Brochure

HPE aruba networking

Cinque principi di progettazione per un data center più smart

Architetture di servizi distribuiti per ridurre la complessità del data center e accelerare l'automazione, l'integrazione e la sicurezza.

Hewlett Packard Enterprise | ANYCORP

Introduzione

Con l'esigenza sempre più pressante di offrire valore, i responsabili IT si affidano alla modernizzazione delle applicazioni e a modelli operativi del cloud come chiavi di volta per iniziative digitali di successo. A questo scopo, è necessario modernizzare la tradizionale infrastruttura, il che però presenta altrettante problematiche di quante ne risolve. Molte organizzazioni sono impreparate perché ancora alle prese con sacche di risorse di elaborazione e storage in silo, architetture di rete e sicurezza disgiunte e operazioni che ostacolano la centralizzazione di aspetti come gestione, orchestrazione, sicurezza, policy e visibilità dell'IT.

Mentre la tecnologia delle reti di data center si è evoluta per offrire fabric leaf-spine da 100/400 G dalle prestazioni più elevate, le architetture di sicurezza e servizi non hanno raggiunto gli stessi livelli avanzati. La modernizzazione della rete richiede automazione e programmabilità basata su API per l'integrazione con piattaforme di orchestrazione e gestione su cloud. Questo significa che è necessario modernizzare anche l'infrastruttura e le operazioni, in linea con le architetture di applicazioni basate su microservizi e incentrate su cloud e con le operazioni agili di provisioning dei servizi IT che nei data center hyperscale si usano da diversi anni.

È paradossale che, sebbene la rete ricopra un ruolo più importante che mai, debba anche funzionare in modo invisibile, senza ostacolare gli sviluppatori di applicazioni o i processi aziendali.

Per compensare, molte organizzazioni usano un fabric di data center stateless, aggiungendo in modo inefficiente servizi di rete a cui vengono applicati complessi concatenamenti. Ma il volume, la velocità e la varietà del traffico di dati richiedono di abbandonare i processi manuali, reattivi e in silo per la gestione delle connessioni di rete e dei flussi di dati a favore di piattaforme basate su ML/AI in grado di stabilire, scalare e proteggere le connessioni e di gestire l'infrastruttura.

Esiste una soluzione migliore: un'architettura di rete che preveda procedure più semplici di provisioning, distribuzione e gestione e che sia reattiva in modo trasparente alle esigenze di sviluppatori di applicazioni, operazioni IT, DevOps e business.

I fabric di data center di nuova generazione consentono alle organizzazioni di abbandonare le architetture legacy e competere allo stesso livello degli hyperscaler consolidando le funzioni stateful nell'intero fabric e fornendo un'ampia varietà di servizi per l'infrastruttura secondo un nuovo modello integrato. Quindi il fabric non dovrà più essere considerato come una semplice soluzione di segmentazione e connettività, ma come struttura di supporto di tutti i servizi per l'infrastruttura consentiti per la scala del carico di lavoro.

Questo documento esamina cinque importanti principi di progettazione del data center da considerare per sviluppi futuri:

- Modernizzazione tramite switch per DPU con accelerazione hardware
- Transizione a un'architettura di servizi distribuiti di quarta generazione
- Estensione della sicurezza zero trust più vicino alle applicazioni
- Fusione di AIOps per rete e sicurezza
- Utilizzo di edge, colocation e IaaS

1 - Modernizzazione con switch per DPU

In passato, la potenza di elaborazione per i data center aziendali e hyperscale era ad esclusivo appannaggio delle CPU. Più di recente, le GPU (Graphics Processing Unit) hanno assunto un ruolo significativo. Originariamente usate per offrire grafica complessa in tempo reale, le funzionalità di elaborazione in parallelo che offrono si sono rivelate ideali per attività di elaborazione accelerate, tra cui applicazioni di intelligenza artificiale, deep learning e analisi dei Big Data.

Sulla scena è emerso un nuovo tipo di processore, DPU (Data Processing Unit), che presto si è imposto come componente importante della famiglia di risorse di elaborazione accelerata incentrate sui dati. Le DPU sono appositamente realizzate per l'offloading del traffico dati, in modo che le attività a elaborazione intensiva possano essere ottimizzate su risorse CPU e GPU.

Usando un proprio processore hardware, le DPU vengono spesso distribuite in server per data center hyperscale ed eseguono un ampio set di funzioni accelerate di elaborazione, cloud, rete, sicurezza e storage, tra cui crittografia, firewall, bilanciamento del carico, NAT, telemetria e altro ancora. Queste funzionalità rendono possibili le piattaforme di elaborazione cloud-native bare metal che definiscono la nuova generazione di elaborazione su scala cloud.

La tecnologia delle DPU si è evoluta e se prima era riservata esclusivamente ai server ora è disponibile negli switch top-of-rack. Questa nuova tecnologia di switch per servizi distribuiti unisce lo switching basato su Ethernet/IP standard con una tecnologia di DPU incorporata, accelerata tramite hardware e completamente programmabile, per formare una soluzione unificata di rete sicura e a elevate prestazioni per il data center e il cloud.

“HPE Aruba Networking e AMD Pensando hanno predisposto la prima architettura per servizi distribuiti del settore che consente alle aziende di creare e gestire l’infrastruttura di rete con prestazioni e scalabilità analoghe a quelle dei colossi dell’infrastruttura hyperscale”.

Alan Weckel, Founder e Technology Analyst, 650 Group

Gli operatori possono quindi estendere le reti leaf-spine standard di settore con servizi distribuiti di micro-segmentazione stateful, firewall east-west, NAT, crittografia e telemetria, erogati più vicino a dove vengono elaborati i carichi di lavoro di elaborazione e storage all’edge della rete.

A differenza delle schede SmartNIC dedicate, installate nei server, gli switch per servizi distribuiti possono essere distribuiti al livello top-of-rack del server e forniscono servizi distribuiti a tutti i server e host presenti nel rack.

Gli switch per servizi distribuiti non richiedono di apportare modifiche all’hardware o al software né di preoccuparsi dei sistemi operativi server. Non richiedono l’installazione di driver o agenti nei server per fornire servizi distribuiti su vasta scala e con prestazioni wire-rate, e possono essere integrati in data center aziendali brownfield e in cloud privati nuovi o esistenti.

2 - Transizione a un’architettura di servizi distribuiti di quarta generazione

Oggi, il silicio e il software consentono ai fabric di data center di fornire i servizi per l’infrastruttura necessari per supportare carichi di lavoro su vasta scala, per cui vanno ben oltre una semplice soluzione di segmentazione e connettività.

Gli hyperscaler hanno scoperto già dieci anni fa che per scalare i fabric è necessario eliminare la complessità associata all’esigenza di avere un’appliance diversa per ogni sistema operativo e servizio del data center. Invece di coinvolgere un nuovo fornitore per ogni servizio per l’infrastruttura, hanno integrato ogni funzione in un singolo sistema operativo gestito attraverso un singolo controller automatizzato. Grazie a questa integrazione e semplificazione, sono riusciti a supportare diversi milioni di carichi di lavoro.

Tradizionale/legacy Terza generazione	Nuova generazione Quarta generazione
• Modello incentrato su switching e connettività • Servizi di rete/sicurezza aggiunti per ogni singola VM • Switch di livello 4-7 altamente centralizzati, scala limitata • Complessità e costi elevati (appliance, agenti) • Capacità limitata di automazione a causa della complessità	• Modello operativo incentrato sul cloud • Unificazione dei servizi per fabric e infrastruttura • Servizi completamente distribuiti tra tutti i carichi di lavoro del data center • Inserimento semplificato di servizi nel fabric di data center • Automazione, visibilità e dati di telemetria completi

Figura 1. Transizione a un fabric di data center di quarta generazione

La **quarta generazione** di architetture data center introduce questo stesso consolidamento di funzioni stateful nell'intero fabric. Al posto di un veicolo di interconnessione stateless che raggruppa carichi di lavoro e servizi, il fabric può ora fornire un'ampia varietà di servizi semplificati e integrati per l'infrastruttura, riducendo la complessità di progettazione e provisioning e garantendo al contempo la disponibilità di servizi stateful all'edge del fabric.

Tutto questo inizia con due delle funzioni più cruciali del data center: la sicurezza east-west, necessaria per qualsiasi distribuzione zero trust, e i dati di telemetria di rete completi (non campionati). Entrambe queste funzioni sono essenziali per i carichi di lavoro scomposti. La sicurezza all'interno del data center è cruciale per prevenire violazioni, mentre la telemetria apre opportunità per soluzioni emergenti basate su machine learning in grado di automatizzare le operazioni di sicurezza e rete in modi non possibili senza dati di telemetria del data center ad alta fedeltà.

Questa nuova architettura supera anche una scelta progettuale non ottimale adottata da molte organizzazioni, ossia l'installazione di agenti software nei server per fornire micro-segmentazione. Incorporando questi servizi nel fabric di rete, gli operatori hanno ora un'opzione progettuale superiore che libera preziosi cicli della CPU dei server, che altrimenti verrebbero sottratti a causa della necessità di elaborare servizi di rete a elaborazione intensiva.

Un'architettura di questo tipo può essere creata contestualmente alla costruzione da zero di nuovi ambienti cloud hyperscale, ma come è possibile invece trarre vantaggio da questa tecnologia all'avanguardia nei data center esistenti?

Il punto logico da cui iniziare sarebbe la distribuzione di questi servizi nello switch leaf top-of-rack (ToR) per sfruttare un'architettura per servizi distribuiti senza un upgrade radicale, oneroso in termini di tempi e costi, dell'intero data center. Questa strategia di distribuzione è particolarmente interessante perché consente alle organizzazioni di eseguire la migrazione di singoli server rack o data center con prestazioni ottimizzate senza creare interruzioni.

Un'architettura di servizi distribuiti di quarta generazione consente di:

- ridurre la latenza e migliorare la sicurezza applicando i servizi quanto più vicino possibile alle applicazioni
- eliminare la proliferazione di appliance, riducendo i costi di infrastruttura e manutenzione
- ridurre o eliminare la necessità di distribuire costosi agenti software nei server (in termini di licenze e di elaborazione della CPU)
- ottimizzare le prestazioni e la larghezza di banda della rete riducendo la latenza con la distribuzione dei servizi all'edge del fabric
- aumentare l'efficienza operativa e delle policy per i team delle operazioni di rete e sicurezza

3 - Estensione della sicurezza zero trust più vicino alle applicazioni

Le minacce alla cybersicurezza sono cambiate radicalmente negli ultimi anni. Zero trust è una prassi di sicurezza enterprise essenziale per prevenire le violazioni dei dati e limitare lo spostamento laterale interno presupponendo che nell'ambiente sia presente un vettore di attacco. Nel data center questo significa considerare non attendibile qualsiasi entità e tutto il traffico sulla rete, a meno che non siano autorizzati esplicitamente da una policy di sicurezza. La segmentazione ispeziona in modalità stateful tutto il traffico east-west nel data center e applica policy per impedire a utenti malintenzionati di spostarsi lateralmente attraverso la rete interna.

I servizi di rete devono supportare la scala di applicazioni disaggregate. Per tradizione, questi servizi vengono tutti distribuiti come appliance o VM dedicate che si connettono alla rete ma non fanno parte del fabric. Questo scenario comporta complessità, con fornitori diversi da gestire, effetti tromboning del traffico attraverso il fabric e difficoltà tra i team di rete e servizi.

“Grazie alla collaborazione con AMD e HPE Aruba Networking, l’uso del CX 10000 come elemento fondamentale nella nostra soluzione ‘DXC Secure Network Fabric’ per data center globali ha rivoluzionato la nostra architettura di sicurezza zero trust per il data center e l’edge. Se prima erano necessari centinaia di firewall virtuali e fisici per soddisfare i nostri requisiti di segmentazione e compliance, ora abbiamo una soluzione erogata in modalità nativa in linea sulla piattaforma con risparmi previsti dell’83% sul TCO”.

- Nitin Jain, Global Network Lead, DXC Technology

Integrando funzionalità di servizi stateful all’interno di un fabric di data center, le funzioni di sicurezza e visibilità vengono spinte più vicino al punto in cui vengono elaborati carichi di lavoro e applicazioni, senza influire sull’architettura di rete o sulle configurazioni software esistenti. La visibilità e la postura di sicurezza del data center risultano così migliorate, a fronte di una riduzione dei costi di acquisizione e di operazioni semplificate. L’architettura ispeziona il traffico direttamente negli switch top-of-rack (ToR), rimuovendo la necessità di ricorrere all’hairpinning tramite le tradizionali appliance centralizzate e riducendo la congestione e la complessità della rete.

Un’architettura di servizi distribuiti estende zero trust più in profondità nel data center, fino all’edge dei server di rete, offrendo micro-segmentazione a granularità fine, oltre a scalare e rafforzare drasticamente la sicurezza dei carichi di lavoro mission-critical, con 100 volte la scala, 10 volte le prestazioni e un terzo del TCO delle soluzioni tradizionali.

4 - Fusione di AIOps per rete e sicurezza

La telemetria viene considerata come fonte di verità per quello che succede nel data center. Ma perché ciò sia vero, i dati di telemetria devono essere accurati e ubiquitari nell'intero data center.

I team delle operazioni di rete si trovano spesso in difficoltà perché la quantità limitata di dati di telemetria da visualizzare non è sufficiente per gestire l'automazione. I fabric di data center di oggi non sono in grado di fornire dati completi di telemetria, quindi per sapere cosa succede è necessario distribuire probe di rete e agenti software. I probe o gli agenti possono fornire dati di telemetria molto dettagliati, ma solo nei punti in cui risiedono, pertanto per aumentare la visibilità sono necessari flussi di traffico campionati nell'intero data center. Con questo metodo vengono acquisiti solo snapshot del traffico dati e non si ottiene la fedeltà necessaria per le attuali soluzioni di automazione basate su ML.

Si tratta di un problema della terza generazione legacy dovuto a un approccio frammentato.

Un'architettura di servizi distribuiti risolve queste problematiche fornendo dati di telemetria accurati e ubiquitari nell'intero data center, in modalità nativa, senza impatto sul traffico o collisioni con l'inserimento in rete dei dispositivi (punti di guasto). I probe e gli agenti non sono più necessari, così come non lo sono le reti di aggregazione TAP per la raccolta di dati di telemetria. E con la telemetria che ora fa parte del fabric di data center, gli operatori possono ridurre l'entità del "punti morti" nei dati.

Le architetture di nuova generazione offrono vantaggi che vanno ben oltre la telemetria:

- forniscono ai team di rete i valori MTTI (mean-time-to-innocence), con la possibilità di esaminare il traffico precedente, applicazione per applicazione, per rilevare l'eventuale flusso in questione e determinare le cause radice di prestazioni insoddisfacenti
- si integrano tramite un'API REST e forniscono i dati sul flusso a un'ampia varietà di tool dedicati alle prestazioni della rete e della sicurezza, tra cui Advanced Security ML (XDR), Application Dependency Mapping (ADM), AI/Operations (AIOps), SIEM/SOAR, regole di compliance del firewall e tool per il mapping dei gruppi di identità
- rilevano automaticamente le anomalie, le raggruppano in base a cause radice correlate degli incidenti e notificano le console di operazioni, i sistemi di ticketing e i sistemi di automazione con analisi dei dati in streaming in tempo reale, liberando i team operativi dalla necessità di visualizzare dati di telemetria non elaborati
- evitano la necessità di distribuire reti di aggregazione TAP complesse e ad alto costo, che offrono solo informazioni limitate, per sfruttare appieno strumenti di AI/ML con i dati di telemetria completi e ad alta fedeltà forniti da un fabric di data center di quarta generazione

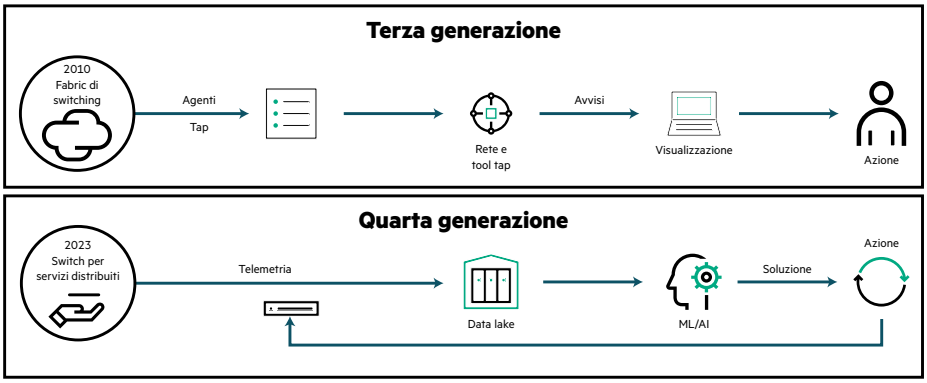


Figura 2. Una nuova era di operazioni di rete

5 - Utilizzo di edge, colocation e IaaS

Due tendenze importanti dell'IT sono diventate convergenti: la colocation e l'infrastructure as-a-service edge to cloud. La maggior parte delle implementazioni esistenti si basa su architetture centralizzate che raccolgono ed elaborano i dati nei data center core, nei centri in colocation o nel cloud. Tuttavia, nel mondo di oggi una grande quantità di dati viene generata all'edge, in luoghi remoti quali fabbriche, punti vendita al dettaglio, strutture sanitarie, edifici e città intelligenti.

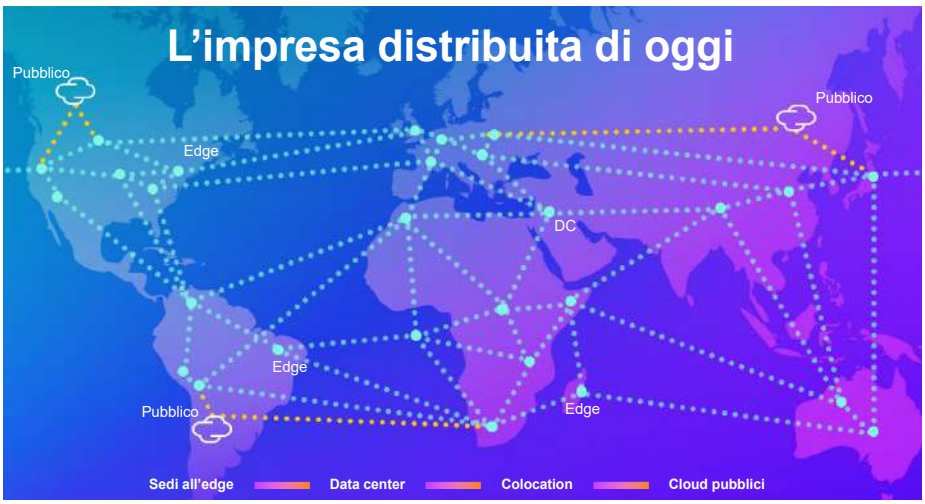


Figura 2. Una nuova era di operazioni di rete

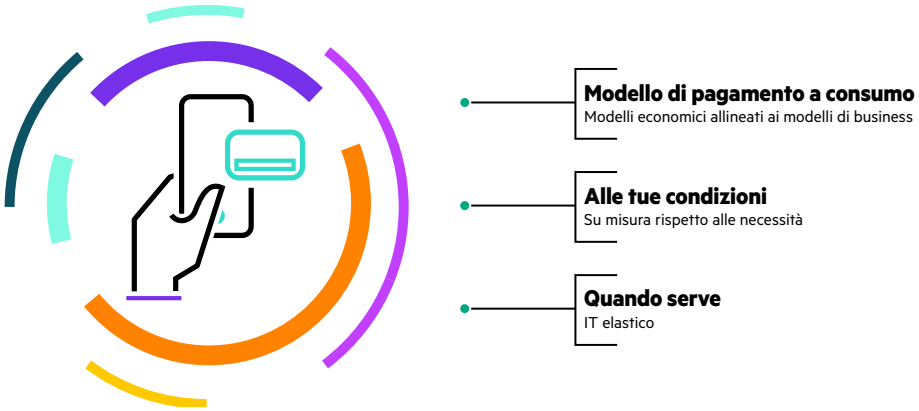
Il posizionamento dei carichi di lavoro delle applicazioni determina le decisioni sull'infrastruttura, e non viceversa. Il cloud ibrido, definito come combinazione di cloud pubblico, struttura di colocation e ambiente on-premise, è ormai la nuova realtà per i carichi di lavoro aziendali mission-critical e per un'ampia varietà di offerte as-a-service on demand.

La colocation abbinata a una piattaforma as-a-service rappresenta una soluzione eccellente. Può infatti offrire:

- esperienza cloud semplificata single-tenant, anche se l'organizzazione mantiene il controllo di dati e applicazioni
- connessioni a bassa latenza e ad ampia larghezza di banda con altri importanti provider di servizi cloud e provider di rete
- maggiore velocità delle transazioni con connessione diretta a un ampio ecosistema di organizzazioni adiacenti
- supporto degli obiettivi di sostenibilità dell'organizzazione con l'eliminazione dell'overprovisioning e strutture energeticamente efficienti
- ottimizzazione della spesa IT senza esborsi anticipati ma con pagamento in base all'uso e senza costi di uscita

Combinando questi vantaggi con un modello di pagamento a consumo per le esigenze operative e dell'infrastruttura, è possibile ottenere il meglio dei due mondi, ossia un'agilità paragonabile al cloud pubblico e un'infrastruttura in colocation, con un singolo contratto, una singola fattura e un unico punto di contatto, oltre che con l'opportunità di spostare il personale dalla gestione di un data center destinandolo ad altre attività di alto valore.

Le moderne architetture di quarta generazione traggono il massimo vantaggio dalla flessibilità di distribuzione e dai modelli di consumo resi disponibili dalle offerte di servizi per il data center as-a-service e in colocation.



Secondo uno studio di Forrester, i clienti che hanno distribuito HPE GreenLake hanno registrato un time to market fino all'80% più rapido con progetti IT globali e complessi.

Conclusioni

Con il passaggio sempre più frequente a data center moderni e distribuiti edge to cloud, e non più centralizzati, sono necessarie nuove architetture che forniscano connettività sicura e un'esperienza eccellente per utenti e applicazioni. Questo nuovo tipo di connettività per data center richiede fabric dalle prestazioni più elevate, servizi distribuiti e opzioni di consumo flessibili.

La nuova era di data center comprime i servizi per l'infrastruttura in un fabric di quarta generazione, eliminando la necessità di fare affidamento su appliance hardware dedicate e agenti software distribuiti in architetture altamente centralizzate e non ottimali.

L'accesso alla semplicità e alla scala in precedenza riservato agli hyperscaler è ora ampiamente disponibile, con un modello di consumo semplificato, servizi di rete accelerati e la possibilità di scegliere come e dove posizionare i carichi di lavoro.

Sono ora disponibili software e silicio per consentire la delivery di tutti i servizi del fabric di data center, stateless e stateful, da una piattaforma comune. Infine, tutti i clienti hanno le possibilità di scelta e la scala che richiedono per il loro business.

I nostri partner per la soluzione

Logo
Ingredient Partner

ABCPartner è un solution provider IT. Da oltre 40 anni aiutiamo i clienti a progettare, implementare e utilizzare la tecnologia per raggiungere il successo. Le principali aree di interesse sono tre: infrastruttura tecnologica, servizi professionali e servizi gestiti del ciclo di vita. La sede centrale è a Città, Stato, con filiali in Stato, Paese.

www.abcpartner.com
Numero di telefono: 812-634-1550
417 Main Street, Jasper IN 47546

HPE Aruba Networking

Nel 2022, HPE Aruba Networking e AMD Pensando™ hanno collaborato per offrire il primo switch del settore per servizi distribuiti. La serie di switch HPE Aruba Networking CX 10000 rappresenta una nuova categoria di switch per data center che combina lo switching L2/3 Ethernet best-of-breed con la tecnologia di DPU incorporata di AMD Pensando.

Ora gli operatori di data center possono inserire tranquillamente servizi stateful nelle loro reti in modalità distribuita, semplificando la progettazione della rete del data center e migliorando la postura di sicurezza.

Lo switch per data center di nuova generazione di HPE Aruba Networking consente alle aziende di garantire esperienze digitali eccellenti a clienti e dipendenti con scalabilità, prestazioni ed efficienza operativa senza precedenti.

HPE GreenLake è un portafoglio di soluzioni cloud e as-a-service che contribuisce a semplificare e accelerare il tuo business. Offre un'esperienza cloud ovunque risiedano dati e applicazioni: all'edge, nel data center, in colocation e su cloud pubblici. Disponibile con modello di pagamento a consumo, HPE GreenLake viene eseguito su una piattaforma edge to cloud aperta e più sicura, con tutta la flessibilità necessaria per creare nuove opportunità.

Per saperne di più

IDC esamina come soddisfare l'esigenza di sicurezza e prestazioni elevate con un fabric di data center moderno

Ulteriori informazioni sulla modernizzazione del data center di HPE Aruba Networking

Visita **ArubaNetworks.com**

Prendi la decisione d'acquisto giusta. Contatta i nostri specialisti della prevendita.

Contattaci

Hewlett Packard Enterprise

BR_SmartDataCenter_RVK_101123