SCELTA DELLA CORRETTA SOLUZIONE DI RIPRISTINO DI EMERGENZA (DISASTER RECOVERY)

E-BOOK INTRODUTTIVO

solarwinds msp

N4B NETWORK for BUSINESS

Distributore Autorizzato

IT al **centro dell'attenzione**

SIAMO GIÀ NUOVAMENTE OPERATIVI?

È un evento fin troppo familiare per le aziende di oggi: qualcosa non va per il verso giusto, dalla semplice cancellazione accidentale alla perdita dei dati dell'intero edificio, e il servizio IT deve risolvere tutto. Proprio ora. (Non è ancora finito?)

Questo compito non è sempre il più semplice. Perché? Può essere utile considerare di aver utilizzato una soluzione di backup e ripristino non adeguata o di aver utilizzato erroneamente quella presente.

DEFINIZIONE DEL DISASTRO

È impossibile pianificare il ripristino se non si sa, in primo luogo, contro quale disastro ci si stia proteggendo. Date uno sguardo a questo elenco di potenziali disastri e identificate quali fra di essi siano per voi importanti (o per il vostro cliente se siete un MSP).

- Perdita di dati: una cartella eliminata, un caso di ransomware che crittografa ogni file sul server o un database danneggiato.
- Perdita di un'applicazione: modifiche alle configurazioni di sicurezza o di sistema o addirittura aggiornamenti che influiscono negativamente sui servizi.
- Perdita di un sistema: un guasto hardware oppure, per chi utilizza server virtualizzati, un SO bloccato.
- Perdita di connettività: quando le applicazioni in hosting all'interno dell'edificio sono utilizzate esternamente.
- Perdita del sito aziendale: interruzione elettrica, incendio, inondazione o addirittura fuoriuscita di sostanze chimiche all'esterno dell'edificio.
- Perdita di attività: qualsiasi fra i disastri precedenti può costituire un completo arresto delle attività aziendali.

NON TUTTI I DATI SONO UGUALI

È fondamentale riconoscere l'importanza dei vostri dati, applicazioni, sistemi, connettività e sedi, in quanto potrebbe essere necessario rispondere con una strategia di ripristino completamente differente in funzione delle varie situazioni.

Per definire veramente i disastri contro i quali desiderate proteggervi, dovrete definire la granularità dell'istanza di perdita. Chiaramente non attribuirete lo stesso livello di importanza a tutti i file di un file server. Dovete esaminare ciascun set di dati, applicazione, sistema e così via e deciderne l'importanza per l'attività.

Ad esempio, quando si parla di una perdita di dati, si potrebbe pensare ad un file server specifico e ad alcuni endpoint critici del cliente. Tuttavia, quando si cerca di proteggere contro la perdita di una sede, si considerano molti più endpoint, applicazioni, processi aziendali e così via. Qui l'obiettivo è accertarsi di conoscere quale parte dell'ambiente necessiti di protezione e da quale disastro deve essere protetta.

Determinate quali siano i **dati critici**

Identificate i vostri **obiettivi di ripristino**

DIVENTARE SPECIFICI PER RTO E RPO

Porre delle specifiche per ciò che riguarda il tempo disponibile per ripristino (Recovery Time Objective o RTO) e quanti dati si è disposti a perdere (Recovery Point Objective o RPO) su una base di set di dati per ripristino è fondamentale.

Ad esempio, un'applicazione mission critical può avere un RTO inferiore a 15 minuti e un RPO inferiore a 30 minuti, mentre i file di un file server possono avere un RTO di 1 giorno e un RPO addirittura di 1 settimana. Domande quali quelle sulla frequenza con la quale eseguire i backup e su dove verranno conservati i dati recuperati devono ottenere una risposta per ciascuno di questi obiettivi.

Ricordate che dovrete applicare questi obiettivi a ciascuna combinazione di "disastri" e dati da proteggere, in quanto riportare un server all'operatività quando vi sia una perdita di dati costituisce un esercizio di backup e ripristino completamente differente rispetto ad un incendio all'interno dell'edificio che incenerisce il server.

DEFINITE LO SCOPO EFFETTIVO DEL RIPRISTINO

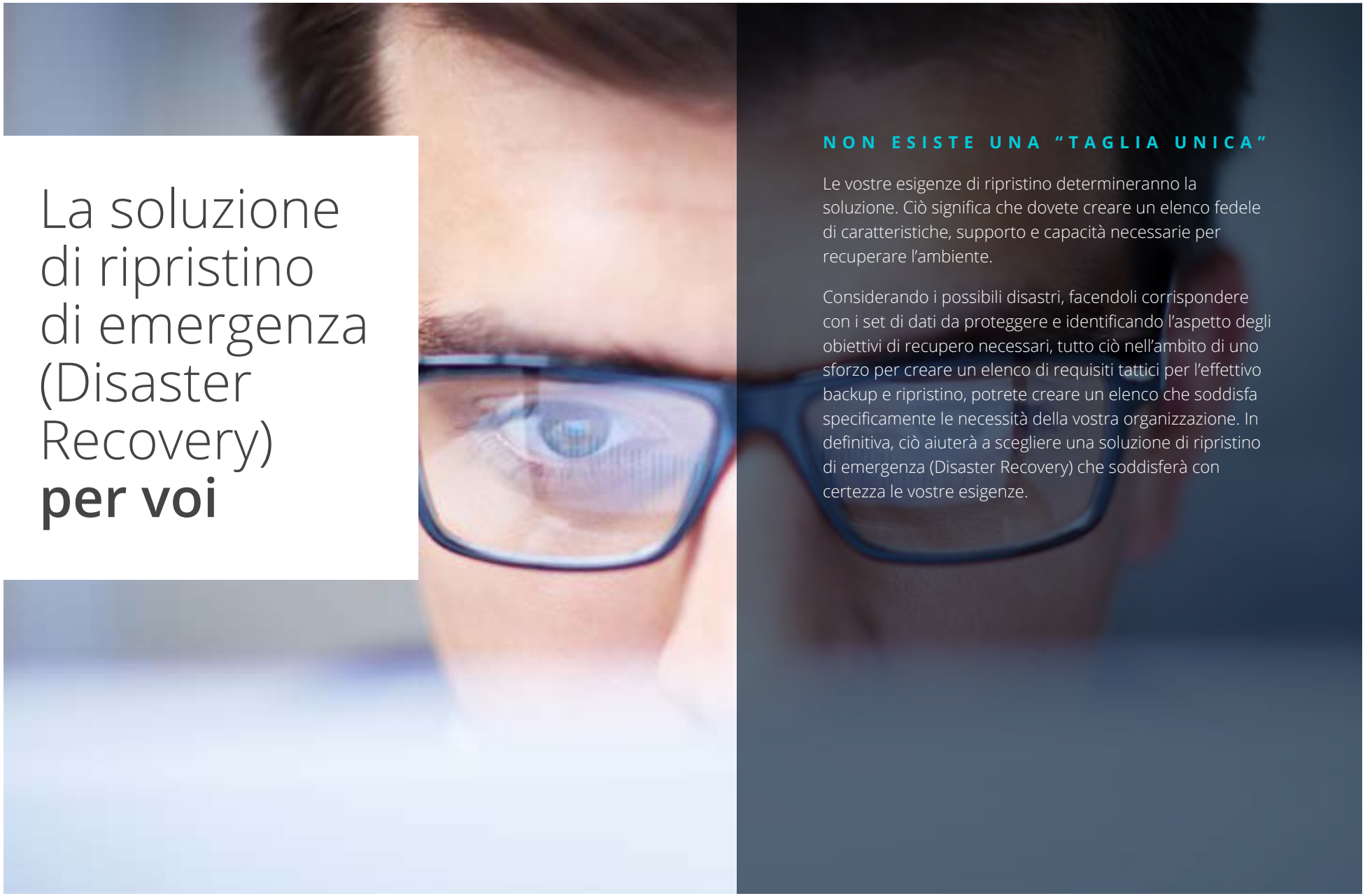
Infine, questo passaggio produrrà una serie di requisiti tecnici che utilizzerete per selezionare una soluzione di ripristino di emergenza (Disaster Recovery). Rispondendo alle domande indicate, partirete dallo scopo effettivo di ripristino di emergenza (Disaster Recovery)—il ripristino—e procederete all'indietro.

Prendete, per esempio, un server Exchange potenzialmente incenerito per delineare le specifiche per backup e ripristino. La sala server è distrutta e voi dovete ripristinare l'operatività in 30 minuti, senza perdere oltre 30 minuti di dati. Utilizzando questi criteri, dovrete essere in grado di ripristinare su una posizione alternativa, utilizzare backup basati su immagini (o non sarete in grado di soddisfare un RTO di 30 minuti), disporre di backup incrementali con una spaziatura non superiore a 30 minuti e utilizzare un tipo di strategia di ripristini continui che ripristini il backup incrementale dell'immagine non appena viene generata.

Ora dovete creare alcune voci nel vostro elenco di requisiti di soluzioni di ripristino di emergenza (Disaster Recovery):

- Backup a livello di immagine
- Supporto per Windows
- Ripristini continui
- Tecnologia di compressione dei dati

Determinate i metodi di backup e ripristino



La soluzione di ripristino di emergenza (Disaster Recovery) **per voi**

NON ESISTE UNA "TAGLIA UNICA"

Le vostre esigenze di ripristino determineranno la soluzione. Ciò significa che dovete creare un elenco fedele di caratteristiche, supporto e capacità necessarie per recuperare l'ambiente.

Considerando i possibili disastri, facendoli corrispondere con i set di dati da proteggere e identificando l'aspetto degli obiettivi di recupero necessari, tutto ciò nell'ambito di uno sforzo per creare un elenco di requisiti tattici per l'effettivo backup e ripristino, potrete creare un elenco che soddisfa specificamente le necessità della vostra organizzazione. In definitiva, ciò aiuterà a scegliere una soluzione di ripristino di emergenza (Disaster Recovery) che soddisferà con certezza le vostre esigenze.

Informazioni su SolarWinds® MSP

N4B SRL
via Sant'Ambrogio 4/2
42123 Reggio Emilia
Tel 0522-1607412
commerciale@n4b.it

solarwinds msp

N4B NETWORK for BUSINESS

Distributore Autorizzato

SolarWinds MSP consente agli MSP di tutto il mondo e di qualsiasi dimensione di creare attività molto efficienti e redditizie che apportano un vantaggio competitivo misurabile. Le soluzioni integrate comprendono automazione, sicurezza e gestione di rete e servizio, sia on-premise che nel cloud, supportate da approfondimenti attuabili basati sui dati che consentono agli MSP di lavorare in modo più semplice e veloce.

SolarWinds MSP consente agli MSP di concentrarsi su quello che conta di più: raggiungere i propri SLA e creare un'attività redditizia.

solarwindsmsp.com

www.n4b.it

BUEB00074IT0517