PERCHÈ LE ORGANIZZAZIONI INCONTRANO ANCORA DIFFICOLTÀ A TRASFORMARSI E INNOVARE DIGITALMENTE

Esaminiamo gli impatti nel mondo reale quando gli obiettivi di Availability non vengono soddisfatti.

2017 Veeam Availability Report

Report completo

Indice

Introduzione alla ricerca

Non siamo mai stati così dipendenti dalla tecnologia come oggi, e non abbiamo mai avuto così tante funzioni business critical e personale in azienda che si affidano così tanto ai dati. E perché le aziende possano raggiungere gli obiettivi di business, devono affidarsi alla digital transformation e al cloud per garantire servizi più efficienti, agili e affidabili e soddisfare le esigenze degli utenti. Nell'ambito di questa trasformazione, i team IT devono impegnarsi sempre di più per garantire la disponibilità e la protezione dei sistemi, rivolgendosi ad ambienti eterogenei e ibridi per assicurare l'efficienza e l'ottimizzazione delle prestazioni.

Veeam®, che ha consentito alle aziende di raggiungere una maggiore disponibilità operativa per oltre un decennio, ha commissionato all'Enterprise Strategy Group (ESG) la sesta edizione del Veeam Availability Report. Questo report cerca di (1) verificare se le aziende riescono a raggiungere gli obiettivi di Availability, (2) valutare l'impatto sulle aziende che riscontrano livelli di servizio insufficienti e (3) comprendere come queste sfide influiscono sulle iniziative strategiche come la digital transformation.

Sintesi

Le aziende continuano ad incontrare difficoltà per assicurarsi l'Availability all'interno dei propri ambienti IT.

Quattro aziende su cinque riconoscono di avere un "divario di disponibilità". Nella ricerca di quest'anno, l'82% degli intervistati ha riconosciuto l'inadeguatezza delle proprie capacità di ripristino rispetto alle aspettative degli SLA delle business unit, dato peraltro coerente con i risultati delle ultime due ricerche annuali. Anche se alcune aziende stanno tentando di migliorare, le crescenti aspettative delle business unit, abbinate a un panorama IT diversificato e in continua evoluzione e al passaggio ad ambienti ibridi ed eterogenei, continuano a creare nuove sfide per offrire servizi di Availability adeguati dell'IT. Tutto questo comporta problemi più grossi per l'azienda, in termini di fiducia dei clienti e dei dipendenti.

In media, le imprese riscontrano costi finanziari diretti di 21,8 milioni di $ riconducibili ai divari di disponibilità e di protezione, e riconoscono che queste cifre possono variare in base al settore, alle dimensioni dell'azienda e alla località. I Gap di Availability e di Protection influiscono anche sulle iniziative strategiche di modernizzazione delle aziende:

- **L'82% delle implementazioni e delle strategie di virtualizzazione delle aziende ha subito l'influenza** della relativa soluzione di protezione dei dati.
- **Il 66% delle aziende riporta che le iniziative di digital transformation sono state ostacolate** (in modo significativo o sotto alcuni aspetti) da interruzioni non pianificate o disponibilità insufficiente delle applicazioni.

Sei aziende su sette non sono confidenti di poter proteggere/ripristinare dati in modo affidabile all'interno dei propri ambienti virtuali. L'85% degli intervistati ha valutato se stesso meno che "molto fiducioso" nelle attuali capacità della propria azienda relativamente a backup e ripristino delle macchine virtuali. Dal momento che la virtualizzazione è la base di ogni moderno ambiente IT, inclusi quelli on-premise e in hosting nel cloud, *qualsiasi* risposta diversa da "molto fiducioso" non è accettabile nel 2017.

Tre aziende su quattro riconoscono di avere un "divario di protezione". Sempre in linea con i sondaggi degli anni passati, il 72% degli intervistati di quest'anno non è in grado di proteggere i propri dati con una frequenza tale da assicurare che le aspettative delle business unit in termini di perdita di dati vengano soddisfatte.

L'82%

delle aziende si trova ad affrontare un divario tra la domanda degli utenti e ciò che l'IT può offrire, ovvero un Availability Gap

21,8M

di $ è il costo finanziario medio dell'Availability Gap e del Protection Gap per le imprese

Il 66%

delle aziende ammette che le iniziative di digital transformation vengono ostacolate dalle interruzioni non pianificate

Inoltre, l'impatto delle interruzioni e della perdita di dati può arrivare ben oltre la perdita economica diretta:

- Da un punto di vista esterno, la metà delle aziende ritiene che le sfide legate all'Availability possano portare alla perdita di fiducia dei clienti, con conseguente ricaduta sull'integrità del marchio, alla riduzione del prezzo delle azioni e alla revoca di licenze e accreditamenti.
- Da un punto di vista interno, molti ritengono che le sfide legate all'Availability possano portare alla perdita di fiducia dei dipendenti, che spesso si traduce con la riallocazione di risorse da progetti a lungo termine o business-critical.

I risultati di questo studio sono in linea con la ricerca ESG e i rapporti Veeam® precedenti: tutti dimostrano chiaramente che le aziende devono riconsiderare le proprie capacità in termini di Availability, protezione e ripristino dei dati. Il fallimento dell'azienda nell'allineare meglio queste capacità fondamentali di resilienza con le aspettative aziendali continuerà a mettere a rischio le aziende stesse e a ostacolare l'innovazione e le strategie di digital transformation.

Perché la disponibilità dei dati e la protezione continuano a rappresentare delle sfide per le organizzazioni?

Molte aziende continuano ad incontrare difficoltà con il ripristino dei dati spendendo energie per assicurare la disponibilità dei sistemi virtualizzati. Infatti, solo il 15% dei responsabili delle decisioni IT intervistati ha fiducia nella capacità della soluzione attuale di effettuare in modo affidabile backup e ripristino di macchine virtuali nel rispetto degli SLA.

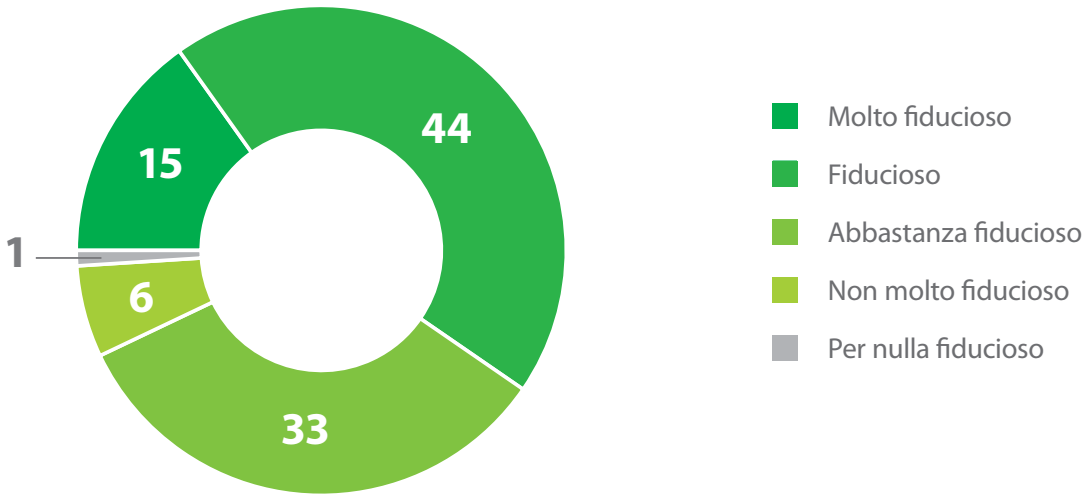

Figura 1. Qual è il livello di fiducia nella capacità della soluzione principale attualmente implementata nella vostra azienda di eseguire backup/ripristino delle VM e di ripristinare ciò che serve nel rispetto degli SLA? (Percentuale di intervistati, N=1.060)

Questa è una percentuale di fiducia reale spaventosamente bassa. Qualsiasi azienda non "molto fiduciosa" nella propria capacità di proteggere la struttura fondamentale del suo moderno data center dovrebbe riesaminare la propria strategia e le tecnologie da cui dipende.

Purtroppo una mancanza di fiducia così diffusa è ben radicata. Consideriamo il fatto che gli intervistati affermano di rispettare RTO (Recovery Time Objectives) e RPO (Recovery Point Objectives) solo per il 72% del tempo. In oltre uno su quattro tentativi, lo sforzo per il ripristino fallisce, impiega troppo tempo o ripristina una quantità inadeguata di dati.

15%

Percentuale dei decicion maker intervistati che è fiduciosa nella capacità della soluzione attuale di effettuare in modo affidabile backup e ripristino di macchine virtuali nel rispetto degli SLA.

Percezione del divario di disponibilità e di protezione

In molte aziende, gli intervistati riconoscono quasi all'unanimità che i team IT non riescono a ripristinare in modo abbastanza veloce, affidabile o preciso. Veeam fa riferimento a queste sfide come divario di disponibilità e divario di protezione.

- **Il divario di disponibilità** si riferisce alla differenza tra i livelli di servizio attesi dalle business unit e la capacità di un'organizzazione di rendere disponibili le applicazioni e le informazioni richieste dagli utenti.
- **Il divario di protezione** si riferisce alla tolleranza di un'azienda per la perdita di dati dovuta all'incapacità dell'IT di proteggere quei dati con una frequenza sufficiente.

E il principale motivo di allarme è che quattro aziende su cinque (tra quelle intervistate) riconoscono di avere un divario di disponibilità, e quasi tre aziende su quattro riconoscono di avere un divario di protezione.

4 su 5

Le aziende intervistate che riconoscono di avere un divario di disponibilità

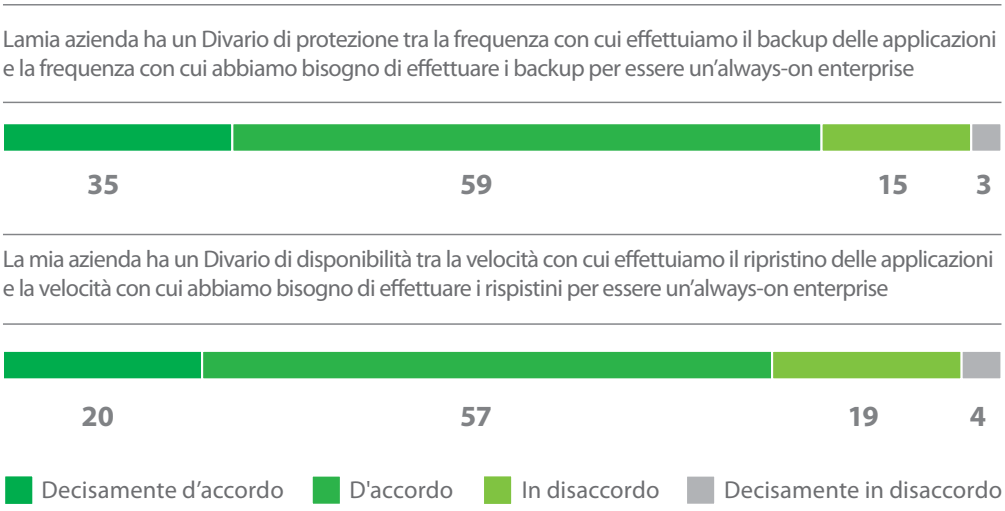

Figura 2. Esprimete quanto siete d'accordo con le seguenti affermazioni: (Percentuale di intervistati, N=1.060)

È da notare che molti decision maker riconoscono, per il terzo anno consecutivo, di continuare a soffrire un divario di disponibilità, con una tendenza apparentemente in relazione con il divario di protezione: ciascuno con una frequenza quasi uguale anno dopo anno.

Questo è molto più di un problema diffuso, è anche persistente nel tempo.

3 su 4

Le aziende intervistate che riconoscono di avere un divario di protezione

Realtà e ramificazioni del ripristino

Per un'azienda è importantissimo riconoscere la precarietà dei suoi sistemi IT ed evitare di banalizzare le interruzioni quando si verificano.

In media, oltre un server su quattro (il 27%) riscontra almeno un'interruzione non pianificata ogni anno. Per comprendere come ESG calcola medie, mode e mediane in questo report, si rimanda all'appendice uno[1].

1 su 4

I server che riscontrano almeno un'interruzione non pianificata ogni anno

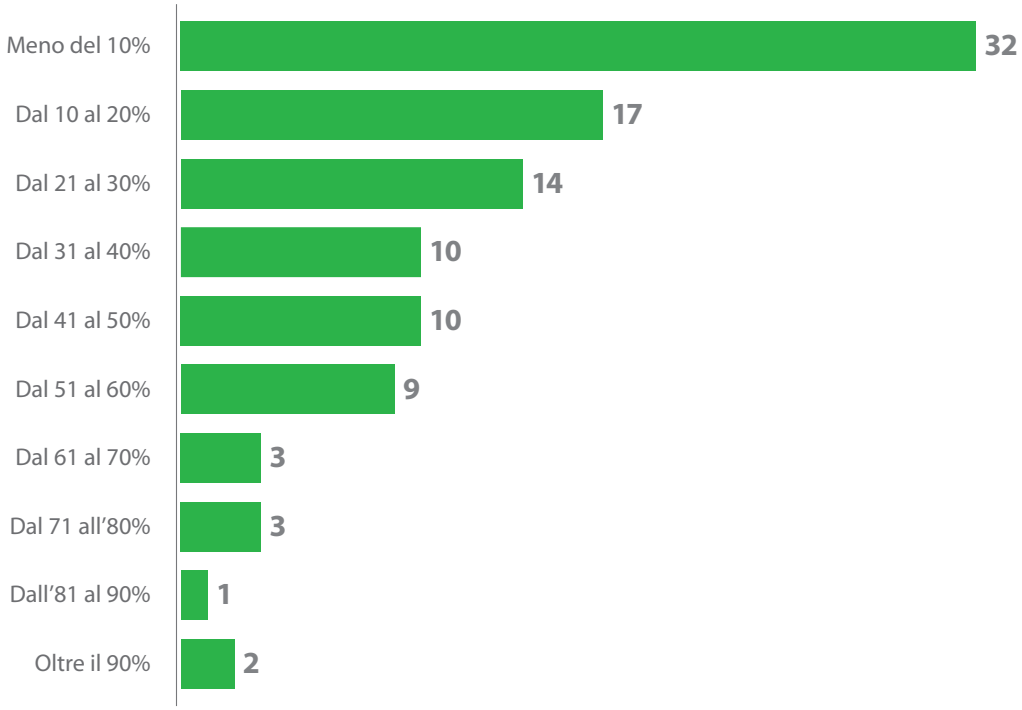

Figura 3. Quale percentuale di server in produzione nella vostra azienda riscontra almeno un'interruzione non pianificata all'anno? (Percentuale di intervistati, N=1.005)

E alcune di queste interruzioni si protraggono per diverso tempo.

[1] Vedere le note relative a calcoli e dati visualizzati in questo rapporto all'appendice: Metodologie di ricerca e demografia degli intervistati

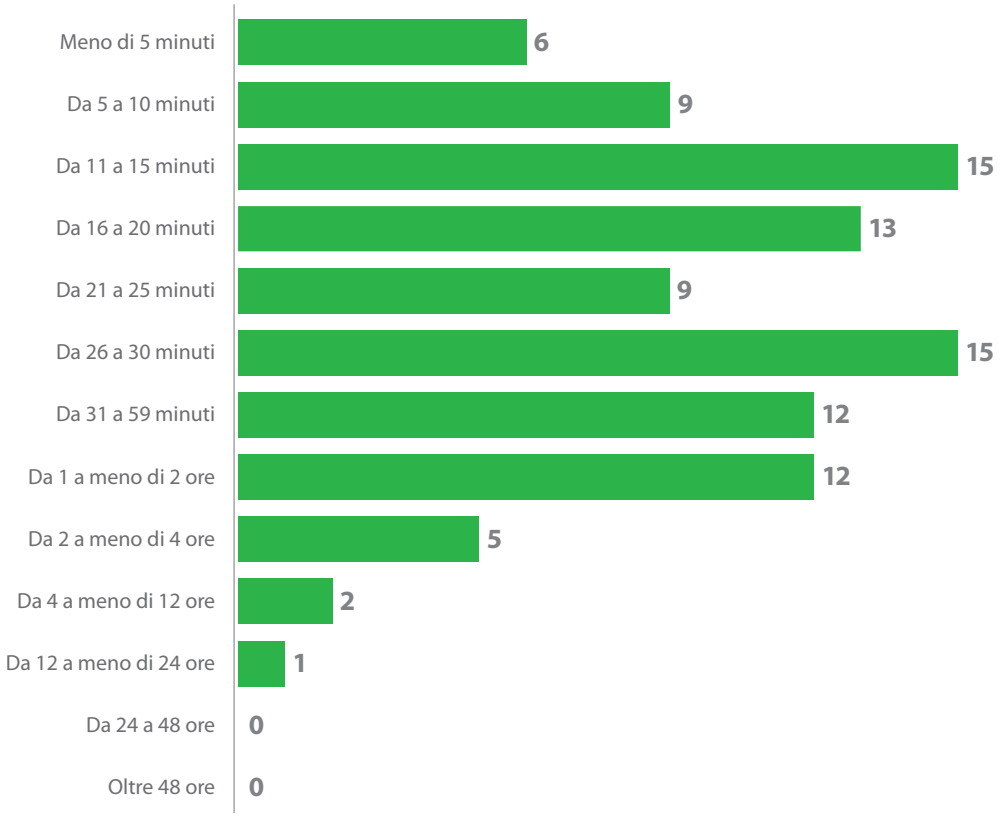

Figura 4. In media, per quanto tempo si protraggono le interruzioni non pianificate? (Percentuale di intervistati, N=989)

La lunghezza mediana[2] di un'interruzione è di 23 minuti. Anche se potrebbe non sembrare molto, provate a considerare:

- Qual è l'impatto su migliaia di passeggeri di una compagnia aerea i cui voli rimangono a terra per 23 minuti?
- Qual è l'impatto per un retailer online e i suoi clienti il cui sito Web è offline anche solo per 23 minuti?
- Qual è l'impatto per un paziente ospedalizzato i cui dati non sono disponibili per soli 23 minuti?

23
minuti è la lunghezza mediana di un'interruzione

Un qualsiasi professionista IT con esperienza può condividere storie drammatiche sulle interruzioni di sistema e come queste interruzioni hanno provocato dei disservizi. In più, i media pubblicano nuovi esempi quasi ogni settimana (suggerimento: non essere uno di loro!). Dagli eventi che cambiano la vita fino alla semplice impossibilità di comunicare con un collega, un cliente o un partner, tutti i processi aziendali sono a rischio quando l'IT non soddisfa i bisogni degli utenti.

Considerando l'impatto potenzialmente elevato delle interruzioni, abbinato all'insufficienza degli sforzi basati sulle risorse IT tradizionali per eseguire backup e ripristini dei dati, il desiderio dei dirigenti IT di cercare strumenti migliori è del tutto legittimo.

[2] Ibid

Il divario di disponibilità e le interruzioni

Guardando con maggiore attenzione alle aziende intervistate che ritengono carichi di lavoro "ad alta priorità" rispetto ai carichi di lavoro "normali", risulta evidente una differenza sorprendente:

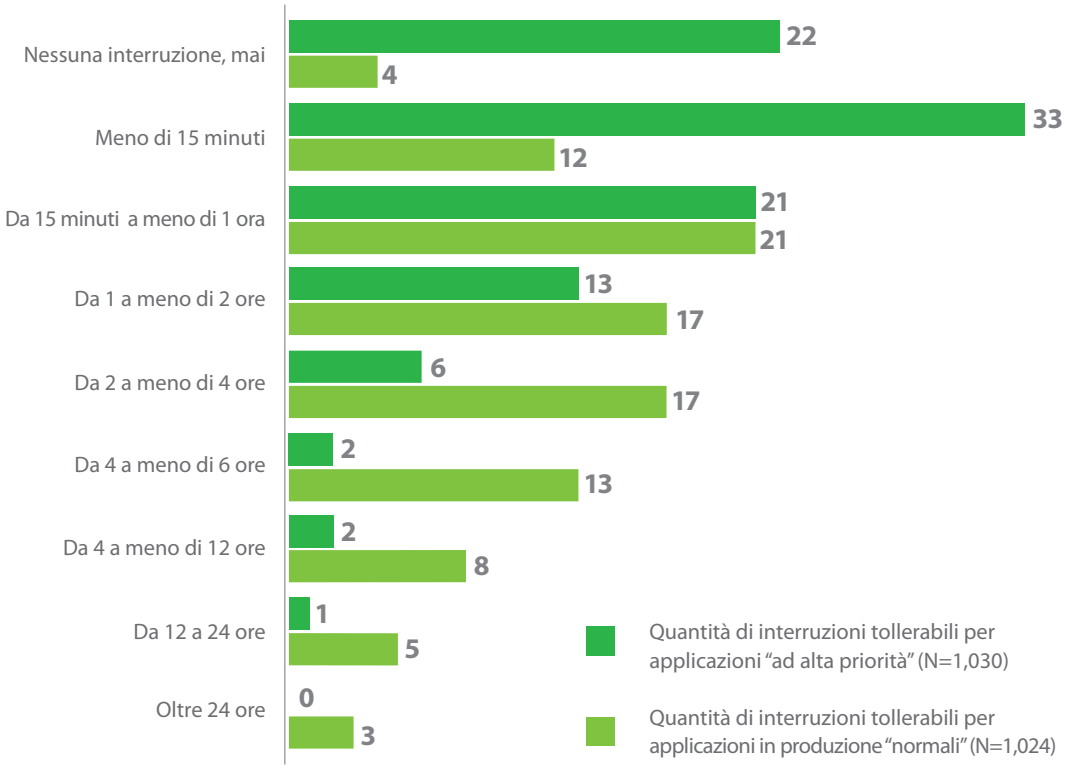

Figura 5. Qual è il numero di interruzioni che la vostra azienda può tollerare per le sue applicazioni in produzione "ad alta priorità" rispetto alle "normali" applicazioni in produzione? (Percentuale di intervistati)

- L'interruzione mediana tollerabile tra le applicazioni *ad alta priorità* è di 7,5 minuti, in cui un'interruzione di "soli 23 minuti" supererebbe il limite della maggioranza delle applicazioni ad alta priorità.
- L'interruzione mediana tollerabile tra applicazioni *normali* è di 90 minuti. Se 23 minuti sembra talvolta più tollerabile, molte applicazioni normali avranno disatteso agli SLA con tale interruzione.

Il divario di protezione e gli SLA della perdita di dati

La disparità tra la velocità a cui l'IT è in grado di ripristinare piattaforme/carichi di lavoro e le aspettative di disponibilità delle business unit e di altri utenti non è l'unica preoccupazione. Le organizzazioni IT stanno inoltre proteggendo i dati in modo inadeguato:

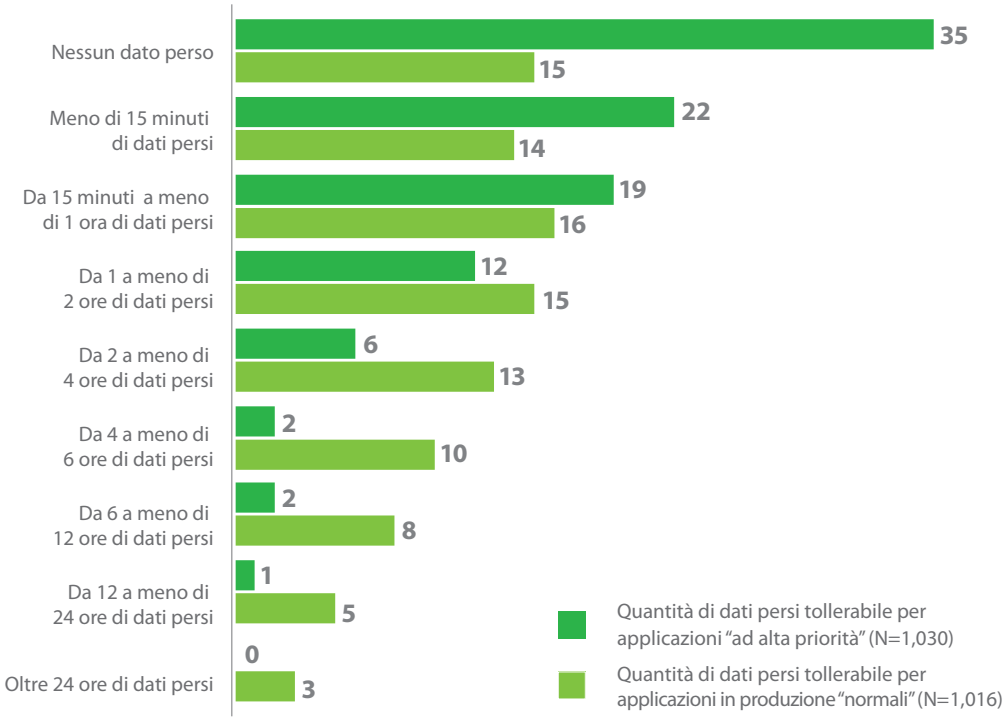

Figura 6. Qual è la quantità di dati persi che la vostra azienda può tollerare per le sue applicazioni in produzione "ad alta priorità" rispetto alle "normali" applicazioni in produzione? (Percentuale di intervistati)

- La perdita media di dati accettabile tra le applicazioni *ad alta priorità* è di 72 minuti, come mostrato nella Figura 6. Tuttavia, le organizzazioni IT intervistate proteggono i dati ad alta priorità circa ogni 127 minuti, in media.
- In modo analogo, mentre la perdita di dati media accettabile tra le applicazioni *normali* è di 240 minuti, le aziende IT intervistate proteggono i dati normali solo ogni 352 minuti, approssimativamente.

Questo è un esempio quantificabile di divario di protezione. Per essere chiari: la maggior parte delle aziende ritiene di avere un divario di disponibilità, un divario di protezione o entrambi. Per superarli, deve iniziare con l'aumentare la frequenza della protezione e potenziare l'agilità e l'affidabilità del ripristino.

I costi del divario di disponibilità e di protezione

In un'epoca in cui le VM mission-critical e le VM non essenziali possono convivere sul medesimo host oggi ma non in prospettiva futura, e il numero di utenti per VM varia ampiamente, calcolare le interruzioni può essere scoraggiante per aziende di qualsiasi tipo. Ai fini di questo rapporto, i costi delle interruzioni includevano gli input seguenti (derivati principalmente da altri punti in questo report):

- Il numero totale medio dei server in produzione (1.200) implementato presso le aziende
- La percentuale di server che riscontrano almeno un'interruzione all'anno (27%)
- La lunghezza media delle interruzioni non pianificate (85 minuti)
- I costi orari medi per le applicazioni business-critical ($108.000) e non business-critical ($48.000) - adattati al rapporto medio tra applicazioni business-critical e non.
- Applicazione media del settore di ESG al rapporto tra i server (0,81)

21,8 M

di $ il costo finanziario Le organizzazioni che partecipano a questa ricerca riscontrano costi diretti pari a 21,8 M di $ all'anno, in media

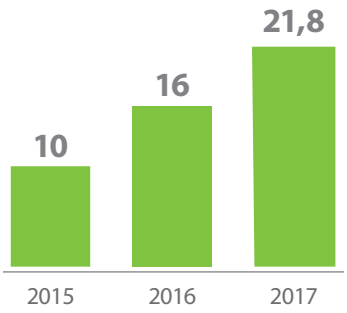

Figura 7. Costi stimati annuali dovuti alle interruzioni per azienda intervistata (in milioni di dollari)

Utilizzando questi input, ESG calcola che le aziende partecipanti a questa ricerca riscontrino in media costi finanziari diretti di 21,8 milioni di dollari all'anno. Questo dato continua la tendenza verso i costi crescenti dovuti alle interruzioni come osservato nel 2016 ($16M) e nel 2015 ($10M).

Ma non finisce qui…

Come le organizzazioni affrontano questi divari?

Nel momento in cui si esaminano le discrepanze tra gli approcci IT antiquati e le aspettative delle business unit, si profilano tre "livelli di realizzazione":

- **In teoria**, anche riconoscere l'esistenza del divario di disponibilità e del divario di protezione significa riconoscere, da punto di vista concettuale o intellettuale, che meccanismi e strategie di protezione e ripristino dei dati devono evolvere.
- **In pratica**, esistono divari inconfutabili e quantificabili tra le capacità di protezione e ripristino dell'IT e le aspettative delle business unit, e sono pervasivi.
- **In realtà,** i costi associati a interruzioni e perdita dei dati portano anche a una gamma diversificata di altri impatti negativi. Ebbene sì, gli impatti economici sono più facili da immaginare, ma le altre ramificazioni sono altrettanto pericolose, se non di più.

Il 41%

riconosce che i problemi di Availability, a cui conseguono la perdita di clienti e di fiducia dei dipendenti, hanno l'impatto potenziale maggiore

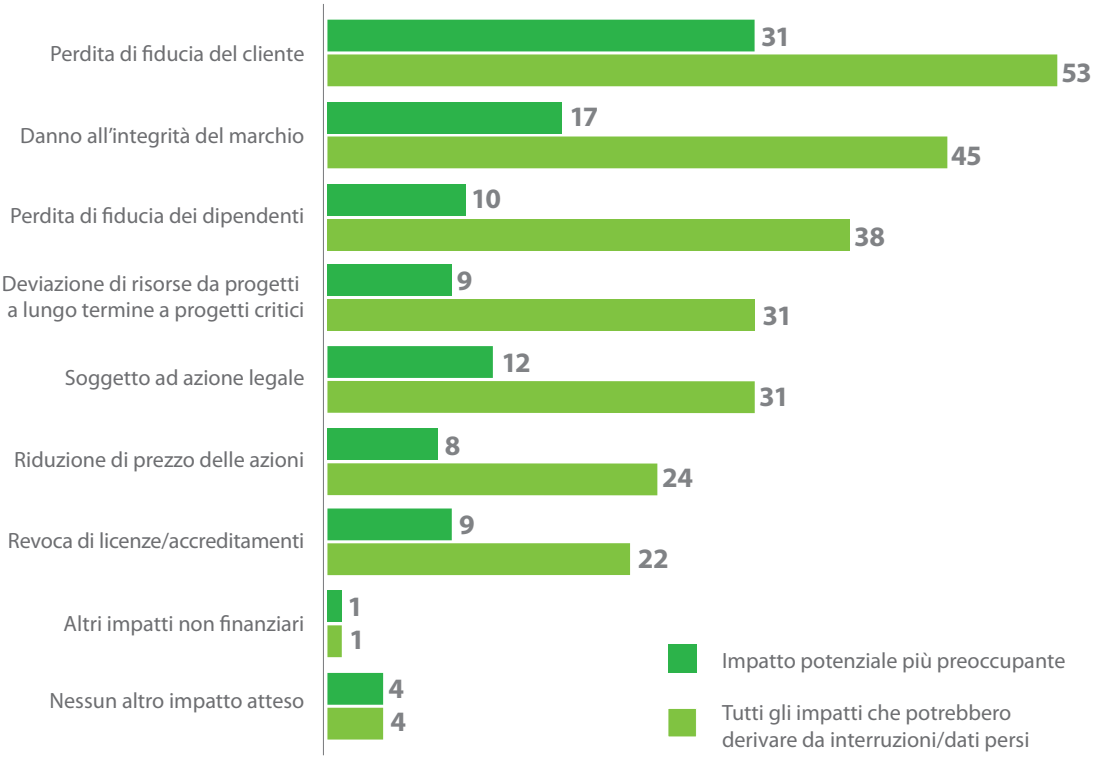

Figura 8. Quale altra implicazione potrebbe derivare nella vostra azienda dalle interruzioni delle applicazioni o dalla perdita dei dati? Quale impatto vi preoccupa di più? (Percentuale di intervistati, N=943)

Considerate, ad esempio, che solo il 4% dei decision maker ritiene che la propria azienda subisca solo impatti monetari in seguito a un'interruzione o a una perdita di dati.

La maggior parte dei decision maker riconosce che i problemi correlati alla disponibilità potrebbero comportare per l'azienda con la contrazione della clientela, la mancanza di fiducia dei dipendenti e i danni all'integrità del marchio.

Nonostante ciò, il peso degli impatti segnalato è identico a quello degli anni precedenti, dalla fiducia del cliente e l'integrità del marchio (i più preoccupanti) al numero basso di persone che nega questi impatti di natura non finanziaria.

E il problema è solo destinato a peggiorare nel tempo. Solo il 13% degli intervistati si aspetta che i costi dovuti alle interruzioni o alla perdita di dati possano diminuire nel futuro. Per tutti gli altri, nel momento in cui le aspettative di disponibilità delle business unit continuano ad aumentare e l'IT continua nella sua lotta, gli impatti secondari riconducibili a interruzioni e perdita di dati sono destinati ad aumentare.

Gli ostacoli alle strategie di virtualizzazione delle organizzazioni

È estremamente importante riconoscere che meccanismi di protezione e ripristino inadeguati non si limitano a ostacolare i sistemi e i processi aziendali di oggi. Ostacolano anche la possibilità di un'azienda di modernizzare il proprio ambiente IT come parte integrante della sua continua evoluzione per il bene delle sue attività.

I server virtualizzati sono le fondamenta su cui si costruisce la maggior parte delle moderne infrastrutture IT. La maggior parte degli intervistati (l'82%) riconosce una certa relazione tra l'adeguatezza della soluzione di backup e il successo relativo della strategia di implementazione della virtualizzazione:

- Una percentuale non trascurabile (il 33%) riconosce che le inadeguatezze della soluzione di backup delle VM hanno ***rallentato*** gli sforzi di implementazione della virtualizzazione in azienda.
- Ma sono in molti (il 49%) a riconoscere che una soluzione di backup delle VM efficace ha consentito loro di ***accelerare in modo significativo*** la strategia di implementazione della virtualizzazione.

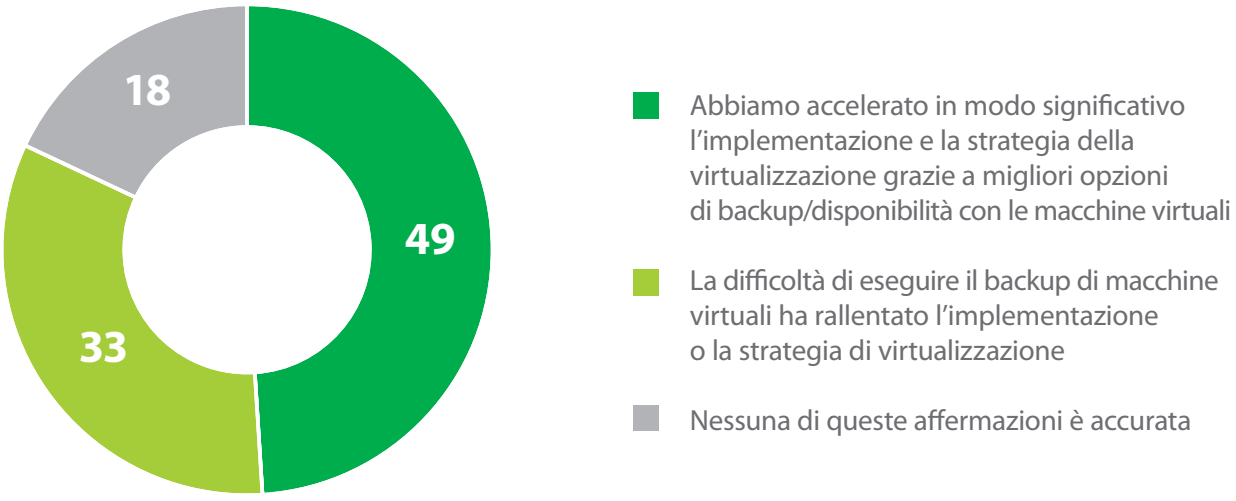

Figura 9. Quale delle seguenti affermazioni sul rapporto tra virtualizzazione server e protezione dei dati è più accurata? (Percentuale di intervistati, N=964)

Gli ostacoli alle strategie cloud delle organizzazioni

Proprio come la virtualizzazione server ha costretto ad adottare nuovi approcci alla protezione e al ripristino dei dati, così fa anche "il cloud", in ciascuno dei suoi numerosi modelli di consumo:

- Coloro che spostano i carichi di lavoro in produzione su servizi IaaS o PaaS in hosting, oppure che si sono rivolti al SaaS, dovranno ripensare gli scenari di protezione e ripristino dei dati; e per molti si renderà necessario cambiare fornitore.
- Nel frattempo, lo storage cloud consente nuove opzioni per la retention dei dati, specialmente se abbinate con servizi di backup "chiavi in mano" (BaaS) o meccanismi di failover (DRaaS).

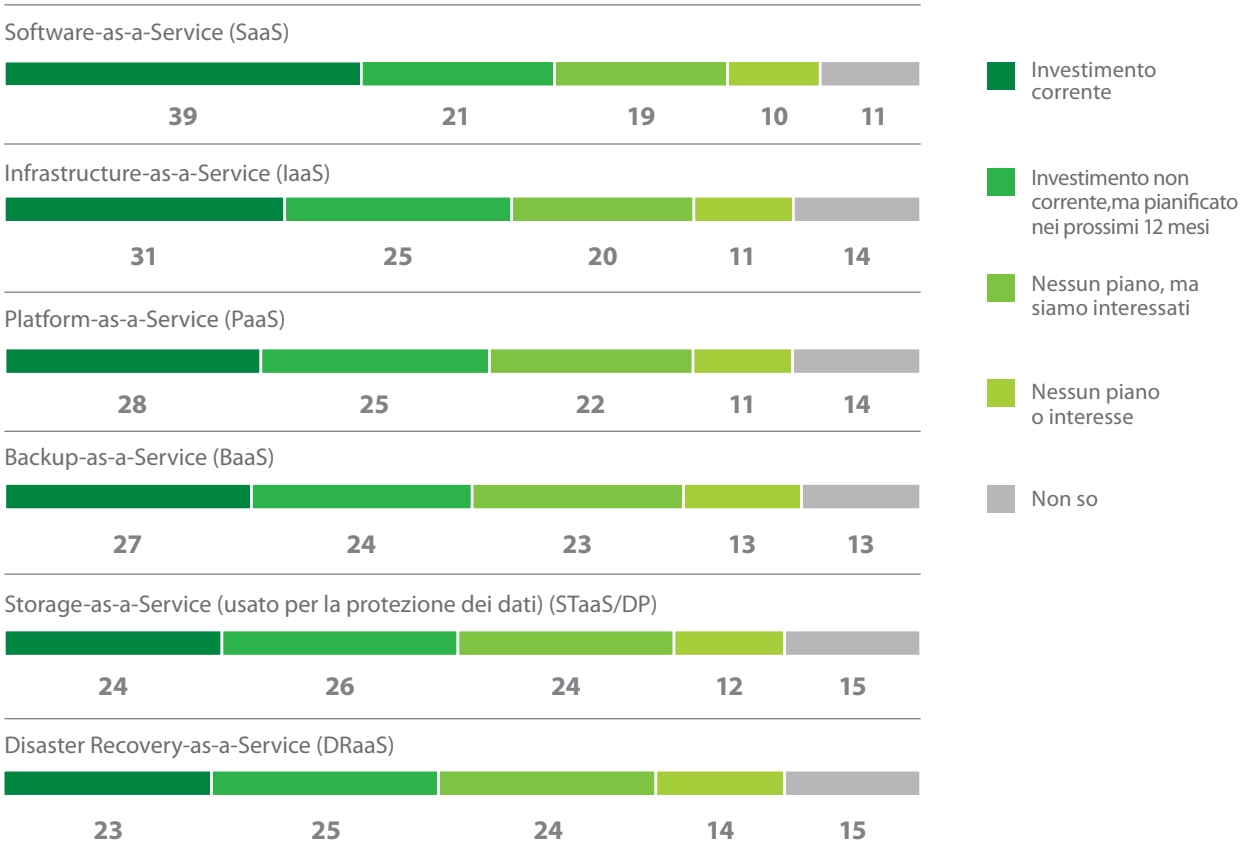

Figura 10. Quali tipologie di servizi basati sul cloud sta attualmente utilizzando (o pensa di utilizzare) la vostra azienda nel corso dei prossimi 12 mesi (se pensa di farlo)? (Percentuale di intervistati, N=1.060)

Dato il livello materiale dell'investimento cloud osservato, è chiaro che i servizi cloud cambieranno inevitabilmente il modo in cui l'IT raggiungerà gli obiettivi di produzione e protezione, ma non tutti i fornitori di protezione dei dati sono predisposti per il cloud.

Gli ostacoli alle iniziative di digital transformation delle organizzazioni

Sebbene alcune aziende stiano ancora modernizzando le proprie infrastrutture fondamentali per la virtualizzazione, molte altre riconoscono che una strategia di *digital transformation* le porterebbe molto più lontano di una semplice modernizzazione.

- Oltre due terzi degli intervistati (il 69%) riconosce che la digital transformation è critica o molto importante per il progresso delle rispettive aziende.
- Detto questo, circa la metà di essi (il 45%) afferma di trovarsi ancora in fase di pianificazione o nelle fasi iniziali delle iniziative di digital transformation.

È allarmante che oltre la metà degli intervistati le cui aziende hanno intrapreso iniziative di digital transformation (il 66%) riporti che tali iniziative vengono inibite a causa di interruzioni non pianificate o disponibilità insufficiente delle applicazioni.

66%

Percentuale di chi riporta che le iniziative di trasformazione in atto vengono inibite a causa di interruzioni non pianificate o disponibilità delle applicazioni insufficiente

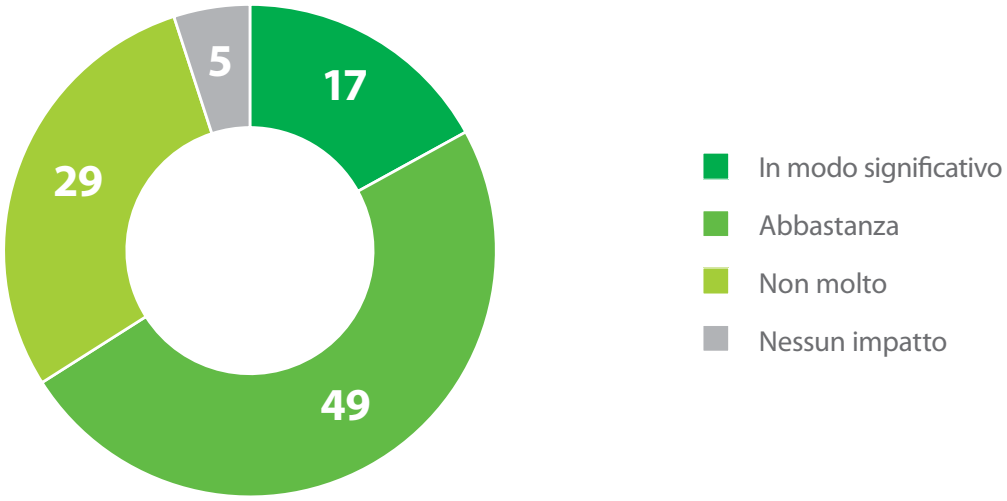

Figura 11. In quale misura le iniziative di digital transformation delle vostra azienda vengono inibite da interruzioni non pianificate o da disponibilità insufficiente delle applicazioni? (Percentuale di intervistati, N=970)

Per far progredire queste importantissime iniziative di digital transformation oltre le prime fasi (nella maggior parte dei casi), molte aziende devono risolvere le proprie carenze relativamente a interruzioni e disponibilità.

Conclusioni

La maggior parte delle aziende IT riconosce (e altri non lo fanno, ma dovrebbero) di avere dei divari nelle capacità di protezione e disponibilità, con conseguenti carenze nel soddisfare le aspettative di business unit, dirigenti, dipendenti, colleghi e clienti. I motivi riconducibili a questa situazione comprendono quanto segue:

- La maggior parte delle infrastrutture IT si trova in uno stato perpetuo di modernizzazione, che include iniziative di digital transformation, strategie di virtualizzazione aggressive, adozione, talvolta sperimentale, di servizi cloud ibridi, diversificazione delle piattaforme di produzione e aspettative sempre maggiori degli SLA, il tutto senza aumenti di budget commisurati.
- Molte aziende non allineano né la frequenza della protezione né i meccanismi di ripristino con gli SLA stabiliti delle business unit, con una disponibilità di conseguenza inadeguata.
- Molte aziende non sono in grado di quantificare in modo efficace la miriade di costi e di impatti dovuti a interruzioni o perdita di dati, ostacolando quindi la capacità di attirare supporto economico e operativo per meccanismi e risultati migliori.

Queste sfide non sono banali, ma sono superabili. Le aziende devono affrontare i Divari di disponibilità e di protezione in atto per non esporre dipendenti e reparti a un'ampia gamma di debolezze a livello produttivo, economico, percettivo e operativo.

- **Una qualsiasi azienda che non riesce a ripristinare dati granulari o intere VM più velocemente di quanto stabilito dagli SLA in relazione ai tempi di interruzione accettabili presenta un *divario di disponibilità*.** Il divario di disponibilità porta con sé la produttività persa degli utenti, la mancata conformità con mandati di accesso garantiti (sia tra partner aziendali che nelle aziende regolamentate applicabili) e la fiducia persa dei dipendenti, dei clienti e dei mercati su cui l'azienda è presente.
- **Qualsiasi organizzazione che non protegge i propri dati con una frequenza maggiore della media dei suoi SLA relativi alla perdita di dati presenta un *divario di protezione*.** Il divario di protezione implicherà la perdita dei dati, che a sua volta comporterà per i dipendenti delle sfide di produttività in termini sia di rigenerazione dei dati sia di servizio ai clienti in mancanza di informazioni complete.

I divari di disponibilità e protezione finiscono invariabilmente con l'ostacolare gli ambienti operativi di oggi, le strategie e le implementazioni di virtualizzazione che modernizzano i data center e, in ultima analisi, le iniziative di digital transformation a cui si affidano così tante istituzioni per garantirsi una sempre maggiore rilevanza sul mercato.

Passi successivi

Il primo passo (e il più importante) nel garantire la sostenibilità dei servizi IT in termini di servizio alle business unit e ai clienti è di presumere la presenza di un divario di disponibilità e di un divario di protezione, fino a prova contraria. Troppe aziende che mancano di metriche precise o di processi di monitoraggio presumono che i loro sistemi siano sufficienti e pertanto vengono ostacolate dalla propria ingenuità. Invece, date per assodato di avere un problema, e poi quantificatelo. Solo una minoranza delle aziende (meno di una su cinque) potrà affermare il contrario, e molte di esse sono probabilmente resilienti a causa degli intensi sforzi verso la disponibilità messi in pratica degli anni precedenti.

Quindi è necessario quantificare gli SLA delle business unit e valutare i meccanismi di protezione e le capacità di ripristino. Solo confrontando le aspettative in termini di disponibilità e protezione con le capacità del mondo reale sarete in grado di determinare le dimensioni dei divari presenti nella vostra strategia IT.

Convertite i divari in analisi dell'impatto. Nel mondo BC/DR, tutto ciò si riferisce a una BIA (Business Impact Analysis), che si esplicita chiedendosi semplicemente, *"Se [il sistema] dovesse riportare un guasto, quali sarebbero i costi per noi [in termini finanziari, di processo, di percezione, ecc.]?"* Guardando ai log di sistema precedenti, la maggior parte scoprirà che tali sistemi hanno subito delle interruzioni in passato, che oggi possono essere quantificate come impatto sul business.

Dopo un'accurata comprensione della frequenza e della durata delle interruzioni all'interno del proprio ambiente, confrontate con le aspettative degli SLA dei componenti aziendali, e dopo una valutazione degli impatti finanziari e percettivi sull'azienda, **siete pronti a reimmaginare che cosa significherebbe diventare un'Always-On Enterprise:**

1. *Riconoscete che la virtualizzazione sarà quasi certamente il fondamento della vostra infrastruttura*, e pertanto dovete assicurarvi che le vostre capacità di protezione e ripristino per i sistemi altamente virtualizzati superino gli SLA aziendali. Solo questo può risolvere una parte significativa dei Divari di disponibilità e protezione.

2. *Comprendete che i servizi cloud giocheranno senza dubbio un ruolo molto più importante per far progredire la vostra strategia,* anche se i tipi di servizi cloud varieranno moltissimo tra storage cloud, servizi di protezione basati sul cloud, infrastruttura basata sul cloud in produzione, scenari BC/DR, e applicazioni basate su cloud (come Office 365). Ciascuna di queste piattaforme influirà sulle vostre opzioni di protezione e ripristino, che, di nuovo, devono essere per prima cosa misurate rispetto agli SLA per garantire Divari di disponibilità e protezione ridotti.
3. E per ultima cosa, ma forse la più importante, r*iconoscete che interruzioni e perdita di dati non sono solo concetti teorici, e che gli RPO/RTO non sono solo semplici metriche per compilare un punteggio IT.* La mancanza di meccanismi di ripristino/disponibilità agili e affidabili ricade sulle basi della virtualizzazione e ostacolerà le iniziative di digital transformation che dovrebbero portarvi nel futuro. *Tutto questo inizia con l'impegno ad essere Always-On.*

Appendice: Metodologie di ricerca e demografia degli intervistati

Metodologia di ricerca

Veeam ha commissionato all'Enterprise Strategy Group, un'azienda leader nel campo dell'analisi, ricerca e strategia IT, di eseguire il sondaggio su cui si basa questo report.

Per raccogliere i dati necessari, ESG ha svolto un sondaggio completo online su 1.060 ITDM provenienti da aziende del settore pubblico e privato con almeno 1.000 dipendenti in 24 paesi diversi tra il 18 novembre 2016 e il 31 dicembre 2017.

La rappresentazione geografica della base degli intervistati è rappresentata nella Figura 12.

Stati Uniti	N=158
Regno Unito	N=103
Francia, Germania	N=78
Benelux (Belgio, Paesi Bassi), Hong Kong	N=75
Australia, Giappone, Cina, Brasile, Singapore	N=50
Canada	N=49
Italia, Paesi Nordici (Svezia, Danimarca, Finlandia), Russia, Tailandia, India, Medio Oriente (Emirati Arabi Uniti, Arabia Saudita, Israele), Messico	N=16-30

Figura 12. Numero di intervistati qualificati per Paese/Regione

Per potersi qualificare e partecipare a questo sondaggio, gli intervistati dovevano essere dipendenti in un ruolo IT con conoscenza quotidiana e/o familiarità con l'ambiente e la strategia di backup/ripristino dei dati/file della propria azienda. Tutti gli intervistati hanno ricevuto un incentivo a completare il sondaggio sotto forma di una somma in denaro e/o equivalenti.

Tutti gli intervistati sono stati sottoposti a un severo processo di controllo qualità, che ha compreso il filtraggio di intervistati non qualificati, la rimozione di risposte duplicate e lo screening delle risposte rimanenti completate (in base a determinati criteri) per l'integrità dei dati.

Vedere la sezione Dati demografici degli intervistati in questo report per maggiori informazioni su questo argomento.

Note relative a calcoli e dati visualizzati in questo report

In questo report le medie e le mediane sono stimate per le domande applicabili in cui le opzioni di risposta sono state presentate come intervalli numerici. Queste operazioni vengono svolte usando il punto medio di ciascun intervallo di dati selezionato da ciascun intervistato come il valore assunto dell'intervistato e calcolando la media (sia essa mediana o media) in base alla distribuzione aggregata delle risposte degli intervistati alle domande rilevanti. I riferimenti alle medie citate in questo report si riferiscono alla media matematica, a meno che non venga citata esplicitamente la mediana.

Inoltre, i totali in cifre e tabelle di tutto il report può non raggiungere il 100% a causa dell'arrotondamento.

Demografia degli intervistati

I dati presentati in questo report si basano su un sondaggio condotto tra 1.060 intervistati qualificati. Le figure comprese tra la 13 e la 17 riportano in dettaglio la demografia della base di intervistati, incluso il ruolo attuale, il numero totale dei dipendenti dell'azienda dell'intervistato, il settore principale e il numero di server.

Intervistati per ruolo

Il ruolo attuale degli intervistati all'interno delle rispettive aziende è riportato nella Figura 13.

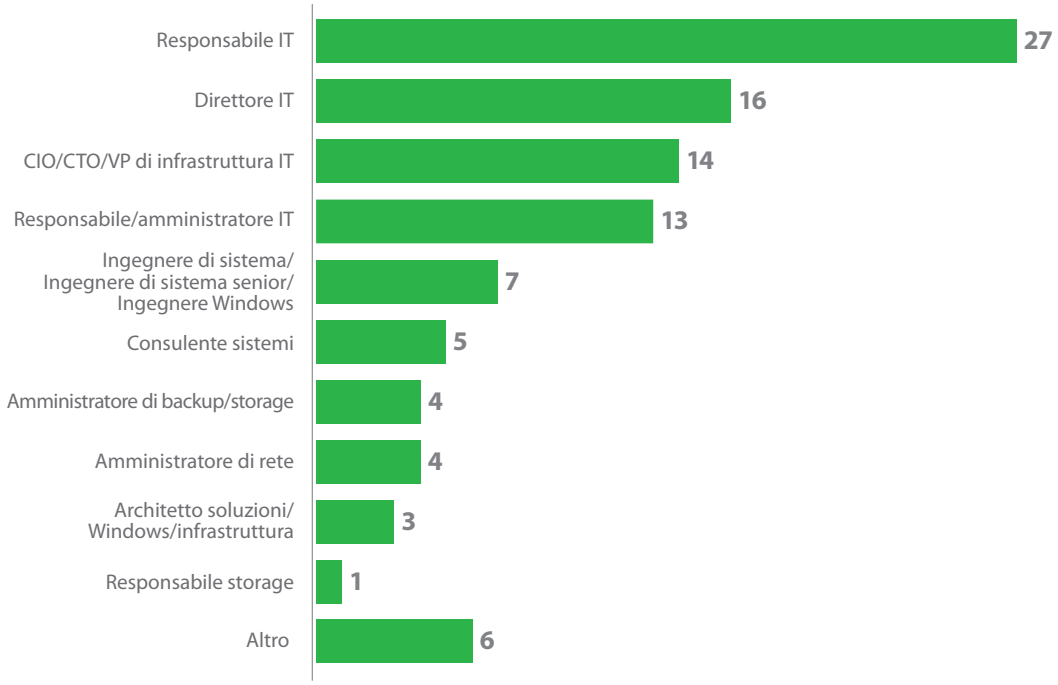

Figura 13. Quale delle seguenti affermazioni descrive meglio il vostro ruolo all'interno dell'azienda? (Percentuale di intervistati, N=1.060)

Intervistati per numero di dipendenti

Il numero di dipendenti nelle aziende degli intervistati è riportato nella Figura 14.

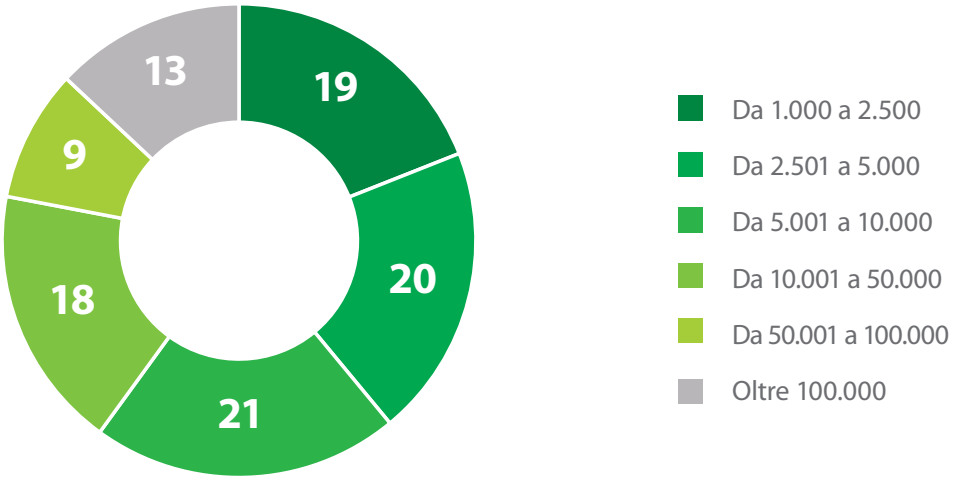

Figura 14. Quanti dipendenti ha la vostra azienda, a livello mondiale? (Percentuale di intervistati, N=1.060)

Intervistati per settore di provenienza

Agli intervistati è stato chiesto di individuare il settore principale dell'azienda. In totale, ESG ha ricevuto risposte complete e qualificate da individui in 12 settori verticali distinti, più una categoria "Altro", riportata nella Figura 15.

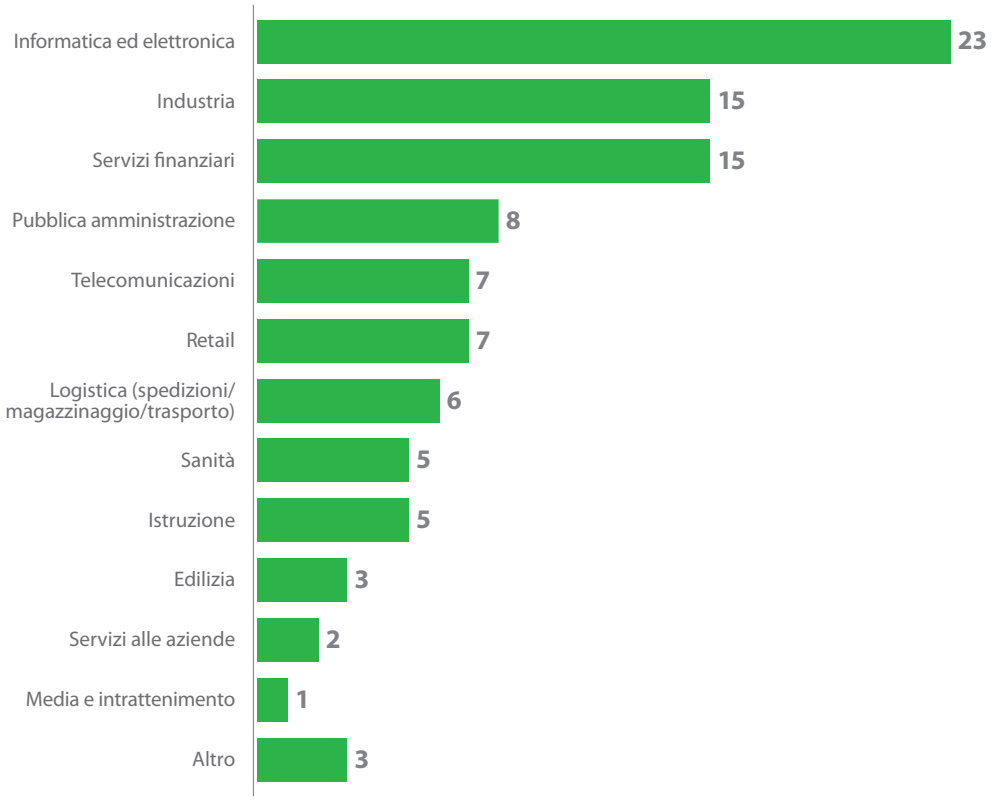

Figura 15. Qual è il settore principale della vostra azienda? (Percentuale di intervistati, N=1.060)

Intervistati per numero di server in produzione

Il numero di server in produzione dell'azienda, fisici e virtuali, è riportato nella Figura 16.

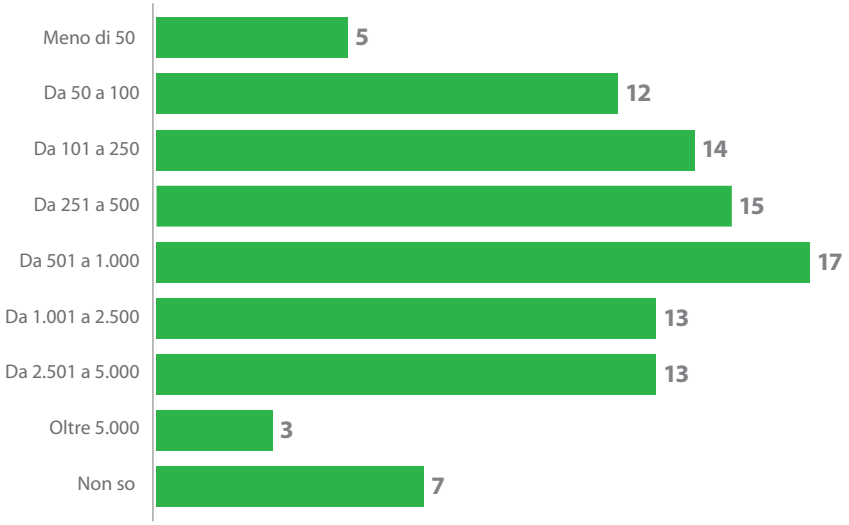

Figura 16. All'incirca, quanti server in produzione totali (sia fisici che virtuali, ma senza includere test e sviluppo) sono attualmente implementati nella vostra azienda? (Percentuale di intervistati, N=1.035)

Intervistati per percentuale di server x86 virtualizzati

La percentuale di server x86 presenti nelle aziende degli intervistati che sono stati virtualizzati fino ad ora, e come questa percentuale si prevede che cambi in due anni, è riportata nella Figura 17.

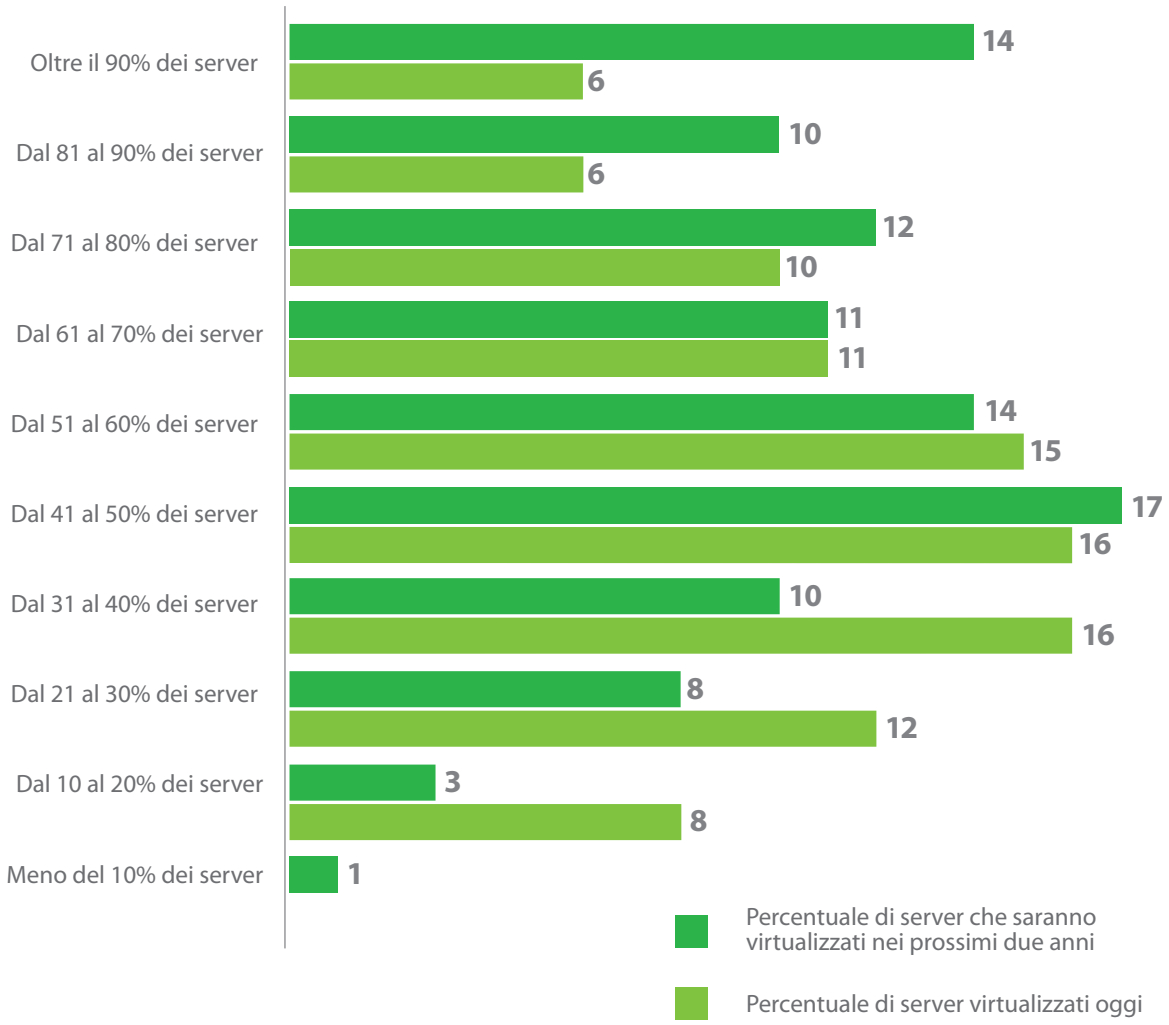

Figura 17. Di tutti i server x86 nella vostra azienda che possono essere virtualizzati, quale percentuale lo è stata? In una prospettiva di due anni, quale percentuale di server ritiene che sarà virtualizzata? (Percentuale di intervistati, N=1.060)

Informazioni su Veeam Software:
Veeam® è consapevole delle nuove sfide che si trovano ad affrontare le aziende di tutto il mondo per rendere possibile l'Always-On Enterprise™, ovvero la modalità operativa 24.7.365. Per rendere possibile tutto questo, Veeam ha creato nuove soluzioni che garantiscono la Availability for the Always-On Enterprise™, aiutando le aziende a raggiungere obiettivi di Recovery Time and Point Objectives (RTPO™) inferiori a 15 minuti per tutte le applicazioni e tutti i dati grazie a ripristini ad alta velocità, nessuna perdita di dati, protezione comprovata, dati ottimizzati e visibilità completa. Veeam Availability Suite™, che include Veeam Backup & Replication™, sfrutta le tecnologie di virtualizzazione, storage e cloud per la creazione di data center moderni che consentono alle aziende di risparmiare tempo, ridurre i rischi e ridurre drasticamente i costi operativi e di capitale, continuando a supportare gli obiettivi aziendali attuali e futuri dei clienti Veeam. Fondata nel 2006, Veeam conta attualmente 45,000 ProPartner e oltre 230,000 clienti in tutto il mondo. La sede globale di Veeam si trova a Baar, Svizzera, e l'azienda ha uffici dislocati in tutto il mondo. Per maggiori informazioni, visitare www.veeam.com/it/enterprise.

Informazioni su ESG
ESG è una società di analisi, ricerca e strategia IT fondata nel 1999 con sede centrale a Milford, Massachusetts. Svolge ricerche con e per fornitori IT, professionisti IT, professionisti del business e partner di canale. ESG mantiene la copertura dell'analisi in corso nel cloud computing networking, storage, protezione dei dati, sicurezza informatica, gestione e analisi dei dati, mobilità enterprise, gestione sistemi e canali.

Informazioni sull'analista principale di questo studio
Jason Buffington è Principal Analyst di ESG e si occupa di tutte le forme di protezione, preservazione ed disponibilità dei dati.
Ha attivamente implementato o fornito consulenze sulla protezione dei dati e le soluzioni di storage per 28 anni lavorando presso partner di canale, diversi fornitori di software per la protezione dei dati e per Microsoft. Jason è stato un relatore di spicco presso eventi relativi a infrastruttura server, continuità di business e storage in tutto il mondo, e i suoi articoli sono apparsi in numerose riviste del settore IT.