



Collegare l'IT e le reti OT: gli access point come piattaforme IOT sicure

I dispositivi IoT presentano problematiche in termini di connettività e sicurezza

La proliferazione dei dispositivi IoT all'edge crea una nuova serie di problematiche per l'IT. I dispositivi IoT utilizzano diversi tipi di connettività e protocolli di comunicazione, e spesso richiedono gateway specifici del fornitore per gestire i dispositivi e raccogliere dati. Di conseguenza, i dispositivi IoT sono fondamentalmente inaffidabili e i gateway IoT oscurano i dispositivi sulla rete, causando una mancanza di visibilità che crea maggiori rischi. L'integrazione dei dati IoT con i processi aziendali è quindi complessa e richiede una conoscenza approfondita dell'IoT, del trasporto dei dati, della sicurezza dei dati e delle applicazioni aziendali.

Combinando le frequenze radio IoT con un framework di rete zero trust, gli access point HPE Aruba Networking possono fungere da piattaforme IoT sicure che rafforzano la protezione della rete, forniscono copertura per un'ampia gamma di dispositivi IoT ed eliminano la necessità di overlay di rete solo per i dispositivi IoT.

Evoluzione degli access point

Siamo abituati a pensare agli access point Wi-Fi nel contesto dell'accesso sicuro alla rete wireless e per molti anni questa è stata la loro funzione principale. L'aggiunta delle frequenze radio BLE agli access point (AP) HPE Aruba Networking ha indicato una nuova strada che guarda oltre l'accesso alla rete, fino a includere dispositivi Internet of Things (IoT), tra cui etichette di asset, pulsanti antipanico mobili, accelerometri multiasse per il monitoraggio di apparecchiature rotanti e un'ampia gamma di altri sensori e attuatori per l'automazione di edifici e fabbriche.

L'introduzione degli AP Wi-Fi 6 e Wi-Fi 6E di HPE Aruba Networking ha annunciato la comparsa di frequenze radio Wi-Fi migliorate con funzionalità di riattivazione per dispositivi a basso consumo, frequenze radio IoT Bluetooth 5 e 802.15.4 Zigbee più recenti e funzionalità delle porte USB ampliate. Quando era necessaria l'elaborazione edge, questi AP potevano eseguire applicazioni specializzate basate su container che elaboravano i dati dei dispositivi IoT in locale per servizi

Vantaggi

- Supporta un'ampia gamma di applicazioni IoT con più frequenze radio IoT e porte USB.
- Elimina il costo e la complessità dei gateway e delle reti overlay IoT.
- Migliora la sicurezza dell'IoT con tunneling, segmentazione dinamica, gestione delle policy e analisi delle anomalie.
- Fornisce un punto di osservazione ideale per la copertura dei dispositivi IoT e contribuisce ad aumentare al massimo la durata della batteria dei dispositivi IoT.
- Supporta porte USB per frequenze radio IoT aggiuntive o sensori alimentati.
- Aggiunge flessibilità di distribuzione con AP per interni, esterni e C1D2/ATEX Zona 2 con enclosure C1D1/Zona 1 opzionali.
- Riduce al minimo o elimina la complessità delle reti mesh IoT proprietarie.

come la deduplicazione dei dati. Nel loro insieme, queste funzionalità hanno ulteriormente trasformato gli AP in hub di comunicazione sicuri e multiuso che erano sia punti di accesso alla rete che piattaforme Internet of Things (IoT) a tutti gli effetti.

Gli access point Wi-Fi 7 HPE Aruba Networking si basano sui punti di forza degli AP Wi-Fi 6 e 6E aggiungendo ulteriori frequenze radio IoT, porte USB ed elaborazione e memoria notevolmente ampliate, per l'elaborazione di applicazioni sempre più sofisticate all'edge. Le doppie porte USB possono supportare contemporaneamente frequenze radio IoT aggiuntive o sensori alimentati come rilevatori di colpi di arma da fuoco o sistemi di monitoraggio della qualità dell'aria. Le applicazioni eseguite negli AP sono gestite da HPE Aruba Networking Central e dalle sue funzionalità IoT Operations. La maggiore memoria e potenza di elaborazione degli AP Wi-Fi 7 consentono di utilizzare applicazioni più potenti, scaricabili dall'App Store di IoT Operations, eseguire elaborazioni sofisticate di dati IoT, gestire il funzionamento dei dispositivi e segnalare lo stato e la posizione dei dispositivi in tempo reale.

Attualmente, tutti i tipi di sistemi edilizi a bassa tensione, tra cui comfort, rilevamento delle intrusioni, gestione energetica, controllo degli accessi, tracciabilità del personale e degli asset, manutenzione preventiva, monitoraggio della qualità dell'aria, etichettatura elettronica degli scaffali e persino monitoraggio dei colpi di arma da fuoco, possono comunicare in modo sicuro e affidabile utilizzando nient'altro che gli AP.

Vantaggio ideale

Dalla loro posizione privilegiata come arredamenti da soffitto, gli AP hanno una visuale panoramica senza ostacoli di tutti i dispositivi vicini, una situazione ideale per le comunicazioni a radiofrequenza (RF) e a infrarossi (IR).

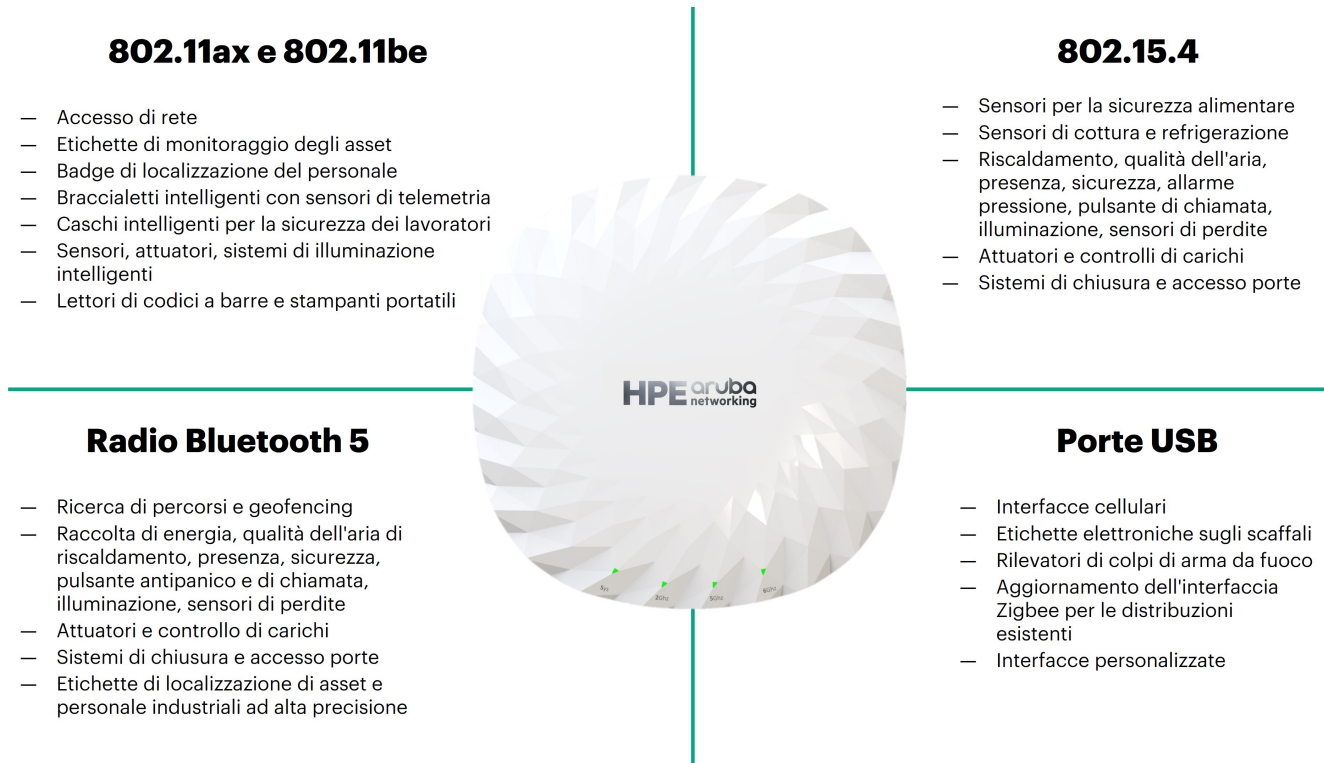


Figura 1. Access point Wi-Fi 7 HPE Aruba Networking come piattaforme IoT sicure

Le velocità in bit diminuiscono proporzionalmente alla distanza, quindi per offrire un'esperienza utente ad alta velocità gli AP sono generalmente distanziati a intervalli di 12-15 metri in aree aperte e spesso uno per stanza. Questa spaziatura fornisce una copertura ottimale per i dispositivi IoT wireless a basso consumo e di raccolta energetica alimentati a batteria.

Molti dispositivi IoT montati a soffitto richiedono una fonte di alimentazione locale, idealmente con batteria di riserva. Tuttavia, le prese alimentate dalla rete elettrica non si trovano generalmente nei plenum a soffitto, né sono presenti gruppi di continuità. Gli AP HPE Aruba Networking offrono una soluzione semplice al problema energetico dell'IoT: Le porte USB forniscono alimentazione e dati ad alta velocità ai dispositivi IoT, senza ulteriori cavi o apparecchiature.

Sebbene i soffitti siano il luogo ideale per i rilevatori alimentati, non sono ottimali per i sensori di temperatura o umidità a causa delle ampie oscillazioni causate dal soffiaggio dell'aria dai sistemi HVAC. Per rilevare i cambiamenti di temperatura e umidità nello stesso modo in cui li percepiranno gli esseri umani, questi sensori sono quasi sempre montati a circa 1,1 metri dal pavimento e le frequenze radio wireless degli AP sono idealmente posizionate per la massima copertura.

Il cablaggio rigido dei sensori montati a parete sugli AP montati a soffitto non è mai consigliato, dato che richiede la perforazione di spazi per plenum o di barriere di controllo delle infezioni in ospedali e camere bianche. Le frequenze radio wireless degli AP possono preservare l'integrità dei plenum e delle barriere, supportando praticamente qualsiasi tipo di sensore interno.

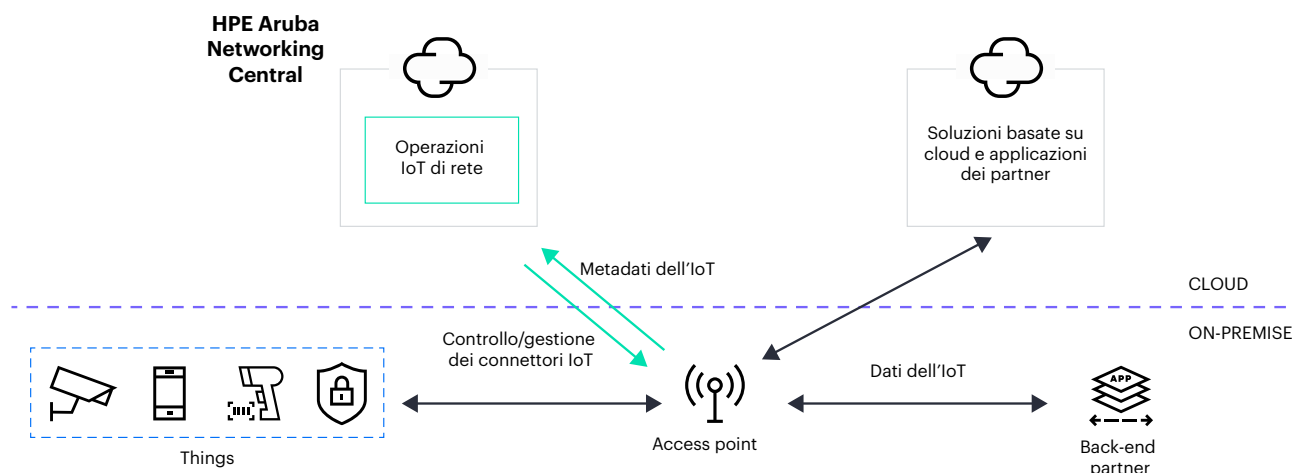


Figura 2. IoT Operations riduce la complessità associata all'IoT estendendo la visibilità alle applicazioni IoT e ai dispositivi IoT non Wi-Fi connessi all'infrastruttura LAN wireless.



Figura 3. Gli AP HPE Aruba Networking conformi ad HazLoc non richiedono un enclosure aggiuntivo per C1D2/ATEX Zona 2.



Figura 4. Enclosure C1D1/ATEX Zona 1 opzionale dei partner nell'ambito della tecnologia di rete HPE Aruba

Meno complesso, più affidabile

Gli access point eliminano la necessità di gateway comunicando direttamente con i dispositivi IoT ed eseguendo il tunneling bidirezionale dei dati alle applicazioni di destinazione. L'eliminazione dei gateway riduce la complessità e i costi del sistema, ne aumenta l'affidabilità complessiva ed elimina una superficie di attacco generalmente vulnerabile.

Comunicando direttamente con i dispositivi IoT, gli AP possono anche ridurre le dimensioni dei cluster delle reti mesh IoT, se non addirittura eliminarle del tutto. Il mesh backhaul moltiplica la larghezza di banda consumata da ogni trasmissione IoT, un effetto che ha un impatto particolarmente evidente nelle bande ISM congestionate da 900 MHz e 2,4 GHz.

Eliminare le reti mesh RF o consentire loro di operare in cluster più piccoli preserva la larghezza di banda e riduce al minimo l'effetto su altri dispositivi IoT che operano sulla stessa frequenza. Tutto questo ha l'ulteriore vantaggio di aumentare la durata della batteria dei dispositivi IoT, che semmai non hanno bisogno di ritrasmettere i pacchetti di backhaul con la stessa frequenza.

HPE Aruba Networking Central IoT Operations è un servizio disponibile per gli AP su cui viene eseguito HPE Aruba Networking Wireless Operating System AOS-10 gestito da HPE Aruba Networking Central, una piattaforma cloud-native basata su microservizi che offre la scalabilità e la resilienza necessarie per ambienti mission-critical all'edge distribuito. Questo consente di eliminare il lungo processo manuale che si rende necessario per spostare le informazioni da un luogo all'altro o per cercare di mettere in correlazione le informazioni provenienti da più visualizzazioni. Unifica la visibilità dell'infrastruttura IT e OT all'interno del dashboard sull'integrità della rete, estendendo il monitoraggio e le informazioni della rete a BLE, Zigbee e altri dispositivi IoT non IP nell'ambiente fisico, insieme ai dispositivi IoT basati su IP.

Maggiore sicurezza e visibilità IoT

I dispositivi IoT sono presi di mira dagli attacchi perché raramente dispongono di una solida sicurezza integrata, non offrono una rigorosa autenticazione e archiviano le password in chiaro a causa di progetti con vincoli di prezzo, capacità di elaborazione limitate ed errori di progettazione. I dispositivi IoT si trovano spesso in aree pubbliche e sono soggetti a indagini, manipolazioni e violazioni della rete. Non c'è da meravigliarsi se le aziende oggi preferiscono affidarsi ai dispositivi IoT e ridurre attivamente al minimo i vettori di attacco.

Il funneling del traffico IoT attraverso gli AP e gli switch HPE Aruba Networking consente di utilizzare più meccanismi di sicurezza attivi e passivi per proteggere i dispositivi IoT e il relativo traffico. I moduli Trusted Platform negli AP memorizzano le credenziali in modo che il controllo di un access point non fornisca dettagli di autenticazione, autorizzazione o crittografia. I dati IoT vengono trasmessi in modo sicuro dagli AP ad HPE Aruba Networking on-premise, virtuale e nel cloud senza alcuna conversione di testo in chiaro nella catena.

Policy basate sui ruoli e diritti di accesso segmentano il traffico dagli AP alle destinazioni, senza configurazioni di rete e VLAN statiche e complesse. Il firewall di applicazione delle policy integrato di HPE Aruba Networking fornisce ispezione approfondita dei pacchetti del traffico ad alto rischio. Ad esempio, è possibile assegnare in modo dinamico a una telecamera di sicurezza un ruolo che ne limita il traffico a server specificati, senza il rischio di accessi dannosi ad altre parti della rete.

HPE Aruba Networking ClearPass rileva le impronte digitali dei dispositivi in modo da assegnare automaticamente le policy appropriate, mentre il motore di analisi delle anomalie di HPE Aruba Networking monitora passivamente l'attività e segnala il comportamento anomalo dei dispositivi prima che possano verificarsi dei danni. Se è consentita l'attenuazione attiva, HPE Aruba Networking può mettere in quarantena i dispositivi IoT che violano le policy, ad esempio tentando di eseguire la scansione delle porte o camuffandosi come un altro dispositivo.

I fornitori IoT che aggirano il funnel di sicurezza, ad esempio tramite una rete LoRa, mettono a rischio l'azienda instradando il traffico e impiegando questi meccanismi di protezione migliori della categoria. Di conseguenza, i dispositivi infetti o compromessi potrebbero semplicemente passare inosservati.

Per ulteriore visibilità, HPE Aruba Networking Central Client Insights offre una migliore visibilità dei dispositivi mobili e IoT con classificazione basata su ML. Questa funzionalità confronta dinamicamente i dispositivi con le impronte digitali in crowdsourcing di client noti e applica la classificazione degli intervalli MAC per i dispositivi sconosciuti. Attraverso l'ispezione approfondita dei pacchetti, i dispositivi di rete vengono classificati automaticamente, con l'applicazione di policy precise in base alle informazioni sul contesto e sul comportamento. Il sistema monitora costantemente il comportamento dei dispositivi, garantendo sempre una visione aggiornata della rete.

Caratteristiche principali degli AP per campus HPE Aruba Networking serie 730

- Wi-Fi 7 (802.11be) supporta il funzionamento multi-link (MLO, Multi-Link Operation) per l'aggregazione dei canali e QAM 4K per un throughput più elevato e una latenza inferiore.
- Sblocca la banda a 6 GHz per raddoppiare la capacità disponibile.
- Copertura tri-band completa su 2,4 GHz, 5 GHz e 6 GHz per offrire una velocità di trasmissione dati aggregata tri-band massima di 9,3 gb/s.
- L'esclusivo filtro Ultra Tri-Band (UTB) consente di operare a 5 GHz e 6 GHz senza limitazioni o interferenze.
- Elevata disponibilità con due porte Ethernet da 5 gb/s per il failover hitless di Ethernet e alimentazione.
- Il ricevitore GPS integrato, il sensore di pressione barometrica e il software intelligente consentono l'autolocalizzazione degli AP, che fungono da punti di riferimento per misurazioni accurate della posizione in interni.

Visita [HPE.com](https://www.hpe.com)

¹ Access point HPE Aruba Networking Wi-Fi 6, Wi-Fi 6E e Wi-Fi 7.

² I servizi disponibili possono variare in base al tipo di dispositivo e all'interfaccia AP.

[Chatta ora \(commerciale\)](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i servizi e i prodotti Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni ed errori tecnici o editoriali contenuti nel presente documento.

Bluetooth è un marchio registrato del proprietario e viene utilizzato da Hewlett Packard Enterprise su licenza. Tutti i marchi di terzi sono di proprietà dei rispettivi titolari.

a00111192ITE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)



Risparmi in termini di batterie

Per i dispositivi Wi-Fi alimentati a batteria, gli AP¹ supportano sia i dispositivi IoT con canale TWT (Target Wake Time) che quelli a 20 MHz. TWT aumenta al massimo il tempo di sospensione dei dispositivi IoT fino a diversi giorni prima del check-in, estendendo la durata della batteria fino a 10 volte rispetto alle precedenti tecnologie Wi-Fi. Con l'orario di riattivazione negoziato tra il dispositivo e l'AP, TWT offre una modalità operativa più deterministica ed efficiente dal punto di vista energetico. L'operatività a 20 MHz consente un funzionamento a potenza ridotta, prolungando ulteriormente la durata della batteria. Inoltre, grazie alla capacità di supportare 1.000 dispositivi IoT per frequenza radio, gli AP possono adattarsi a distribuzioni IoT di qualsiasi dimensione².

Piattaforma di riferimento

Molte aziende non fanno più distinzione tra dispositivi IT e IoT a causa della diffusa proliferazione di dispositivi IoT sull'infrastruttura IT. Per ottenere un funzionamento più affidabile e deterministico, con policy di sicurezza uniformi e visibilità sui dispositivi IT e IoT, è necessario un nuovo approccio all'implementazione del sistema. Gli access point ricchi di funzionalità di HPE Aruba Networking sono la piattaforma ideale per questa trasformazione.

Per ulteriori informazioni, visita hpe.com/it/it/aruba-access-points.html

