



Colmare il divario tra l'IT e le Operation per una trasformazione digitale vincente

White paper

Alcatel•Lucent 
Enterprise

Indice

- | L'IoT favorisce la collaborazione tra l'IT e i team operativi
- | Nuovi casi d'uso e opportunità
- | Una visione condivisa e tecnologie di base
- | Il giusto partner tecnologico



L'IoT favorisce la collaborazione tra l'IT e i team operativi

Fino a poco tempo fa, in genere, aveva senso che i team IT e quelli operativi funzionassero come unità distinte all'interno delle aziende. I due mondi non si sovrapponevano. I team IT si focalizzavano sull'implementazione e la manutenzione dell'infrastruttura di rete dell'azienda e sul rafforzamento della sicurezza informatica, mentre i team Operativi ponevano più attenzione sulle attività quotidiane, come la gestione delle strutture e della produzione, le vendite, il marketing e la sicurezza degli edifici.

Ora che i team Operativi si affidano sempre più a soluzioni IoT per raggiungere i loro obiettivi e trasformare digitalmente l'azienda, c'è la necessità che i team collaborino tra loro e condividano le competenze. Le soluzioni IoT sono un modo per automatizzare e accelerare le operazioni per aumentare l'agilità e la continuità di business e migliorare l'esperienza del cliente. Queste soluzioni richiedono la connessione di centinaia o migliaia di nuovi dispositivi alla rete aziendale, attività che rientra nel dominio dell'IT.

Le aziende che abbattano i muri tra i vari team, incoraggiandoli a collaborare in modo naturale possono ridurre in misura significativa questi rischi, riuscendo anche a massimizzare i vantaggi che l'IoT e altre iniziative di trasformazione digitale apportano all'azienda.

White paper

Colmare il divario tra l'IT e le Operation per una trasformazione digitale vincente



Quando i team non collaborano, i rischi aumentano

I team IT e quelli Operativi che non sono a conoscenza delle reciproche attività o che non si coordinano e non collaborano, mettono a rischio le iniziative di trasformazione digitale e l'azienda da più punti di vista:

- **Sicurezza informatica.** Quando l'IT non è a conoscenza dei nuovi dispositivi IoT introdotti dai team operativi, non può assicurare che i dispositivi siano conformi alle policy di sicurezza aziendali. I dispositivi IoT sono dotati di livelli molto variabili di funzionalità di sicurezza informatica e potrebbero non offrire le ultime migliori pratiche di protezione. Questi dispositivi non autorizzati, cosiddetti "shadow IT", potrebbero eseguire qualsiasi software ed essere già infettati da virus e malware. Se non controllati, possono facilmente introdurre nuove vulnerabilità e vettori di attacco nella rete.
- **Efficienza finanziaria e operativa.** Quando i team IT e i team operativi implementano soluzioni tecnologiche senza confrontarsi, potrebbero comportare un raddoppiamento di costi e sforzi. Ad esempio, il personale del team operativo potrebbe acquistare una soluzione di monitoraggio e gestione dei dispositivi IoT, senza sapere che l'IT dispone già di una soluzione in grado di svolgere queste attività. Avere un'unica soluzione in grado di soddisfare le esigenze di entrambe i team è sempre l'opzione più conveniente ed efficiente dal punto di vista operativo.
- **Prestazioni e affidabilità.** I team IT sanno come ottimizzare e mettere a punto la rete aziendale per soddisfare requisiti specifici, come ad esempio la qualità del servizio (QoS) per implementazioni IoT. Se i team operativi non possono beneficiare di questa esperienza, si corre il rischio di implementare iniziative di trasformazione digitale critiche per l'azienda con elevate carenze in termini di prestazione e affidabilità della rete.



Nuovi casi d'uso e opportunità

Poiché i team IT e quelli Operativi hanno aree di interesse e competenze diverse, ogni gruppo fornisce capacità uniche e importanti. I team Operativi capiscono quali soluzioni IoT possono aiutare meglio l'azienda ad aumentare l'efficienza e a ridurre i costi. Le organizzazioni IT dispongono degli strumenti e del know-how necessari per automatizzare e semplificare ogni aspetto di tali soluzioni, dall'implementazione, dal monitoraggio, alla manutenzione, agli aggiornamenti: vantaggi che si moltiplicano con l'aumento delle implementazioni IoT.

Insieme, i team dispongono delle conoscenze, delle competenze e degli strumenti necessari alle aziende per sfruttare i nuovi casi d'uso e le opportunità che supportano il business ad avere successo. Allo stesso tempo, l'IT diventa una risorsa strategica fondamentale che aiuta il team Operation e l'azienda a raggiungere gli obiettivi finanziari e operativi.

Quando IT e team Operativi collaborano per mettere al servizio dell'azienda soluzioni IoT sicure, economiche e affidabili, le opportunità sono illimitate. Di seguito sono riportati solo alcuni esempi che possono essere facilmente adattati alle esigenze di diversi settori e organizzazioni.

Aumentare l'agilità e la reattività con comunicazioni in tempo reale

Le soluzioni IoT che collegano automaticamente persone e sistemi sulla base di eventi in tempo reale garantiscono elevata velocità alle operazioni di business.

Negli aeroporti, gli addetti ai bagagli possono essere avvisati dell'atterraggio degli aerei, per poter disporre i trasportatori a nastro e i veicoli di trasferimento. In caso di emergenza, la soluzione è in grado di connettere automaticamente il personale che si occupa della gestione dell'aeroporto, le squadre di sicurezza e il personale delle forze dell'ordine, consentendone il coordinamento per affrontare la situazione. Nelle scuole e nelle città, le notifiche in tempo reale permettono di sapere quando gli autobus stanno per arrivare e aiutano i funzionari a rispondere rapidamente a eventi imprevisti.

Ridurre i costi automatizzando le attività di routine

Molte aziende e strutture pubbliche si affidano ancora a ispezioni manuali, che richiedono molto tempo, per lo svolgimento di compiti banali, come controllare se i cestini della spazzatura sono pieni. Grazie a sensori che monitorano i livelli della spazzatura, l'operaio o il sistema di riferimento viene automaticamente avvisato quando ogni contenitore raggiunge la soglia predefinita. Non si sprecano tempo e denaro per ispezioni manuali, il personale addetto alla manutenzione può dedicare più tempo a compiti di maggior valore e i costi dei sacchi della spazzatura e dello smaltimento sono ridotti, poiché i cestini vengono svuotati solo quando necessario.

Aumentare l'efficienza con l'asset tracking

Conoscere in ogni momento la posizione precisa degli asset critici per l'azienda aiuta le persone a lavorare con maggiore efficienza ed efficacia.

Nei centri medici, la possibilità di individuare la posizione più vicina della bombola d'ossigeno, del carrello di emergenza, della sedia a rotelle e di altri apparecchi consente un'assistenza più tempestiva e ottimizza i flussi di lavoro. Negli aeroporti, la stessa tecnologia di asset tracking consente al personale di sapere dove si trovano le attrezzature di supporto a terra, come i rimorchiatori di spinta, i trasportatori di pallet e i veicoli per il catering, per accelerare i tempi di rotazione degli aerei.

Migliorare l'esperienza del cliente grazie a un viaggio senza intoppi

La tecnologia di localizzazione può essere utilizzata anche per migliorare il percorso end-to-end del cliente. Ad esempio, un ospedale può utilizzare i dati raccolti dai braccialetti dei pazienti abilitati all'IoT per analizzare il tempo trascorso dalle persone in ogni fase dell'assistenza, compresi i reparti di emergenza, i ricoveri, le sale d'attesa, la radiologia, le sale operatorie, il recupero, la fisioterapia e la dimissione. Si possono quindi utilizzare i dati per ottimizzare i processi e i flussi di lavoro e migliorare l'esperienza e la soddisfazione dei pazienti.

Negli aeroporti, la tecnologia di localizzazione avanzata può aiutare i viaggiatori a seguire i percorsi più efficienti attraverso i terminal più estesi. Con un'app che indica il percorso più veloce dalla posizione reale al gate, i passeggeri hanno molte meno probabilità di perdersi o di seguire un percorso lento e contorto che aumenta il rischio che il volo subisca ritardi.

Aumentare la resilienza monitorando i sistemi critici

Le soluzioni IoT sicure e affidabili sono il modo ideale per i fornitori di servizi e le aziende di monitorare in modo proattivo le prestazioni di infrastrutture e sistemi critici, come i sistemi di distribuzione di gas, acqua ed elettricità.

In questo tipo di soluzioni, i sensori inviano automaticamente avvisi quando vengono superate le soglie di indicatori di prestazioni chiave (KPI) quali temperatura, pressione, vibrazioni, coppia di torsione e umidità. Con una notifica immediata del degrado delle prestazioni, il personale addetto alla manutenzione può affrontare in modo proattivo i problemi per evitare danni alle apparecchiature, guasti e interruzioni del servizio.

White paper

Colmare il divario tra l'IT e le Operation per una trasformazione digitale vincente



Rafforzare la sostenibilità con soluzioni per edifici intelligenti

Le soluzioni per gli edifici intelligenti aiutano le aziende e le organizzazioni pubbliche a ottimizzare l'uso di energia e risorse, consentendo di raggiungere obiettivi ecologici e ridurre i costi operativi.

Esistono numerose soluzioni per edifici intelligenti che si basano su dispositivi IoT connessi, alcune delle più comuni includono soluzioni che automatizzano l'illuminazione, l'acqua e i sistemi di riscaldamento, ventilazione e condizionamento (HVAC) in base all'ora del giorno, ai livelli di domanda e alla presenza umana.

Ridurre l'inquinamento con soluzioni di traffico intelligente

Le città impegnate nella riduzione dell'inquinamento atmosferico adottano sempre più spesso soluzioni IoT per monitorare le emissioni dei veicoli lungo le strade più trafficate e agli incroci più congestionati. Possono quindi analizzare i dati raccolti e utilizzare le informazioni ottenute per apportare miglioramenti che le aiutino a snellire i flussi di traffico.

Le città intelligenti stanno anche sfruttando le tecnologie IoT per implementare soluzioni di parcheggio intelligenti grazie alle quali i cittadini possano trovare più velocemente il posto per l'auto e ridurre la congestione del traffico e le emissioni dei veicoli.

Migliorare la conformità grazie a una visibilità completa dei dispositivi

Infine, quando i team IT e quelli Operativi collaborano per implementare l'IoT e le tecnologie di rete di supporto, possono introdurre soluzioni che forniscono la visibilità e la gestione di tutti i dispositivi che accedono alla rete. Questa visione completa rende più facile dimostrare la conformità agli standard normativi, alle policy aziendali e alle migliori prassi in materia di sicurezza informatica. Dagli audit non emergono sorprese che destano preoccupazione. I dispositivi con firmware o patch di sicurezza non aggiornati vengono immediatamente identificati e il rischio di incorrere in sanzioni di settore è notevolmente ridotto.

White paper

Colmare il divario tra l'IT e le Operation per una trasformazione digitale vincente





Una visione condivisa e tecnologie di base

Ogni organizzazione si trova in una fase evolutiva e di trasformazione digitale differente, pertanto non esiste un unico approccio per intensificare la collaborazione tra i team IT e quelli Operativi. Sebbene alcune organizzazioni siano più avanti nel percorso di digitalizzazione rispetto ad altre, la maggior parte utilizza ancora una combinazione di tecnologie moderne e legacy che riflette la loro storia unica.

Indipendentemente dalla situazione in cui si trova un'azienda, ci sono argomenti e considerazioni sulla tecnologia che accomunano i team IT e Operativi che vogliono collaborare. Per valutare adeguatamente le diverse soluzioni IoT, i team dovrebbero confrontarsi partendo dai requisiti di rete e di sicurezza informatica, tra cui:

- I tipi di dispositivi che accederanno alla rete e il mezzo di connessione richiesto da ciascuno di essi, ad esempio via cavo o wireless, indoor o outdoor. Inoltre, occorre tenere conto di fattori ambientali quali calore estremo, freddo, vibrazioni, vento, pioggia, neve o ghiaccio.
- Le policy in materia di sicurezza informatica a cui ogni tipo di dispositivo deve attenersi e le applicazioni con cui ogni tipo di dispositivo può comunicare.
- Come le informazioni provenienti da ciascun tipo di dispositivo devono fondersi con quelle provenienti dalla rete e dai sistemi aziendali per garantire che le informazioni e i dati arrivino alle persone giuste al momento giusto.

Una volta definita la visione condivisa delle soluzioni IoT, è il momento di valutare le tecnologie necessarie per implementare con successo la visione.

Per molti team IT, i nuovi requisiti per supportare le elevate richieste di connettività IoT da parte di vari reparti possono sembrare eccessivi. Tuttavia, le principali soluzioni di rete oggi disponibili sono state progettate per supportare in modo sicuro e semplificare ogni aspetto delle maggiori strutture IoT. Con il giusto approccio all'infrastruttura di rete e alle piattaforme di gestione, i team IT possono passare dall'essere un potenziale ostacolo per l'implementazione dell'IoT a un fattore cruciale per l'azienda.



Le reti sicure e automatizzate semplificano l'implementazione dell'IoT

Le reti moderne rilevano automaticamente i nuovi dispositivi IoT e sono in grado di classificare e segmentare ogni tipo di dispositivo in base alle policy in materia di sicurezza informatica. Supportano inoltre un'architettura di rete basata sul principio "zero trust" (ZTNA) che stabilisce una "premessa di non fiducia" nei confronti di qualsiasi utente, dispositivo o applicazione, indipendentemente dalla sua ubicazione - in loco, nel cloud o fuori sede - per ridurre al minimo i rischi di sicurezza informatica. Le soluzioni di rete più avanzate supportano la macro e la microsegmentazione per consentire un approccio granulare alla sicurezza informatica:

- La macrosegmentazione suddivide gli utenti, i dispositivi e le applicazioni sulla rete in base al loro dominio funzionale. Ad esempio, la telefonia desktop e IP appartiene a un macrosegmento, mentre la videosorveglianza rientra in un macrosegmento diverso.
- La microsegmentazione definisce il modo in cui gli utenti, i dispositivi e le applicazioni all'interno di un macrosegmento possono interagire tra loro ed è in genere regolata da policy di sicurezza molto specifiche.

In un ospedale, un macrosegmento potrebbe essere dedicato alle apparecchiature mediche, come i monitor dei pazienti e a un gruppo specifico di utenti. Il macrosegmento può anche essere utilizzato per garantire che l'accesso alla rete sia fornito con specifici parametri di qualità del servizio (QoS) e di sicurezza. I sensori e i controlli per l'illuminazione e i sistemi

HVAC verrebbero mappati in un macrosegmento distinto, al pari delle tecnologie legate alla sicurezza, come le telecamere a circuito chiuso e i sistemi di chiusura delle porte. Con questo tipo di segmentazione, un termostato compromesso non sarebbe in grado di comunicare con un monitor del paziente o con un sistema di serrature.

La microsegmentazione regola le attività all'interno del macrosegmento. Ad esempio, una telecamera di sorveglianza non dovrebbe potersi interfacciare con una serratura, nonostante si tratti dello stesso macrosegmento relativo alla sicurezza.

La gestione unificata della rete rafforza l'efficienza

L'utilizzo di un'unica piattaforma di gestione e di analisi dei dati che fornisce una visione olistica end-to-end di tutte le reti cablate e wireless e dei dispositivi IoT rende la gestione e la risoluzione dei problemi più veloce, più semplice e meno soggetta a rischi rispetto all'utilizzo di sistemi di gestione multipli e diversi. Ad esempio, se un dispositivo IoT ha problemi di connettività, l'operatore di rete può determinare se la causa del problema è il dispositivo stesso o l'apparecchiatura di rete cablata o wireless a cui si connette.

L'azienda può anche evitare i costi aggiuntivi associati all'acquisto e alla gestione di più sistemi di gestione per dispositivi cablati, wireless e IoT. Inoltre, le policy in materia di sicurezza informatica vengono applicate in modo coerente a tutti i tipi di dispositivi, riducendo il rischio di introdurre vulnerabilità di sicurezza nella rete.



Le innovazioni di nuova generazione connettono persone e informazioni

I team IT e Operativi dovrebbero anche valutare nuove tecnologie che li aiutino a sfruttare al meglio i dati provenienti dai dispositivi IoT.

Le applicazioni di asset tracking che identificano la posizione di risorse e persone in tempo reale sono un buon esempio dei recenti progressi che dovrebbero essere presi in considerazione. Queste applicazioni utilizzano tag abilitati a GPS, BLE o RFID per rintracciare e trovare rapidamente e facilmente risorse o persone. Incluse anche le analisi dei dati che aiutano le imprese a ottimizzare l'uso delle loro risorse, tra cui:

- Il tempo che le persone devono attendere per accedere alle apparecchiature
- Quali reparti utilizzano più spesso ciascun tipo di apparecchiatura
- Quale attrezzatura viene utilizzata di meno
- La frequenza con cui le apparecchiature vengono spostate all'interno dei locali e la distanza percorsa ogni giorno
- Quando è stata effettuata l'ultima manutenzione dell'apparecchiatura

I motori del flusso di lavoro sono un altro buon esempio. Queste piattaforme combinano i dati provenienti da dispositivi IoT, infrastrutture di rete, applicazioni aziendali e altri sistemi e li comunicano alle persone quando ne hanno più bisogno. Ad esempio, se un sensore IoT segnala una perdita di monossido di carbonio in un edificio pubblico, il motore del flusso di lavoro può notificare immediatamente e in contemporanea i team di manutenzione interni, gli esperti esterni, il personale che si occupa della gestione e della sicurezza dell'edificio. Può anche consentire a tutte le parti notificate di unirsi spontaneamente a una chat room, a una conferenza audio o video per discutere del problema. Ciascuna parte beneficia delle informazioni in tempo reale provenienti dai sensori IoT e può allo stesso tempo vedere un feed di videosorveglianza consentendole di valutare meglio la situazione.



Il giusto partner tecnologico

Nel momento in cui i team IT e Operativi decideranno di intensificare la collaborazione, avranno bisogno di un partner tecnologico esperto che fornisca indicazioni, competenze e soluzioni durante il loro percorso.

Alcatel-Lucent Enterprise riconosce i vantaggi finanziari e operativi che le aziende ottengono quando i team IT e Operativi collaborano nelle iniziative di trasformazione digitale. E' anche a conoscenza di come i team IT e Operativi possono sfruttare le moderne tecnologie e soluzioni per rafforzare la sicurezza informatica, l'affidabilità e l'efficienza della rete, riducendo al contempo rischi e costi. Le soluzioni Alcatel-Lucent Enterprise semplificano e accelerano la trasformazione digitale, indipendentemente dallo stadio evolutivo in cui si trovano oggi le organizzazioni:

- Le soluzioni di rete cablate e wireless con connettività IoT integrata e automatizzata semplificano le implementazioni e garantiscono pieno supporto alle strategie di sicurezza ZTNA.
- Le soluzioni di gestione unificata della rete forniscono una gestione coesa e una visibilità completa dei dispositivi cablati e wireless che accedono alla rete.
- Le soluzioni di asset tracking si affidano alla tecnologia BLE per una localizzazione altamente accurata e al tempo stesso efficiente dal punto di vista energetico
- [Rainbow™-workflow e la piattaforma di comunicazione cloud di Alcatel-Lucent Enterprise](#) connette persone, macchine e processi utilizzando chat, voce e video

Supportiamo le nostre soluzioni con servizi di personale esperto, per aiutare i nostri clienti a realizzare i loro obiettivi di trasformazione digitale in modo efficiente ed economico.

White paper

Colmare il divario tra l'IT e le Operation per una trasformazione digitale vincente

Sostenere gli obiettivi di trasformazione digitale dei clienti

Aziende leader nel mondo, operanti in diversi settori di mercato, collaborano con Alcatel-Lucent Enterprise grazie alla possibilità di combinare soluzioni tecnologiche all'avanguardia e competenze di alto livello. Di seguito alcuni esempi:

- [Liverpool City Region Combined Authority](#) nel Regno Unito, utilizza soluzioni di rete, di gestione e di comunicazione di ALE per migliorare l'esperienza dei viaggiatori e l'efficienza operativa. Le nostre soluzioni supportano dispositivi IoT mission-critical per telecamere a circuito chiuso, gestione del traffico, rilevamento di incendi e fumi e sistemi di controllo di supervisione e acquisizione dati (SCADA), nonché servizi di pedaggio come il riconoscimento automatico delle targhe (ANPR) e l'integrazione di sistemi intercomunicanti. L'organizzazione sostiene anche i miglioramenti previsti, come le comunicazioni da nave a terra, la connettività per i traghetti fluviali e l'espansione della biglietteria intelligente per il trasporto pubblico.
- [L'amministrazione metropolitana di Bangkok](#) in Thailandia si affida alle soluzioni di rete e di gestione di ALE per sviluppare una rete ridondante ad alta velocità per i dispositivi IoT delle smart city che contribuiranno a migliorare la qualità della vita e le opportunità economiche dei cittadini. Bangkok, in quanto capitale del Paese, con la sua rete moderna e le innovazioni smart city svolge un ruolo fondamentale nell'aiutare il governo nazionale a raggiungere gli obiettivi di Thailandia 4.0.
- [Aster DM Healthcare](#) negli Emirati Arabi Uniti (UAE), utilizza le soluzioni di rete, gestione, comunicazione e collaborazione di ALE per fornire al personale ospedaliero un accesso 24 ore su 24, 7 giorni su 7, ai dati medici e alle applicazioni sanitarie critiche, quando e dove necessario. La soluzione convergente consente inoltre al personale di Aster di connettersi e collaborare in modo sicuro e senza interruzioni tra le varie sedi, anche durante gli spostamenti, in modo da poter dedicare più tempo ai pazienti. Offre ai pazienti anche un accesso affidabile al Wi-Fi, in modo che possano rimanere in contatto con familiari e amici mentre si trovano nelle strutture Aster.
- [La California State University](#), negli Stati Uniti, utilizza le soluzioni di rete ALE per migliorare la sicurezza, fornire Wi-Fi ovunque e offrire servizi cloud aperti e condivisi per migliorare l'esperienza complessiva del campus. La rete altamente affidabile e flessibile supporta in modo sicuro più di 500.000 utenti negli oltre 20 campus dell'università e ha contribuito a risparmiare più di 100 milioni di dollari in costi di infrastruttura.
- [Energy One](#) in Australia, utilizza le soluzioni di rete e di gestione di ALE per automatizzare e semplificare la gestione e la manutenzione della rete nelle sue sedi di Sydney e Melbourne. La rete autonoma semplifica l'inserimento di nuovi siti, libera il personale IT che può concentrarsi sulle attività prioritarie e migliora le prestazioni della rete e la copertura Wi-Fi, in modo che i dipendenti possano lavorare in modo più produttivo grazie a una maggiore mobilità e a un'esperienza utente uniforme in tutte le sedi.



Ulteriori informazioni

Per sapere come possiamo aiutare la tua organizzazione a trasformarsi digitalmente in modo efficiente ed economico, [visita il nostro sito web](#) o [contattaci oggi](#) per potere confrontarci sulle tue esigenze specifiche.

