aanmaakt: doel, rechtsgrond, mate van identificeerbaarheid, ontvangers en bewaartermijn voor elke categorie. Elke nacht verwijdert een opschoonronde de rijen waarvan de bewaartermijn is verstreken, in delen zodat een geopende locatie nooit vastloopt, en legt van elke ronde een rij vast, ook van mislukte. Dat register is het bewijs waar een auditor als eerste om vraagt.

Gegevenscategorie	Standaardbewaartermijn	Minimum
Aanwezigheid bij een exhibit	400 dagen	1 dag
Aanrakingen en keuzes	400 dagen	1 dag
Wat er werd afgespeeld, en wanneer	1825 dagen	365 dagen
Playerlogs	30 dagen	1 dag
Wie wat deed (audit)	730 dagen	180 dagen

De maatregelen zijn gebouwd volgens de technische eisen van ISO/IEC 27701, de privacy-uitbreiding van ISO/IEC 27001. Wij zijn voorzichtig met deze bewering: een product kan niet volgens 27701 worden gecertificeerd; een organisatie wel, na een audit. taleor implementeert de maatregelen die de norm technisch maakt en levert het bewijs dat een auditor nodig heeft; de instelling moet nog steeds een privacyverantwoordelijke aanstellen, haar effectbeoordeling uitvoeren, haar verwerkersovereenkomsten afsluiten en mededelingen in de zalen ophangen.

5.7 Noodmelding

Met één bedieningselement start u een noodmelding voor de hele locatie, één verdieping, één zone of gekozen players. Het bericht vult het hele scherm, onderaan loopt een mededeling mee, en het exhibitgeluid wordt stil. Een player die tijdens een omroep opnieuw verbinding maakt, ontvangt die alsnog. De noodmelding kan worden gestart en beëindigd vanaf een handheld van het personeel, en wordt net als elke andere handeling in het auditlog vastgelegd. Wij zeggen bewust "exhibitgeluid": taleor maakt stil wat het aanstuurt, en het is geen omroepinstallatie.

5.8 Afscherming en air gap

Het pakket voor de lokale server installeert een eigen afgeschermd PostgreSQL-cluster, dat alleen luistert op de loopback-interface en op een niet-standaardpoort, zodat het nooit in aanraking komt met een database die al op de computer staat. Niemand typt het databasewachtwoord: bij de installatie wordt een willekeurig wachtwoord gegenereerd, dat alleen staat in een configuratiebestand dat leesbaar is voor het systeem en de beheerders. Er is geen containerruntime nodig. De air-gapped modus is hetzelfde pakket zonder internet (sectie 4.2).

Apparatuur op het netwerk van de locatie wordt altijd aangestuurd vanuit dat netwerk, door de playeragents of de lokale server. De cloudconsole heeft nooit een route naar uw gebouw nodig; de agents maken een uitgaande verbinding.

5.9 Storingen met een veilige afloop

- Een player die de server kwijtraakt, blijft zijn laatste goede configuratie afspelen uit zijn lokale cache, ook na herstarts, totdat de server terug is.
- Een player die wegvalt, geeft een melding met zijn naam, waar hij staat, wat hij zou moeten tonen en sinds wanneer. De melding verdwijnt vanzelf wanneer de player terugkomt; een herhaalde storing werkt de bestaande melding bij.
- De server maakt volgens een planning een back-up van zijn database, met een doorlopende geschiedenis en herstel vanaf elk moment. Alles wat uit de contentbibliotheek wordt verwijderd, is 30 dagen lang terug te halen.
- De server weigert een locatie vast te zetten op mutual TLS zolang een apparaat buitengesloten zou worden, weigert een verouderd plan van de assistent en weigert een niet-ondertekende driver. Tussen gokken en stoppen kiest taleor voor stoppen, en zegt waarom.

5.10 Hoe wij ons eigen werk controleren

Vóór de lancering zijn de console, de player en de website van taleor onderworpen aan een beveiligingsbeoordeling van de applicaties: een schriftelijk dreigingsmodel, proof-of-concept-exploits voor elke vermoede zwakte, scanners voor afhankelijkheden en statische analyse, en een nieuwe scan na de herstelacties. Bevindingen krijgen een ernst, een eigenaar en een geverifieerde oplossing; een controlepunt wordt niet gepasseerd zolang er een blokkerende bevinding openstaat. Vraag elke leverancier om hetzelfde.

6 Ingericht door een assistent

6.1 Wat de assistent doet

Het inrichten van een interactief exhibit was altijd specialistisch werk dat één persoon in de locatie beheerste. taleor bevat in de console een assistent, Oli genaamd. U typt wat u wilt:

Als iemand binnen een meter van het lobbyscherm komt, schakel dan over naar de welkomstfilm, en weer terug na dertig seconden zonder iemand.

De assistent leest de locatie (exhibits, players, reels, opgegeven ingangen) en stelt een plan voor waarin de exacte wijzigingen staan:

Leest lobbyscherm: aanwezigheidssensor opgegeven, 2 reels.

Stelt voor: bij een afstand van 100 cm of minder "welkomstfilm" afspelen, na 30 s terug.

Wacht op uw controle.

U leest het. U drukt op Toepassen, of op Verwerpen. Wanneer er iets ontbreekt, zegt de assistent wat: geen reel met de naam "welkomstfilm", of geen aanwezigheidssensor op die player. Bij een dubbelzinnig verzoek stelt de assistent één vraag tegelijk, en gaat nooit uit van hardware die er niet is.

De assistent stelt triggers, reeltoewijzingen en het inschakelen van een trigger voor, en voert ze door zodra u akkoord geeft. Elke functie blijft ook handmatig beschikbaar.

6.2 Het bevoegdhedenmodel

De assistent is geen gebruiker met bijzondere rechten. Hij heeft geen eigen bevoegdheden.

- **Lezen.** De tools waarmee de assistent naar de locatie kijkt, zijn alleen-lezen en beperkt tot de locatie waarin de persoon werkt.
- **Voorstellen.** De plantools leggen alleen een voorgestelde stap vast. Er wordt niets uitgevoerd. Dit wordt getest.
- **Doorvoeren.** Bij Toepassen lopen de opgeslagen stappen via dezelfde servicefuncties, validatie en bevoegdheidscontroles als wanneer de persoon elke wijziging met de hand had gedaan, zodat iemand die iets niet mag wijzigen, het ook niet door de assistent kan laten wijzigen. Het auditlog legt het resultaat vast als doorgevoerd door de assistent voor die bij naam genoemde persoon.
- **Veroudering.** Een plan dat verouderd is, omdat een reel tussen voorstel en goedkeuring is verwijderd, wordt geweigerd in plaats van aangevuld met een gok.
- **Inperking.** De assistent staat uit en is verborgen wanneer hij niet is geconfigureerd. Het gebruik wordt gemeten, met een harde maandelijkse limiet voor de hele server. Foutmeldingen van de onderliggende dienst worden nooit letterlijk getoond.

6.3 Waarom eerst controleren en dan doorvoeren

Een systeem dat verandert wat er op tweehonderd schermen speelt, moet kunnen antwoorden op de vraag "wie heeft dit gewijzigd, en heeft een persoon het goedgekeurd?" Leg die vraag voor aan elk product dat geautomatiseerde inrichting aanprijst.

7 Analyse: wat een locatie te weten komt

7.1 Gebouwd op wat de players werkelijk rapporteren

De analyse van taleor, in de console Inzichten genoemd, is gebouwd op wat de players en sensoren rapporteren, niet op een apart telsysteem: de sensor die een film start, is de sensor die telt wie bleef staan en hoe lang. Elk cijfer geldt voor de hele locatie, een verdieping, een zone of een player, over vandaag, deze week, deze maand of dit jaar, met de periode daarvoor ter vergelijking.

7.2 Wat u ziet

Bezoekersaantallen en verblijftijd. Bezoekers per uur, dag of maand, op basis van sensoren en aanrakingen. Gemiddelde verblijftijd bij betrokken bezoeken. De drukste zones en uren, als heatmap van zone per uur.

Wat het best werkte. Exhibits gerangschikt naar bezoeken en verblijftijd, zodat een stille hoek opvalt voordat een conservator er voorbijloopt. Bezoekers en verblijftijd horen bij het exhibit; uptime en afspeelbeurten bij elke player.

Bewijs van afspelen. Elk item, elke afspeelbeurt, wel of niet volledig afgespeeld, met een CSV-export die dezelfde reikwijdte en periode volgt. Standaard vijf jaar bewaard, zodat het langer meegaat dan een licentieperiode en een sponsorovereenkomst.

Playerstatus en uptime. Uptime per player over de periode, op basis van momentopnamen van de status. Geen momentopnamen in een periode betekent onbekend, niet gezond.

7.3 Eerlijke cijfers

Een cijfer dat niet kan worden gemeten, zegt "niet gemeten", nooit nul. Een zone zonder sensor meldt geen nul bezoekers; ze meldt dat er daar geen bezoekers zijn gemeten.

7.4 Nogmaals: privacy door het ontwerp

De gebeurtenissen achter elk cijfer zijn die uit sectie 5.6, zonder identificatie van de bezoeker: geen camera's, geen gezichtsdetectie, geen apparaattracking, geen cookies.

8 Draait overal, werkt met wat u al hebt

8.1 Platforms

Onderdeel	Draait op
Console (web-app)	Elke actuele browser, op app.taleor.net of op uw lokale server
Console (desktop-app)	Windows, macOS, Linux
Lokale server, ook air-gapped	Windows, macOS, Linux
Playeragent	Windows, macOS, Linux, Raspberry Pi, Android
Browserplayer	Elke actuele browser; koppelen met een zescijferige code

De desktop-app opent de console in een eigen venster, kan het exhibit op dezelfde computer afspelen en behoudt de laatste goede configuratie na een herstart.

8.2 Hardware, via open standaarden

taleor stuurt apparatuur van elk merk aan via de standaarden die die apparatuur al spreekt.

Familie	Voorbeelden	Via
Displays	Elk scherm aan een computer met de taleor player, of met de browserplayer	taleor player · browserplayer · HDMI
Projectoren	Elke projector die PJLink spreekt; fabrikantsspecifieke seriële protocollen	PJLink · ESC/VP21 · RS-232 · TCP
Sensoren	Aanwezigheid, afstand (lidar, ultrasoon), air button, drukknop, RFID; sensorcontrollers achter elke player	Serial · USB · TCP
Controllers	OSC in vanaf een lichttafel of showcontroller, OSC uit vanuit een trigger, USB-toetsen, pedalen en seriële boards, een handheld	OSC · USB · serial
Geluid	Audioprocessors en luidsprekers in het netwerk, van een headset bij één exhibit tot een hele zaal	REST · TCP
Verlichting	Architectuur- en exhibitverlichting	DALI

Standaarden, volledig: PJLink · RS-232 · TCP · DALI · MQTT · OSC · REST · WebSocket · serieel · USB.

Voor deze families zijn drivers beschikbaar, en wij testen ze met uw apparatuur voordat u opengaat; dat leggen wij schriftelijk vast in plaats van een lijst met logo's te claimen. Als een apparaat niet wordt ondersteund, kan een integrator met de driverkit er zelf een schrijven: een manifest, een adapter, een handtekening. Fabrikanten kunnen ons een apparaat brengen en wij bouwen de integratie.

8.3 Wat dit betekent voor leveranciersafhankelijkheid

De besturingslaag spreekt open standaarden, dus de hardware is niet gebonden aan taleor. De server draait op uw eigen computer met een eigen database, dus de gegevens zijn niet gebonden aan onze cloud. Content bestaat uit gewone mediabestanden en de configuratie wordt als gewone data geëxporteerd, dus een locatie die vertrekt, neemt haar content en haar geschiedenis mee. Media kunnen ook in de eigen Google Drive van de locatie blijven: taleor leest alleen de gekozen bestanden, en schermen bewaren een kopie om offline af te spelen. Wij worden liever gehouden omdat het product goed is dan omdat vertrekken onmogelijk is.

9 Implementatiemodellen en hoe u ze beoordeelt

9.1 Drie modellen

Cloud. De snelste start: open app.taleor.net, maak de locatie aan, installeer de agent op elke exhibitcomputer. Agents maken een uitgaande verbinding; niets maakt een inkomende verbinding. Voor locaties zonder serverinfrastructuur, en voor integrators die meerdere locaties beheren.

Lokale server. Het serverpakket op een computer in het gebouw, met of zonder internet. Voor instellingen met een eigen IT-afdeling, en voor elke locatie waarvan de aanbestedingsregels vereisen dat gegevens op de eigen locatie blijven.

Air-gapped. De lokale server volledig zonder internet; updates worden door medewerkers binnengebracht. Voor locaties met een strikt netwerkbeleid of zonder betrouwbare verbinding, en voor iedereen die heeft besloten dat de zalen niet afhankelijk mogen zijn van een verbinding waar men zelf geen controle over heeft.

Alle drie draaien dezelfde software en dezelfde console, en de keuze kan later veranderen.

9.2 Een checklist voor aanbestedingscommissies

Leg deze vragen voor aan elke leverancier. Onze antwoorden, met de onderbouwende sectie:

Vraag	taleor	Waar
Hoe bewijst elke player zijn identiteit? Komt er een gedeelde sleutel of een wachtwoord aan te pas?	Certificaat per player; sleutel op de computer gegenereerd, nooit gekopieerd; één instantie per locatie	5.1
Is de playerverbinding versleuteld en in beide richtingen geverifieerd? Kunnen certificaten worden vernieuwd zonder bezoek ter plaatse?	TLS 1.3; mutual TLS; certificaten van 398 dagen worden vernieuwd via de eigen verbinding van de player	5.2
Zijn drivers ondertekend? Worden updates geverifieerd voordat ze worden geïnstalleerd?	Drivers met Ed25519-handtekening, niet-ondertekende geweigerd; SHA-256-controlesom geverifieerd op de player	5.3
Kan een slechte update een exhibit platleggen?	Installatie buiten de openingstijden; teruggedraaid en geblokkeerd bij een mislukte statuscontrole	5.3
Kan een technicus een scherm herstarten zonder het te kunnen verwijderen?	Vijf rollen; ja	5.4
Draagt elke handeling een persoon, tijdstip en adres? Kan een beheerder het log inkorten of wissen?	Ja; CSV-export; minimale bewaartermijn van 180 dagen; wissen laat een tombstone achter, geen gat	5.5
Wat legt het systeem vast over bezoekers, en hoe lang?	Locatie, apparaat, zone, status, tijdstip; geen identificatie, afgedwongen door een schematest; bewaartermijn per categorie, verwijdering aantoonbaar	5.6
Is er een noodmelding, en wat bereikt die?	Locatie, verdieping, zone of gekozen players; volledig scherm; exhibitgeluid stil	5.7
Kan het hele systeem op de eigen locatie draaien, zonder internet?	Ja; lokale server en air-gapped	5.8, 9.1
Wat gebeurt er met de exhibits wanneer de server niet beschikbaar is?	Players blijven afspelen uit de lokale cache, ook na herstarts	5.9
Is het product aan een beveiligingsbeoordeling onderworpen, en kunnen wij de bevindingen inzien?	Ja; dreigingsmodel, proofs of concept, scanners, geverifieerde oplossingen	5.10

Vraag	taleor	Waar
Als de inrichting geautomatiseerd is, keurt een persoon dan elke exacte wijziging goed, op eigen naam?	Ja; voorstellen, controleren, doorvoeren; in het auditlog vastgelegd als doorgevoerd voor de bij naam genoemde persoon	6.2
Welke platforms en hardwarestandaarden?	Players op Windows, macOS, Linux, Raspberry Pi, Android en elke browser; PJLink, RS-232, TCP, DALI, MQTT, OSC, REST, WebSocket, serieel, USB	8
Wat bezitten wij als wij vertrekken?	Content als gewone bestanden, configuratie als gewone data, de database op uw computer	8.3

9.3 Waar u in een pilot om vraagt

Een paper is geen product. Vraag om een pilot met een paar exhibits waarin de maatregelen op de proef worden gesteld: meld een player aan met mutual TLS en bekijk zijn certificaat; probeer een tweede computer met een kopie van zijn configuratie en stel vast dat die wordt geweigerd; laat een facilitair manager een scherm herstarten en het daarna proberen te verwijderen; laat de assistent een trigger voorstellen, verwerp die, keur er daarna een goed en lees het auditlog; trek een netwerkkabel los en zie hoe de player blijft afspelen; exporteer het auditlog en het bewijs van afspelen als CSV; vraag om het verslag van de laatste opschoonronde voor bewaartermijnen. Elk onderdeel kost een paar minuten en vertelt een commissie meer dan welke lijst met functies ook.

10 Over taleor

taleor is een veilige, agentische manier om een belevingslocatie te beheren: de content, interactieve toepassingen, players en hardware, vanuit één console, in de cloud, op een lokale server of volledig air-gapped. taleor is er voor musea, wetenschapscentra, merkbelevingscentra, erfgoedlocaties en attracties, en voor de mensen die ze leiden en er inkopen voor doen.

taleor wordt gelanceerd in november 2026. Schrijf naar hello@taleor.net om een pilot af te spreken of om het datasheet voor aanbestedingen aan te vragen in het Engels, Duits, Nederlands of Pools.

Bronnen en verificatie

Elke technische bewering in deze paper berust op een benoemde bron in de code, de ontwerpdocumenten of de beveiligingsbeoordeling van taleor, vastgelegd in een claimregister dat elke bewering vermeldt, de sectie waarin ze staat en het bestand waaruit ze afkomstig is. Schrijf naar hello@taleor.net voor het register.

Openbare bronnen gebruikt in sectie 2, geen ervan met cijfers: het Mirai-botnet van 2016 (breed gedocumenteerd, onder meer door het Amerikaanse Cybersecurity and Infrastructure Security Agency); BSI IT-Grundschutz (Duitsland); de Baseline Informatiebeveiliging Overheid (Nederland); Richtlijn (EU) 2022/2555, bekend als NIS2; en de Baseline Requirements van het CA/Browser Forum voor de certificaatlevensduur van 398 dagen.

