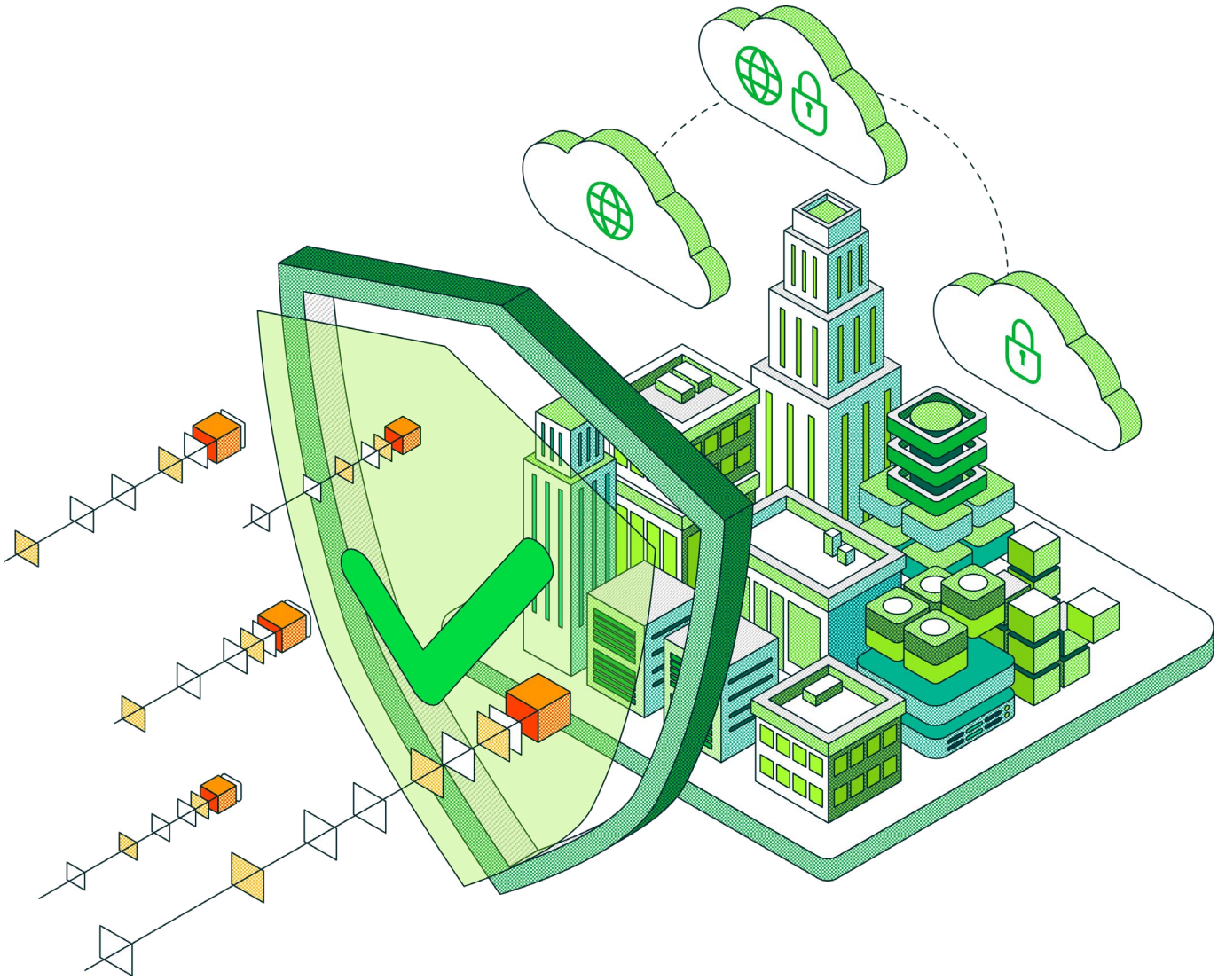
EXECUTIVE BRIEF

Tendenze nella protezione dei dati 2023

Edizione italiana



Al termine del 2022, una società di ricerca indipendente ha completato un sondaggio tra 4.200 leader e implementatori IT imparziali su una varietà di fattori trainanti, problematiche e strategie, tra questi, 312 erano in Italia. Questo ampio studio di mercato tra organizzazioni imparziali viene condotto ogni anno per conto di Veeam per comprendere come continua a evolversi il mercato della protezione dei dati, in modo che Veeam possa garantire che le strategie di prodotto e le iniziative di mercato siano allineate alle tendenze del mercato stesso.

Se Gartner prevede un aumento del 5,1% nei budget IT complessivi e IDC prevede un aumento del 5,2% nella spesa complessiva per l'IT, questo sondaggio ha rivelato che per i budget per la protezione dei dati è previsto un incremento globale del 6,5% nel 2023. Il Report sulle tendenze nella protezione dei dati 2023 completo è disponibile all'indirizzo https://vee.am/DPR23.

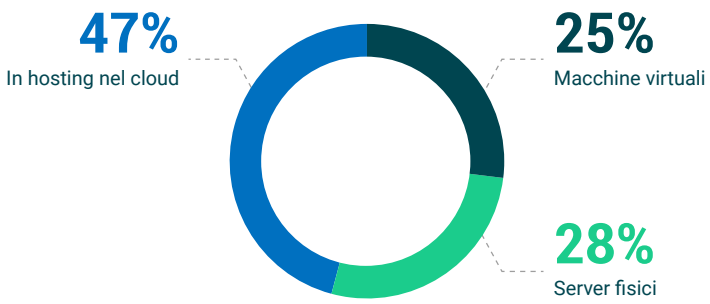
Le organizzazioni in Italia prevedono di aumentare il proprio budget per la protezione dei dati per il 2023 del

6,3%

Infrastruttura ibrida dal 2020 al 2025

Ogni anno il sondaggio chiede alle organizzazioni di stimare i server on-premises (fisici e virtuali) e quelli in hosting nel cloud, per l'anno in corso, così come le previsioni per i due anni successivi. **Dai un'occhiata al report completo** per un riepilogo delle **12.000** risposte nelle quattro indagini annuali per il periodo 2020-2025. Per il 2023, la distribuzione delle istanze server nell'IT ibrido di **4.200** organizzazioni è la seguente:

Panorama dell'IT ibrido nel 2023 (globale)



Complessivamente, i server **fisici** e le macchine **virtuali** si sono stabilizzati attorno al **50%** del piano IT complessivo delle organizzazioni, mentre il resto si trova **in hosting nel cloud**, con il continuo, seppur graduale, passaggio all'hosting nel cloud, principalmente a causa della strategia cloud-first delle organizzazioni per i nuovi carichi di lavoro, che vengono avviati nei cloud a tassi più elevati rispetto al numero di carichi di lavoro legacy dismessi nel data center, diluendo così il data center all'interno di una strategia complessiva di IT ibrido.

		REGIONE									
	GLOBALE	EMEA	DACH	UKI	Francia	Benelux	**Italia**	Iberia	Paesi Nordici	Europa dell'est	MEA
Server fisici	28%	28%	29%	28%	28%	28%	**29%**	29%	28%	27%	29%
Macchine virtuali	25%	26%	25%	27%	25%	25%	**25%**	25%	26%	25%	25%
In hosting nel cloud	47%	46%	46%	45%	47%	47%	**46%**	46%	47%	48%	46%

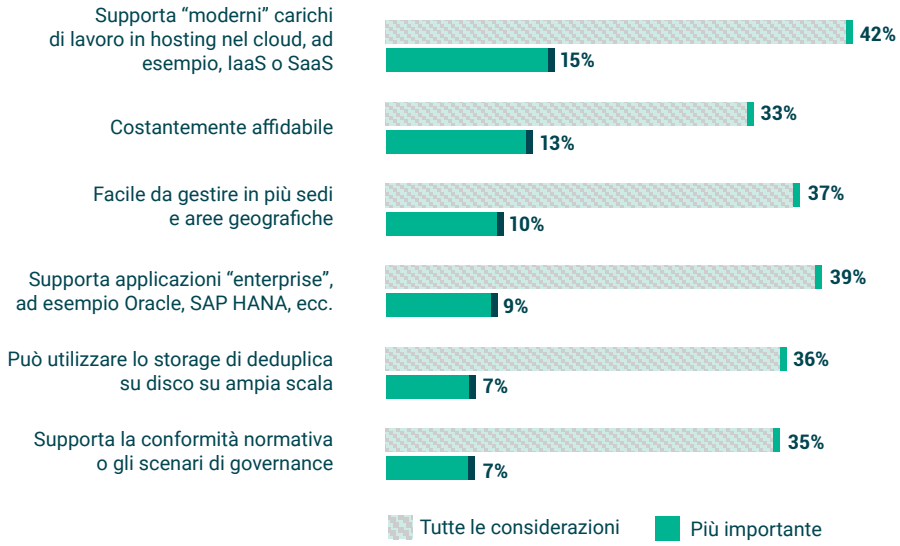
Il punto chiave è che le moderne soluzioni di protezione dei dati devono fornire il giusto livello di funzionalità in tutte e tre le architetture (fisica, virtuale e cloud). Inoltre, si dovrebbe pianificare il trasferimento dei carichi di lavoro tra diversi cloud e il loro ritorno on-premises e, ancora una volta, la strategia di protezione dei dati dovrebbe recepire tale fluidità.

Che cosa significa "backup enterprise"?

Per il secondo anno consecutivo, l'attributo più importante di una soluzione di "backup enterprise" è la **protezione di IaaS e SaaS.** Questa non dovrebbe essere una sorpresa considerando l'attuale transizione delle infrastrutture al cloud.

Ciò che potrebbe sorprendere, invece, è che garantire **l'affidabilità** è il secondo criterio più importante. Tuttavia, se si considera che molte organizzazioni potrebbero eseguire soluzioni di backup legacy progettate per l'era del data center fisico, è verosimile ritenere che tali soluzioni adottino approcci basati su agenti per proteggere i carichi di lavoro nel cloud. I meccanismi di backup legacy raramente producono buoni risultati quando si proteggono i carichi di lavoro moderni.

Per questo, ha senso che la protezione e l'affidabilità in hosting nel cloud siano viste come contigue e fondamentali.



12%

Percentuale delle organizzazioni in Italia alla ricerca di una soluzione di backup aziendale che considera **"la protezione dei carichi di lavoro IaaS e SaaS, oltre al data center"**, la capacità più importante

Figura 1.2

Cosa significa "backup enterprise" per te?

Se la tua organizzazione considerasse una nuova soluzione di "backup enterprise" oggi, quale caratteristica riterrebbe più importante?

In effetti, quando alle organizzazioni è stato chiesto cosa le avrebbe indotte a cambiare la soluzione di backup principale, il motivo più comune, oltre che più importante, è risultato **il miglioramento dell'affidabilità,** in linea con l'obiettivo ricercato dalle organizzazioni in una soluzione di backup enterprise.

34%

Percentuale delle organizzazioni in Italia che ha dichiarato che **"migliorare l'affidabilità/il successo dei backup"** è la ragione per cui desidera sostituire le soluzioni di backup

Per il 2023, protezione dei dati "moderna" significa "resilienza informatica"

Quando si considerano le problematiche che la moderna protezione dei dati deve risolvere, vale la pena notare che il report di ricerca completo rivela che, per il terzo anno consecutivo, gli attacchi informatici continuano a essere il motivo principale delle interruzioni di maggiore impatto, mentre la frequenza degli attacchi ransomware continua a salire:

- Nel 2021, il **76%** delle organizzazioni è stata attaccata con successo dal ransomware almeno una volta.
- Nel 2022, l'**85%** delle organizzazioni ha dichiarato la stessa cosa.

	GLOBALE	REGIONE EMEA	DACH	UKI	Francia	Benelux	**Italia**	Iberia	Paesi Nordici	Europa dell'est	MEA
Nessun attacco nel 2022	15%	16%	21%	24%	18%	25%	**14%**	22%	13%	17%	14%
Solo 1 attacco	18%	19%	24%	19%	17%	24%	**17%**	21%	23%	23%	18%
2 o 3 attacchi	48%	46%	40%	36%	49%	39%	**52%**	41%	44%	36%	48%
4 o più attacchi	18%	18%	14%	18%	15%	10%	**16%**	15%	18%	22%	21%

Per quanto sorprendenti possano essere queste statistiche, i risultati degli attacchi sono anche peggiori. Quando alle organizzazioni è stato chiesto degli attacchi più significativi subiti nel 2022, hanno affermato che:

- Il **39%** dell'intero set di dati in produzione è stato crittografato o distrutto con successo
- Solo il **55%** dei dati crittografati/distrutti è stato recuperabile

Quindi, non c'è da sorprendersi che l'aspetto più comune e più importante di una "moderna soluzione di protezione dei dati" sia l'integrazione della protezione dei dati all'interno di una strategia di preparazione informatica.

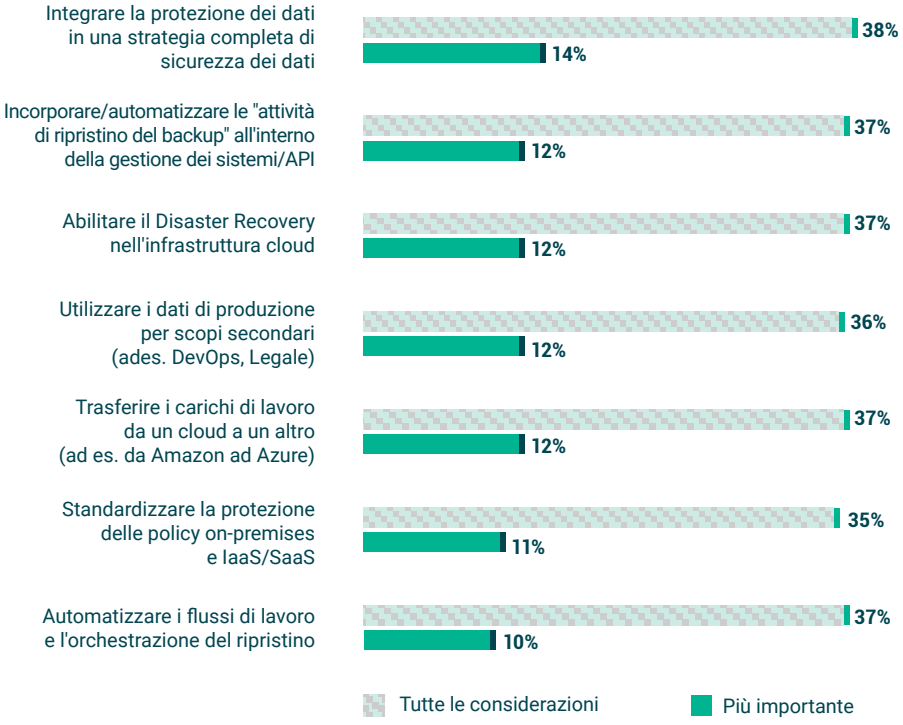


Figura 1.5

Quali considereresti gli aspetti determinanti di una soluzione di protezione dei dati "moderna" o "innovativa" per la tua organizzazione? L'aspetto più importante?

Tuttavia, anche se la resilienza informatica continua a essere al primo posto per molti leader IT, sarebbe un errore strategico significativo focalizzare tutta la pianificazione della protezione dei dati sugli attacchi. Le interruzioni dei sistemi, causate da guasti di rete, delle applicazioni o dell'hardware o da problemi del sistema operativo sono tutti ancora comuni anche nei moderni data center. Le organizzazioni dovrebbero essere preparate sia per le interruzioni che continuano a verificarsi, sia per gli eventi provocati dall'uomo, come gli errori utente e i criminali informatici.

Metodi e meccanismi del BC/DR

Man mano che i servizi cloud diventano sempre più comuni nelle strategie di protezione dei dati, molti si chiedono se ripristinare i dati sui server on-premises o nelle infrastrutture in hosting nel cloud. Mentre i risultati della ricerca dimostrano un interesse relativamente equilibrato tra i ripristini on-premises e in hosting nel cloud nel 2023, la maggior parte dei dati del ripristino giungerà dai backup in hosting nel cloud, poiché è stata seguita la prassi di avere meno punti di ripristino on-premises e di trasferire i dati fuori dai data center fisici verso uno storage basato sul cloud per la retention dei dati o la preparazione al ransomware o al BC/DR.

Se si considera la best practice di presupporre che gli esperti principali non saranno disponibili durante una crisi, una delle principali raccomandazione dei pianificatori di BC/DR è di utilizzare flussi di lavoro orchestrati, in cui le competenze possono essere integrate nei processi. Si consiglia inoltre di testare i flussi di lavoro nello stesso modo in cui verrebbero eseguiti durante una vera crisi. Purtroppo, i risultati del sondaggio di quest'anno hanno rivelato che solo il **18%** dispone attualmente di una capacità di flusso di lavoro orchestrato nell'ambito dell'attuale strategia di protezione dei dati o di failover.

52%

Percentuale delle organizzazioni in Italia che prevede di utilizzare server on-premises per il BC/DR, mentre il **48%** intende sfruttare l'infrastruttura in hosting nel cloud per lo stesso scopo

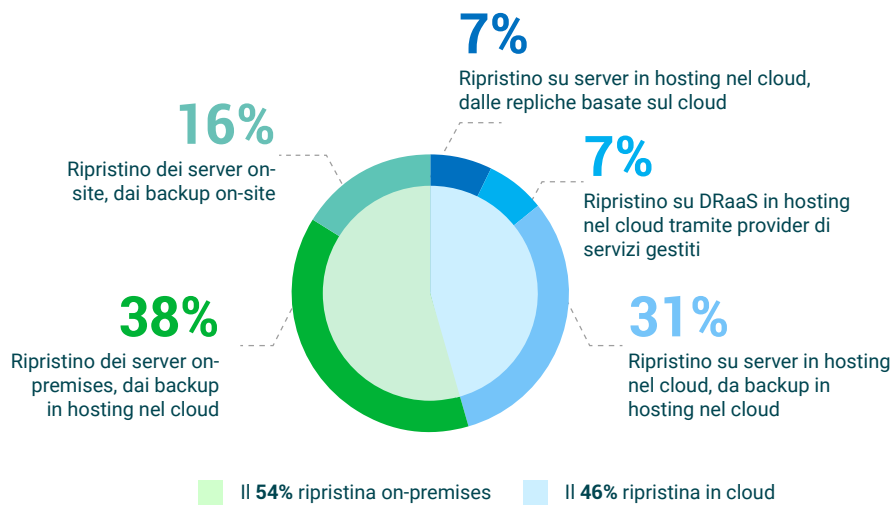


Figura 2.3

Come vengono ripristinate le operazioni per la funzione DR dell'organizzazione?

La protezione dei dati basata sul cloud continua a guadagnare popolarità

Lo storage basato sul cloud è un "killer del nastro?" Secondo i risultati del sondaggio, il **50%** dei dati viene ancora scritto su nastro in un qualche punto del ciclo di vita dei dati, mentre il **63%** dei dati è ora archiviato nel cloud, sebbene il processo possa variare nei diversi Paesi o regioni.

	GLOBALE	REGIONE EMEA	DACH	UKI	Francia	Benelux	**Italia**	Iberia	Paesi Nordici	Europa dell'est	MEA
% dei dati su nastro	50%	53%	48%	42%	51%	53%	**51%**	49%	52%	53%	52%
% dei dati nei cloud	63%	63%	63%	56%	64%	65%	**66%**	63%	63%	69%	64%

Molte organizzazioni hanno un modello operativo a tre livelli per la retention dei dati che include:

- Disco on-premises per 90-120 giorni
- Copie cloud, comprese le copie correnti e le versioni precedenti da due a cinque anni
- Nastro per la minoranza di dati che devono essere archiviati per oltre 10 anni

Come alternativa alla "percentuale dei dati che utilizzano il cloud", vale la pena considerare la "percentuale di organizzazioni che utilizzano i backup basati sul cloud", dato che il **67%** degli intervistati globali utilizzano i servizi cloud come parte integrante della strategia odierna di protezione dei dati, cifra che raggiungerà il **74%** entro il 2025.

Una delle sinergie realmente più potenti tra i servizi basati sul cloud e la protezione dei dati è l'avvento del disaster recovery basato sul cloud, in cui vengono sfruttatele infrastrutture cloud al posto di un data center secondario o in aggiunta a esso. Nel 2020, il **53%** delle organizzazioni aveva predisposto capacità di BC/DR, mentre il **71%** è in grado di effettuare il BC/DR nel 2023. Ancora più importante è il riconoscimento che, mentre circa il **30%** delle organizzazioni continua a sfruttare più data center per il BC/DR, la percentuale delle organizzazioni che utilizza i servizi cloud (IaaS/DR o DRaaS) per il BC/DR è più che raddoppiata dal 2020 **(23%)** al 2023 **(47%)**, e si prevede che il **55%** utilizzerà il DR basato sul cloud entro il 2025.

74%

Percentuale delle organizzazioni in Italia che prevede di utilizzare i servizi cloud come parte integrante della propria soluzione di protezione dei dati entro il 2025

	REGIONE									
	GLOBALE	EMEA	DACH	UKI	Francia	Benelux	**Italia**	Iberia	Paesi Nordici	Europa dell'est	MEA
% di organizzazioni che utilizza infrastruttura in hosting nel cloud per il BC/DR	47%	41%	49%	41%	46%	47%	**40%**	52%	54%	49%	41%
% di organizzazioni con più data center per il BC/DR	24%	25%	23%	34%	23%	22%	**26%**	23%	24%	24%	25%

Il 2023 sarà un anno di "cambiamento"?

Tra le preoccupazioni per il ransomware, le pressioni per garantire i servizi IT e le problematiche di protezione dei moderni carichi di lavoro IaaS e SaaS, si potrebbe presumere che molte organizzazioni cambieranno probabilmente le soluzioni di backup per adattarle a queste pressioni e condizioni in continuo mutamento. Ed è proprio così! Ignorando il **35%** di risposte pressoché neutre:

- Solo per l' **8%** delle organizzazioni è poco probabile una sostituzione della soluzione di backup principale nel 2023
- Mentre il **57%** degli intervistati ha dichiarato che intende probabilmente o sicuramente cambiare soluzioni di backup

51%

Percentuale delle organizzazioni in Italia che prevede di cambiare le proprie soluzioni di backup nel 2023

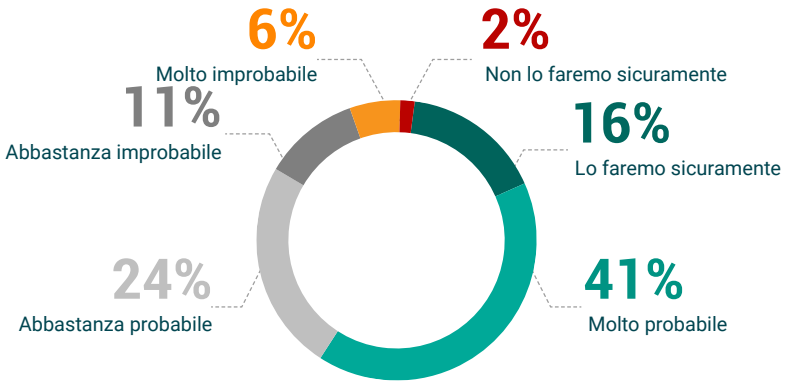


Figura 3.6

Qual è la probabilità che la tua organizzazione sostituirà le sue principali soluzioni/servizi di backup nei prossimi dodici mesi?

Il punto di vista di Veeam

La Veeam Data Platform

Mentre le organizzazioni continuano a trasformare la propria infrastruttura, garantendo il supporto per aspetti del cloud come backup, consumo e mobilità, è necessaria una soluzione che renda la complessità più completa. La Veeam® Data Platform offre:

- Controllo dei costi di storage con un'architettura di tiering dello storage cloud intelligente
- Backup e ripristino appositamente creati e nativi di Kubernetes, disaster recovery e mobilità per applicazioni containerizzate
- Ampio supporto dei carichi di lavoro nei servizi IaaS/PaaS/SaaS
- Monitoraggio e gestione centralizzati, insieme a un'ampia copertura API

Gli utenti Veeam nuovi o già esistenti dovrebbero dare un'occhiata a Veeam Backup *for AWS, Azure, Google Cloud, Microsoft 365, Salesforce* e Kasten for Kubernetes per scoprire le funzionalità leader di settore create per le specifiche esigenze del cloud ibrido.

Per gli utenti Veeam alla ricerca di una soluzione "as a Service" o di colmare una lacuna nelle risorse, Veeam collabora con una vasta rete di provider di BaaS e DRaaS, oltre a specialisti di servizi professionali, per garantire agli utenti di massimizzare i loro investimenti in Veeam e nel cloud.

Fai clic qui per visualizzare il rapporto di ricerca globale completo

Le domande relative a questi dati di ricerca e approfondimenti possono essere indirizzate a StrategicResearch@veeam.com