

# Migliorare la sicurezza nell'intero ciclo di vita dei server



## Dalla progettazione alla dismissione, le aziende devono adottare un approccio olistico alla sicurezza server.

Viviamo in un mondo in cui l'intelligenza è ampiamente distribuita. Oggi l'elaborazione si estende dai data center e dal cloud a milioni di dispositivi presenti nei nostri uffici, nelle nostre case, nelle fabbriche, negli ospedali e nelle strutture pubbliche. L'intelligenza artificiale (AI) raccoglie i dati che provengono da questi dispositivi e li utilizza per promuovere l'innovazione e creare nuovi servizi.

Ma la nuova era di elaborazione distribuita basata sull'AI ha anche esteso di vari ordini di grandezza la superficie dei cyberattacchi, offrendo agli aggressori la possibilità di puntare su nuovi bersagli.

Oggi le organizzazioni subiscono in media circa 2000 cyberattacchi alla settimana, ovvero il 75% in più rispetto a un anno fa.<sup>1</sup> E poiché le aziende conservano le infrastrutture legacy, nella speranza di ridurre le spese di capitale estendendo i cicli di vita dei server, si ritrovano sempre più esposte.

La modernizzazione è essenziale per le difese di un'organizzazione. Se l'hardware dei server di un'azienda non è sicuro, non lo saranno nemmeno dati e applicazioni. Le imprese devono pensare alla sicurezza in modo olistico, cominciando dalle macchine stesse. Ecco perché Hewlett Packard Enterprise adotta un approccio di difesa multilivello, esaminando ogni fase del ciclo di vita del server, dalla progettazione iniziale alla dismissione finale.

<sup>1</sup> "A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide," Check Point Research, Oct 18, 2024.

## Silicon Root of Trust

Negli ultimi sette anni, i server HPE ProLiant sono stati forniti con la tecnologia Silicon Root of Trust, un Baseboard Management Controller (BMC) personalizzato che funge da impronta digitale immutabile. Il BMC contribuisce a garantire che il firmware di un server corrisponda al codice installato in fabbrica e impedisce l'avvio della macchina qualora il firmware sia stato compromesso. La Silicon Root of Trust consente inoltre di ripristinare facilmente uno stato sicuro precedente dei server in caso di attacco e di impedire la diffusione di codice dannoso.

Con l'ultima generazione di server HPE, questa tecnologia si estende ad altri componenti hardware nel percorso dati, tra cui schede NIC e controller di storage. I server HPE ProLiant Gen11 confermano automaticamente che i dispositivi connessi soddisfino le specifiche SPD (Security Protocol and Data Model) stabilite dall'organizzazione per gli standard Distributed Management Task Force. I dispositivi che non possono essere autenticati o il cui firmware è stato modificato, non possono accedere alla rete.

## Configurazioni Trusted Supply Chain

Gli attacchi alla supply chain hardware sono in aumento. Le aziende devono essere certe che i server su cui fanno affidamento non siano stati manomessi prima di raggiungere i loro data center.

I clienti che optano per le configurazioni HPE Trusted Supply Chain ottengono server conformi ai più rigorosi standard di sicurezza al mondo. Ad esempio, macchine come HPE ProLiant DL380T Gen11 vengono assemblate in strutture protette situate in luoghi geograficamente sicuri in tutto il mondo.

Questi server possono essere configurati per funzionare in modalità a elevata sicurezza, che richiede un'autenticazione specifica tramite crittografia prima che gli utenti possano effettuare l'accesso. Abilitando HPE Server Configuration Lock è possibile acquisire le impronte digitali di ciascuna configurazione del server; il sistema visualizza quindi un avviso qualora siano state modificate opzioni hardware o firmware. Questi sistemi possono anche essere dotati di rilevamento delle intrusioni nello chassis, segnalando i possibili casi in cui personale non autorizzato ha tentato di accedere all'hardware del server, una funzionalità essenziale per le distribuzioni all'edge.



## Connessioni da remoto sicure

HPE ProLiant Compute sfrutta il firmware proprietario noto come HPE iLO, consentendo agli amministratori di sistema affidabili di accedere ai server da remoto, anche se le macchine sono offline. Mediante HPE iLO, gli amministratori possono riavviare e ripristinare i server e persino accedervi in periodi di crisi digitale, come eventi meteorologici estremi o attacchi DDoS (Distributed Denial-of-Service), evitando costosi downtime.

## Gestione per ambienti distribuiti

Entro il 2027, un nuovo server su quattro sarà distribuito in sedi all'edge,<sup>2</sup> e le aziende devono saper gestire questi ambienti in continua evoluzione.

Le imprese devono avere la possibilità di creare un'unica policy di sicurezza e di applicarla automaticamente e in modo coerente a ogni server e dispositivo dell'organizzazione, indipendentemente dalla presenza o meno di personale IT

<sup>2</sup> "Gaining Timely Insights with AI Inference at the Edge," IDC, March 2024.

in loco. Ecco perché HPE ha implementato HPE Compute Ops Management nelle ultime generazioni di sistemi HPE ProLiant Compute. La soluzione basata su cloud consente agli amministratori di gestire migliaia di dispositivi da un'unica console, supportando il provisioning zero touch e gli aggiornamenti di sicurezza automatizzati. La gestione dei dispositivi aziendali a livello di parco macchine semplifica la verifica della loro corretta configurazione e consente all'IT di monitorare lo stato di integrità di ogni server durante il suo ciclo di vita.

### **Cancellazione sicura con un solo pulsante**

Prima o poi i server si guastano, raggiungono la data di fine vita del supporto o semplicemente non riescono a stare al passo con le esigenze dei moderni carichi di lavoro basati sull'AI. Ma i dati in essi contenuti non scompaiono e questo può costituire una minaccia reale per la sicurezza enterprise.

I dispositivi dismessi rappresentano una fonte significativa e spesso trascurata di violazioni dei dati. I vecchi componenti hardware possono contenere non soltanto informazioni riservate o regolamentate, come elenchi di clienti o dati dei dipendenti, ma anche credenziali di sicurezza e dati di accesso che potrebbero permettere agli aggressori di accedere alla rete aziendale in uso.

I server HPE includono la cancellazione sicura con un solo pulsante per garantire che dai dispositivi di storage collegati a un server siano stati eliminati tutti i dati, comprese le informazioni di identificazione personale e altri materiali sensibili o proprietari.



### **Verso un'impresa più sicura**

Con l'aumento costante della complessità dell'IT, continueranno a crescere anche le minacce alla sicurezza enterprise. Dalla progettazione alla dismissione, HPE ha adottato misure per garantire che i suoi server siano tra i più sicuri mai realizzati.

Le organizzazioni che non adottano un approccio olistico alla sicurezza e non si affidano ai sistemi hardware più sicuri mettono a rischio se stesse e i propri clienti. Modernizzare i server ora può contribuire a impedire che accada il peggio in futuro.

## **Ulteriori informazioni alla pagina**

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

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

 **Avvia chat**