O'REILLY®
Report

Ridefinire l'approccio alla scelta del sistema operativo

Trasforma la tua strategia Linux in un vantaggio competitivo

Ned Bellavance e Chris Hayner

Red Hat Enterprise Linux

Trasforma la scelta del sistema operativo in un vantaggio competitivo

Accelera l'innovazione con una piattaforma moderna. Scopri i vantaggi di Red Hat Enterprise Linux, una soluzione che offre agilità e controllo per rispondere al meglio al variare delle esigenze del mercato.

Scopri di più

Ridefinire l'approccio alla scelta del sistema operativo

Trasforma la tua strategia Linux in un vantaggio competitivo

Ned Bellavance e Chris Hayner

O'REILLY®

Ridefinire l'approccio alla scelta del sistema operativo
di Ned Bellavance e Chris Hayner

Pubblicato da O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401.

I libri O'Reilly si possono acquistare per scopi educativi, aziendali o promozionali. La maggior parte dei titoli è disponibile anche nella versione online (*http://oreilly.com*). Per ulteriori informazioni, contatta il nostro reparto vendite corporate/istituzionali: 800-998-9938 oppure *corporate@oreilly.com*.

Acquisitions Editor: Megan Laddusaw
Development Editor: Gary O'Brien
Production Editor: Jonathon Owen
Copyeditor: Stephanie English
Cover Designer: Ellie Volckhausen
Interior Designer: David Futato
Interior Illustrator: Kate Dullea

Febbraio 2026: Prima edizione

Cronologia delle revisioni per la prima edizione
13-02-2026: Prima versione

979-8-341-66786-0

[LSI]

Sommario

Introduzione

Storicamente, le organizzazioni sono sempre state abbastanza lente nel modificare la propria strategia di deployment dei sistemi operativi. In passato la scelta del sistema operativo era dettata dai requisiti tecnici e dalle preferenze aziendali e si utilizzavano più soluzioni solo se strettamente necessario. Ad esempio, si eseguiva il passaggio o l'upgrade a un nuovo sistema operativo se costretti dai requisiti specifici delle applicazioni critiche o quando la piattaforma in uso raggiungeva il termine del supporto. Questo ha portato per molto tempo le organizzazioni a considerare la scelta del sistema operativo come una mera esigenza tecnica. Oggi però, di fronte al panorama tecnologico globale che si evolve a un ritmo incalzante, la scelta del sistema operativo assume una rilevanza strategica.

Al giorno d'oggi le aziende si trovano a dover affrontare cambiamenti senza pari. In pochi anni tecnologie come la containerizzazione hanno reso i flussi di lavoro più flessibili, gli strumenti e le strategie di deployment delle applicazioni sono cambiati radicalmente e tecnologie come l'IA e il quantum computing hanno stravolto tutte le concezioni precedenti. Per affrontare al meglio un'epoca così turbolenta, le aziende sono chiamate a riconsiderare le proprie esigenze tecnologiche e al contempo ad adattare la strategia di selezione dei sistemi operativi.

In questo report illustreremo i fattori chiave per cui oggi la scelta del sistema operativo è diventata a tutti gli effetti una necessità strategica e, avvalendoci di ricerche empiriche, tra cui sondaggi e resoconti analitici, identificheremo le sfide specifiche per le organizzazioni IT moderne. Come vedremo, ad essere determinanti sono una serie di

fattori molto attuali. In primo luogo, l'accelerazione dell'innovazione che spinge le organizzazioni odierne a cercare nuove applicazioni, hardware e piattaforme che riescano a tenere il passo. Ma esistono anche altri aspetti con cui le aziende devono fare i conti, ad esempio: il clima economico incerto, le sofisticate minacce alla sicurezza informatica e le preoccupazioni geopolitiche, in particolare la sovranità dei dati e la sicurezza della catena di distribuzione.

Nel corso del report mostreremo come le aziende stanno ridefinendo il loro approccio alla scelta del sistema operativo dopo aver preso coscienza che oggi non si tratta più di una mera necessità tecnica ma che una decisione lungimirante in tale ambito può portare vantaggi strategici importanti.

CAPITOLO 1

Un nuovo approccio strategico alla scelta del sistema operativo

I requisiti imposti dagli ambienti IT moderni stanno modificando radicalmente l'infrastruttura dei sistemi operativi aziendali e la strategia di deployment delle app. I vantaggi di un ecosistema tradizionale immutabile e incontestabile, cioè gestione e distribuzione semplificate, minore necessità di formazione, ecc., vengono oggi riconsiderati alla luce dell'evoluzione tecnologica incalzante. Le organizzazioni prendono atto che rimanere ancorati a preferenze rigide in materia di sistemi operativi finisce per essere più un ostacolo che un punto di forza e che garantire flessibilità e crescita rapida delle funzionalità è più importante dello status quo. Le aziende incapaci di cambiare prospettiva rischiano di rimanere indietro rispetto ai concorrenti più preparati e flessibili. Oltre alla rapidità con cui cambia il panorama tecnologico, a complicare la situazione ci sono anche fattori geopolitici che influenzano direttamente le decisioni di acquisto.

Tematiche e cambiamenti principali

Sono diversi i fattori che le aziende moderne devono prendere in considerazione quando scelgono un sistema operativo. Non si tratta di tendenze isolate, ma piuttosto di forze interconnesse che stanno ridefinendo il modo di pianificare la strategia per l'infrastruttura. Approfondiremo tutti i fattori elencati di seguito più avanti nel report.

L'*accelerazione dell'innovazione* è un fattore determinante per la scelta del sistema operativo. Tecnologie come l'intelligenza artificiale (IA), l'automazione, l'edge e il cloud computing, l'IoT e le nuove soluzioni hardware personalizzate si evolvono a un ritmo senza precedenti,

tanto che molte aziende non riescono a tenere il passo. Tra l'altro, proprio a causa di questa evoluzione tecnologica rapida crescono anche le preoccupazioni circa il debito tecnico. Se un tempo le tecnologie emergenti richiedevano anni per arrivare alla fase di produzione, ora si passa dalla fase di ideazione all'implementazione in pochi mesi. Per questo motivo le aziende devono scegliere accuratamente sistemi operativi che permettano loro di mantenere un vantaggio competitivo.

L'*incertezza globale* sulle catene di distribuzione è in aumento da diversi anni. Le aziende moderne sono chiamate a guardare oltre i propri contesti locali e a considerare la catena di distribuzione nel suo complesso, in modo che questa includa sempre strumenti, software e servizi sicuri. La scelta di affidarsi a un unico fornitore, specialmente se estero, è ritenuto oggi un potenziale rischio data l'alta probabilità di interruzioni nella catena di distribuzione. Per questo motivo la diversificazione dei fornitori è ormai un imperativo strategico e un aspetto cruciale per mitigare i rischi.

Le *pressioni economiche* si fanno via via più intense e le aziende moderne devono dare priorità a ottimizzazione e ritorno sull'investimento (ROI). I vincoli di budget e la carenza di competenze sono tra gli aspetti chiave da considerare quando si sceglie un sistema operativo. In passato era raro che un amministratore fosse specializzato sull'uso di più sistemi operativi e per le aziende non era sostenibile avere più esperti di alto livello nel proprio organico. Per questo motivo in genere si optava per l'utilizzo di un unico sistema operativo in tutto l'ambiente. Oggi invece le aziende tentano di contenere i costi concentrandosi su soluzioni che siano intuitive e di facile utilizzo.

Le *preoccupazioni relative alla sicurezza* hanno ridefinito i requisiti dell'infrastruttura. Si distribuiscono sempre più sistemi e sempre più rapidamente, il che aumenta notevolmente la superficie di attacco per le aziende. Di fronte alle nuove implementazioni dell'IA, alle numerose minacce informatiche e ai rigorosi requisiti normativi, oggi alle organizzazioni occorrono approcci moderni.

Infine l'*IA* che ha rivoluzionato tutto ciò che pensavamo di sapere sull'utilizzo dei computer. La velocità con cui amministratori e sviluppatori creano nuove applicazioni grazie all'aiuto dei modelli

linguistici di grandi dimensioni (LLM) non ha precedenti. Che l'obiettivo sia collegarsi a un LLM per ottenere risposte, creare un chatbot o sviluppare sofisticati strumenti di Agentic AI, le aziende devono trovare il sistema operativo più adatto a ciascun progetto.

Quanto conta la scelta del sistema operativo

Come abbiamo visto, oggi a differenza del passato sono molti di più gli aspetti da tenere in considerazione quando si decide quale sistema operativo adottare. Un sistema operativo poco adatto può limitare l'accesso a funzionalità di IA critiche, compromettere le prestazioni ed esporre le organizzazioni a rischi di sicurezza o vulnerabilità della catena di distribuzione. Il giusto sistema operativo si dimostra invece un alleato formidabile che permette di cogliere tutte le opportunità offerte da quest'epoca moderna e frenetica. Un'attenta selezione strategica del sistema operativo assicura un vantaggio competitivo e la flessibilità digitale, due elementi essenziali per le aziende che desiderano sfruttare a pieno tutte le potenzialità delle tecnologie emergenti.

Analizziamo ora in dettaglio i fattori che influiscono sul processo decisionale.

Accelerazione dell'innovazione

Il ritmo inarrestabile del progresso ha cambiato radicalmente il modo in cui le aziende prendono le decisioni relative all'infrastruttura. In questa sezione esaminiamo cosa si intende per accelerazione dell'innovazione e come le aziende stanno cambiando il loro approccio alle strategie di deployment.

Cicli tecnologici più rapidi

Come afferma il McKinsey Technology Trends Outlook 2025: "Il panorama tecnologico globale sta subendo cambiamenti significativi a causa dalla rapida evoluzione delle tecnologie."[1] In effetti, il progresso tecnologico procede oggi a un ritmo mai visto prima, che non farà altro che aumentare in futuro. Pensiamo ad esempio all'adozione del

[1] McKinsey & Company, "McKinsey Technology Trends Outlook 2025", 22 luglio 2025, *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top- trends-in-tech*.

cloud. In quel caso l'implementazione è stata graduale: le aziende hanno iniziato adottando dapprima ambienti di sviluppo e test nel cloud per poi passare nel corso degli anni a carichi di lavoro di produzione completi. Molto diversa è stata invece l'implementazione di tecnologie quali IA generativa (IA gen) o Agentic AI, che sono passate da semplici esperimenti a veri e propri prodotti aziendali nel giro di pochi mesi.

In una strategia per l'infrastruttura tradizionale le aziende cercano di utilizzare per quanto possibile i sistemi operativi esistenti e di far funzionare le nuove tecnologie al loro interno. Tuttavia, il mercato globale odierno evolve così rapidamente che questo approccio non è più sostenibile. Oggi infatti sempre più spesso i team di sviluppo preferiscono orientarsi su nuove piattaforme che funzionino meglio con le ultime tecnologie, invece di adattare la vecchia infrastruttura. Questo approccio favorisce sicuramente la sperimentazione: se il sistema operativo attuale non è in grado di fare ciò che gli sviluppatori e gli ingegneri desiderano, questi ne cercheranno un altro che possa farlo.

Investimenti mirati

La necessità di riconsiderare ed eventualmente passare a un diverso sistema operativo è dettata principalmente dai requisiti delle nuove tecnologie. Come accennato in precedenza, sviluppatori e amministratori preferiscono oggi orientarsi su una nuova infrastruttura adatta alle tecnologie emergenti piuttosto che cercare di farle funzionare sulle soluzioni in uso. Questo non significa però che le organizzazioni abbiano risorse illimitate da investire. È infatti essenziale che il processo decisionale sia efficace e oculato così da ridurre i costi e gli sforzi. La scelta del sistema operativo è quindi una decisione da valutare con la massima cautela perché va ben oltre il singolo server e si inserisce all'interno di una piattaforma molto più ampia.

La decisione di investire su nuovi sistemi operativi è volta a soddisfare le esigenze aziendali e consentire alle imprese di tenere il passo con l'evoluzione tecnologica. Ad esempio, si è visto che le funzionalità di IA richiedono un'infrastruttura e strumenti di sviluppo specializzati e che un sistema operativo aziendale standard difficilmente sarà all'altezza del compito. Per supportare le esigenze degli strumenti di IA occorrono infatti enormi farm di server basati su GPU. Le organizzazioni lungimiranti si sono accorte della velocità dell'innovazione e adattano le loro strategie per l'infrastruttura in

modo da non perdersi nessuna opportunità. Oggi le aziende puntano a evolversi abbastanza rapidamente da massimizzare i vantaggi delle nuove tecnologie, piuttosto che limitarsi a implementarle e sperare che vada tutto bene.

Incertezza globale

L'incertezza globale è un altro dei fattori chiave che influisce sulla strategia tecnologica. Le tensioni geopolitiche e le conseguenti preoccupazioni economiche hanno oggi un impatto più marcato sul processo decisionale rispetto al passato. Le organizzazioni moderne non possono permettersi di considerare i fornitori solo per le capacità tecniche che offrono, ma devono valutarli anche alla luce di tutta una serie di questioni geopolitiche. Il livello di preoccupazione rispetto al clima di incertezza globale è cresciuto esponenzialmente.[2] Le organizzazioni odierne devono infatti barcamenarsi fra dazi, conformità alle normative vigenti e controllo delle esportazioni. Le tensioni geopolitiche sono una minaccia per le catene di distribuzione globali e a via via spingono sempre più aziende a mantenere i propri ecosistemi tecnologici all'interno dei confini nazionali.

Dazi e controllo delle esportazioni

Le preoccupazioni relative all'applicazione di dazi e ai potenziali cambiamenti valutari stanno portando le aziende a guardare con occhi nuovi l'acquisto di soluzioni da fornitori esteri. Se dovesse crescere la volatilità e dovessero cambiare le dinamiche valutarie tra i Paesi, un contratto a lungo termine con un provider estero potrebbe apparire molto diverso a un anno dalla firma. Si tratta di una questione cruciale che sta attualmente condizionando l'intera strategia IT e che rappresenta un cambiamento significativo rispetto al passato, quando simili questioni influivano meno sul processo decisionale per l'acquisto di soluzioni IT.

[2] McKinsey & Company, "Navigating the New Geopolitical Uncertainty", 16 gennaio 2025, *https://www.mckinsey.com/capabilities/geopolitics/our-insights/navigating-the-new-geopolitical-uncertainty*.

Sovranità digitale

Le pressioni geopolitiche vanno ben oltre la sfera economica: ad esempio i requisiti normativi variano da Paese a Paese e questo ha un impatto importante sulle dinamiche tra clienti e fornitori. Un esempio eclatante è quello del cloud computing: in seguito all'applicazione di normative come il Regolamento generale sulla protezione dei dati (GDPR) sempre più aziende chiedono soluzioni cloud "EU-only" per avere la certezza che dati rimangano all'interno dell'UE. Oggi quindi si nota da parte delle organizzazioni un interesse e una ricerca attiva di provider di servizi cloud che siano in linea con le specifiche esigenze normative dell'azienda.

Incertezza economica

Da sempre le pressioni economiche hanno avuto un forte impatto sull'IT. Oggi però a questo aspetto se ne accompagnano anche altri, come la velocità dell'innovazione e le pressioni globali, che complicano notevolmente la situazione. Le difficoltà principali sono due: i vincoli di budget e la carenza di professionisti specializzati. Questo significa che mancano i fondi, ma paradossalmente anche che se ci fosse la possibilità di finanziare una nuova posizione di amministratore, non è detto le aziende riuscirebbero a trovare un professionista da assumere.

In un tale contesto di incertezza economica, l'ottimizzazione dei costi diventa un punto imprescindibile nella scelta del sistema operativo. Le aziende sono sempre più concentrare sull'operare scelte mirate ed efficaci che assicurino un ritorno sull'investimento (ROI) rapido e permettano di contenere i costi.

Sicurezza e violazione dei dati

La sicurezza delle risorse IT è stata per molti anni una delle principali preoccupazioni delle aziende e sondaggi come il 2025 Developer Survey di Stack Overflow mostrano chiaramente che la sicurezza, l'analisi delle vulnerabilità e i test sono una priorità per gli sviluppatori. Infatti, i partecipanti al sondaggio hanno indicato "preoccupazioni relative alla sicurezza e alla privacy" come motivazione principale per l'abbandono di una determinata tecnologia.

Attacchi alla catena di distribuzione

Conoscere la provenienza di un software non è più sufficiente. Oggi le aziende hanno bisogno di conoscere anche l'origine di tutte le dipendenze del software. Questo è un aspetto cruciale perché se un pacchetto minore ma essenziale per il funzionamento di un software viene compromesso, allora anche tutta l'organizzazione è a rischio. Forse l'esempio più famoso è l'attacco alla SolarWinds del 2021 che ha esposto i dati sensibili di un numero imprecisato di clienti a causa di una catena di distribuzione non sicura. Il problema dell'affidabilità delle dipendenze è ancora molto diffuso. Ad esempio, solo recentemente il registro JavaScript npm ha subito un attacco alla catena di distribuzione, con cui gli hacker sono riusciti a distribuire pacchetti all'apparenza sicuri sui dispositivi degli utenti per minare le criptovalute.

L'IA offre innumerevoli vantaggi per la produttività e le funzioni aziendali, ma rappresenta anche una minaccia per la sicurezza. Negli ultimi anni infatti abbiamo assistito al boom degli attacchi basati sull'IA e sembra che questa tendenza sia destinata ad aumentare. In un recente report di Experian l'IA figura tra le minacce più rilevanti, tanto che secondo l'agenzia nel 2026 supererà l'errore umano come causa principale delle violazioni dei dati.[3]

Preoccupazioni relative alla crittografia quantistica

Il quantum computing come minaccia emergente alla sicurezza è diventato oggetto di studio negli ultimi anni. La preoccupazione è che, a causa dell'approccio completamente diverso adottato dai computer quantistici al problema della crittografia classica, ad un certo punto (alcuni credono entro il decennio) tutti gli algoritmi di crittografia esistenti saranno decifrabili in pochi secondi. Questo renderà tutti i file e i datastore protetti con crittografia classica completamente vulnerabili. Gli hacker questo lo sanno bene e stanno già perpetrando un attacco chiamato "harvest now, decrypt later" che prevede di scaricare oggi tutti i dati possibili e violarne la crittografia in futuro quando avranno i mezzi per farlo.

[3] Experian, 2026 Data Breach Industry Forecast, 5 dicembre 2025, *https://www.experian.com/thought-leadership/business/2026-data-breach-industry-forecast-report*.

Con crittografia post-quantistica (PQC) si intende una crittografia di nuova generazione progettata per resistere ai computer quantistici. Questo tipo di crittografia, che impedisce agli hacker di portare avanti il loro attacco "harverst now, decrypt later", è però un campo di ricerca relativamente nuovo nell'ambito dell'informatica e non tutti i sistemi operativi dispongono di tale tecnologia.

IA

L'IA si è imposta come forza dominante che guida oggi molte delle decisioni relative agli investimenti tecnologici. Questa tendenza è evidente ormai da tempo e non sembra che assisteremo a cambi di rotta nel prossimo futuro. In particolare, l'IA influisce sempre più sulla scelta del sistema operativo e di tutta la tecnologia che lo circonda.

Vibe coding

L'IA ha trasformato gli scenari di utilizzo dei sistemi operativi. La programmazione, l'analisi dei dati e l'analisi del business sono ora accessibili anche a persone che non hanno competenze tecniche o specialistiche. Pensiamo al vibe coding, ovvero un metodo basato sull'IA che permette agli utenti di creare applicazioni senza che questi debbano necessariamente avere competenze specifiche di programmazione o sviluppo applicativo. Sempre più spesso il mercato premia i sistemi operativi intuitivi che offrono strumenti di sviluppo assistito dall'IA perché possono essere utilizzati da chiunque in azienda.

Accelerazione hardware

L'IA ha ancora scenari di utilizzo tradizionali che richiedono ampie funzionalità del sistema operativo. Per svolgere attività come l'inferenza, l'addestramento dei modelli o l'hosting di un chatbot basato su LLM, è essenziale che il sistema operativo interagisca efficacemente con le GPU e gli altri componenti hardware personalizzati. Garantire la compatibilità dell'hardware è un punto chiave perché assicura l'utilizzo lineare di chip specializzati che aiutano a incrementare la velocità, la portata e la versatilità delle funzionalità di IA. Le capacità di automazione e gestione basate sull'IA continueranno a mettere a dura prova le risorse hardware. Per questo motivo quando si sceglie un sistema operativo è cruciale valutare la sua capacità di interagire con soluzioni hardware avanzate.

Conclusioni

Quest'epoca turbolenta caratterizzata da repentine trasformazioni del mercato, caos globale e innovazione travolgente spinge le organizzazioni a rivalutare i sistemi operativi in uso e offre loro un'occasione senza precedenti. Sempre più aziende scelgono oggi di esplorare proattivamente nuove opportunità, invece di restare ancorate alle piattaforme in uso, ormai incapaci di tenere il passo con il cambiamento. La scelta del sistema operativo non deve più essere percepita come un'incombenza, ma deve essere vissuta come un'opportunità per migliorare le operazioni aziendali adottando il giusto strumento.

CAPITOLO 2

Dai problemi alle soluzioni

Nel Capitolo 1 abbiamo individuato i diversi fattori critici che influenzano la scelta del sistema operativo: l'accelerazione dell'innovazione, l'incertezza globale, le pressioni economiche, le preoccupazioni relative alla sicurezza e le esigenze dell'IA. Questo però è solo il primo step. Una volta riconosciuti gli aspetti chiave da tenere in considerazione, è necessario valutare come rispondere in modo efficace a tali sfide senza generare confusione operativa o nuove vulnerabilità. Il successo delle organizzazioni moderne dipende proprio dalla loro capacità di analizzare le sfide del mercato odierno e reagire in modo produttivo e competitivo. In questo capitolo ripercorreremo quindi tutte le sfide ed esamineremo le possibili soluzioni.

Strategie per l'accelerazione dell'innovazione

L'accelerazione dell'innovazione è diventata una priorità per i leader IT. Oggi non è più sufficiente tenere il passo della concorrenza, ma bisogna muoversi rapidamente e batterla sul tempo per ottenere il massimo vantaggio. Per fare ciò serve che la piattaforma alla base sia all'altezza ed è quindi importante valutare con cura l'acquisto del sistema operativo, che deve rispondere a esigenze specifiche e offrire vantaggi identificabili. Accelerare l'innovazione non significa apportare cambiamenti arbitrari, ma è un sottile gioco di equilibri e ogni modifica deve essere soppesata con la massima attenzione. Un sistema operativo efficace favorisce la sperimentazione senza però che questo vada a compromettere sicurezza, prestazioni e affidabilità.

Sperimentazione ponderata e rapida

Di fronte all'accelerazione dell'innovazione tecnologica i metodi tradizionali di sviluppo e valutazione si rivelano oggi inadeguati perché troppo lenti. Nell'ambito dello sviluppo applicativo questa tendenza all'accelerazione si può notare già da tempo: le aziende sono infatti passate dal ciclo di rilascio annuale basato su modello a cascata, allo sviluppo software basato su metodologia agile, alla distribuzione continua di DevOps, fino agli odierni modelli di implementazione iperveloci con aggiornamenti multipli giornalieri. In realtà, questa tendenza si può osservare bene o male in tutto il panorama tecnologico e gli stessi leader IT riconoscono la necessità di seguire l'esempio per rimanere competitivi.

Per accelerare l'innovazione bisogna implementare cicli rapidi di sviluppo e test, il tutto garantendo un buon livello di sicurezza per non mettere a rischio le aziende. Una sperimentazione efficace richiede ambienti sandbox sofisticati che forniscano condizioni simili a quelle di produzione, senza mettere a rischio i dati aziendali (o il sistema operativo che ospita l'applicazione). Questo è il modo più efficiente per ottenere ambienti di test realistici dove è possibile esaminare in tempi brevi le prestazioni in condizioni di produzione reali.

Allo stesso modo le applicazioni hanno bisogno di un percorso affidabile che consenta loro di passare in maniera rapida e in tutta sicurezza dalla fase di test a quella di produzione. Dovrebbe essere un processo senza soluzione di continuità che permetta alle applicazioni testate di funzionare in modo affidabile in produzione. Questa non è solo una questione di comodità: l'affidabilità e la ripetibilità assicurano upgrade efficienti (e sicuri) tanto quanto il deployment di test iniziale.

Alla luce di ciò è evidente che quando si tratta di scegliere un sistema operativo conviene mantenere una mentalità aperta e che in un periodo di innovazione rapida l'agilità rappresenta un importante vantaggio strategico. In sostanza, il sistema operativo ospita le applicazioni e, con i requisiti delle applicazioni che cambiano così rapidamente, le organizzazioni devono sapere che il sistema operativo sarà in grado di tenere il passo. Anche studi e analisi condotti da aziende come IDC e McKinsey confermano la bontà di un simile approccio. Nel giugno 2024 McKinsey ha dichiarato: "La verità è che non esiste un approccio universalmente valido. Al contrario, le

aziende devono trovare il giusto equilibrio fra il desiderio di innovare e la necessità di avere infrastrutture tecnologiche robuste e affidabili."[1]

Le organizzazioni devono selezionare con attenzione gli strumenti e le tecnologie da implementare. Cambiare solo per il gusto di cambiare è pericoloso, soprattutto quando si parla di uno strumento così fondamentale come il sistema operativo. Apportando modifiche arbitrarie si rischia infatti di aggiungere complessità senza un reale beneficio. Il passaggio a una nuova soluzione è giustificato se questo apporta vantaggi chiaramente misurabili alle capacità dell'organizzazione. Cambiare sull'onda dell'entusiasmo senza un valido ragionamento dietro si rivela spesso controproducente. A questo proposito, il processo decisionale per la scelta di una nuova soluzione deve essere anche lungimirante e tenere conto non solo delle capacità attuali del sistema operativo ma anche del suo potenziale e stabilità futuri.

Architettura incentrata sulla sicurezza

La rapidità dell'innovazione tecnologica non va a vantaggio solo delle aziende legittime. Le minacce alla sicurezza informatica continuano a evolversi e rappresentano un rischio reale per le aziende che non adottano misure appropriate. Alcune ricerche di mercato, come il *2025 Global Threat Report* di CrowdStrike, mostrano che le minacce informatiche si evolvono più rapidamente dei sistemi di difesa. Infatti, di fronte al complesso panorama di minacce moderne molti framework di sicurezza e strumenti IT tradizionali stanno dimostrando tutta la loro inadeguatezza. Questo aspetto non deve essere preso alla leggera perché la capacità di contrastare le minacce moderne è oggi più importante che mai.

L'architettura di sicurezza è uno dei fattori chiave da prendere in considerazione quando si intende implementare un nuovo sistema operativo. Le organizzazioni che trascurano questo aspetto rischiano di esporre ad attacchi non solo le applicazioni ospitate sul sistema ma anche il sistema stesso. Ciò è particolarmente vero oggi che sempre più fornitori di sistemi operativi arricchiscono le loro piattaforme con funzionalità di IA e per far sì che possano svolgere attività come

[1] McKinsey, "Rethinking Conventional Wisdom: Future of Digital Tech Infrastructure", 26 giugno 2024, *https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/ tech-forward/rethinking-conventional-wisdom-future-of-digital-tech-infrastructure*.

l'amministrazione automatizzata del sistema, garantiscono loro privilegi di accesso molto estesi.

La sicurezza dei dati è essenziale

Un buon sistema operativo deve offrire ambienti sicuri in cui le applicazioni possano funzionare e i dati si possano archiviare senza correre rischi. Un'azienda deve essere certa che tutto ciò che viene eseguito, che si tratti di un componente integrato o di un'applicazione ospitata dal sistema operativo, sia sempre al sicuro. Quando si parla di sicurezza dei dati, i "dati" a cui si fa riferimento sono di tre tipi:

Dati inattivi
: I dati archiviati per un utilizzo futuro.

Dati in transito
: I dati che passano da un'applicazione all'altra. Possono spostarsi da un sistema a un altro oppure all'interno dello stesso sistema.

Dati in uso
: I dati che sono elaborati attivamente dalla piattaforma di elaborazione.

La sicurezza dei dati inattivi e di quelli in transito viene di norma garantita tramite crittografia, mentre la protezione dei dati in uso è più complessa. Le moderne architetture dei sistemi operativi risolvono il problema incorporando un ambiente di esecuzione attendibile (TEE). Si tratta di una sezione del sistema riservata a software altamente affidabili e accessibile solo tramite meccanismi strettamente controllati. Ciò che è in esecuzione all'interno di un TEE solitamente non è accessibile dall'esterno. Un TEE può essere una soluzione hardware o software e in genere si estende oltre un singolo server e richiede l'aggiornamento puntuale di driver e compatibilità per funzionare correttamente. Come poi viene implementato in pratica un TEE varia da fornitore a fornitore, ma questo aspetto esula dall'ambito del report. Quello che più ci preme sottolineare è l'esistenza di questi ambienti sicuri e la loro importanza per la sicurezza dei dati.

I carichi di lavoro dell'IA richiedono misure aggiuntive

Come accennato in precedenza, le aziende moderne devono garantire la protezione e la sovranità dei dati. Questo è vero per i carichi di

lavoro standard, ma lo è ancora di più per i carichi di lavoro dell'IA che, dato l'impiego massiccio di dati, la relativa novità della tecnologia e la complessità del processo di elaborazione, si dimostrano particolarmente vulnerabili.

Sottolineiamo il fatto che l'IA è una tecnologia relativamente recente perché significa che non c'è stato ancora il tempo per testare i carichi di lavoro di produzione, o almeno non così approfonditamente come è stato fatto con quelli standard. La sicurezza è come sappiamo uno sforzo collaborativo perché il mercato è in grado di effettuare molti più test e controlli di qualità di quanto possa fare un singolo fornitore. Questo vale sia per il prodotto stesso che per il modo in cui viene configurato/utilizzato. Secondo il *Tenable Cloud Security Risk Report 2025* i carichi di lavoro nel cloud a supporto dell'IA sono più vulnerabili rispetto agli altri. Sicuramente, l'impiego massiccio di dati da parte dell'IA unito a configurazioni errate e vulnerabilità persistenti richiede oggi organizzazioni più attente e solerti in materia di sicurezza, ma questo indipendentemente dall'ambiente in cui si eseguono i carichi di lavoro dell'IA.

Quando valutano la scelta del sistema operativo, le organizzazioni devono assicurarsi di tenere conto dei rischi specifici dell'IA. Non farlo significa introdurre un livello di rischio sconosciuto che potrebbe compromettere i carichi di lavoro attuali e quelli futuri.

Conclusioni

Pianificare in maniera strategica l'acquisto di un sistema operativo richiede alle organizzazioni di uscire dai vecchi schemi mentali e valutare le tecnologie con un approccio nuovo. In questo capitolo abbiamo elencato le sfide principali che le aziende moderne devono saper riconoscere e affrontare per mantenere il vantaggio competitivo e al termine di questo report esamineremo un framework decisionale che include tutti gli aspetti visti finora. Per il momento limitiamoci a prendere atto che la scelta di un nuovo sistema operativo richiede un cambio di prospettiva e soluzioni moderne. Le organizzazioni che accettano la sfida e pensano in modo strategico si troveranno avvantaggiate e potranno sfruttare a piano il potenziale delle tecnologie emergenti.

CAPITOLO 3

La piattaforma Linux moderna

La grande maggioranza delle aziende moderne esegue le operazioni dei server su piattaforme Linux. Un dato che è stato confermato da numerosi studi nel corso degli ultimi 10 anni. Per citarne solo uno, nell'agosto 2025 SQ Magazine ha riportato che il 61,4% delle grandi aziende esegue almeno un carico di lavoro critico su Linux e che il 78,3% dei server web collegati a Internet utilizza Linux.[1] Dopo anni di crescita esponenziale, fenomeno che non accenna a rallentare, Linux è oggi senza dubbio una realtà leader di settore.

Raramente però le analisi su Linux si soffermano sulle differenze fra le diverse distribuzioni, il che induce molti decision maker nell'errata convinzione che un sistema Linux valga l'altro. Ma non è così. Se è vero che tutte le distribuzioni Linux utilizzano lo stesso kernel Linux di base, il modo in cui questo kernel viene implementato e l'ecosistema di strumenti e applicazioni che lo circonda possono variare notevolmente da una distribuzione all'altra.

Quando un'organizzazione sta vagliando diversi sistemi operativi, deve individuare i fattori chiave che differenziano ciascuna soluzione dalle concorrenti. Ad esempio, quasi tutti i sistemi operativi moderni offrono funzionalità all'avanguardia, ma ogni piattaforma gestisce queste funzionalità in maniera differente, per cui non è detto che le metta a disposizione tutte in tutti gli ambienti. Tra le altre cose, un buon sistema operativo dovrebbe offrire: modelli di deployment moderni e sicuri, strumenti di sistema integrati con l'IA, strumenti per la gestione del parco risorse, sicurezza di livello enterprise, supporto

[1] Robert A. Lee, "Linux Statistics 2025: Desktop, Server, Cloud & Community Trends", *SQ Magazine,* aggiornato il 18 novembre 2025, *https://sqmagazine.co.uk/linux-statistics*.

esteso e partner certificati. Fondamentale è anche valutare le funzionalità di un sistema operativo alla luce dei requisiti dei carichi di lavoro che verranno eseguiti su di esso.

Rivoluzionare il deployment dei sistemi operativi

Il deployment dei sistemi operativi non è cambiato molto nel corso degli anni. La distribuzione tradizionale prevedeva un programma di installazione che copiava il kernel e altri strumenti sul disco rigido, seguito poi dall'installazione dalle applicazioni da parte degli utenti. Con il tempo si è passati alla gestione dei pacchetti. Questo approccio ha segnato un grande passo in avanti per la gestione delle applicazioni e l'amministrazione dei sistemi perché non richiedeva più di scrivere da zero il codice ogni volta che si installava o si aggiornava un'applicazione.

Una distribuzione Linux moderna dovrebbe fornire una modalità di deployment in cui i sistemi sono trattati come container immutabili e si possono sostituire in base alle esigenze. Così facendo agli utenti basterebbe scaricare una nuova immagine e con un semplice riavvio eseguire l'upgrade (o il downgrade) del componente che desiderano modificare. In questo modo si ottengono massima sicurezza e affidabilità, oltre ad avere la certezza che tutti i sistemi eseguono sempre la versione dei file binari e delle librerie prevista.

Le immagini create si gestiscono come i container (o le immagini) delle applicazioni, ma si opera su una scala più ridotta (a livello dei file binari e persino del kernel del sistema operativo stesso). Si tratta di un notevole miglioramento rispetto al precedente modello di aggiornamento basato sui pacchetti. Rispetto alla compilazione da zero, il modello a pacchetti è sicuramente superiore, ma genera comunque diversi problemi legati alla compatibilità, ai requisiti dei pacchetti e a potenziali conflitti tra le versioni. Un modello basato sui container invece elimina queste criticità perché è tutto contenuto nell'immagine. Le versioni degli elementi inclusi nel container rimangono coerenti e questo riduce notevolmente le preoccupazioni di molti amministratori di sistema circa gli errori di configurazione. Inoltre, l'installazione dell'immagine è molto più facile e veloce perché è sufficiente scaricare l'immagine, applicarla e riavviare il sistema.

Le immagini sono immutabili e questo è ottimo dal punto di vista della sicurezza, dato che nessun utente malintenzionato o malware potrà modificare l'immagine in loco, né sostituirla. Come già accennato, queste immagini si gestiscono come i container delle applicazioni e quindi per visualizzarle si possono utilizzare gli stessi strumenti standard che si usano per i container, come Podman o altre note piattaforme. Il fatto di poter utilizzare strumenti con cui gli amministratori hanno già dimestichezza garantisce processi di deployment del sistema operativo più rapidi e lineari.

Infine, le immagini create si possono utilizzare in qualunque ambiente. Che si esegua il deployment in ambienti fisici, virtualizzati, cloud o edge, l'immagine verrà distribuita ed eseguita ovunque in maniera coerente. Con questo approccio risulta anche più facile gestire il ciclo di vita delle immagini. La Figura 3-1 mostra un processo in modalità immagine suddiviso in tre semplici passaggi: creazione, distribuzione delle immagini e gestione delle immagini dopo il deployment.

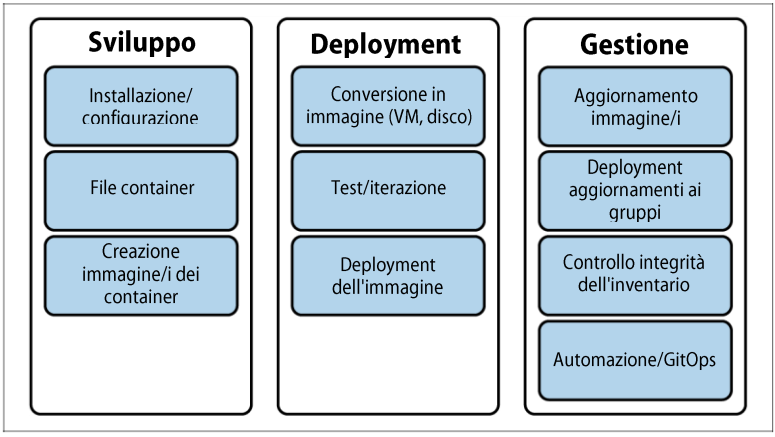

Figura 3-1. Modello di deployment di un sistema operativo containerizzato (modalità immagine)

Amministrazione dei sistemi assistita dall'IA

Sempre più sviluppatori di applicazioni integrano l'IA direttamente negli strumenti di amministrazione dei sistemi, servendosi ad esempio di emulatori di terminale (che danno accesso alla riga di comando).

Questi strumenti sono estremamente preziosi perché consentono agli amministratori di interrogare gli LLM senza dover aprire una finestra del browser o un'applicazione separata. Visto il trend è logico pensare che a breve anche i produttori di sistemi operativi andranno in quella direzione, incorporando l'IA nelle loro soluzioni. Questa sarebbe una fantastica opportunità per gli utenti che potrebbero richiamare l'assistente IA dalla riga di comando, indipendentemente dal terminale in uso. Una simile funzionalità sarebbe utile per gli amministratori di tutti i livelli, ma in particolare per gli amministratori junior che potrebbero interrogare l'assistente IA direttamente dalla riga di comando e chiarire eventuali dubbi sul loro lavoro.

Tuttavia, come qualunque strumento di IA, anche gli assistenti da riga di comando si devono utilizzare con cautela. Ad esempio, bisogna prestare particolare attenzione a come si formulano le query perché lo strumento possa fornire risposte accurate, specialmente quando si tratta di generare stringhe di codice come uno script di shell.

Quando in dubbio sulla bontà dell'output, sarebbe quindi consigliabile per gli amministratori junior rivolgersi a un collega senior e valutare insieme se la risposta fornita dall'assistente IA darà il risultato sperato.

In teoria, questi strumenti saranno più efficaci degli script bash di base perché saranno in grado di fornire consigli pratici sulla configurazione di applicazioni e servizi e riusciranno a utilizzare le funzionalità del sistema operativo per risolvere i problemi. Prima però occorrerà un addestramento mirato su Linux in generale, sui dettagli più specifici della distribuzione e sulle sue esigenze e requisiti particolari. Niente di nuovo nel mondo dell'IA, dove il fine tuning si utilizza regolarmente per addestrare gli LLM generici su scenari di utilizzo specifici. In questo modo si migliora l'accuratezza dei modelli in ambiti particolari e si ottengono strumenti davvero efficaci con un potenziale incredibile.

Un assistente da riga di comando sarebbe decisamente utile per strumenti come Security-Enhanced Linux (SELinux) e il firewall integrato. Entrambi sono molto importanti per il funzionamento del sistema ma sono complessi e per questo motivo le loro configurazioni vengono modificate solo di rado. Con l'aiuto di un assistente da riga di comando invece l'attività di configurazione risulterebbe molto più agevole e veloce. Inoltre, lo strumento di IA metterebbe a disposizione molti esempi verificati, il che permetterebbe agli utenti di prendere

dimestichezza con le best practice e consentirebbe loro di individuare configurazioni errate difficilmente rilevabili anche dagli amministratori più esperti.

Infine, gli assistenti da riga di comando potrebbero essere utili anche per comprendere la struttura degli strumenti in uso. Ad esempio, se un utente volesse sapere come si implementano i moderni firewall basati su host, gli basterà chiedere all'assistente. Questo interrogherà le risorse pertinenti alla ricerca di best practice ed esempi rilevanti e formulerà una risposta in inglese. Nella risposta saranno integrate le modifiche alla configurazione o al codice sorgente per permettere all'utente di capire meglio i suggerimenti dell'IA.

Strumenti per la gestione del parco risorse

I due strumenti visti finora sono soluzioni potenti che permetterebbero di semplificare davvero la gestione, a livello però di singolo sistema. Lo strumento di cui parliamo ora offrirebbe invece un vantaggio a livello più ampio perché permetterebbe agli utenti di gestire in modo proattivo l'intero ambiente Linux. Uno strumento di questo tipo avrebbe profonde connessioni con tutto ciò che offre il produttore di sistemi operativi e permetterebbe di gestire l'intera piattaforma da un'unica interfaccia, semplificando così le attività di amministrazione e verifica. Idealmente, dovrebbe includere anche una funzionalità di pianificazione che aiuti le organizzazioni a comprendere i cicli di vita delle applicazioni in uso e come questi influenzano i sistemi in esecuzione nell'ambiente. Grazie a queste integrazioni sarebbe possibile monitorare e convalidare la sicurezza e le configurazioni in tempo reale e in tutta l'organizzazione.

Le funzionalità di pianificazione fornirebbero informazioni dettagliate in merito al rilascio delle nuove versioni di app e sistemi operativi in modo che le organizzazioni possano pianificare con largo anticipo gli aggiornamenti.

Gli strumenti per la gestione del parco risorse si possono utilizzare anche per l'aggiornamento dei sistemi. L'applicazione coordinata delle patch (automatizzata o pianificata), gli aggiornamenti o i rollout di funzionalità/software e la gestione centralizzata della configurazione rendono la gestione di migliaia di server una passeggiata.

Sicurezza di livello enterprise

Un sistema operativo incentrato sulla sicurezza non può limitarsi alle strategie di sicurezza elencate finora, come immagini immutabili e gestione della configurazione.

Oggi si parla molto di crittografia post-quantistica e delle sue potenzialità contro le minacce informatiche future. I suoi algoritmi infatti sono progettati per resistere al quantum computing e si applicano a chiavi, crittografia e firme digitali. Questa è una funzionalità essenziale da avere in un sistema operativo per ottenere dati e applicazioni a prova di attacchi informatici, oggi e in futuro.

Una piattaforma di livello enterprise deve offrire anche funzionalità di sicurezza per la catena di distribuzione, che deve diventare una priorità, soprattutto per chi si orienta su pratiche DevSecOps. Per garantire la sicurezza della catena di distribuzione, le aziende possono scegliere di ubicare le dipendenze applicative note in una posizione sicura; ma questa è solo una delle molte tecniche disponibili. Idealmente, una piattaforma DevSecOps dovrebbe fornire ai team di sviluppo una pipeline di sicurezza end to end per tutte le loro applicazioni e dipendenze.

L'utilizzo sinergico di PQC, strumenti di sicurezza automatizzati per amministratori e sviluppatori e gestione proattiva dei software crea una struttura di difesa a più livelli che rimane sempre aggiornata e permette di affrontare al meglio le minacce moderne. Inoltre, dato che gli strumenti e il sistema operativo in uso già forniscono tutte le tecnologie e funzionalità di sicurezza necessarie, le organizzazioni non dovranno più fare ulteriori investimenti per acquistare soluzioni di sicurezza di terze parti.

Supporto e certificazione hardware e software ampliati

Per quanto avanzato e completo possa essere un sistema operativo, le organizzazioni hanno comunque bisogno di compatibilità esterna. Questo vale sia per l'hardware su cui viene eseguito il sistema operativo che per il software di terze parti che verrà utilizzato nel sistema in esecuzione.

Al giorno d'oggi la compatibilità hardware è un mercato in rapida evoluzione. Le soluzioni hardware per l'IA, in particolare, cambiano molto rapidamente per cui è necessario adottare sistemi operativi capaci di tenere il passo e garantire sempre la perfetta compatibilità. È importante assicurarsi che la distribuzione scelta offra librerie, driver e applicazioni di IA aggiornate, oltre a ottimizzazioni hardware per produttori come NVIDIA, Intel e AMD. In linea generale, le aziende dovrebbero puntare su produttori di sistemi operativi che dispongono di un solido ecosistema di terze parti. Qui potranno trovare le ultime funzionalità e integrarle nella loro soluzione in modo rapido, sicuro e affidabile.

Conclusioni

Le funzionalità di sicurezza, l'ecosistema e il set di funzionalità incluse nella piattaforma sono fattori importanti da considerare quando si valuta l'acquisto di un sistema operativo. In questo capitolo abbiamo voluto passare in rassegna le caratteristiche principali che fanno emergere un sistema operativo dalla concorrenza, sia in termini di capacità che di facilità di gestione. Oggi le aziende cercano fornitori che offrano non solo funzionalità all'avanguardia ma anche un ampio ecosistema di partner.

CAPITOLO 4

Passaggi successivi

La scelta del sistema operativo è una decisione di importanza cruciale perché può assicurare il successo aziendale e razionalizzare la gestione interna dell'infrastruttura. Per affrontare le sfide moderne, quali accelerazione dell'innovazione, incertezza globale, vincoli economici, esigenze di sicurezza e dell'IA, è necessaria una piattaforma solida e affidabile appositamente progettata per supportare le aziende in questi tempi turbolenti.

La scelta del sistema operativo non deve essere presa alla leggera. Il processo decisionale dovrebbe comporsi di quattro passaggi fondamentali:

- Identificare le priorità per l'organizzazione.
- Mappare i carichi di lavoro in base ai requisiti di capacità.
- Valutare il valore complessivo per l'azienda.
- Verificare la sicurezza della catena di distribuzione e la sostenibilità a lungo termine.

Identificare le priorità per l'organizzazione

Team diversi hanno ovviamente priorità diverse. Ad esempio, i team dei prodotti di IA saranno focalizzati su innovazione e requisiti hardware, mentre quelli che operano in settori regolamentati si concentreranno maggiormente su funzionalità di sicurezza e conformità. Le organizzazioni dovrebbero classificare i diversi aspetti (accelerazione dell'innovazione, incertezza globale, vincoli economici, esigenze di sicurezza e IA) in base alla rilevanza che hanno per loro

oggi e che avranno in futuro, così da distinguere gli elementi solo utili da quelli davvero indispensabili.

Mappare i carichi di lavoro in base ai requisiti di capacità

Saranno i carichi di lavoro più importanti per l'organizzazione a determinare i requisiti. Un'analisi dei carichi di lavoro rivelerà se l'organizzazione può davvero beneficiare dall'ottimizzazione specifica per carichi di lavoro o se non è più utile adottare un approccio di standardizzazione ad ampio spettro. Questo passaggio è utile per le organizzazioni di grandi e piccole dimensioni poiché il numero e l'importanza dei carichi di lavoro non sono necessariamente correlati alle dimensioni dell'azienda.

Valutare il valore per l'azienda

Una volta analizzati i carichi di lavoro, l'organizzazione avrà un'idea chiara del numero di server, numero di dipendenti (e del loro livello di competenza) e del numero totale dei carichi di lavoro. Dati alla mano potrà valutare i costi diretti, come le licenze del sistema operativo, il supporto e l'infrastruttura. E potrà anche stimare i costi indiretti, come il livello di competenza interna, i ritardi nel deployment dei carichi di lavoro dovuti a vincoli imprevisti e le opportunità di business perse a causa della mancanza di flessibilità dell'infrastruttura. Queste informazioni approfondite permettono di prendere decisioni strategiche più informate che miglioreranno l'efficienza operativa e aumenteranno il vantaggio competitivo.

Verificare la sicurezza della catena di distribuzione e la sostenibilità a lungo termine.

Prima di decidere se acquistare un sistema operativo o una qualsiasi piattaforma, l'organizzazione deve assicurarsi che il sistema operativo o la piattaforma in questione saranno disponibili a lungo termine. Deve inoltre studiare attentamente il fornitore: conoscerne la storia, sapere in che modo controlla le sue applicazioni, l'affidabilità e l'ampiezza del suo ecosistema di partner e la sua esperienza in merito

ad aspetti critici, come la conformità normativa e l'IA. I carichi di lavoro moderni hanno cicli di vita pluriennali. Per questo motivo è essenziale che la piattaforma sia in grado di rispondere alle esigenze di oggi e a quelle future.

Conclusioni

La chiave per operare una scelta vincente è comprendere che le decisioni relative all'infrastruttura creano dipendenze. Le scelte fatte oggi possono determinare il successo dell'organizzazione oppure limitarne le capacità e le prestazioni per gli anni a venire. Le organizzazioni che affrontano la scelta del sistema operativo in maniera strategica saranno in grado di tenere il passo dell'innovazione, affrontare con successo l'incertezza e ottimizzare sia la produttività che la sicurezza, oggi e in futuro.

Informazioni sugli autori

Ned Bellavance è un professionista IT e un formatore tecnico con oltre 20 anni di esperienza nel settore. È stato operatore di helpdesk, amministratore di sistema, architetto cloud e product manager. Oggi Ned gestisce Ned in the Cloud LLC, dove sviluppa corsi, conduce podcast, scrive libri e crea contenuti originali per fornitori tecnologici. Ned è Microsoft MVP dal 2017 e HashiCorp Ambassador dal 2020. Vive secondo tre principi cardine: accetta il disagio, preparati al fallimento e sii gentile.

Chris Hayner è un professionista IT esperto che vanta un'esperienza decennale in ambiti quali sistemi operativi, infrastruttura, cloud computing e sicurezza informatica. La sua carriera è cominciata nel datacenter, dove ha gestito una vasta gamma di sistemi, dai mainframe agli AlphaServer fino ai server x86 white box. Nel corso degli anni il suo bagaglio di competenze si è ampliato, includendo virtualizzazione, tecnologie cloud, sicurezza informatica e strategie IT. Negli ultimi 15 anni Chris ha lavorato come consulente in qualità di esperto in materia (SME), architetto e analista. Ha affiancato centinaia di organizzazioni aiutandole a colmare il divario tra gli obiettivi aziendali e le soluzioni IT e promuovendo l'innovazione e il successo operativo. Oltre a possedere una certificazione CISSP e numerose certificazioni di fornitori e settore, Chris ha conseguito un MBA presso la Temple University.