WHITE PAPER

L'INTERNET OF THINGS PERTINENTE

RAGGIUNGERE TRAGUARDI STRATEGICI SULLA BASE DEGLI OBIETTIVI DI BUSINESS GRAZIE AL CONTESTO E AI DATI IOT

aruba
a Hewlett Packard Enterprise company

INDICE

IL PROFESSORE E IL BOSCAIOLO

Alcuni anni fa il direttore del dipartimento di Ingegneria industriale dell'Università di Yale ha affermato: "Se avessi solo un'ora per risolvere un problema, dedicherei due terzi del mio tempo a tentare di definire quale sia il problema".[1] Analogamente, si racconta che a un boscaiolo venne chiesto: "Che faresti se avessi solo cinque minuti per abbattere un albero?" La risposta fu: "Dedicherei i primi due minuti e mezzo ad affilare la mia ascia".[2] Indipendentemente dal settore in cui si opera o dell'attività da portare a termine, è importante essere preparati, definire attentamente gli obiettivi e scegliere gli strumenti necessari per raggiungerli.

Purtroppo questo insegnamento viene spesso ignorato quando si tratta dei progetti IoT. Sarà l'attrattiva o il fraintendimento dei principi dell'IoT, la paura di essere superati dalla concorrenza o la pressione di dover proporre qualcosa di nuovo, in ogni caso le aziende spesso si buttano a capofitto nei progetti IoT senza definire chiaramente gli obiettivi, le proposte di valore o l'adeguatezza degli strumenti. Ne consegue un elevato tasso di fallimento dei progetti IoT e insoddisfazione tra i clienti.[3]

Una parte del problema è dovuto all'espressione stessa, Internet of Things, che crea confusione e malintesi. Inizialmente intesa per descrivere un ecosistema di macchine interconnesse, in seguito questa espressione è passata a indicare letteralmente la connessione di tutti i dispositivi tramite Internet. L'obiettivo primario dell'IoT non consiste nel collegare in rete ogni singolo dispositivo dell'azienda, né tantomeno nel collegare tutti i dispositivi tramite Internet. I dispositivi IoT sono contenitori tramite cui veicolare il contesto e i dati, nei quali includere solo le informazioni e i dispositivi pertinenti.

In che modo è possibile stabilire se un'informazione è pertinente o meno? La pertinenza si basa su una concatenazione di fattori che vanno dai traguardi strategici, agli obiettivi di business delineati per raggiungere tali traguardi, oltre che ai "momenti di business" (secondo la definizione di Gartner), ovvero delle opportunità transitorie relative ai clienti che possono essere sfruttate dinamicamente.[4] Un momento di business è il punto di convergenza tra i traguardi strategici dell'azienda e il contesto/i dati IoT pertinenti (figura 1) che, se sfruttati correttamente, migliorano il comportamento, l'atteggiamento e/o l'opinione del cliente.

I momenti di business devono essere accuratamente orchestrati dall'azienda, anche se devono risultare spontanei per il cliente. Per raggiungere il successo è necessaria un'altra concatenazione di fattori che vanno dal contesto e dai dati IoT pertinenti all'architettura IoT necessaria per accedere e fornire tali informazioni a un momento di business di destinazione. Se la concatenazione non è ottimale, ad esempio perché l'architettura IoT non riesce a estrarre informazioni pertinenti, il momento di business potrebbe passare senza risultati oppure potrebbe addirittura generare opinioni negative a scapito dei traguardi strategici.

Tutto ciò ci riporta al professore e al boscaiolo. Il primo compito in qualsiasi progetto IoT consiste nell'identificare i traguardi strategici di business da raggiungere, che devono confluire in una serie di obiettivi specifici che si basano su momenti di business correttamente forniti. L'architettura IoT è lo strumento che consente di estrarre e sfruttare il contesto e i dati IoT per riorientare il comportamento, l'atteggiamento e le azioni del cliente a favore dei traguardi strategici.

I traguardi e gli obiettivi di business indicano l'architettura IoT e i dispositivi pertinenti da adottare, non il contrario. Le soluzioni IoT scelte solo perché si presentano bene o sono molto pubblicizzate, risulteranno deludenti.

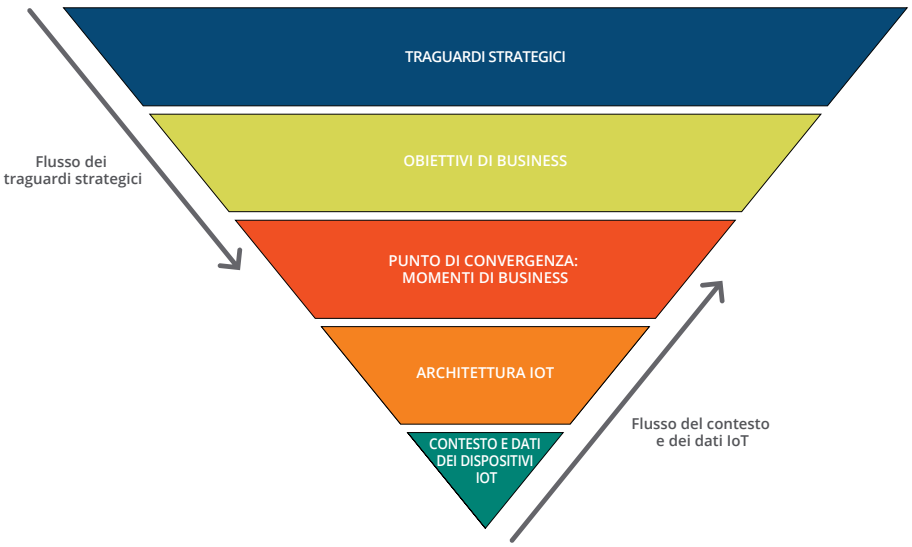


Figura 1: Gerarchia strategica IoT

CREAZIONE DI UNA SINERGIA

Riuscire a creare una sinergia tra i traguardi di business e l'architettura IoT necessaria per raggiungerli può risultare molto difficile senza un framework che guidi il processo. I soggetti coinvolti di diverse business unit devono verosimilmente mettere da parte i propri impegni individuali per allinearsi agli obiettivi aziendali. Sono necessari nuovi livelli di collaborazione tra gli ambiti della gestione, produzione, progettazione, IT e delle operazioni.[5] Può essere necessario abbandonare progetti e tecnologie per far posto ad alternative più pertinenti. Inoltre, potrebbe essere necessario accantonare relazioni consolidate con fornitori per accogliere nuovi fornitori che propongono soluzioni più pertinenti.

Il Ciclo di valore IoT (figura 2) fornisce questo tipo di framework suddividendo gli obiettivi di business in quattro elementi principali: visibilità, sicurezza, innovazione e redditività. I primi due elementi sono associati all'infrastruttura IoT che estrae il contenuto e i dati pertinenti ai traguardi e obiettivi di business. Gli altri due definiscono i momenti di business che sfruttano il contesto e i dati. Orientando correttamente le parti coinvolte alla definizione e implementazione di questi quattro elementi, è possibile garantire che le soluzioni IoT siano appropriate ai momenti di business di destinazione e soddisfino gli obiettivi di business a cui fanno riferimento.

La visibilità fornisce una risposta alla domanda "Sono completamente connesso?" e si ottiene interfacciandosi con tutti i dispositivi, le macchine e altre origini di contesto e dati relativi a processi, business e clienti pertinenti. L'infrastruttura con cui si implementa tutto ciò varia in base all'applicazione. Un'applicazione nel settore automobilistico può richiedere soluzioni telematiche cellulari, un sistema di controllo generale e acquisizione dati può richiedere una LAN e mesh wireless, mentre una piattaforma petrolifera off-shore può richiedere un'infrastruttura Wi-Fi a prova di esplosione di Classe 1 Divisione 1.

Indipendentemente dalla posizione fisica dei dispositivi pertinenti, è necessario accertarsi di ricevere e utilizzare solo dati sicuri da origini attendibili. Analogamente, i dati IoT devono essere protetti e gestiti, sia in transito che in archivio, durante tutto il loro ciclo di vita. I dispositivi, i sistemi operativi, i BIOS e l'infrastruttura devono essere protetti dalla manomissione, sia dall'esterno che dall'interno dell'azienda. Inoltre, le persone che installano e si occupano della manutenzione delle soluzioni IoT, nonché gli strumenti che adoperano, devono essere gestiti in piena sicurezza. L'assicurazione delle applicazioni e dei sistemi è necessaria per garantire una funzionalità ininterrotta, e una governance appropriata deve essere applicata costantemente all'utilizzo dei dati. L'affidabilità è un valore fugace in quanto il panorama della sicurezza informatica è in costante evoluzione. Pertanto, la domanda "Sono completamente protetto?" deve essere posta ripetutamente nel corso di un progetto IoT per garantire che vengano sempre adottati gli strumenti di protezione più recenti.

Figura 2: Ciclo di valore IoT

La visibilità e la sicurezza determinano l'architettura necessaria per raggiungere l'origine dei dati, assicurare l'attendibilità e controllare il ciclo di vita delle informazioni estratte. Esse costituiscono il secondo livello della Gerarchia strategica IoT.

Alla base della Gerarchia strategica IoT è necessario allineare accessibilità e attendibilità con il contesto e i dati pertinenti generati dai dispositivi IoT e in essi contenuti. La ricerca in ogni dispositivo senza considerare la pertinenza è dispendiosa sotto vari punti di vista: i costi legati ai dispositivi aumentano quando si incrementa la connettività, per estendere la visibilità e la sicurezza è richiesta più forza lavoro e capitali, i dati estratti devono essere elaborati e archiviati, inoltre sono necessaire molte risorse per identificare i dati utili.

Le linee guida che determinano la pertinenza e ci aiutano a individuare specifici dispositivi IoT rientrano nell'ambito della redditività e produttività. Per garantire la redditività, è necessario incrementare i profitti e/o ridurre i costi offrendo un servizio migliore ai clienti, adattando i prodotti e i servizi alle loro preferenze, e migliorando il loro comportamento e atteggiamento nei confronti dell'azienda. La domanda "Sto introducendo innovazioni su tutti i fronti?" riguarda come garantire l'eccellenza nel servizio, coinvolgere i clienti, differenziarsi rispetto alla concorrenza, semplificare le interazioni, migliorare la fidelizzazione, convalidare le performance dei prodotti e monetizzare i servizi.

La produttività, il quarto e ultimo elemento del Ciclo di valore IoT, si concentra sulla valorizzazione degli asset umani e di capitali per lavorare nella maniera più efficiente. Per ottenere questo risultato è necessario ottimizzare l'uptime, ridurre il downtime, semplificare i processi di vendita e supporto, gestire al meglio i clienti e il personale, migliorare la gestione degli asset e la velocità effettiva dei processi, nonché reagire più prontamente alle richieste e ai cambiamenti. La domanda "Sto sfruttando al meglio le conoscenze?" riguarda il modo in cui sfruttare il contesto e i dati IoT per migliorare l'efficienza.

Le esigenze di visibilità, sicurezza, redditività e produttività sono diverse per ogni singolo cliente, pertanto non esiste una soluzione IoT adatta a tutti, anche nell'ambito di una specifica verticale. Sottili differenze nei traguardi e obiettivi di un'azienda possono determinare esigenze diverse per la soluzione necessaria per raggiungerli. Sebbene sia utile osservare le scelte della concorrenza, le soluzioni da loro adottate potrebbero non essere appropriate se i traguardi, gli obiettivi e i momenti di business non coincidono esattamente. Seguire l'esempio di un'azienda concorrente potrebbe non essere una scelta valida.

È possibile creare una sinergia tra obiettivi e architettura sovrapponendo il Ciclo di valore IoT alla Gerarchia strategica IoT (figura 3). Gli elementi Redditività e Produttività identificano le origini pertinenti di contesto e dati, mentre gli elementi Visibilità e Sicurezza indicano l'architettura e l'infrastruttura necessarie per attingere a tali origini.

Il miglior modo di visualizzare la sinergia è tramite gli esempi. Nelle prossime sezioni esamineremo scenari di diversi mercati verticali, a cominciare dalla vendita al dettaglio, dopo un'attenta analisi della sicurezza.

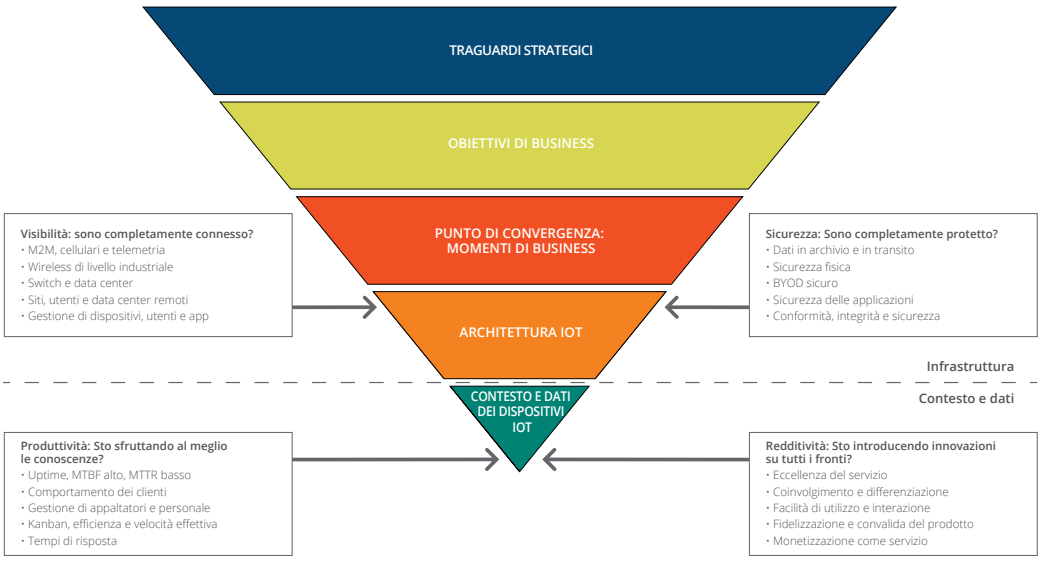


Figura 3: Sinergia tra gli obiettivi di business, l'architettura e il contesto/dati IoT

SICUREZZA SOTTO TUTTI I PUNTI DI VISTA

I casi di penetrazione nelle reti IoT e di violazione dei dati sono ormai all'ordine del giorno in ogni settore, ad esempio in ambito nucleare, vendita a dettaglio, sanitario e consumer. Le motivazioni sono abbastanza semplici: la maggior parte dei dispositivi e delle implementazioni IoT non è affidabile a causa dei livelli inadeguati di sicurezza adottati. Gli ingegneri che progettano i dispositivi IoT in genere sono esperti di affidabilità dei processi e architetture specifiche per un determinato ambito di applicazione. Queste competenze rientrano nella sfera della tecnologia operativa (OT), il cui scopo consiste nel migliorare l'affidabilità dei prodotti. L'esperienza nell'ambito della sicurezza informatica, d'altro canto, è prerogativa degli ingegneri informatici (IT). Se l'ambito OT e quello IT non collaborano alla progettazione di prodotti e sistemi, i risultati non possono essere affidabili.

Non è quindi prudente affidarsi a informazioni e processi IoT che possono essere manipolati intenzionalmente o accidentalmente. L'integrità e l'attendibilità delle informazioni che utilizziamo devono essere inattaccabili, pertanto è necessario garantirle end-to-end: a partire dai dispositivi IoT fino alle applicazioni che ne fanno uso. Per questo scopo è necessario incorporare funzionalità di sicurezza nei nuovi dispositivi IoT e avvolgere i dispositivi legacy in una bolla protettiva, in modo da creare un framework difensivo in cui nessun dispositivo o utente sia ritenuto affidabile finché ciò non sia stato provato. Il framework deve utilizzare informazioni sul contesto tratte da una moltitudine di origini al fine di valutare il comportamento di utenti e dispositivi per quanto concerne la sicurezza prima e dopo la loro connessione.

Il framework di sicurezza IoT Aruba, Connect-and-Protect, include i seguenti meccanismi protettivi:

- Autenticazione dei dispositivi di origine/destinazione e monitoraggio degli schemi di traffico, inclusi i bus e gli input dei sensori.
- Crittografia dei pacchetti di dati basata su standard commerciali e, quando possibile, governativi.
- Protezione dei pacchetti all'interno di un tunnel sicuro per garantirne il transito solo verso la destinazione prestabilita.
- Utilizzo di impronte digitali per i dispositivi IoT allo scopo di stabilire se sono attendibili, inaffidabili o sconosciuti, e conseguente applicazione di ruoli appropriati e policy basate sul contesto per controllare l'accesso e i servizi di rete.
- Analisi del traffico da nord a sud tramite i firewall per applicazioni e i sistemi di rilevamento malware per monitorare e gestire i comportamenti.
- Utilizzo dei sistemi di gestione della mobilità aziendale (EMM), di gestione delle applicazioni mobili (MAM) e di gestione dei dispositivi mobili (MDM) per monitorare i comportamenti e proteggere i dispositivi in caso di violazione delle policy.

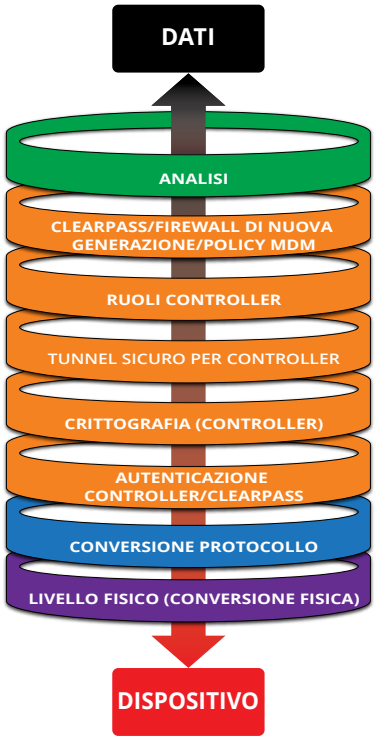


Figura 4: Meccanismi di sicurezza IoT Connect-and-Protect

Particolarmente importante è il ruolo svolto da Aruba ClearPass Policy Manager nella valutazione dei dispositivi IoT in base a creazione di profili, identità e situazione. La creazione di profili consente di rilevare le impronte digitali e classificare i dispositivi IoT nel momento in cui tentano di connettersi per poter differenziare i diversi tipi di dispositivi e individuare gli impostori. L'identità contrassegna i dispositivi IoT con un ruolo che determina i tempi e le modalità di connessione, indicando la posizione, l'orario, la data e la situazione corrente in merito alla sicurezza, allo scopo di fornire un controllo degli accessi basato sui ruoli più dettagliati. La situazione viene valutata in base a una serie di controlli dell'integrità per determinare vulnerabilità note, porte attive, versione del sistema operativo e sicurezza SNMP tra altri aspetti, e deve essere verificata periodicamente per garantire la conformità. Qualora la situazione dovesse risultare inferiore agli standard, ai dispositivi attendibili potrebbe essere impedito l'accesso.

ClearPass utilizza i profili, l'identità e la situazione per identificare i dispositivi IoT come attendibili, inaffidabili o sconosciuti e agire di conseguenza. Creando dei profili per i dati si evidenzia se un dispositivo cambia il normale funzionamento o simula il comportamento di un altro dispositivo IoT, di conseguenza ClearPass modificherà automaticamente i privilegi di autorizzazione del dispositivo. Ad esempio, se un controllore a logica programmabile (PLC) tenta di simulare il comportamento di un PC Windows, l'accesso alla rete verrà immediatamente negato.

Le policy sono efficaci solo se lo sono anche le informazioni utilizzate per definirle e gli strumenti esecutivi a disposizione per proteggerle. L'applicazione di un approccio a livello di sistema alla sicurezza contribuisce a identificare i vettori di minacce per l'IoT e le tecnologie di sicurezza necessarie per porvi rimedio.

Lo scopo ultimo dell'IoT è di consentire la trasformazione delle aziende attraverso lo sfruttamento delle preziose origini di dati racchiuse all'interno dei dispositivi IoT. Progettando appositamente le misure di sicurezza appropriate, è possibile garantire l'attendibilità dell'intera soluzione IoT. L'attenzione potrà quindi essere orientata nuovamente sui traguardi strategici basandosi sulla comprovata architettura IoT. Esaminiamo ora alcuni esempi del funzionamento di questo processo di allineamento.

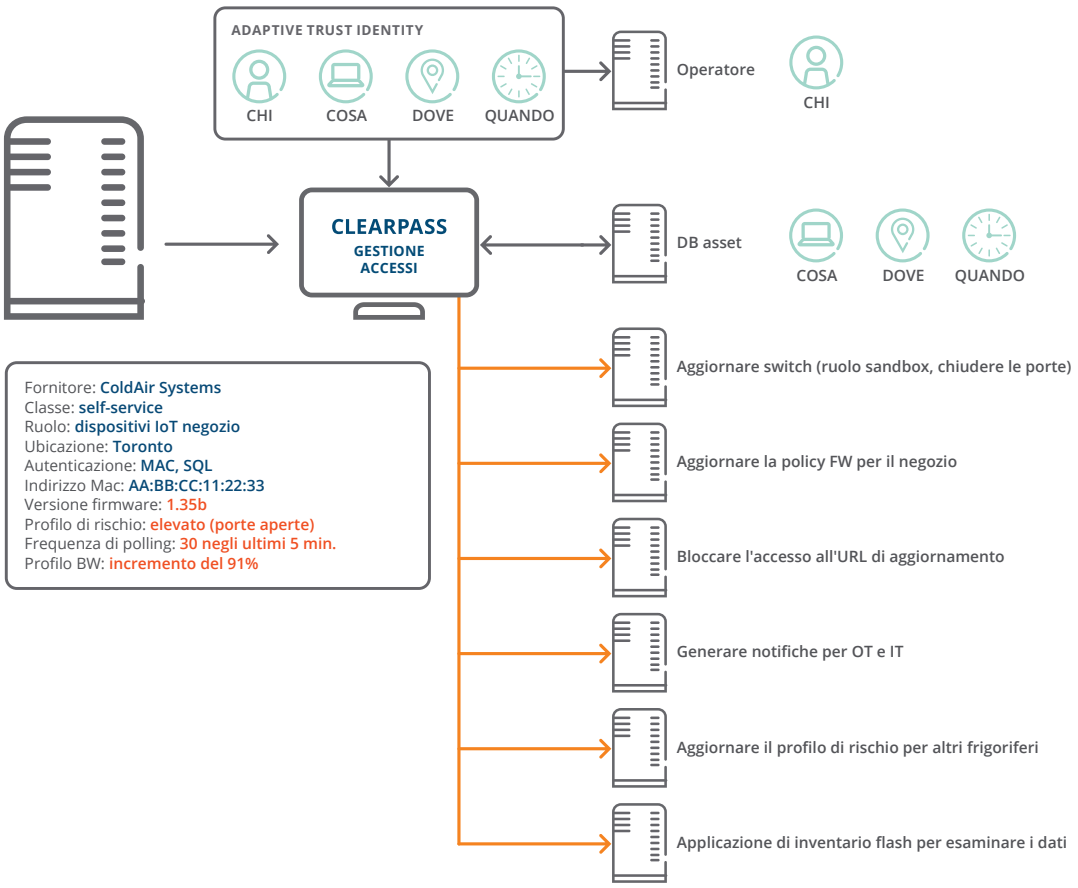


Figura 5: Flusso di lavoro in caso di violazione della sicurezza dei dispositivi IoT ClearPass

ORIENTAMENTO VERTICALE: VENDITA AL DETTAGLIO

Un superstore si prefigge per l'anno prossimo di incrementare le entrate del 10% e dimezzare il tasso di abbandono del negozio per raggiungere il suo target di fatturato. Per raggiungere questi traguardi è necessaria un'esperienza clienti più coinvolgente che si realizza tramite una serie di obiettivi. Innanzitutto, ai clienti devono essere proposti prodotti pertinenti, facilmente accessibili e con prezzi alla loro portata affinché non abbandonino il negozio per frustrazione. Inoltre, i clienti che usano il negozio solo per controllare i prezzi e osservare da vicino i prodotti che successivamente intendono acquistare online (showrooming) devono essere convinti ad acquistare nel negozio stesso e questo richiede un intervento attivo. Infine, i clienti che non riescono a trovare gli articoli desiderati devono essere serviti rapidamente affinché non lascino il negozio, pertanto è necessaria un'attenta gestione del rapporto clienti-commessi.

Poiché i clienti, i commessi e l'inventario sono mobili, i servizi basati sulla posizione IoT, che devono funzionare in sinergia con le applicazioni CRM del backend, del punto vendita e dell'inventario, rappresentano gli strumenti più appropriati allo scopo. I servizi basati sulla posizione consentono di rispondere a una o più delle seguenti domande:

- "Dove mi trovo?"
- "Dove sono?"
- "Dov'è?"

Per questa applicazione di vendita al dettaglio dobbiamo raggiungere i seguenti obiettivi di business:

- Identificare i clienti preesistenti che entrano in negozio, in modo che il rivenditore possa analizzare i comportamenti di acquisto passati e sul Web per promuovere offerte in tempo reale che possono risultare interessanti durante la loro visita in negozio.
- Consentire ai clienti di eseguire ricerche in inventario tramite i propri smartphone e di ricevere indicazioni passo passo per identificare gli articoli in magazzino o articoli sostitutivi utilizzando un percorso che ottimizzi le opportunità di upselling per incrementare le vendite.
- Fornire l'accesso gratuito al Wi-Fi in modo che i clienti possano navigare sul Web e i rivenditori possano vedere quali applicazioni vengono utilizzate dai clienti e dove le usano. Ad esempio, in risposta all'attività di showrooming, il rivenditore aggiornerà i display elettronici e invierà messaggi push relativi alla concorrenzialità dei prezzi rispetto a Internet. Anche al personale del negozio verranno notificate le informazioni pertinenti in modo da avere maggiori possibilità di convincere il cliente ad acquistare nel negozio.
- Monitorare la posizione e il rapporto tra clienti e commessi, in modo che non restino sprovviste parti del negozio.

Dopo aver definito gli obiettivi di business, passiamo alla scelta degli strumenti IoT appropriati. Nella tabella seguente è illustrata la gamma di opzioni per i servizi basati sulla posizione IoT di Aruba. La scelta della soluzione inizia dall'alto rispondendo alle domande di primo livello e termina in basso con la raccomandazione di uno specifico strumento IoT.

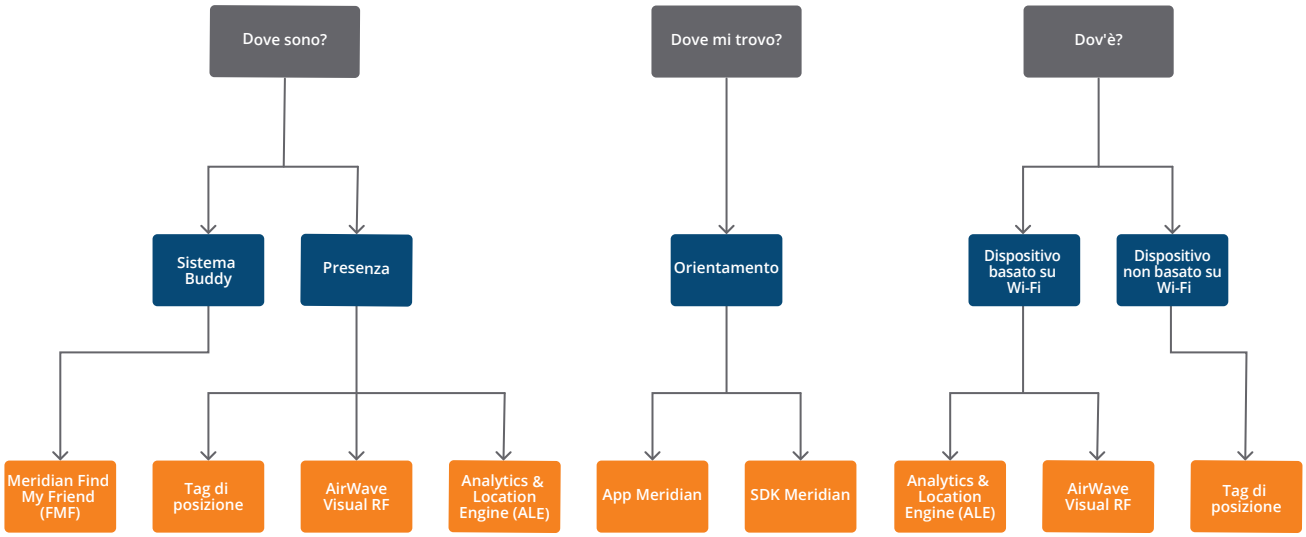


Figura 6: Opzioni di servizi basati sulla posizione

Sono necessari quattro diversi tipi di strumenti basati sulla posizione per realizzare gli obiettivi di business identificati:

- Orientamento (Wayfinding): un'app che aiuta i clienti a esplorare autonomamente un sito con servizi interni simili al GPS, invia avvisi quando attraversano un confine definito tramite geofence e fornisce messaggi push diretti al cliente.
- Informazioni sulla presenza: determinano quali clienti sono presenti, cosa fanno online e quando attraversano un confine definito tramite geofence.
- Sistema Buddy (Buddy System): individua la posizione dei commessi in ogni area del negozio.
- Individuazione asset non basata sul Wi-Fi: identifica la posizione degli asset, dei pallet e della merce.

Il livello più elevato di coinvolgimento del cliente si ottiene tramite l'interazione diretta che è in grado di cambiare il comportamento in tempo reale, ad esempio un'applicazione eseguita sullo smartphone o sul tablet del cliente che consente di fornirgli direttamente gli strumenti di orientamento, messaggistica push e geofencing. Il servizio Aruba Meridian offre questi tre servizi essenziali in un'unica app. La soluzione fornisce un'esperienza di orientamento analoga all'uso di GPS per interno, guida i clienti con indicazioni passo-passo e indica la posizione in tempo reale su una mappa. La funzionalità Find A Friend di Meridian consente ai responsabili del negozio di osservare direttamente la posizione dei commessi. Il geofencing può attivare azioni e applicazioni in base alla posizione.

Meridian può interfacciarsi con applicazioni di gestione delle relazioni con i clienti (CRM), per punti vendita (PoS) e di altre applicazioni backend, nonché con motori di regole aziendali per implementare complesse elaborazioni di condizioni Booleane. Una funzionalità di messaggistica push propone feedback, offerte e aggiornamenti istantanei. Se il rivenditore dispone già di un'app, l'SDK Meridian può invece fornire gli stessi servizi all'app preesistente.

Passare dall'orientamento al rilevamento dello showrooming non è semplice, poiché è necessario sapere quando un cliente utilizza un servizio di acquisti online, come Amazon. Aruba Analytics & Location Engine (ALE) calcola la posizione sull'asse x/y di tutte le persone presenti nel negozio che hanno un dispositivo abilitato al Wi-Fi e aderiscono, quindi monitora il comportamento di consultazione degli URL sulla rete Wi-Fi.
Se utilizzato insieme a un motore di analisi backend, ALE può aiutare i rivenditori a identificare l'attività di showrooming e convertire più opportunità in vendite del negozio.

Il monitoraggio sull'asse x/y di ALE può anche essere utilizzato con applicazioni backend o cloud per monitorare il rapporto tra clienti e commessi. Quando il rapporto scende al di sotto di un livello minimo accettabile può essere inviata una notifica sia ai commessi che al responsabile del negozio. L'elaborazione della posizione condotta da ALE ha un ulteriore vantaggio collaterale, infatti può monitorare i clienti che passano davanti al negozio senza entrare rispetto a quelli che entrano, in modo da poter valutare quale percentuale del traffico pedonale entra nel negozio.

La figura 5 mostra in che modo i traguardi strategici del rivenditore confluiscono nei momenti di business e come vengono gestiti tali momenti tramite l'infrastruttura IoT e i dati dei dispositivi definiti in modo specifico per lo scopo. In questo esempio viene illustrato come passare da un traguardo di livello elevato a uno specifico set di strumenti IoT che garantisca momenti di business efficaci.

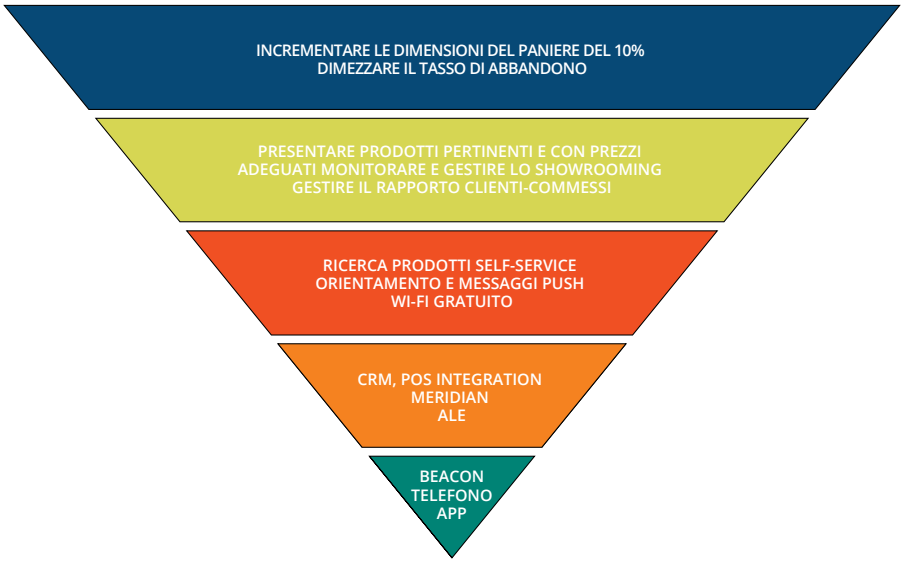


Figura 7: Allineamento dell'infrastruttura IoT ai traguardi strategici del rivenditore

I progetti IoT deviano dal percorso ottimale quando i traguardi e gli strumenti non sono allineati. Ad esempio, se ci si limita a rilevare passivamente la posizione dei clienti tramite l'analisi della presenza, si ottiene una visione inversa del comportamento dei clienti, ovvero si individuano in punti in cui è stato il cliente, ma non è possibile modificarne il comportamento in tempo reale. Molti progetti di analisi della presenza sono stati avviati perché facilmente implementabili nell'infrastruttura Wi-Fi esistente, ma successivamente sono falliti poiché non era possibile convertire i dati di analisi della presenza in vendite. Il concetto è chiaro: occorre accertarsi che la soluzione IoT e gli obiettivi di business siano perfettamente allineati prima di imbarcarsi in un progetto IoT.

ORIENTAMENTO VERTICALE: SETTORE SANITARIO

Passiamo a esaminare un esempio nel settore sanitario che si avvale di alcuni dei servizi basati sulla posizione illustrati nello scenario della vendita al dettaglio. Un'azienda sanitaria gestita a cui fanno capo numerosi ospedali e cliniche desidera incrementare il numero delle visite fatturabili del 10% per l'anno successivo senza ampliare gli immobili, assumere personale o pagare straordinari. Dai sondaggi condotti tra pazienti e personale per rilevare il livello di soddisfazione emerge che non è possibile ridurre la durata degli appuntamenti poiché il tempo dedicato alla visita di ogni paziente è già a stento accettabile. Gli stessi sondaggi evidenziano la frustrazione di pazienti e personale per quanto riguarda gli orari degli appuntamenti non rispettati. I pazienti sono arrabbiati a causa della difficoltà di muoversi all'interno di strutture troppo vaste, mappe del sito difficili da interpretare da parte dei pazienti anziani e da quelli che non conoscono la lingua, nonché dal cambiamento di sede della visita il giorno stesso senza aver ricevuto alcun preavviso. Il personale e i medici sono frustrati perché agli appuntamenti del mattino i pazienti spesso non si presentano o arrivano in ritardo, generando così lunghe attese che si protraggono oltre il turno previsto, e malcontento fra i pazienti che si vedono costretti a riprenotare l'appuntamento per un altro giorno.

Per raggiungere il traguardo aziendale è necessaria una soluzione più efficiente che consenta a tutti i pazienti, indipendentemente dalla loro lingua madre, di muoversi agevolmente all'interno delle strutture in modo che ogni appuntamento si svolga con puntualità, evitando recuperi a fine giornata. Nell'ambito delle domande sulla posizione "Dove mi trovo?", "Dove sono?" e "Dov'è?", gli obiettivi target includono:

- All'arrivo alla clinica inviare un messaggio a ogni paziente, nella sua lingua di origine, in merito all'orario dell'appuntamento e al numero esatto dell'ambulatorio.
- Inviare un messaggio aggiornato qualora sia stato modificato il luogo o l'orario dell'appuntamento.
- Fornire indicazioni passo passo e il tempo necessario per arrivare all'appuntamento successivo, che tenga conto dell'ingresso o del parcheggio da cui il paziente accede alla struttura.
- Offrire la stessa messaggistica push e funzionalità di orientamento ai medici e al personale esterno o temporaneo, in modo che possa raggiungere facilmente il luogo del successivo appuntamento.
- Consentire al personale di individuare la posizione dei pazienti mentre si muovono all'interno della struttura in modo da poterli contattare telefonicamente in caso di ritardo.

Sono necessarie tre diverse categorie di strumenti per realizzare questi obiettivi:

- Un'app di orientamento che aiuti i pazienti, il personale e i medici a muoversi autonomamente all'interno della struttura, grazie a indicazioni fornite nella lingua preferita.
- Funzionalità di geofencing che si attivino quando un paziente entra nella struttura e interagiscano con il sistema di pianificazione degli appuntamenti per inviare un messaggio di benvenuto in cui sia indicato il luogo e l'orario dell'appuntamento.
- Servizi di localizzazione delle persone che consenta al personale di trovare i pazienti e i medici esterni che sono in ritardo per gli appuntamenti.

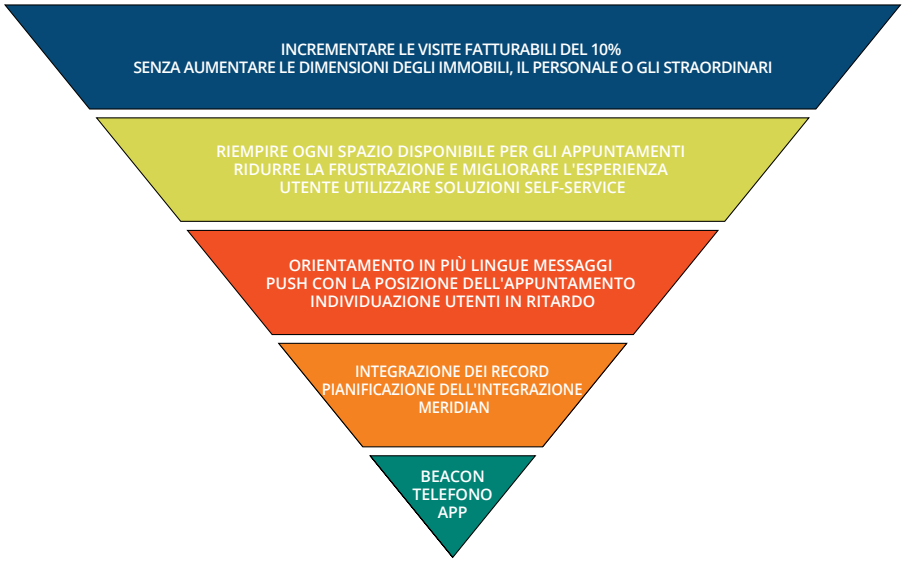


Figura 8: Allineamento dell'infrastruttura IoT ai traguardi strategici dell'azienda sanitaria

Il servizio Aruba Meridian, descritto in precedenza, funziona sia su rete mobile che tramite Wi-Fi, quindi può essere offerto nei parcheggi e nelle aree esterne in cui può mancare la copertura mobile e/o Wi-Fi. Poiché Meridian è indipendente dalla rete Wi-Fi, può funzionare sia su sistemi Wi-Fi Aruba che di altro tipo.

Questa soluzione deve essere integrata con i sistemi di gestione dei dati sui pazienti, della contabilità e del personale. Sebbene tutto ciò richieda uno sforzo notevole al momento dell'implementazione, la soluzione può fungere da piattaforma per una serie di servizi che possono essere aggiunti in seguito, ad esempio per ottimizzare i tempi e gli spostamenti, o per utilizzare le proprietà immobiliari e segnalare parcheggi pieni o disponibili.

D'altra parte, se si perdono di vista gli obiettivi è possibile che si scelgano fornitori non provvisti di soluzioni ottimali. Ad esempio, utilizzare i servizi basati sulla posizione per generare e-mail o SMS potrebbe non essere altrettanto efficace, e potrebbero non essere ricevuti in tempo, rispetto a un'app di orientamento in tempo reale. Per supportare mappe in più lingue può essere necessario un maggiore impegno di configurazione iniziale, ma è possibile garantire che i pazienti e chi li assiste siano in grado di selezionare la lingua che preferiscono. Infine, aggiornando il personale in tempo reale si ottimizza la pianificazione degli appuntamenti o la possibilità di trovare i pazienti che cercano di orientarsi, con il minimo sforzo.

ORIENTAMENTO VERTICALE: PETROLIO E GAS

Passeremo ora a un esempio di IoT industriale che sfrutta sia i servizi basati sulla posizione che l'analisi edge. Durante il prossimo anno fiscale una compagnia petrolifera che dispone di 25.000 pompe di estrazione e 15.000 appaltatori intende ridurre il downtime delle pompe del 10%, abbassare i costi degli appaltatori del 10% senza incidere sulla produzione dei pozzi e ridurre gli ammanchi di pezzi di ricambio del 25% senza compromettere la produttività. La compagnia ha tentato, senza riuscirci, di allineare i programmi di manutenzione delle pompe a teoretiche percentuali di guasto delle stesse. Come risultato, sono aumentati i casi di inutilizzabilità delle pompe e, di conseguenza, si sono ridotti i profitti della produzione. Inoltre, la perdita, l'errata collocazione o il furto dei pezzi di ricambio delle pompe e delle tubature sta facendo lievitare i costi e incide sulla tempestiva riparazione delle apparecchiature. Non è chiaro chi sia responsabile degli ammanchi nell'inventario e se siano imputabili a furti o errata registrazione. Infine, associare manualmente le fatture per i servizi degli appaltatori alle effettive prestazioni in loco è complicato, in quanto il numero di appaltatori è elevato mentre il personale contabile è esiguo.

Per raggiungere gli obiettivi aziendali è necessario identificare un modo per monitorare le pompe in tempo reale e prevedere i guasti sulla base dell'osservazione di comportamenti anomali. Le pompe sono strumenti dotati di sensori e attuatori che forniscono input ai controlli locali a ciclo chiuso, ma i dati non vengono elaborati in altro modo. Considerato l'elevato numero di pompe in funzione e che i costi delle reti mobili WAN sono variabili, inoltrare i dati delle pompe per l'analisi in remoto risulterebbe troppo costoso. Molto più conveniente risulterebbe invece eseguire le analisi in locale presso le pompe di estrazione e notificare a un centro di monitoraggio solo i casi di comportamento anomalo. Se necessario, il centro di monitoraggio potrebbe richiedere ulteriori dati generati dai sensori, purché siano stati archiviati presso il sito in cui si trova la pompa. Il centro può inoltre analizzare i dati operativi cronologici rispetto ai database dei produttori della pompa allo scopo di determinare il modo migliore per affrontare l'anomalia.

Rilevando i tempi di arrivo e partenza degli appaltatori presso le pompe di estrazione e i cantieri logistici per poi condividere tali dati con le applicazioni contabili della compagnia, si consentirebbe il confronto diretto tra le ore da fatturare rispetto a quelle effettivamente trascorse in loco. La soluzione richiede un metodo automatizzato di reporting che non generi altri costi di manodopera legati ai processi manuali. È inoltre necessaria una modifica contrattuale che imponga la totale partecipazione di tutti gli appaltatori come requisito per ricevere il compenso per i propri servizi.

La stessa soluzione di monitoraggio utilizzata per gli appaltatori nelle sedi delle pompe può essere adottata anche per i cantieri logistici. Condividendo i dati basati sulla posizione con i sistemi di controllo degli accessi e di monitor a circuito chiuso sarebbe possibile collegare l'identità di un appaltatore a una sua visita in loco e agevolare l'identificazione di possibili sospettati in caso di ammanchi nell'inventario.

Gli obiettivi di business per la compagnia petrolifera includono:

- Consentire alle pompe di estrazione di elaborare dati analogici e digitali generati dai sistemi di controllo della pompa e di segnalare anomalie.
- Implementare un centro di monitoraggio remoto per gestire il sistema di raccolta dati su una vasta area geografica, eseguire meta-analisi sui dati delle pompe e integrare un'applicazione che esegue analisi predittive sfruttando dati cronologici sui guasti.
- Imporre a tutti gli appaltatori l'uso di un'app di servizi basati sulla posizione per segnalare il loro arrivo (e partenza) presso la pompa o il cantiere logistico. Poiché gli appaltatori sono agenti indipendenti, per motivi di privacy le applicazioni devono essere attivate esclusivamente all'arrivo e alla partenza dalle strutture della compagnia petrolifera. Non è infatti accettabile adoperare strumenti di tracciamento GPS sempre disponibili.

Sono necessarie diverse categorie di strumenti per realizzare questi obiettivi:

- Gateway che acquisiscano i dati dei sensori e degli attuatori dalle pompe di estrazione, eseguano applicazioni di analisi per elaborare i dati e forniscano una rete WAN per comunicare i risultati a una postazione di monitoraggio remota.
- Un sistema di monitoraggio remoto che gestisca la rete WAN, esegua analisi sui dati aggregati e si interfacci con altri repository di dati, ad esempio la cronologia delle manutenzioni e i database del produttore.
- Funzionalità di geofencing che attivino un'app sugli smartphone o i tablet degli appaltatori quando arrivano o lasciano la pompa o le sedi logistiche.
- Interfacce per applicazioni di controlli degli accessi e videosorveglianza tramite le quali sia possibile scambiare i dati di identificazione degli appaltatori e di registrazione di data/ora ogni volta che un appaltatore entra o esce da un sito. Se un appaltatore non è autorizzato ad accedere a una struttura, il sistema di controllo degli accessi negherà l'accesso.

Per prevedere i problemi a un livello elevato, sono necessari alcuni fattori base che possono essere combinati per soddisfare diversi requisiti di implementazione: il dispositivo IoT intelligente, il dispositivo di accesso, il mezzo di comunicazione, il controller IoT, l'applicazione aziendale e di analisi IoT e gli strumenti di gestione del sistema.

Il dispositivo IoT intelligente è una macchina, in questo caso una pompa di estrazione, che genera dati di rete analogici, digitali e/o di controllo che l'azienda vuole esaminare.

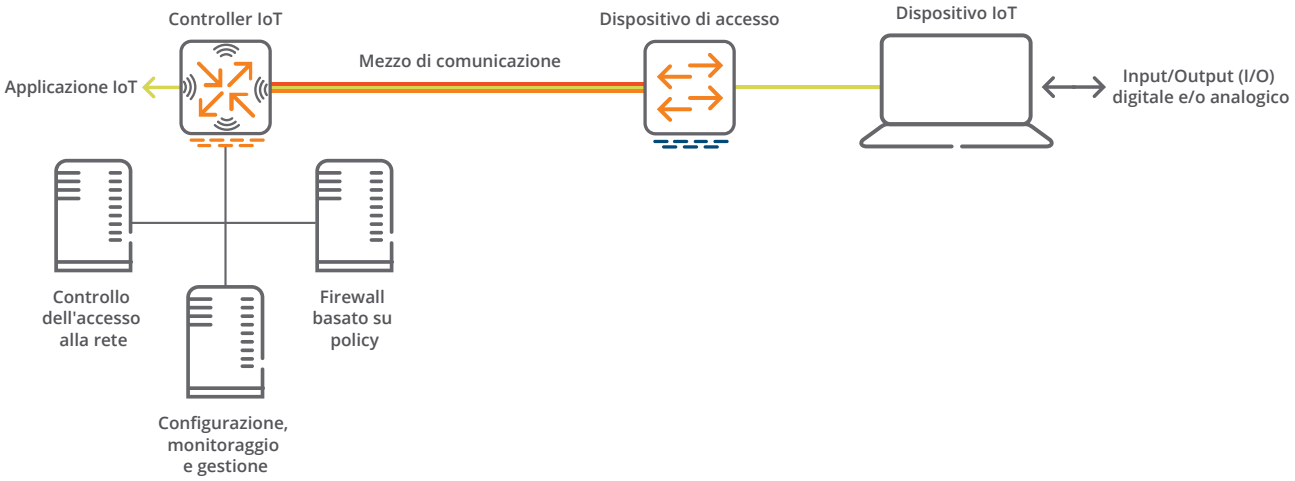


Figura 9: Fattori base del monitoraggio per prevedere i problemi

Il dispositivo di accesso si interfaccia con il dispositivo IoT, immette i dati e quindi interviene in locale e/o invia i dati al controller IoT presso il sito di monitoraggio remoto.

Esistono due tipi di dispositivi di accesso: Gateway e sistemi IoT convergenti. Un gateway converte i flussi di dati dai dispositivi IoT in un formato sicuro che sia compatibile con la rete in uso. I gateway vengono utilizzati quando un dispositivo IoT non è in grado di comunicare in modo affidabile con una rete (LAN, mobile, Wi-Fi), non può eseguire un client VPN locale per l'accesso remoto sicuro oppure dispone di input/output (I/O) seriali, analogici o proprietari che sono incompatibili con la rete WAN.

Figura 10: Dispositivo di accesso Aruba Edgeline Gateway

Un dispositivo IoT convergente dispone di interfacce I/O e della capacità di elaborazione necessaria per analizzare in locale i dati provenienti dai dispositivi IoT. Questa soluzione viene utilizzata per limitare la latenza dei processi, ridurre il volume e il costo del traffico delle comunicazioni di dati nelle WAN, elaborare e archiviare l'attività IoT locale, e/o inviare a un data center remoto un riepilogo di tale attività. I dispositivi IoT convergenti svolgono queste attività eseguendo in locale motori di apprendimento automatico e analisi dei dati, inoltre sono caratterizzati da potenti motori di elaborazione, dalla capacità di acquisire dati generati dai sensori in formato analogico/digitale e il traffico del bus di controllo, nonché di capacità di gestione remota.

Figura 11: Dispositivi convergenti Aruba di accesso ai sistemi IoT

Nel caso della compagnia petrolifera, un sistema IoT convergente è il dispositivo di accesso più appropriato poiché sono necessarie informazioni dettagliate locali per ridurre al minimo le spese della rete WAN. Il sistema utilizzerà la telefonia mobile quale mezzo di comunicazione per ridurre i tempi di implementazione e poiché i sistemi cellulari in genere sono resilienti in caso di indisponibilità di un singolo ripetitore.

I costi della telefonia mobile verranno affrontati tramite il servizio Hewlett Packard Enterprise Mobile Virtual Network Operator (MVNO) che usufruisce di vantaggiose tariffe su abbonamento prestabilite per le applicazioni IoT a ridotta larghezza di banda, quali le applicazioni di monitoraggio delle macchine. La pre-elaborazione dei dati IoT in loco tramite un sistema IoT convergente che si avvale di software di analisi ridurrà notevolmente il volume e i costi delle comunicazioni mobili.

La VPN Aruba VIA crittograferà i dati e li trasmetterà tramite tunnel tra le pompe di estrazione e il centro di monitoraggio. VIA supporta la crittografia AES con chiave a 256+ bit e offre autenticazione peer a livello della rete, autenticazione delle origini dati, integrità dei dati e protezione della replica. Per le applicazioni IoT governative, VIA è anche disponibile con la crittografia basata su curve ellittiche per la Suite B per proteggere le informazioni divulgabili fino al livello di classificazione Top Secret.

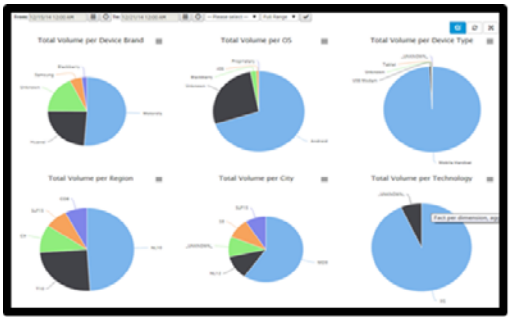
La VPN VIA terminerà con il controller IoT presso il data center della compagnia petrolifera. Il controller gestisce la crittografia e l'autenticazione della rete, e si interfaccia con il firewall, il controllo dell'accesso di rete e le applicazioni di gestione delle policy che applicano la sicurezza a livello delle applicazioni, l'assegnazione di priorità ai pacchetti e le regole di accesso. Le istanze software del controller possono essere utilizzate al posto dei controller hardware per le applicazioni cloud pubbliche e private.

Figura 12: Controller Aruba

Le applicazioni di analisi possono essere eseguite sia nei sistemi IoT convergenti che nei sistemi di monitoraggio e sfruttano i dati IoT oltre a modelli matematici, statistici, di apprendimento automatico e/o di previsione per evidenziare comportamenti anomali e prevedere problemi attraverso lo studio approfondito dei pool di dati forniti dai fornitori delle pompe, dai record di servizio interni e anche da altri siti dell'azienda. Alcuni esempi di applicazioni includono HPE Vertica, SAP HANA, GE Predix e Schneider Wonderware.

I siti delle pompe di estrazione vengono monitorati tramite l'applicazione HPE Universal IoT Platform (UIoT), un'efficace suite di applicazioni che include una gamma di servizi specializzati per il monitoraggio dei dispositivi IoT. I servizi includono:

- API che consentono alle applicazioni client di sfruttare i dati.
- Servizi digitali attraverso i quali è possibile introdurre rapidamente nuove applicazioni, micro-servizi e algoritmi.
- Acquisizione di dati da gateway Aruba e piattaforme IoT convergenti, nonché da protocolli IoT tramite brokering di messaggi open source.
- Gestione dell'infrastruttura mobile.
- Analisi predittiva efficace con algoritmi predefiniti e modelli pronti all'uso.
- Allineamento agli standard oneM2M o di strutture dati equivalenti e librerie di protocolli incorporate per i protocolli di controllo di uso comune.
- Accodamento messaggi tramite bus di messaggistica basati su standard aperti, che include la gestione di dispositivi e abbonamenti.



FEATURES	CORE BASELINE	OPTION	MODULE
Managing devices and services	Yes		DSM
Uplink and downlink data acquisition	Yes		NIP
Data acquisition and validation	Yes		DAV
APIs exposure	Yes		SGF PRM
Advanced dashboard	Yes		Console
Relational database	Yes		EDB
Dashboard designer		Yes	Console designer
Analytic columnar database		Yes	Vertica
Alarms handling and correlation		Yes	TeMIP/UCA
Micro service design and execution		Yes	SIS

Figura 13: Sistema di monitoraggio dei dispositivi IoT UIoT

UIoT allinea il supporto dei dispositivi IoT allo standard di settore oneM2M e supporta un'ampia gamma di applicazioni e processi IoT È possibile creare rapidamente istanze delle nuove applicazioni su vasta scala, incluso il rilevamento dei dispositivi, la configurazione e il controllo del traffico IoT (escluso il traffico voce e dati tradizionale) sulla stessa piattaforma cloud privata o ibrida.

Analogamente alla piattaforma Meridian, UIoT può fungere da base per svariati servizi a valore aggiunto, oltre quelli necessari per soddisfare i traguardi strategici correnti. UIoT supporta innovative applicazioni mobili di telematica, si interfaccia con i sistemi wireless LoRa e Sigfox ad ampio raggio e dispone di un'ampia gamma di API utilizzabili per interfacciarsi con altre applicazioni di monitoraggio, reporting e auditing.

È possibile fornire servizi basati sulla posizione per appaltatori attraverso i servizi di geofencing e di messaggistica push Aruba Meridian. Le pompe di estrazione e i siti logistici che dispongono di Aruba BLE Beacon stabiliscono dei confini di geofencing intorno alle aree di manutenzione e stoccaggio delle pompe. Le dimensioni dell'area di geofencing saranno adattate alle esigenze delle singole situazioni. Quando lo smartphone o il tablet di un appaltatore attraversa il confine di geofencing, una notifica viene inviata all'app di contabilità indicando l'identità, l'ora e la posizione del trigger di geofencing. Anche all'appaltatore può essere inviato un messaggio per verificare che Meridian abbia correttamente registrato l'attività. Imponendo agli appaltatori l'uso dell'app Meridian per ricevere il compenso per i servizi resi, la compagnia petrolifera può garantire un elevato tasso di conformità.

Meridian include API che consentono di condividere i dati basati sulla posizione con altre posizioni, ad esempio i flussi di lavoro contabili, di controllo degli accessi e di videosorveglianza. Grazie a questa capacità è possibile utilizzare gli stessi Beacon e le app presso le pompe di estrazione ed attivare sistemi di protezione presso le strutture logistiche in modo che i prelievi e le consegne possano essere correlate all'accesso con badge e ai dati di videosorveglianza. Se gli ammanchi in inventario sono associati all'attività di un appaltatore, l'identificazione degli appaltatori sarà un componente essenziale per gestire la sicurezza.

Questo esempio dimostra in che modo la compagnia petrolifera può passare da traguardi di altro livello che mirano all'uptime delle pompe, alla gestione del costo degli appaltatori e alla riduzione degli ammanchi a un set specifico di strumenti IoT di analisi, reporting e servizi basati sulla posizione che soddisfino questi traguardi.

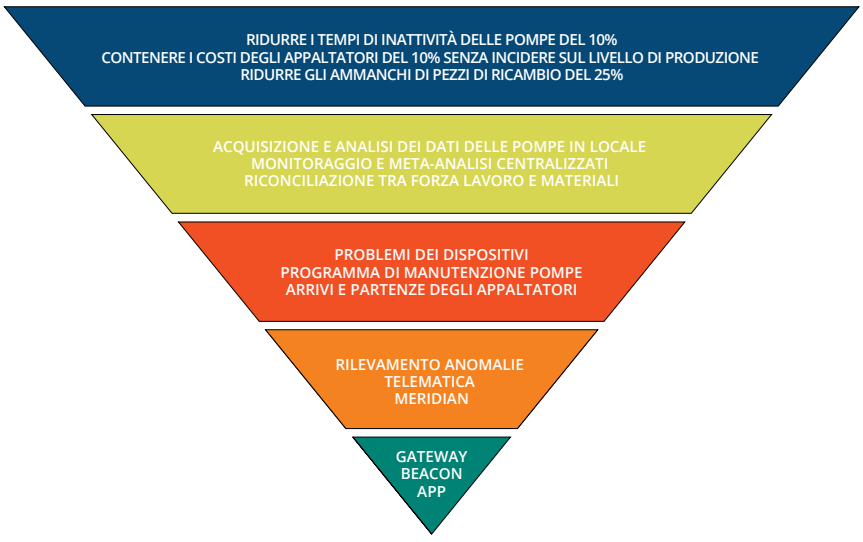


Figura 14: Allineamento dell'infrastruttura IoT ai traguardi strategici della compagnia petrolifera

IL PRIMO PASSO NEL PROCESSO DI TRASFORMAZIONE DELL'IoT

Gli strumenti IoT devono essere scalabili ed flessibili in modo da poter fungere da piattaforma per affrontare gli obiettivi di business futuri. In tutti i casi discussi in precedenza, le soluzioni Aruba e UIoT sono altamente scalabili e flessibili, pertanto sono adatte a gestire un'ampia gamma di use case.

Le difficoltà tecniche associate alla creazione di una sinergia tra obiettivi di business e l'architettura IoT possono essere risolte più facilmente rispetto agli ostacoli politici legati al raggiungimento di un allineamento all'interno di un'organizzazione. Gli impegni esistenti e i progetti in corso possono catalizzare diverse interpretazioni dei traguardi strategici o degli obiettivi di business che rendono difficile l'allineamento di altri gruppi alla loro interpretazione. I soggetti coinvolti di diverse business unit possono contendersi il controllo dei progetti e dei programmi, minacciando di ritirare il supporto o i finanziamenti qualora la propria visione non venisse implementata.

Per raggiungere i nuovi livelli di collaborazione necessari nelle organizzazioni di gestione, produzione, progettazione, IT e operazioni, può essere necessario l'intervento di una terza parte neutra. Per questo scopo l'organizzazione HPE Technical Services Consulting ha realizzato uno specifico workshop IoT per aiutare a definire una visione unitaria per i progetti IoT, creare armonia tra i diversi soggetti coinvolti e identificare obiettivi strategici e traguardi di facile attuazione. Per ulteriori informazioni, vedere https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-7269ENW.pdf.

CONCLUSIONE

L'obiettivo principale dell'IoT consiste nel far convergere i traguardi strategici dell'azienda con il contesto e i dati IoT pertinenti per garantire momenti di business efficaci. Per essere efficace, un momento di business deve essere orchestrato attentamente per sfruttare dinamicamente le opportunità contingenti relative ai clienti, e in tal senso il contesto e i dati IoT hanno un ruolo fondamentale per contribuire a migliorare il comportamento, l'atteggiamento e/o l'opinione dei clienti rispetto all'azienda.

La sequenza di fattori che collega il contesto e i dati IoT pertinenti all'architettura IoT deve essere adeguatamente realizzata. In questo white paper è stato illustrato come creare una sinergia tra gli elementi della gerarchia IoT, estraendo il contesto e i dati pertinenti dai dispositivi IoT e quindi implementando un'architettura appropriata per sfruttarli. La preparazione accurata, la definizione degli obiettivi e la selezione degli strumenti saranno efficaci se affiancati all'allineamento dell'organizzazione sui traguardi e gli obiettivi. Dopo aver provveduto a questi aspetti, anche gli obiettivi di business più ardui potranno essere realizzati.

RIFERIMENTI

1. William H. Markle, "The Manufacturing Manager's Skills" in *The Manufacturing Man and His Job* di Robert E. Finley e Henry R. Ziobro, American Management Association, Inc., New York 1966
2. C. R. Jaccard, "Objectives and Philosophy of Public Affairs Education" in *Increasing Understanding of Public Problems and Policies: A Group Study of Four Topics in the Farm Foundation*, Chicago, Illinois 1956
3. Alfonso Velosa, W. Roy Schulte, Benoit J. Lheureux, *Hype Cycle for the Internet of Things*, 2016, Gartner, 14 luglio 2016
4. Un momento di business è una serie transitoria di interazioni sensibili al contesto tra persone, business e cose che porta a un risultato negoziato anziché a un risultato predeterminato, ovvero un'offerta personalizzata e mirata di un rivenditore in base al luogo, al tempo e ai dati CRM. Vedere Frank Buytendijk, *Digital Connectivism Tenet 4: We Do Not Differentiate Between People and Things*, Gartner, 1 novembre 2016
5. Dale Kutnick and Saul Brand, *Exploit Enterprise Architecture to Guide IoT Deployments at Scale*, Gartner, 15 dicembre 2016

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com WP_InternetOfRelevantThings_011817