Business white paper

Il futuro del Data Center

come ottimizzare sicurezza, sostenibilità e prestazioni

Hewlett Packard Enterprise

intel

La cybersecurity dei server e dell'intera infrastruttura IT è oggi certamente in primo piano tra le sfide che i responsabili dei sistemi informativi sono chiamati ad affrontare per mantenere la continuità aziendale: tuttavia, nei server moderni, anche prestazioni e sostenibilità diventano requisiti nodali per supportare le applicazioni di ultima generazione, e contemporaneamente minimizzare l'impatto dei data center sull'ambiente. Questo white paper analizza l'attuale scenario tecnologico, normativo e di business, illustrando poi le peculiarità e i fattori di differenziazione che rendono i server HPE ProLiant Gen 11 con Intel Xeon di quinta generazione una soluzione interessante, sul piano della sicurezza, delle performance, dell'efficienza energetica e della manutenibilità.

Sommario

Sicurezza e operatività dei server: sempre più connesse, e sempre più a rischio

La continua evoluzione della trasformazione digitale ha cambiato profondamente il **ruolo dei computer e delle reti informatiche.** La rete oggi universalmente nota come Internet, affonda le sue radici in Arpanet, avviata nel 1969, all'epoca della guerra fredda: una rete decentralizzata, concepita per continuare a funzionare anche in caso di attacco devastante, ma fondamentalmente aperta, ancora dotata di limitati meccanismi di cifratura e protezione dei dati, e inizialmente usata per connettere tra loro mainframe universitari o computer governativi. Oggi internet è utilizzata da oltre cinque miliardi di utenti come fonte primaria di informazioni, e supporta quotidianamente processi di business e transazioni di e-commerce online per imprese e organizzazioni di ogni settore industriale, integrando differenti sistemi e misure di cybersecurity.

Negli odierni data center, i mainframe sono molto più compatti ed efficienti di quelli di un tempo, e **i server fisici costituiscono l'infrastruttura portante del software applicativo e dei dati di business**, sempre più distribuiti tra ambienti on-premise, edge e cloud.

La sicurezza dei server gioca un ruolo sempre più cruciale per mantenere la stabilità e l'affidabilità di funzionamento delle applicazioni azeindali, soprattutto nell'attuale scenario di crescente interconnessione dei sistemi e di iperconnettività digitale, in cui aumenta fortemente la superficie di attacco sfruttabile dagli attacchi cibernetici. Gli attori delle minacce oggi adottano tecniche particolamente sofisticate, che possono far leva sull'intelligenza artificiale (AI) e sulla AI generativa (GenAI) per analizzare le vulnerabilità dei sistemi, delle applicazioni software, degli individui, in modo da lanciare attacchi più mirati. La GenAI è in grado di automatizzare diverse fasi delle azioni di hacking finalizzate alla compromissione dei server, dei sistemi e delle reti informatiche aziendali, e consente di aumentare la complessità, la portata, il grado di personalizzazione e la difficoltà di rilevamento degli attacchi cyber.

Data center: la continuità aziendale richiede hardware e software sicuro "by design"

Le organizzazioni lottano ogni giorno per contenere i cyber-attacchi: e il numero, in continuo aumento, nonché la varietà e la sofisticatezza delle minacce cyber rappresentano un problema che conquista ormai da tempo la massima priorità nelle agende di IT manager, chief information officer (CIO), responsabili della sicurezza informatica (CISO), ma anche responsabili finanziari e amministratori delegati. Mai come oggi, infatti, **cybersicurezza e cyber resilience diventano requisiti nodali e irrinunciabili per mantenere nel tempo la continuità operativa aziendale**, conservare in salute l'attività imprenditoriale e rafforzare la fiducia negli utenti, nei clienti, che i loro dati e informazioni verranno gestiti dall'organizzazione in conformità con i tutti i criteri e regolamenti di sicurezza e privacy vigenti in materia.

Nel data center, adottare server, hardware e software sicuri by design, e sviluppare strategie di cybersecurity e cyber resilience aiuta le imprese a ridurre i rallentamenti o le interruzioni (downtime) della produzione, della continuità aziendale, e a minimizzare al contempo le perdite di dati critici o sensibili.

Diversamente, aumenta il rischio, in seguito a un attacco cibernetico andato a buon fine, di subire conseguenze più o meno pesanti a livello finanziario, o di mancata compliance con le normative di settore, senza considerare i possibili danni in termini di riduzione della capacità competitiva, o di ripercussioni sull'immagine e la reputazione aziendale.

Attacchi cyber, la portata dei danni

Due recenti esempi di attacchi cibernetici sono utili a ricordare fin dove possono arrivare le conseguenze della compromissione dei sistemi informatici. Il primo che vale la pena richiamare alla memoria è la violazione perpetrata nel maggio 2021, attraverso il ransomware del gruppo hacker DarkSide, ai danni della rete di oleodotti di **Colonial Pipeline**, tra le più estese degli Stati Uniti, con una lunghezza di 8.850 chilometri. Il malware, in fase di attacco, non ha colpito direttamente i dispositivi e sistemi di tecnologia operativa (OT) dell'oleodotto che movimentano il petrolio, ma in poco tempo ha sottratto 100 gigabyte di dati. Successivamente, il ransomware ha infettato l'infrastruttura IT, compromettendo vari sistemi informatici, tra cui quelli di fatturazione e contabilità. Ciò ha costretto Colonial Pipeline ha chiudere l'oleodotto, come misura precauzionale per prevenire la diffusione del ransomware, causando di conseguenza carenze di carburante per giorni, lungo tutta la costa orientale degli Usa.
L'altro emblematico esempio delle conseguenze che un attacco cyber è in grado di produrre è la violazione informatica che a fine 2020 ha preso di mira **SolarWinds**, società texana fornitrice di Orion, una piattaforma software di monitoraggio di reti e sistemi IT, coinvolgendo a cascata centinaia di migliaia di organizzazioni in tutto il mondo. Tale violazione, di entità senza precedenti, è stata catalogata come **attacco alla supply chain**: e la ragione di questa classificazione è che il gruppo hacker Nobelium, identificato come responsabile della violazione, ha dapprima guadagnato accesso non autorizzato alla rete di SolarWinds, iniettando codice malevolo nella piattaforma Orion. Quest'ultima, in un secondo tempo, ha contaminato, con un gigantesco effetto domino, i sistemi delle aziende utenti di Orion che avevano scaricato via rete gli aggiornamenti e le patch del software distribuiti dalla società produttrice. Ciò ha consentito agli hacker di accedere a reti, sistemi, dati di tutte le organizzazioni coinvolte nella violazione.

Cyber Resilience Act e NIS2, le nuove normative per rafforzare la cybersecurity

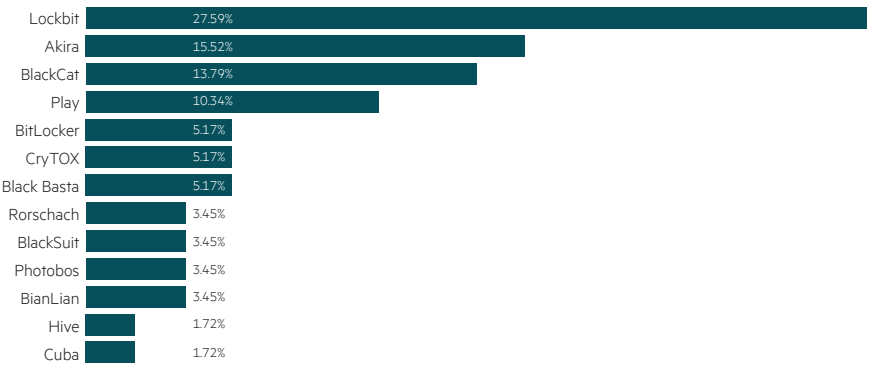
Oltre ad attacchi cibernetici come quelli a Colonial Pipeline o SolarWinds, le violazioni informatiche sono in grado di causare danni non solo a server, applicazioni e infrastrutture digitali, ma anche ai sistemi cyber-fisici (CPS), compromettendo o alterando le funzionalità della tecnologia operativa (OT) che controlla i processi e la **sicurezza delle infrastrutture critiche**. Queste ultime possono includere, ad esempio, centrali, reti elettriche, oleodotti, impianti di distribuzione energetica. Con l'obiettivo di rafforzare ulteriormente l'impianto legislativo che disciplina la sicurezza informatica, nel contesto di crescente pericolosità delle minacce cyber, il Cyber Resilience Act (CRA) si pone come la prima legge dell'Unione europea che introduce maggiori responsabilità per i costruttori, allo scopo di garantire la sicurezza dei prodotti hardware e software, che contengono elementi digitali, lungo tutto il loro ciclo di vita.

Il CRA introduce requisiti mandatori di cybersecurity per i produttori, disciplinando la pianificazione, la progettazione, lo sviluppo e la manutenzione di tali prodotti, attraverso obblighi che devono essere rispettati in ogni fase della catena del valore.
Il Cyber Resilience Act gioca, tra l'altro, un ruolo complementare rispetto alla direttiva **NIS2**, il framework di cybersecurity entrato in vigore nel 2023 nell'Unione europea, che richiede ai paesi membri di migliorare le proprie capacità di sicurezza informatica, introducendo al contempo misure di gestione del rischio e obblighi di rendicontazione per le entità di più settori, e anche stabilendo regole per la cooperazione, la condivisione delle informazioni, la supervisione e l'applicazione delle misure di cybersecurity.

Settori critici e piccole imprese sotto attacco ransomware

Nel mondo, sempre più frequenti sono le segnalazioni di **attacchi ransomware** che hanno come obiettivo i servizi governativi e altri settori critici in molti paesi: il dato emerge dal rapporto Global Cybersecurity Index 2024 pubblicato dall'**ITU** (International Telecommunication Union), che sottolinea anche come entità, frequenza, intensità degli incidenti o delle violazioni di cybersecurity riguardino settori nodali, come l'industria manifatturiera, dell'energia o dei servizi IT.
Le violazioni dei dati hanno portato le autorità europee per la protezione dei dati ad emettere multe, per infrazioni al GDPR (general data protection regulation), per un valore di oltre 1,9 miliardi di euro nel 2023. In questo stesso anno, il costo medio globale di una singola violazione dei dati è stato stimato a 4,45 milioni di dollari. Inoltre, le interruzioni delle infrastrutture IT hanno impattato l'integrità e la disponibilità dei sistemi, dei servizi e delle catene di fornitura.
Il ransomware, conferma il Sophos 2024 Threat Report, rimane la principale minaccia per le piccole imprese. In particolare, il ransomware LockBit è risultato essere la maggiore minaccia nei casi di sicurezza delle piccole imprese presi in carico dal servizio Sophos Incident Response nel 2023.

Small business ransomware incidents handled by Sophos Incident Response, 2023

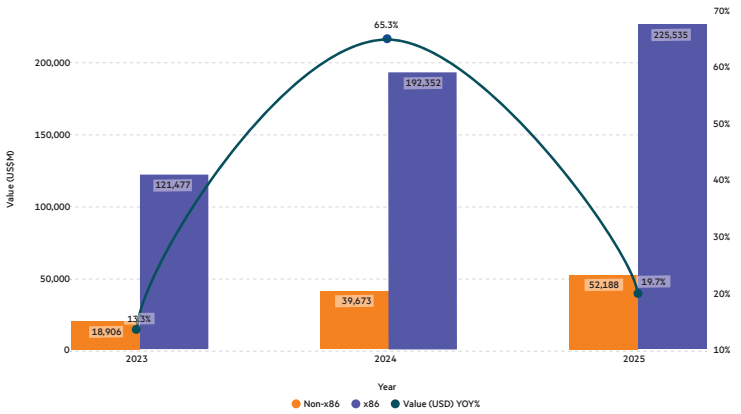


Nel panorama degli attacchi cyber,indica il rapporto Clusit 2024 sulla sicurezza ICT in Italia, la sanità emerge come il settore più colpito a livello globale, ma, nel nostro paese, nel primo semestre del 2024, il comparto manifatturiero è quello che registra il maggior numero di incidenti cyber (19% del totale).

Prestazioni, ma anche sostenibilità: un altro binomio inscindibile

Oltre a soddisfare rigorosi standard e moderni requisiti di sicurezza, **l'hardware dei server aziendali oggi è chiamato a erogare anche molta più potenza di calcolo**, necessaria per supportare le applicazioni di ultima generazione. **Il mercato globale dei server**, stando ai dati e alle stime più aggiornati pubblicati dalla società di ricerche e consulenza **IDC**, ha registrato una crescita della spesa del 100,8% nel terzo trimestre del 2024, trainata dalla continua, massiva implementazione di server con GPU, attuata dagli hyperscaler e da altri grandi acquirenti IT.
Il mercato dei server si è dimostrato resiliente negli ultimi anni, spiega IDC, in quanto l'infrastruttura IT è diventata sempre più mission-critical per molte organizzazioni. La società di ricerche prevede che il mercato crescerà nei prossimi cinque anni registrando un CAGR (tasso di crescita annuale composto) del 21,8%, grazie all'ottimismo economico e all'entusiasmo per l'intelligenza artificiale, che alimenteranno gli investimenti in infrastrutture. Le iniziative di modernizzazione, intelligenza artificiale (AI), machine learning (ML), cloud e le implementazioni edge favoriranno l'ulteriore crescita del mercato, e saranno al centro di molti investimenti mission-critical nei prossimi anni.

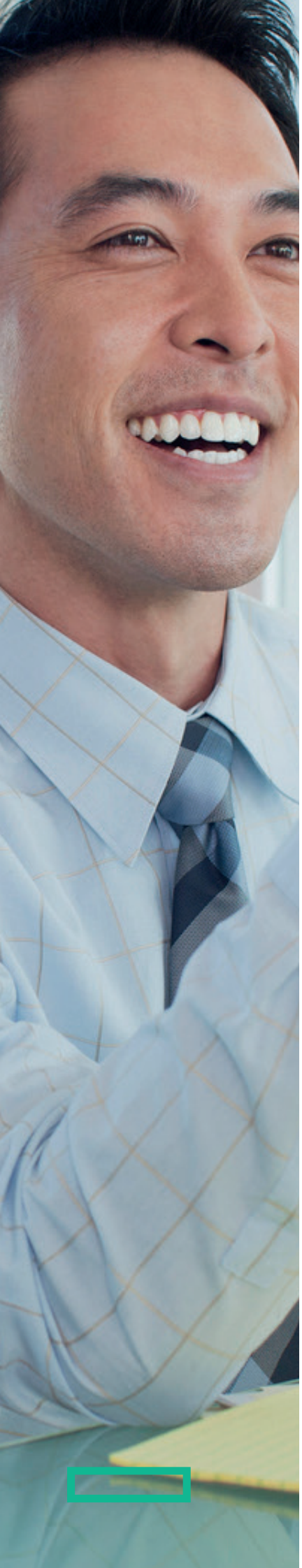
Worldwide Server Market Forecast 2023 - 2025 Value (US$M)
View Dataset →



Allo stesso tempo, oltre a incorporare nella configurazione hardware più capacità di calcolo (CPU, GPU, ecc.) per raggiungere nuovi livelli di prestazioni, i server dovranno sviluppare anche un'**efficienza energetica sempre maggiore**, armonizzando l'erogazione di elevate performance con il rispetto di tutti gli odierni criteri e requisiti normativi di **sostenibilità** ambientale. Nell'Unione europea, ad esempio, la direttiva sull'efficienza energetica (Energy Efficiency Directive - EED) richiede agli operatori di data center di rendicontare i consumi energetici, incentivandoli al contempo a investire sull'adozione di tecnologie e soluzioni innovative per migliorare l'efficienza. Tale direttiva ha evidentemente un **impatto diretto anche sulle macchine server** ospitate all'interno degli stessi data center: server di cui occorrerà ridurre e ottimizzare i consumi di energia. La direttiva EED è poi strettamente correlata alla direttiva CSRD (Corporate Sustainability Reporting Directive), che considera in maniera più ampia la sostenibilità, includendo le performance ESG (Environmental, Social, and Governance).

Manutenibilità dei server

Come accennato, le organizzazioni sono oggi sotto pressione per migliorare le proprie performance ESG: in tema di data center, nell'ottica di raggiungere tale obiettivo, un'altra leva su cui possono agire è **potenziare la capacità di gestione dei server**, in ambienti IT che in prospettiva diventano sempre più complessi da amministrare. Gli attuali ambienti informatici sono spesso caratterizzati dalla presenza di sistemi IT legacy nel data center on-premise, che si interconnettono con molteplici ambienti multicloud e infrastrutture di edge computing. Server, applicazioni e dati risultano, di conseguenza, sempre meno centralizzati e sempre più distribuiti in differenti ambienti e cloud ibridi, richiedendo soluzioni tecnologiche con funzionalità di gestione e manutenzione che permettano di amministrare con maggior agilità, flessibilità e facilità l'intero complesso di risorse informatiche.



Modernizzare il data center: perché i server HPE Proliant Gen 11

Tra le soluzioni per data center che consentono di rispondere alle moderne sfide di sicurezza, prestazioni e sostenibilità dell'hardware fin qui tratteggiate, **la gamma di server HPE ProLiant Gen11 alimentati da Intel Xeon di quinta generazione** si posiziona sul mercato con numerosi punti di forza, e con caratteristiche uniche. In primo luogo, la dotazione hardware di queste macchine beneficia della **collaborazione e dello sviluppo tecnologico congiunto tra HPE e Intel**, che arricchisce l'architettura industry-standard x86, attraverso l'ingegnerizzazione di componenti hardware e software orchestrati armonicamente per massimizzare sicurezza e operatività dei server, ma anche per migliorare prestazioni, sostenibilità e manutenibilità delle macchine.

Sicurezza fidata "by design"

Sotto il profilo della sicurezza e della protezione dei dati in fase di elaborazione, i server ProLiant Gen11 sfruttano le moderne funzionalità dei processori Intel Xeon di quinta generazione, tra cui la tecnologia di **confidential computing**, in grado di creare, all'interno del processore stesso, un ambiente di esecuzione protetto e fidato (Trusted Execution Environment – TEE).
Nella realizzazione della gamma di server ProLiant Gen11, HPE e Intel hanno cooperato a stretto contatto per sviluppare una **sicurezza by design** che viene perseguita, a livello hardware e software, in ogni singola fase del processo di progettazione, produzione e gestione del ciclo di vita del prodotto: dalla sicurezza dell'ecosistema di partner fidati che fanno parte della catena di produzione e fornitura dei componenti, alla sicurezza embedded a livello hardware, fino alla sicurezza a livello software, dall'avvio del firmware, al boot del sistema operativo della macchina.
Il fulcro del paradigma di sicurezza sta nella cosiddetta '**silicon root of trust**' (RoT), una tecnologia firmware che **integra la security direttamente nell'hardware dei server HPE**, creando un'impronta digitale immutabile nel silicio, capace di fornire livelli avanzati di protezione contro gli attacchi al firmware. In particolare, un'impronta digitale del firmware **HPE iLO** (Integrated Lights-Out) – la tecnologia di gestione proprietaria incorporata nei prodotti HPE che semplifica la configurazione e il controllo remoto dei server ProLiant Gen11 – viene integrata da un fabbricante fidato nel chip iLO, che funziona come RoT, rendendo impossibile l'inserimento di malware, virus, o codice malevolo in grado di alterare e corrompere il processo di avvio del server.
In sostanza, in fase di boot, prima di essere eseguito, iLO verifica e valida la propria integrità, dopodiché, in caso positivo, procede alla verifica e all'avvio del sistema UEFI (Unified Extensible Firmware Interface) e, così via, degli altri componenti. La funzionalità UEFI Secure Boot garantisce che ogni componente lanciato durante il processo di boot sia firmato digitalmente. In aggiunta, il modulo TPM (Trusted Platform Module) integrato, basato su hardware dedicato, fornisce un ulteriore livello di sicurezza e affidabilità del sistema.
Un elemento chiave di differenziazione dei server HPE ProLiant rispetto ad altri server della concorrenza è poi il fatto che ogni componente del chip ASIC (application-specific integrated circuit) che costituisce parte integrante dell'hardware ed è montato sulla scheda madre del server, è interamente ideato e progettato da HPE.

Modello di sicurezza zero-trust

Nel loro complesso, tutte le citate funzionalità di sicurezza contribuiscono a instaurare un **approccio di cybersecurity 'zero-trust'**, che viene implementato sia a livello hardware, sia sulle componenti software, ed è finalizzato a proteggere applicazioni e dati. Anche dopo il controllo e l'avvio iniziale del server, il modello di sicurezza zero-trust monitora e verifica di continuo l'integrità del sistema, rilevando eventuali modifiche non autorizzate al firmware o al software. L'approccio zero-trust include poi il costante monitoraggio dell'affidabilità di ogni applicazione, segmento di rete, e delle attività sull'intera infrastruttura IT, per assicurare che ciascun dispositivo e utente sia autenticato, ed autorizzato ad accedere alle sole risorse di rete necessarie per svolgere quel determinato compito. Isolando segmenti di rete e applicazioni, si attua una protezione proattiva, riducendo la superficie di attacco e aumentando la resilienza: in questo modo, anche in caso di compromissione di un server o di una parte dell'infrastruttura, è possibile contenere i danni e **garantire la continuità operativa aziendale**.
La gestione del ciclo di vita dei server, dall'edge fino al cloud, beneficia infine dei meccanismi di sicurezza forniti dalla console di gestione cloud-based **HPE GreenLake for Compute Ops Management**, anch'essa improntata sul paradigma zero-trust, e sviluppata integrando tecniche di protezione evolute, come la cifratura dei dati e l'autenticazione multifattoriale (MFA).

Performance sostenibili

Sul versante delle prestazioni, l'architettura dei server HPE ProLiant Gen11 è basata sui processori **Intel Xeon di quinta generazione**, che sono ottimizzati per accelerare i workload AI, ma allo stesso tempo si posizionano come **processori per data center in grado di migliorare le performance per watt nella gestione di tutti i carichi di lavoro, e di aumentare l'efficienza energetica dei server, potenziandone la sostenibilità**.
Tra i casi d'uso in cui i processori Intel Xeon di quinta generazione danno il meglio vi sono le applicazioni di apprendimento automatico (machine learning) e apprendimento profondo (deep learning), ma anche il calcolo ad alte prestazioni (HPC), e l'elaborazione dati legata alla gestione di database e strumenti di analisi dei dati.
I server HPE ProLiant Gen11 sono ingegnerizzati per **ambienti IT ibridi**, e caratterizzati da un'architettura aperta, che conferisce a queste macchine flessibilità di configurazione in rapporto alla tipologia di workload da supportare, che possono essere di tipo tradizionale, o cloud-native.
Le prestazioni, naturalmente, aumentano rispetto alla generazioni precedenti (ProLiant Gen10, Gen10 Plus) anche se possono variare in modo notevole a seconda del tipo di carico di lavoro, di componenti specifici (processore, risorse di memoria, storage) o della configurazione del sistema. In ogni caso, in termini di capacità grafiche, per singolo server la densità di GPU ad elevate performance aumenta fino al 33%, con un miglior rapporto prezzo/prestazioni, un recupero di spazio rack del 43%, e un aumento del 25% delle performance per kW (kilowatt) rispetto ai server Gen10 Plus. Forti di tutti questi miglioramenti, i server HPE ProLiant Gen11 possono essere adottati nei progetti di modernizzazione del data center per attuare politiche di consolidamento dei server che portino a una marcata riduzione del numero di macchine fisiche e a consistenti risparmi di energia, in modo da massimizzare la sostenibilità del data center stesso.

Razionalizzare la capacità di gestione dei server in ambienti IT ibridi

Come già accennato, i server HPE ProLiant Gen11 sono stati progettati per adattarsi e integrarsi in ambienti IT ibridi e distribuiti. Da questo punto di vista, la console di gestione cloud-native **HPE GreenLake for Compute Ops Management** consente di accedere ai server HPE ProLiant Gen11, monitorandoli e gestendoli in modo sicuro lungo tutto il loro ciclo di vita, in ambienti on-premise, edge e cloud.
Più in dettaglio, Compute Ops Management unifica e semplifica la gestione dei server, anche distribuiti a livello geografico, attraverso un 'single pane of glass', quindi una sola interfaccia, che viene resa disponibile e fruibile come servizio (as-a-service) elevando l'esperienza utente.
Oltre a unificare tramite una singola console cloud-based l'amministrazione dell'intera infrastruttura di calcolo, indipendentemente dalle aree geografiche e dagli ambienti informatici in cui è distribuita, Compute Ops Management fornisce anche **funzionalità di automazione** delle attività di provisioning che aiutano a semplificare e velocizzare la gestione dei server durante tutto il loro ciclo di vita, inclusa la fase di dismissione delle macchine (decommissioning). Tali funzionalità consentono, ad esempio, di facilitare l'implementazione e la configurazione dei nuovi server, di automatizzare le attività di aggiornamento del firmware e del software dell'intera flotta di server, ma anche di aumentare o ridurre con agilità le risorse di elaborazione, per rispondere alle mutevoli esigenze delle organizzazioni che devono supportare di volta in volta differenti e variabili carichi di lavoro aziendali. L'automazione di tutte queste operazioni permette di minimizzare le interruzioni dei servizi informatici e di aumentare la produttività dello staff IT, migliorando l'efficienza di gestione della flotta distribuita di server.

Conclusioni

Come ampiamente analizzato in questo documento, le moderne sfide di sicurezza informatica, capacità elaborativa e sostenibilità rendono le strategie di modernizzazione dei server aziendali un imperativo categorico per i responsabili dei sistemi informativi. La linea di server HPE ProLiant Gen11 con Intel Xeon di quinta generazione rappresenta una risposta tecnologica efficace a tutti i requisiti di sicurezza, prestazioni e sostenibilità ambientale che le imprese di ogni settore industriale oggi richiedono alle macchine server.

Informazioni su Hewlett Packard Enterprise

Hewlett Packard Enterprise (NYSE: HPE) è l'azienda globale Edge-to-cloud che aiuta le organizzazioni ad accelerare i risultati sbloccando valore da tutti i loro dati, ovunque. Facendo leva su decenni di innovazione e capacità di re-immaginare il futuro per far progredire il modo in cui le persone vivono e lavorano, HPE offre soluzioni tecnologiche uniche, aperte e intelligenti, anche in modalità as-a-service. L'offerta di HPE Compute comprende server, servizi cloud, calcolo ad alte prestazioni e intelligenza artificiale, Intelligent Edge, software e storage. HPE offre un'esperienza coerente dall'Edge al cloud passando per i data center, aiutando i clienti a sviluppare nuovi modelli di business e nuove modalità di gestione per aumentare le prestazioni operative.

Per maggiori informazioni visita: www.hpe.com/it

Informazioni su Intel

La missione di Intel è plasmare il futuro della tecnologia per contribuire a creare un futuro migliore per il mondo intero. Progredendo in campi come l'intelligenza artificiale, l'analisi e la tecnologia cloud-to-edge, il lavoro di Intel è al centro di innumerevoli innovazioni. Dalle principali scoperte come le auto a guida autonoma e la ricostruzione delle barriere coralline, a cose che migliorano la vita di tutti i giorni come gli effetti speciali e le esperienze di acquisto migliorate, sono tutte basate sulla tecnologia Intel.

Per maggiori informazioni visita: www.intel.com

Learn more at

HPE.com/us/en/servers/ProLiant-workload-solutions-ecosystem

Best practice to gain your competitive edge

Hewlett Packard Enterprise

a00137727ENW