
Gestire in sicurezza un luogo esperienziale

Perché un museo, un science center o un centro esperienziale di marca va gestito come un'infrastruttura IT ben governata, e come lo fa taleor: ogni dispositivo identificato, ogni connessione cifrata, ogni modifica attribuita, ogni visitatore anonimo.

White paper · ottobre 2026 · Versione 1.0

Per direttori, responsabili tecnici e IT, integratori AV, consulenti e commissioni di gara di musei, science center, centri esperienziali di marca, siti del patrimonio culturale e attrazioni.

taleor

Indice

1	Sintesi	3
2	Il problema: una sede oggi è un'infrastruttura IT	3
3	Di che cosa ha davvero bisogno una sede	5
4	Come funziona taleor	6
5	Sicurezza fin dalla progettazione	8
6	Configurato da un assistente	12
7	Analisi: che cosa apprende una sede	14
8	Funziona ovunque, con ciò che già possiede	15
9	Modelli di implementazione e come valutarli	17
10	Informazioni su taleor	19
	Fonti e verifiche	19

1 Sintesi

Un luogo esperienziale un tempo era un edificio con qualche schermo. Oggi è una rete: centinaia di computer, display, proiettori, altoparlanti, luci e sensori di una dozzina di produttori, ciascuno con il proprio firmware, un indirizzo e spesso una password, gestiti da un piccolo team che non è un team IT.

Questo documento sostiene che una sede dovrebbe essere gestita come si gestisce un'infrastruttura IT ben governata: ogni dispositivo identificato, ogni connessione cifrata, ogni modifica attribuita, ogni aggiornamento verificato, ogni visitatore anonimo. La sezione 3 espone sette principi, le sezioni da 4 a 8 descrivono come taleor li rispetta e la sezione 9 si chiude con una checklist che una commissione di gara può sottoporre a qualsiasi fornitore, noi compresi.

taleor è un modo sicuro e agentic di gestire un luogo esperienziale: contenuti, applicazioni interattive, schermi e hardware, da un'unica console. Si fonda su tre pilastri: è sicuro fin dalla progettazione; viene configurato da un assistente che non applica mai una modifica senza l'approvazione di una persona identificata per nome; e le sue analisi indicano «non misurato» anziché zero. Funziona come web app, come app desktop per Windows, macOS e Linux e come server locale nel Suo edificio, anche in modalità completamente air gap. I suoi schermi funzionano su Windows, macOS, Linux, Raspberry Pi e Android. Pilota apparecchiature di qualsiasi marca tramite standard aperti.

2 Il problema: una sede oggi è un'infrastruttura IT

2.1 Centinaia di dispositivi, decine di marche, un team ridotto

Conti i computer nelle sale di un museo contemporaneo: uno dietro la maggior parte delle installazioni, più display di rete, proiettori, processori audio, controller luci, sensori, lettori e pulsanti. In una sede di dimensioni modeste si arriva a qualche centinaio. I dati di esempio usati per sviluppare taleor, modellati su un tipico museo regionale, comprendono 69 installazioni e 342 dispositivi che usano 49 protocolli di controllo. È un parco dispositivi ordinario.

Ogni produttore porta il proprio protocollo, il proprio strumento di gestione e la propria idea di come debbano funzionare gli aggiornamenti. I contenuti cambiano ogni stagione. Il team è di solito composto da due a cinque persone, i cui ruoli non sono stati concepiti per includere la gestione di un parco dispositivi e l'applicazione delle patch.

2.2 Rischi per la sicurezza

Quattro punti deboli si aggravano a vicenda.

Credenziali predefinite. Le apparecchiature AV professionali escono di fabbrica con un'interfaccia di gestione e una password predefinita che viene cambiata di rado, perché cambiarla su duecento dispositivi è una settimana di lavoro di cui nessuno è responsabile. Nel 2016 la botnet Mirai reclutava dispositivi provando un breve elenco di password di fabbrica. Le apparecchiature AV delle sedi non fanno eccezione.

Schermi non aggiornati. Il computer dietro un'installazione spesso esegue ancora il sistema operativo con cui è stato messo in servizio, perché aggiornarlo significa chiudere l'installazione. Una macchina senza patch sulla stessa rete della biglietteria e della gestione dell'edificio è una via d'accesso. I quadri di riferimento rispetto ai quali vengono valutati gli enti pubblici in Germania, nei Paesi Bassi e in Polonia (BSI IT-Grundschutz, la Baseline Informatiebeveiliging Overheid e gli obblighi derivanti da NIS2) considerano l'applicazione tempestiva delle patch e l'inventario degli asset come controlli di base.

Segreti condivisi. Molti sistemi di controllo autenticano uno schermo con una chiave contenuta in un file di configurazione. Chiunque possa leggere quel file può spacciarsi per quello schermo.

Dipendenza dal cloud. Un sistema che si ferma quando cade internet o il cloud del fornitore ha spostato il punto unico di guasto in un luogo dove la sede non può intervenire. Per un ente pubblico è anche una questione di appalti: chi detiene i dati, secondo quale legge, e che cosa succede alla scadenza del contratto.

2.3 Fermi, punti ciechi e dipendenza dal fornitore

I fermi sono il guasto più visibile e il meno misurato. Uno schermo si blocca alle 10, un visitatore lo segnala a mezzogiorno, il tecnico lo viene a sapere alle 14, e nulla ha registrato le quattro ore perse.

La maggior parte delle sedi conta i visitatori all'ingresso e in nessun altro punto. Non sa dire davanti a quale installazione le persone si sono fermate, per quanto tempo, né se un filmato è stato guardato fino alla fine. Dove una misurazione esiste, spesso è un sistema separato, troppo spesso con telecamere che identificano le persone.

Ogni sottosistema arriva con il proprio fornitore e il proprio contratto. Quando un fornitore viene acquisito o abbandona un prodotto, i contenuti realizzati per un sistema di riproduzione proprietario non possono essere trasferiti, e l'hardware

che dialoga con un solo controller diventa un rottame. La domanda che una commissione dovrebbe porre non è «questo fornitore supporta il nostro hardware?» ma «se questo fornitore sparisse, che cosa resterebbe nostro?»

3 Di che cosa ha davvero bisogno una sede

Questi problemi sono già stati risolti, nell'informatica generale. Ciò che è mancato finora è la loro applicazione alla forma specifica di un luogo esperienziale: molti piccoli computer, molte marche, un team ridotto, un pubblico di visitatori e un edificio che deve aprire alle 10. Proponiamo sette principi.

1. **Ogni dispositivo ha un'identità che non può essere copiata.** Una chiave generata sul proprio hardware e che non lo ha mai lasciato. Non una password. Non un token in un file.
2. **Ogni connessione è cifrata e autenticata in entrambe le direzioni.** Qualunque soluzione meno rigorosa permette a un estraneo sulla rete della sede di allestire un falso convincente.
3. **Su uno schermo non viene eseguito nulla che non sia stato prima verificato.** Driver e aggiornamenti vengono controllati sullo schermo stesso tramite una firma o un checksum, non solo all'origine.
4. **Ogni modifica ha un nome e un orario.** Una traccia di audit che un amministratore può ridurre a un giorno, o modificare, non è una traccia di audit.
5. **Le persone ricevono i permessi richiesti dal loro lavoro, e non di più.** Un facility manager può riavviare uno schermo bloccato senza poterlo eliminare.
6. **I visitatori restano anonimi per costruzione, non per policy.** Una proprietà dello schema del database, verificata da test.
7. **La sede è proprietaria del proprio sistema.** Può far funzionare tutto nel proprio edificio, senza internet, e può cambiare fornitore senza perdere i propri contenuti.

È ciò che un reparto IT competente chiederebbe a qualsiasi parco di duecento computer. Il resto di questo documento descrive come taleor soddisfa questi principi.

4 Come funziona taleor

4.1 Le componenti

La console. Un'applicazione web in cui il personale vede ogni installazione, ogni schermo e ogni apparecchiatura, carica i contenuti, imposta programmazioni e trigger, monitora lo stato e gli allarmi e consulta le analisi. Funziona in qualsiasi browser aggiornato o come app desktop per Windows, macOS e Linux.

L'agente dello schermo. Un piccolo servizio in background sul computer dietro ogni installazione. Mantiene con il server una connessione persistente e mutuamente autenticata, riproduce ciò che gli viene indicato, pilota le apparecchiature collegate a quel computer, legge i suoi sensori, segnala il proprio stato e si mantiene aggiornato. Per impostazione predefinita conserva una copia locale di 4 GB dei propri contenuti e continua la riproduzione quando il server non è raggiungibile. Gli agenti funzionano su Windows, macOS, Linux, Raspberry Pi e Android. Uno schermo senza computer si abbina come schermo nel browser, con un codice a sei cifre letto direttamente sul vetro.

Driver. Un pacchetto firmato che indica a taleor che cosa sa fare un'apparecchiatura e come comunicare con essa. La console chiede un comando, ad esempio accensione, sorgente o volume; il driver gestisce il protocollo.

Il server. Il database, gli hub WebSocket che trasportano lo stato in tempo reale, l'autorità di certificazione di ciascuna sede, l'archivio dei media, il motore delle programmazioni, il monitoraggio degli allarmi, il registro di audit e le analisi. È lo stesso software nel nostro cloud o su una macchina nel Suo edificio, con o senza internet.

4.2 Un unico software, tre modalità di esercizio

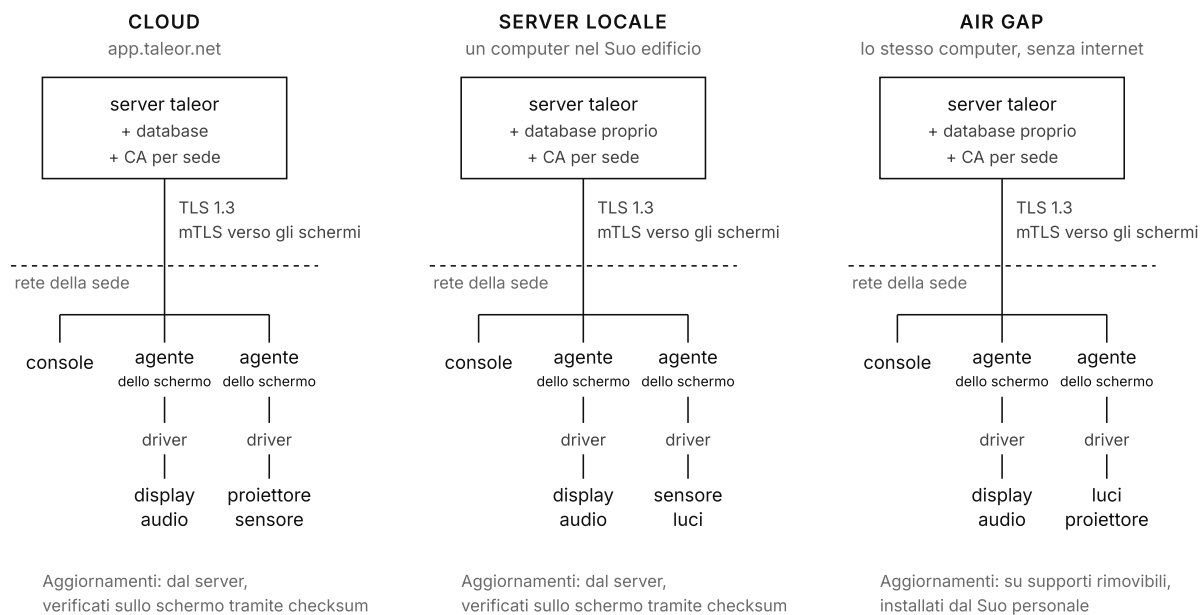


Figura 1. Un unico software, tre modalità di esercizio. Lo stesso server, la stessa console e gli stessi agenti degli schermi nel cloud, su un server locale nell'edificio o in modalità air gap, senza internet.

In modalità cloud la console e il server risiedono su app.taleor.net e sono gli agenti ad aprire la connessione verso di essi; le apparecchiature sulla rete della sede sono pilotate dagli agenti all'interno di quella rete. In modalità server locale lo stesso pacchetto si installa su una macchina Windows, macOS o Linux nell'edificio, con il proprio database privato e la propria autorità di certificazione, così console, schermi, media e registro di audit restano tutti all'interno. In modalità air gap quel server funziona senza alcuna connessione a internet: runtime e database sono inclusi nel pacchetto, durante l'installazione non viene scaricato nulla e gli aggiornamenti vengono introdotti su supporti rimovibili dal Suo stesso personale. Un'unica base di codice, un'unica console; una sede che inizia nel cloud può riportare tutto al proprio interno.

5 Sicurezza fin dalla progettazione

5.1 Identità: una chiave che non lascia mai la macchina

taleur sostituisce il segreto condiviso con un certificato. Quando uno schermo viene registrato, genera sulla propria macchina una coppia di chiavi asimmetriche e invia soltanto la metà pubblica, in una richiesta di firma del certificato, all'autorità di certificazione della sede, che firma e restituisce un certificato. La chiave privata non viaggia mai. Da quel momento lo schermo dimostra la propria identità producendo una firma, in tempo reale, durante ogni handshake TLS. Non c'è nulla da copiare.

Un'autorità di certificazione per ogni sede, che un amministratore attiva dalla console. La compromissione di una sede non può generare un'identità in un'altra. La chiave privata dell'autorità è cifrata a riposo con un segreto distinto dagli altri segreti del server.

La richiesta non è considerata attendibile. Dalla richiesta di firma viene presa solo la chiave pubblica; il soggetto, il periodo di validità e ogni estensione sono stabiliti dal server, quindi uno schermo non può chiedere di essere chiamato con il nome di un altro schermo né di diventare un'autorità di certificazione. I certificati degli schermi sono emessi solo per l'autenticazione client, quindi un certificato rubato non può servire ad allestire un server falso.

Non esiste un pulsante «Emettere certificato». Un certificato la cui chiave privata sia stata anche solo una volta in possesso del server vanificherebbe lo scopo.

5.2 Trasporto: cifrato e verificato, in entrambe le direzioni

Ogni connessione tra un browser, uno schermo e la console viaggia su TLS 1.3 (per i client meno recenti è accettato 1.2). Le connessioni degli schermi usano il TLS reciproco: ciascuna parte presenta il proprio certificato all'altra.

Un certificato valido è necessario ma non sufficiente. A ogni connessione il server verifica inoltre, sul database e non su un elenco in cache, che il certificato non sia revocato né scaduto, che il dispositivo a cui si riferisce esista ancora e che il dispositivo appartenga alla sede per cui il certificato è stato emesso.

I certificati durano 398 giorni, il limite massimo del CA/Browser Forum per i certificati pubblicamente attendibili, e si rinnovano negli ultimi 30 giorni attraverso la connessione TLS reciproca dello schermo stesso, così un parco dispositivi rinnova le proprie credenziali senza sopralluoghi. L'emissione di un nuovo certificato revoca il precedente.

L'attivazione del TLS reciproco avviene per fasi: una modalità di rotazione accetta sia un certificato sia la credenziale precedente mentre il parco migra sala per sala, poi una modalità obbligatoria quando ogni endpoint è certificato. Il server rifiuta questo passaggio finché c'è anche un solo dispositivo in connessione che resterebbe escluso, perché l'alternativa è un museo al buio. Riportare la modalità su spento annulla subito il passaggio.

5.3 Integrità: non viene eseguito nulla che non sia stato verificato

I driver sono firmati. Un driver è un pacchetto con un manifest e una firma Ed25519 separata, calcolata sul digest del pacchetto. Per impostazione predefinita un server di produzione rifiuta un pacchetto non firmato, perché un driver è codice che apre socket e dialoga con l'hardware. Integratori e produttori possono scrivere e firmare i propri driver con il kit per driver.

Gli aggiornamenti degli schermi sono verificati tramite checksum. Il server pubblica una versione con il relativo checksum SHA-256. Lo schermo verifica il checksum prima di ogni altra cosa, estrae l'aggiornamento in una directory di staging, lo sostituisce alla versione in uso e si riavvia. Una verifica non riuscita equivale a un aggiornamento rifiutato.

Gli aggiornamenti rispettano l'edificio. Un aggiornamento si installa solo fuori dall'orario di apertura. Una nuova versione che non supera il controllo dello stato entro dieci minuti viene annullata con un rollback e bloccata per ulteriori tentativi. Una sede può escludere uno schermo dagli aggiornamenti; uno schermo escluso o rimasto indietro viene contrassegnato nella console come «Non attuale», quindi non viene mai dimenticato senza che nessuno se ne accorga.

5.4 Accesso e ruoli

taleor prevede cinque ruoli assegnabili.

Ruolo	A che cosa serve
Amministratore di rete	Tutto, in tutte le sedi gestite dall'organizzazione
Amministratore generale	Tutti i permessi a livello di sede, nelle sedi di un gruppo
Amministratore della sede	Tutti i permessi a livello di sede, in una sola sede
Responsabile dei contenuti	Contenuti, reel, programmazioni e modelli
Facility manager	Gestione delle apparecchiature: riavvio, accensione, sorgente, volume

I ruoli sono volutamente poco granulari, perché un modello di permessi che nessuno sa spiegare è un modello che nessuno applica. Ogni endpoint verifica sia il ruolo sia la sede, quindi chi ha diritti in una sede non vede nulla di un'altra. L'accesso è personale, mai condiviso; un nuovo account deve cambiare la password al primo utilizzo.

5.5 La traccia di audit

Ogni scrittura finisce nel registro di audit con la persona, l'azione, l'ora e l'indirizzo di rete di provenienza. Questo vale anche per le azioni eseguite dall'assistente, che vengono registrate come applicate dall'assistente per conto di una persona identificata per nome. Il registro può essere filtrato nella console ed esportato in CSV con gli stessi filtri, così un revisore può portarlo con sé.

Due proprietà proteggono il registro da chi ha più potere su di esso. La categoria audit ha una soglia minima di conservazione obbligatoria di 180 giorni: una sede può conservare il proprio registro più a lungo, mai meno. E quando un membro del personale esercita il diritto alla cancellazione, l'account diventa un record segnaposto (tombstone): identità oscurata, indirizzi di rete eliminati, azioni conservate, così il registro indica ancora che qualcuno, poi cancellato, ha pubblicato una scena il giorno 3. Un amministratore non può cancellare il proprio account.

5.6 Privacy dei visitatori, per costruzione

I visitatori di una sede sono persone del pubblico, molte delle quali bambini. La progettazione corretta è quella in cui il sistema non è in grado di registrare chi siano.

Le due tabelle che contengono il comportamento dei visitatori, eventi di presenza ed eventi di interazione, riportano una sede, un dispositivo, una zona, una parola di stato o di evento e una marca temporale. Non contengono alcun identificativo della persona: nessun indirizzo di rete, nessun volto, nessun cookie, nessuna sessione. È una proprietà dello schema, non una promessa contenuta in una policy; un test la verifica sulle definizioni effettive delle tabelle e fa fallire la build se qualcuno aggiunge una colonna di questo tipo.

Alle spalle c'è un registro dei trattamenti che risiede nel codice e viene revisionato nella stessa modifica del codice che genera i dati: finalità, base giuridica, grado di identificazione, destinatari e periodo di conservazione per ogni categoria. Una pulizia notturna elimina le righe oltre il periodo di conservazione, a blocchi per non rallentare mai una sede aperta, e scrive una riga per ogni esecuzione, comprese quelle non riuscite. Quel registro è la prima prova che un revisore chiede.

Categoria di dati	Conservazione predefinita	Minimo
Presenza presso un'installazione	400 giorni	1 giorno
Tocchi e scelte	400 giorni	1 giorno
Che cosa è stato riprodotto, e quando	1.825 giorni	365 giorni
Log degli schermi	30 giorni	1 giorno
Chi ha fatto che cosa (audit)	730 giorni	180 giorni

I controlli sono realizzati secondo i requisiti tecnici della ISO/IEC 27701, l'estensione per la privacy della ISO/IEC 27001. Siamo cauti con questa affermazione: un prodotto non può essere certificato secondo la 27701; un'organizzazione sì, dopo un audit. taleor implementa i controlli che la norma rende tecnici e produce le evidenze di cui un revisore ha bisogno; l'istituzione deve comunque nominare un referente per la privacy, svolgere la propria valutazione d'impatto, stipulare i contratti con i responsabili del trattamento e affiggere le informative nelle sale.

5.7 Emergenza

Un solo comando attiva un messaggio di emergenza su tutta la sede, su un piano, su una zona o su schermi scelti. Il messaggio occupa l'intero schermo, un avviso scorre nella parte inferiore e l'audio delle installazioni si spegne. Uno schermo che si riconnette durante una trasmissione la riceve comunque. Il messaggio di emergenza può essere avviato e terminato da un palmare del personale ed è registrato come qualsiasi altra azione. Diciamo «audio delle installazioni» di proposito: taleor silenzia ciò che controlla e non è un impianto di diffusione sonora per annunci al pubblico.

5.8 Isolamento e air gap

Il pacchetto del server locale installa un proprio cluster PostgreSQL privato, in ascolto solo sull'interfaccia di loopback e su una porta non standard, così non entra mai in contatto con un database già presente sulla macchina. Nessuno digita la password del database: ne viene generata una casuale durante l'installazione, conservata solo in un file di configurazione leggibile dal sistema e dai suoi amministratori. Non serve alcun runtime per container. La modalità air gap è lo stesso pacchetto senza internet (sezione 4.2).

Le apparecchiature sulla rete della sede sono sempre pilotate dall'interno di quella rete, dagli agenti degli schermi o dal server locale. La console cloud non ha mai bisogno di un accesso verso il Suo edificio; sono gli agenti a connettersi verso l'esterno.

5.9 Modalità di guasto sicure

- Uno schermo che perde il contatto con il server continua a riprodurre l'ultima configurazione valida dalla propria cache locale, anche dopo i riavvii, finché il server non torna disponibile.
- Uno schermo che si disconnette genera un allarme che indica quale schermo, dove si trova, che cosa dovrebbe mostrare e da quando. L'allarme si chiude da solo quando lo schermo torna; un guasto ripetuto aggiorna l'allarme esistente.
- Il server esegue il backup del proprio database secondo una programmazione, con uno storico progressivo e ripristino da qualsiasi punto. Tutto ciò che viene eliminato dalla Libreria media è recuperabile per 30 giorni.
- Il server rifiuta di vincolare una sede al TLS reciproco finché c'è anche un solo dispositivo che resterebbe escluso, rifiuta un piano dell'assistente non più attuale e rifiuta un driver non firmato. Tra tirare a indovinare e fermarsi, taleor si ferma e spiega perché.

5.10 Come verifichiamo il nostro lavoro

Prima del lancio, la console, il software degli schermi e il sito web di taleor sono stati sottoposti a una revisione della sicurezza applicativa: un modello delle minacce scritto, exploit proof-of-concept per ogni vulnerabilità sospetta, scanner delle dipendenze e di analisi statica, e una nuova scansione dopo le correzioni. Ogni rilievo ha una gravità, un responsabile e una correzione verificata; una fase di controllo non è superata finché resta aperto un rilievo bloccante. Chieda lo stesso a qualsiasi fornitore.

6 Configurato da un assistente

6.1 Che cosa fa

Configurare un'installazione interattiva è sempre stato un lavoro specialistico che nella sede sa svolgere una sola persona. taleor include nella console un assistente, chiamato Oli. Lei scrive ciò che desidera:

Quando qualcuno arriva a meno di un metro dallo schermo dell'atrio, passare al filmato di benvenuto e tornare indietro dopo trenta secondi senza nessuno.

L'assistente legge la sede (installazioni, schermi, reel, ingressi dichiarati) e propone un piano con l'elenco esatto delle modifiche:

Legge lo schermo dell'atrio: sensore di presenza dichiarato, 2 reel.

Propone: a una distanza di 100 cm o meno, riprodurre «filmato di benvenuto», tornare indietro dopo 30 s.

In attesa della Sua revisione.

Lei lo legge. Preme «Applicare» oppure «Scartare». Quando manca qualcosa, l'assistente dice che cosa: nessun reel chiamato «filmato di benvenuto», oppure nessun sensore di presenza su quello schermo. Quando una richiesta è ambigua pone una domanda alla volta, e non presume mai hardware che non c'è.

L'assistente propone trigger, assegnazioni di reel e l'attivazione di un trigger, e li applica dopo la Sua approvazione. Ogni comando resta disponibile anche manualmente.

6.2 Il modello dei permessi

L'assistente non è un utente privilegiato. Non ha permessi propri.

- **Lettura.** I suoi strumenti per esaminare la sede sono di sola lettura e limitati alla sede in cui la persona sta lavorando.
- **Proposta.** I suoi strumenti di pianificazione registrano solo un passaggio proposto. Non viene eseguito nulla. Questo è verificato da test.
- **Applicazione.** Premendo «Applicare», i passaggi memorizzati passano attraverso le stesse funzioni di servizio, le stesse convalide e gli stessi controlli dei permessi che si avrebbero se la persona avesse eseguito ogni modifica a mano, quindi chi non è autorizzato a modificare qualcosa non può farlo modificare all'assistente al proprio posto. Il registro di audit riporta il risultato come applicato dall'assistente per quella persona identificata per nome.
- **Piani non più attuali.** Un piano diventato obsoleto, perché un reel è stato eliminato tra la proposta e l'approvazione, viene rifiutato anziché completato per supposizione.

- **Contenimento.** L'assistente è disattivato e nascosto finché non è configurato. Il suo utilizzo è misurato, con un tetto mensile rigido per l'intero server. Gli errori del servizio sottostante non vengono mai mostrati alla lettera.

6.3 Perché revisionare prima di applicare

Un sistema che cambia ciò che va in onda su duecento schermi deve saper rispondere a «chi ha cambiato questo, e una persona lo ha approvato?» Ponga questa domanda a qualsiasi prodotto che pubblicizzi una configurazione automatica.

7 Analisi: che cosa apprende una sede

7.1 Costruite su ciò che gli schermi segnalano davvero

Le analisi di taleor, chiamate «Statistiche» nella console, si basano su ciò che segnalano gli schermi e i sensori, non su un sistema di conteggio separato: il sensore che avvia un filmato è lo stesso che conta chi si è fermato e per quanto tempo. Ogni dato può riferirsi all'intera sede, a un piano, a una zona o a uno schermo, per oggi, questa settimana, questo mese o quest'anno, con il periodo precedente come confronto.

7.2 Che cosa vede

Affluenza e permanenza. Visitatori per ora, giorno o mese, rilevati da sensori e tocchi. Permanenza media delle visite con coinvolgimento. Le zone e le ore di maggiore affluenza, come mappa di calore zona per ora.

Che cosa ha funzionato meglio. Installazioni classificate per visite e permanenza, così un angolo poco frequentato emerge prima che un curatore ci passi davanti. Visitatori e permanenza appartengono all'installazione; tempo di attività e riproduzioni a ciascuno schermo.

Prova di riproduzione. Ogni elemento, ogni riproduzione, completata o no, con un'esportazione CSV che rispetta lo stesso ambito e lo stesso periodo. Conservata per cinque anni per impostazione predefinita, così sopravvive alla durata di una licenza e a un accordo di sponsorizzazione.

Stato degli schermi e tempo di attività. Tempo di attività per schermo nel periodo, ricavato dai rilevamenti dello stato. In assenza di rilevamenti in un periodo, il valore risulta «sconosciuto», non «funzionante».

7.3 Numeri onesti

Un dato che non può essere misurato indica «non misurato», mai zero. Una zona senza sensore non riporta zero visitatori; riporta che lì i visitatori non sono stati misurati.

7.4 Privacy per costruzione, ancora una volta

Gli eventi alla base di ogni dato sono quelli della sezione 5.6, senza alcun identificativo del visitatore: niente telecamere, niente rilevamento dei volti, niente tracciamento dei dispositivi, niente cookie.

8 Funziona ovunque, con ciò che già possiede

8.1 Piattaforme

Componente	Funziona su
Console (web app)	Qualsiasi browser aggiornato, su app.taleor.net o sul Suo server locale
Console (app desktop)	Windows, macOS, Linux
Server locale, anche in modalità air gap	Windows, macOS, Linux
Agente dello schermo	Windows, macOS, Linux, Raspberry Pi, Android
Schermo nel browser	Qualsiasi browser aggiornato; si abbina con un codice a sei cifre

L'app desktop apre la console in una finestra dedicata, può riprodurre l'installazione sullo stesso computer e mantiene l'ultima configurazione valida anche dopo un riavvio.

8.2 Hardware, tramite standard aperti

taleor pilota apparecchiature di qualsiasi marca tramite gli standard che già supportano.

Famiglia	Esempi	Tramite
Display	Qualsiasi schermo collegato a un computer su cui gira l'agente taleor, oppure che mostra lo schermo nel browser	agente taleor · schermo nel browser · HDMI
Proiettori	Qualsiasi proiettore compatibile con PJLink; protocolli seriali specifici del produttore	PJLink · ESC/VP21 · RS-232 · TCP
Sensori	Presenza, distanza (lidar, ultrasuoni), pulsante senza contatto, pulsante a pressione, RFID; controller di sensori dietro qualsiasi schermo	Seriale · USB · TCP
Controller	OSC in ingresso da un mixer luci o da uno show controller, OSC in uscita da un trigger, tasti USB, pedali e schede seriali, un palmare	OSC · USB · seriale
Audio	Processori audio e altoparlanti di rete, dalle cuffie di una singola installazione a un'intera sala	REST · TCP
Illuminazione	Illuminazione architettonica e delle installazioni	DALI

Gli standard, nel dettaglio: PJLink · RS-232 · TCP · DALI · MQTT · OSC · REST · WebSocket · seriale · USB.

Per queste famiglie sono disponibili driver, e li testiamo con le Sue apparecchiature prima dell'apertura; lo dichiariamo per iscritto anziché esibire un elenco di loghi. Se un dispositivo non è coperto, il kit per driver consente a un integratore di scriverne uno: un manifest, un adattatore, una firma. I produttori possono portarci un dispositivo e ne realizzeremo l'integrazione.

8.3 Che cosa significa per la dipendenza dal fornitore

Il livello di controllo usa standard aperti, quindi l'hardware non è vincolato a taleor. Il server funziona sulla Sua macchina con il proprio database, quindi i dati non sono vincolati al nostro cloud. I contenuti sono normali file multimediali e la configurazione si esporta come semplici dati, quindi una sede che se ne va porta con sé i propri contenuti e il proprio storico. I media possono anche restare nel Google Drive della sede: taleor legge solo i file selezionati e gli schermi ne conservano una copia per la riproduzione offline. Preferiamo che i clienti restino con noi perché il prodotto è valido, non perché andarsene sia impossibile.

9 Modelli di implementazione e come valutarli

9.1 Tre modelli

Cloud. L'avvio più rapido: apra app.taleor.net, crei la sede, installi l'agente su ogni computer delle installazioni. Gli agenti si connettono verso l'esterno; nessuna connessione arriva dall'esterno. Per le sedi senza infrastruttura server e per gli integratori che gestiscono più sedi.

Server locale. Il pacchetto server su una macchina nell'edificio, con o senza internet. Per le istituzioni con un proprio reparto IT e per qualsiasi sede le cui regole di approvvigionamento richiedano che i dati restino in loco.

Air gap. Il server locale senza alcuna connessione a internet; gli aggiornamenti vengono introdotti dal personale. Per siti con policy di rete rigorose o senza una connettività affidabile, e per chiunque abbia deciso che le proprie sale non debbano dipendere da una connessione che non controlla.

Tutti e tre eseguono lo stesso software e la stessa console, e la scelta può cambiare in seguito.

9.2 Una checklist per le commissioni di gara

Ponga queste domande a qualsiasi fornitore. Le nostre risposte, con la sezione di riferimento:

Domanda	taleor	Dove
Come dimostra la propria identità ciascuno schermo? È coinvolta una chiave condivisa o una password?	Certificato per ogni schermo; chiave generata sulla macchina, mai copiata; un'autorità per sede	5.1
La connessione dello schermo è cifrata e autenticata in entrambe le direzioni? I certificati possono essere rinnovati senza sopralluogo?	TLS 1.3; TLS reciproco; certificati di 398 giorni rinnovati tramite la connessione dello schermo stesso	5.2
I driver sono firmati? Gli aggiornamenti vengono verificati prima dell'installazione?	Driver firmati Ed25519, quelli non firmati vengono rifiutati; checksum SHA-256 verificato sullo schermo	5.3
Un aggiornamento difettoso può mettere fuori servizio un'installazione?	Si installa fuori dall'orario di apertura; rollback e blocco se il controllo dello stato non riesce	5.3
Un tecnico può riavviare uno schermo senza poterlo eliminare?	Cinque ruoli; sì	5.4

Domanda	taleor	Dove
Ogni azione riporta persona, ora e indirizzo? Un amministratore può accorciare o cancellare il registro?	Sì; esportazione CSV; conservazione minima di 180 giorni; la cancellazione lascia un record segnaposto, non un vuoto	5.5
Che cosa registra il sistema sui visitatori, e per quanto tempo?	Sede, dispositivo, zona, stato, ora; nessun identificativo, garantito da un test sullo schema; conservazione per categoria, cancellazione documentata	5.6
Esiste un messaggio di emergenza, e che cosa raggiunge?	Sede, piano, zona o schermi scelti; schermo intero; audio delle installazioni silenziato	5.7
L'intero sistema può funzionare in loco, senza internet?	Sì; server locale e air gap	5.8, 9.1
Che cosa succede alle installazioni quando il server non è disponibile?	Gli schermi continuano la riproduzione dalla cache locale, anche dopo i riavvii	5.9
Il prodotto è stato sottoposto a una revisione della sicurezza, e possiamo vederne i rilievi?	Sì; modello delle minacce, proof of concept, scanner, correzioni verificate	5.10
Se la configurazione è automatizzata, una persona approva ogni singola modifica, a proprio nome?	Sì; proposta, revisione, applicazione; registrato come applicato per la persona identificata per nome	6.2
Quali piattaforme e quali standard hardware?	Schermi su Windows, macOS, Linux, Raspberry Pi, Android e qualsiasi browser; PJLink, RS-232, TCP, DALI, MQTT, OSC, REST, WebSocket, seriale, USB	8
Che cosa resta nostro se ce ne andiamo?	Contenuti come normali file, configurazione come semplici dati, il database sulla Sua macchina	8.3

9.3 Che cosa chiedere in un progetto pilota

Un documento non è un prodotto. Chieda un progetto pilota su alcune installazioni che metta alla prova i controlli: registrare uno schermo con TLS reciproco e ispezionarne il certificato; provare una seconda macchina con una copia della sua configurazione e verificare che venga rifiutata; far riavviare uno schermo a un facility manager, poi fargli tentare di eliminarlo; far proporre un trigger all'assistente, scartarlo, poi approvarne uno e leggere il registro di audit; staccare un cavo di rete e osservare lo schermo che continua la riproduzione; esportare in CSV il registro di audit e la prova di riproduzione; chiedere la

documentazione dell'ultima pulizia per scadenza della conservazione. Ciascuna prova richiede pochi minuti e dice a una commissione più di qualsiasi elenco di funzionalità.

10 Informazioni su taleor

taleor è un modo sicuro e agentic di gestire un luogo esperienziale: contenuti, applicazioni interattive, schermi e hardware, da un'unica console, nel cloud, su un server locale o in modalità completamente air gap. Si rivolge a musei, science center, centri esperienziali di marca, siti del patrimonio culturale e attrazioni, e alle persone che li gestiscono e che effettuano gli acquisti per loro conto.

taleor sarà lanciato a novembre 2026. Scriva a hello@taleor.net per organizzare un progetto pilota o per richiedere la scheda tecnica per le gare d'appalto in una delle nostre sette lingue: inglese, tedesco, olandese, polacco, francese, spagnolo o italiano.

Fonti e verifiche

Ogni affermazione tecnica contenuta in questo documento si basa su una fonte identificata nel codice, nei documenti di progettazione o nella revisione della sicurezza di taleor, annotata in un registro delle affermazioni che elenca ciascuna affermazione, la sezione in cui compare e il file da cui è tratta. Scriva a hello@taleor.net per ricevere il registro.

Riferimenti pubblici utilizzati nella sezione 2, nessuno con dati numerici: la botnet Mirai del 2016 (ampiamente documentata, anche dall'agenzia statunitense Cybersecurity and Infrastructure Security Agency); BSI IT-Grundschutz (Germania); la Baseline Informatiebeveiliging Overheid (Paesi Bassi); la Direttiva (UE) 2022/2555, nota come NIS2; e i Baseline Requirements del CA/Browser Forum per la durata dei certificati di 398 giorni.

