Solution Brief

Zscaler Resilience™

Continuità operativa senza interruzioni durante blackout, cali di tensione e della qualità ed eventi catastrofici

La continuità operativa è una delle preoccupazioni principali per i responsabili IT

Il modo in cui lavoriamo è cambiato, e questo cambiamento ha reso la continuità operativa una priorità assoluta per i responsabili IT, i quali ora devono concentrarsi sulla prevenzione delle interruzioni dei servizi fondamentali per il business e sul supporto della produttività costante come se fosse la normalità. Con i giusti strumenti e processi e la tecnologia adeguata, i team IT possono ripristinare rapidamente e facilmente la piena funzionalità delle loro organizzazioni, anche in caso di eventi catastrofici.

Il passaggio ai servizi cloud per lo storage, l'elaborazione e la sicurezza consente alle organizzazioni di avere sistemi flessibili e scalabili, migliore continuità operativa, costi IT ridotti e minore complessità. Nonostante tutti questi vantaggi, le aziende devono riuscire a ottimizzare la continuità aziendale in caso di eventi disastrosi, come calamità naturali, attacchi fisici o minacce da parte di Stati nazionali.

Zscaler Resilience è un set completo di funzionalità di resilienza che assicura ai clienti una continuità operativa senza interruzioni in caso di blackout, cali di tensione e della qualità o eventi catastrofici. È una soluzione costruita sull'architettura avanzata di Zscaler Zero Trust ExchangeTM e potenziata dall'eccellenza operativa di questa piattaforma, per offrire ai clienti un'elevata disponibilità e semplicità di manutenzione in qualsiasi momento. Le funzionalità di disaster recovery di Zscaler controllate dal cliente, in combinazione con un consolidato set di opzioni di failover, supportano le attività di pianificazione della continuità aziendale dei clienti in tutti gli scenari di guasto. Questa serie completa di funzionalità di resilienza rende il security cloud di Zscaler il più sicuro e resiliente del settore.

Resilienza sul cloud: perché è necessaria?

Se da un lato i leader aziendali si concentrano sulla creazione di un ambiente che favorisca la massima produttività, dall'altro i team IT devono anche garantire la continuità del business e della produttività anche quando problemi di connettività, blackout o guasti ai servizi interrompono la normale operatività aziendale.

Per garantire la continuità azienda, il traffico degli utenti verso le applicazioni fondamentali per il business, come app SaaS, Internet e private, deve poter proseguire costantemente. Le interruzioni potrebbero derivare da un guasto del cloud o da un problema di connettività alle applicazioni. La resilienza sul cloud comprende sia la resilienza del cloud stesso che la resilienza rispetto al cloud.

La resilienza del cloud
La resilienza del cloud garantisce che il cloud stesso sia costruito su un'infrastruttura efficace e disponga di processi operativi consolidati per supportare le funzioni aziendali di tutti i giorni. Il cloud Zscaler gestisce in autonomia molti guasti di gravità ridotta (crash del nodo, problemi al disco, ecc.), senza alcun intervento da parte del cliente e senza incorrere nella perdita di connettività o in un calo delle prestazioni. I nostri robusti sistemi hardware sfruttano l'over–provisioning della capacità di elaborazione e la ridondanza, e costituiscono la base per un'elevata resilienza.

Resilienza al cloud
La resilienza al cloud è un aspetto essenziale di una soluzione completa di resilienza sul cloud. La connettività al cloud dipende dalla sua disponibilità e dai mezzi per connettersi, che consentono agli utenti di raggiungere le applicazioni o i dati. Quando l'accesso al cloud viene interrotto, è necessario trovare un percorso alternativo e ottimale verso le applicazioni. Questa ottimizzazione è data da un insieme di azioni manuali o automatiche che possono essere eseguite per affrontare i guasti, che possono prendere la forma di un calo delle prestazioni di rete o di un'interruzione totale. Zscaler Resilience è un set completo di funzionalità che assicura una continuità operativa senza interruzioni anche al verificarsi di un qualsiasi tipo di guasto, da quelli meno gravi a quelli più catastrofici.

Garantire la resilienza al cloud in tutti gli scenari di guasto

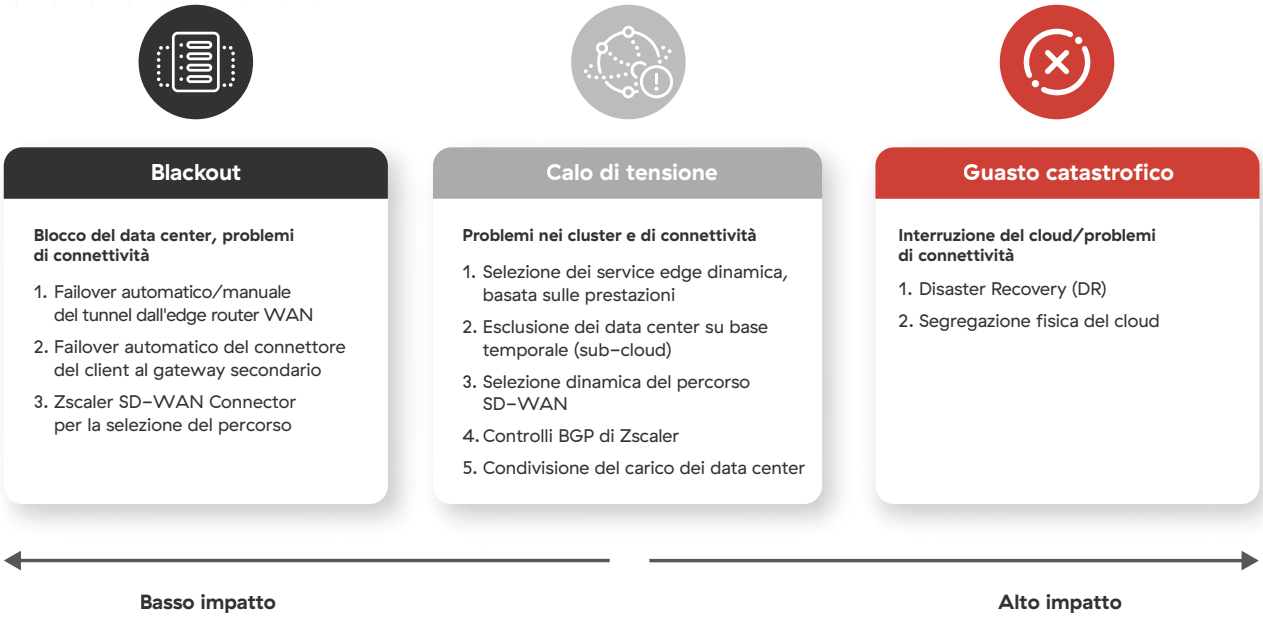

Figura 1: diverse opzioni per rispondere agli scenari di guasto

Guasti di gravità ridotta

I guasti meno gravi includono glitch prestazionali, problemi di compatibilità e problemi operativi o qualitativi che non costituiscono guasti gravi o critici. Alla base di questi guasti isolati potrebbero esserci arresti dei nodi o problemi del disco. I guasti meno gravi si verificano più frequentemente e passano spesso inosservati. Questi guasti possono portare a rallentamenti, problemi operativi e frustrazione degli utenti. L'architettura cloud resiliente di Zscaler e la sua eccellenza operativa sono in grado di evitarli. I guasti vengono gestiti in background con un'interazione minima del cliente e la garanzia di una produttività costante.

I principali vantaggi di Zscaler Resilience

Continuità operativa con una sicurezza senza interruzioni

Applicazione delle policy di sicurezza critiche concedendo al contempo l'accesso zero trust a Internet, SaaS e app private, anche durante eventi catastrofici.

Esperienze fluide in tutti gli scenari di guasto

Gestione di blackout, cali di tensione e della qualità e guasti catastrofici in modo semplice, sfruttando l'architettura di livello superiore e l'eccellenza operativa di Zscaler Zero Trust Exchange.

Riduzione di costi e complessità

Evita le interruzioni e i cali di produttività derivanti dall'impossibilità di accedere alle applicazioni critiche, eliminando i costi per l'infrastruttura di backup legacy e le VPN on-premise.

Blackout

Le interruzioni dei data center (come l'interruzione di gennaio 2022 avvenuta nella struttura di Interxion a Londra) o i problemi di connettività maggiori come le interruzioni di carrier o provider di transito, sono considerati scenari di blackout che impediscono alle organizzazioni di inoltrare il traffico al data center di Zscaler colpito. La nostra architettura ridondante, basata su data center carrier-neutral con più provider e Internet Exchange (IX), è molto efficace nel ridurre al minimo le interruzioni dovute alla perdita di un carrier e ad altri problemi di connettività. Indipendentemente dalla tempistica di ripristino, l'impatto negativo per i nostri clienti è quello di non poter continuare a usufruire dei servizi nel data center colpito.

Per continuare a lavorare, i clienti devono quindi reindirizzare il traffico verso un data center di Zscaler secondario nelle vicinanze. Per questo, utilizziamo un mix di carrier e provider di data center, al fine di mitigare efficacemente le interruzioni subite da qualsiasi fornitore garantendo la disponibilità di un data center secondario. Inoltre, effettuiamo l'over-provisioning e manteniamo una capacità di riserva nel data center per supportare un carico transitorio aggiuntivo.

La continuità operativa implica la comprensione e la pianificazione di diversi possibili scenari di guasto. Zscaler offre un'infrastruttura all'avanguardia progettata per fornire una disponibilità del 100%.

Traffico dall'ufficio tramite dispositivo SD-WAN
Quando si invia il traffico da un ufficio utilizzando un dispositivo di routing/SD-WAN, i clienti devono seguire le best practice di distribuzione di Zscaler e disporre di un tunnel IPsec/GRE di backup pronto all'uso nel caso in cui quello primario non sia raggiungibile. Le modalità di attivazione del failover dipendono dalle capacità del dispositivo e dalla progettazione della rete. Ad esempio, una SD-WAN con doppi circuiti Internet può eseguire in automatico il failover verso il tunnel di backup su un circuito secondario quando il tunnel attivo diventa irraggiungibile o supera una soglia di latenza (con i controlli di integrità L7 abilitati). Nel caso di dispositivi più datati, i clienti devono attivare manualmente il tunnel di backup. Una volta ripristinato il data center primario, è responsabilità del cliente effettuare nuovamente la commutazione.

Il traffico con Zscaler Client Connector
Quando si invia il traffico utilizzando Zscaler Client Connector, Zscaler controlla entrambi gli edge del tunnel ed effettua automaticamente il failover dal gateway primario a quello secondario utilizzando la logica del file App Profile PAC. Zscaler Client Connector (ZCC) effettuerà poi la commutazione al gateway primario quando questo sarà di nuovo raggiungibile. In alcuni casi, i clienti possono scegliere di modificare manualmente i file PAC per attivare un failover.

Cali di tensione e della qualità

Se non gestito correttamente, un calo involontario o inatteso della tensione o della qualità del servizio della rete (anche definito brownout) può rivelarsi costoso, sia in termini di mancati guadagni che di produttività: se gli utenti segnalano un problema di questo tipo prima che il team IT lo abbia rilevato e abbia iniziato a lavorare per risolverlo, la situazione può generare grande frustrazione per l'utente, e tutto il sistema rischia di subire rallentami. Oltre alle modalità di gestione dei blackout, Zscaler aiuta anche a mitigare i cali di tensione attraverso i seguenti metodi.

Zscaler effettua la selezione dinamica dei service edge in base alle prestazioni

Zscaler Client Connector seleziona il percorso ottimale tra lo ZIA Service Edge primario e quello secondario, indipendentemente dalla vicinanza geografica e basandosi invece sullo stato di ogni ZIA Service Edge, come mostrato nella figura 2. Una connessione HTTP end-to-end calcola la latenza rilevando continuamente il ping di entrambi i gateway. Grazie a tutto questo, Zscaler è in grado di offrire la selezione dei data center in base alla latenza, per affrontare efficacemente le situazioni in cui si verificano cali di tensione o della qualità.

Esclusione dei data center controllata dal cliente

Un altro modo per preservare la continuità operativa durante i cali di tensione o della qualità del servizio consiste nella selezione dei data center controllata dal cliente, come illustrato nella figura 3. Quando un cliente riscontra dei problemi di capacità in un data center, come ad esempio un problema di peering di un'applicazione SaaS a Los Angeles (che potrebbe richiedere ore per essere risolto), quel data center può essere escluso dal subcloud tramite il portale dell'amministratore. Zscaler Client Connector recupera quindi il nuovo gateway primario e secondario e instaura uno Z-tunnel verso un nuovo data center. Questa esclusione del data center controllata dal cliente è temporanea e, decorso un periodo di tempo prestabilito, si ritornerà alla selezione del data center originale.

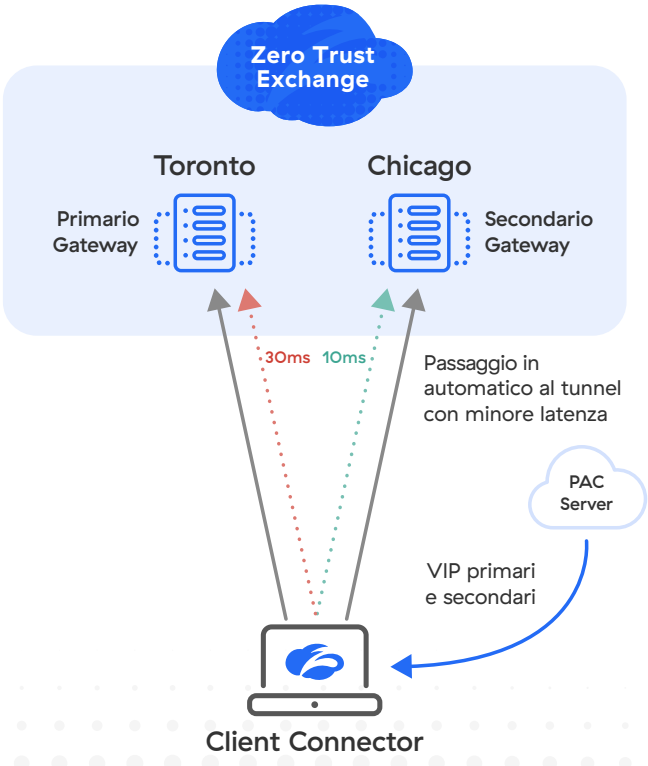

Figura 2: selezione dinamica dei service edge in base alle prestazioni

Failover del tunnel da dispositivi di routing sensibili ai cali di tensione o della qualità

Quando si invia il traffico da un ufficio utilizzando un dispositivo di routing/SD-WAN su cui Zscaler non ha un controllo diretto, le opzioni del cliente sono vincolate alle capacità del dispositivo edge. Ad esempio, un router SD-WAN può essere in grado di rilevare la riduzione di un servizio utilizzando algoritmi proprietari basati sui controlli di integrità L7 sugli endpoint di probing di Zscaler. Una volta rilevato un potenziale calo di tensione o della qualità, il dispositivo SD-WAN può eseguire automaticamente il failover verso un tunnel di backup sullo stesso link o su un link secondario. Quando i controlli di integrità forniranno risultati migliori, il dispositivo tornerà al tunnel primario.

Controlli BGP di Zscaler

La nostra architettura ridondante, basata su data center carrier-neutral con più provider e Internet Exchange (IX), è molto efficace nel ridurre al minimo cali di tensione o della qualità, congestione o altre problematiche relative ai singoli carrier. Quando Zscaler CloudOps rileva che un ISP upstream fornisce un routing non ottimale, siamo in grado di reindirizzare il traffico verso un ISP secondario, mentre lavoriamo con quello primario per risolvere il problema.

Condivisione del carico dei data center di Zscaler

In caso di congestione della rete o di altri problemi di connettività di un particolare data center, Zscaler è in grado di reindirizzare proattivamente i client che eseguono Zscaler Client Connector verso data center secondari nelle vicinanze, senza utilizzare un metodo statistico.

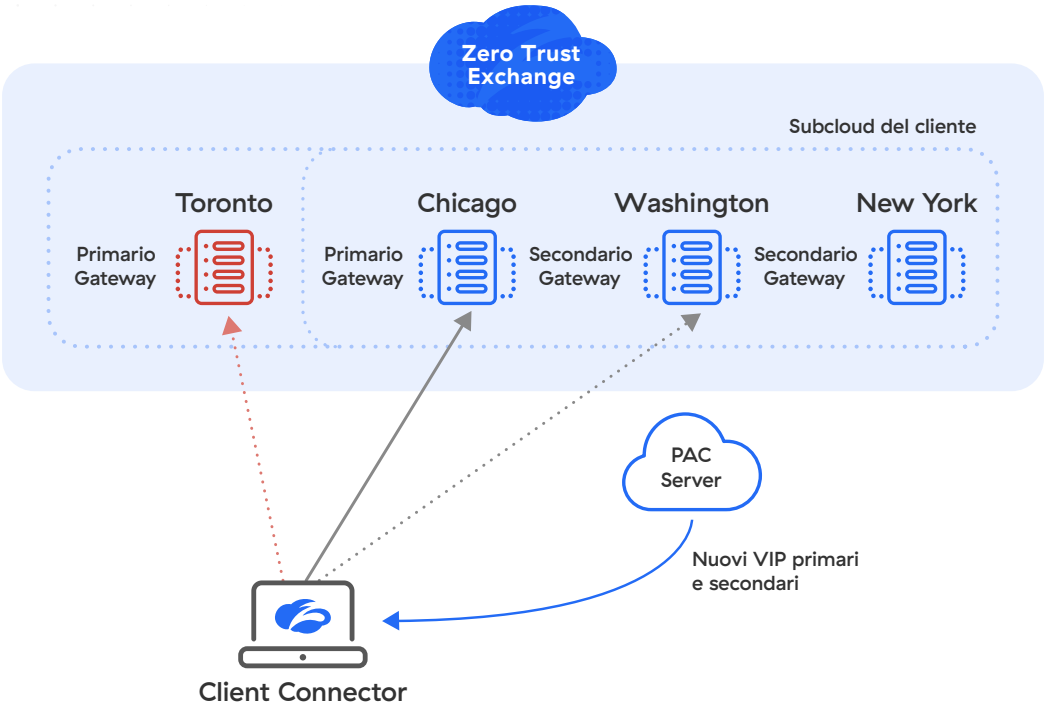

Figura 3: esclusione dei data center controllata dal cliente

Guasti catastrofici

Funzionalità di Disaster Recovery di Zscaler per ZIA/ZPA

Zscaler Disaster Recovery (DR) per il cloud offre agli utenti un'operatività ininterrotta, garantendo l'accesso alle applicazioni mission-critical anche in caso di eventi imprevisti.

Zscaler Disaster Recovery è una soluzione per la continuità operativa controllata dal cliente, che consente alle organizzazioni di preservare l'operatività anche durante un potenziale evento catastrofico che potrebbe colpire il cloud di Zscaler.

Zscaler Disaster Recovery viene avviato aggiornando il record TXT del DNS. Quando viene avviato il failover di DR, Zscaler Disaster Recovery fornisce agli utenti che si collegano da qualsiasi luogo un percorso per accedere alle applicazioni mission-critical private, SaaS o Internet, come illustrato nella figura 4. Con Zscaler Disaster Recovery i clienti possono controllare a quali applicazioni private o SaaS critiche per l'azienda possono accedere gli utenti durante un'interruzione del cloud globale di Zscaler.

Gli utenti si connettono alle applicazioni private critiche attraverso un Private Service Edge di Zscaler Private Access™ (ZPA™), una versione distribuita localmente del cloud Zscaler, e alle applicazioni SaaS critiche e Internet in base alle policy salvate nell'istanza AWS S3. Qualsiasi cliente che ha Zscaler Client Connector installato può utilizzare Zscaler Disaster Recovery. Grazie al trigger di DR basato su DNS e avviato dal cliente, quest'ultimo può determinare e controllare quando attivare la funzione di disaster recovery.

Per un accesso sicuro alle applicazioni private, gli amministratori possono configurare il DR nello Zscaler Admin Portal per i segmenti delle applicazioni critiche, i gruppi App Connector e i gruppi ZPA Private Service Edge, per garantire la continuità operativa qualora si verifichi un evento catastrofico con conseguenze sull'infrastruttura cloud globale di ZPA.

Accesso alle applicazioni critiche definite dal cliente
Nel pannello di controllo dell'interfaccia utente di ZPA, i clienti possono definire le applicazioni critiche, per garantire la continuità operativa in caso di disastro e assicurarsi che gli utenti vi abbiano accesso durante un evento di DR.

Per offrire l'accesso sicuro alle applicazioni su Internet tramite Zscaler Internet Access™ (ZIA™), gli amministratori possono scegliere tra le seguenti opzioni di disaster recovery (questi controlli sono forniti tramite Zscaler Client Connector e configurati nello Zscaler Portal):

- **Fail Open:** nel remoto caso in cui si verifichi un'interruzione di Zscaler Cloud, gli utenti accederebbero direttamente a Internet. Tuttavia, questo comporterebbe il rischio di un accesso illimitato a qualsiasi sito web su Internet senza restrizioni di sicurezza.
- **Accesso Controlled Fail Open a un elenco di destinazioni Internet definito da Zscaler:** gli utenti hanno accesso alle applicazioni web più comuni e critiche (Microsoft 365, Google Workspace, ecc.). Zscaler definisce e ospita questo elenco su AWS, in modo che sia disponibile nell'eventualità in cui Zscaler Cloud sia in fase di ripristino dopo un'interruzione. I clienti possono aggiungere il proprio elenco di siti Internet e ogni sito web non presente nell'elenco sarà bloccato. L'applicazione del blocco avviene all'endpoint dell'utente tramite Zscaler Client Connector, che scaricherà periodicamente l'elenco per mantenerlo aggiornato e accurato.
- **Fail Closed:** i clienti più attenti alla sicurezza, che non vogliono concedere agli utenti l'accesso indistinto a tutto ciò che è presente su Internet senza Zscaler Internet Access, possono bloccare tutti gli accessi.

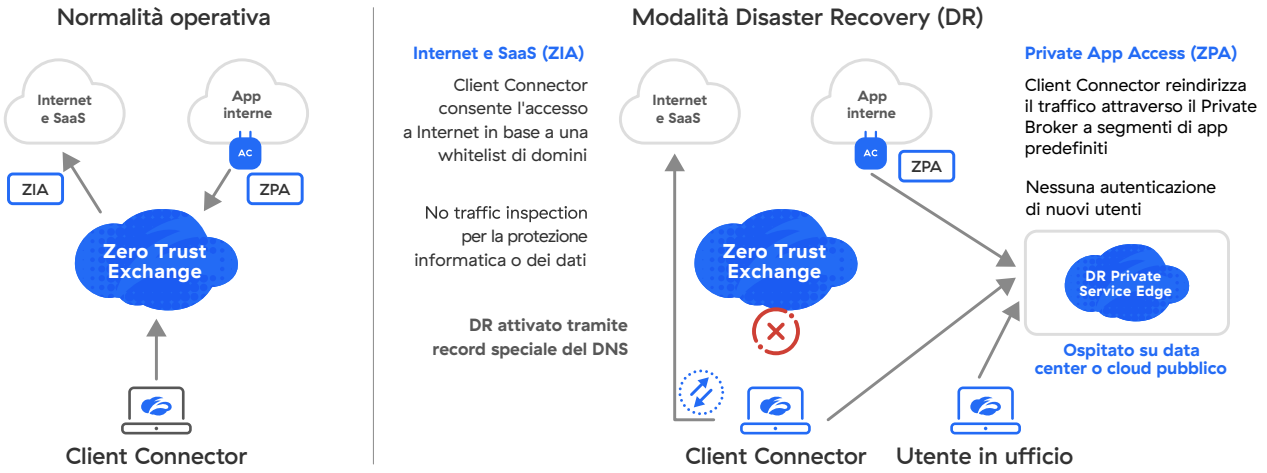

Figura 4: Disaster Recovery per il servizio mission-critical di Zscaler

L'abilitazione della funzione di disaster recovery garantisce la continuità operativa nel caso in cui si verifichi un evento catastrofico con conseguenze sull'infrastruttura del cloud globale di Zscaler. Questa implementazione offre agli utenti di tutto il mondo un accesso senza interruzioni alle applicazioni critiche.

Durante le normali operazioni, l'accesso alle applicazioni mission-critical viene mediato attraverso Zero Trust Exchange. In caso di disastro, tutte le connessioni alle applicazioni private saranno mediate attraverso il servizio ZPA Private Service Edge installato localmente nel data center del cliente o sul cloud privato, mentre tutte le connessioni a Internet e alle applicazioni SaaS verranno eseguite in base alle policy salvate nel bucket di AWS S3. In questo modo, anche durante un evento catastrofico, l'esperienza utente rimane ottimale. Al ripristino della funzionalità di Zscaler Cloud, il prodotto può tornare a funzionare normalmente, per consentire di sfruttare appieno la sicurezza e la connettività zero trust offerte da Zero Trust Exchange. Zscaler Digital Experience rileva i guasti meno gravi, i cali di tensione o della qualità e i blackout, per aiutare i clienti a eseguire le attività di correzione prima che gli utenti ne subiscano le conseguenze. La piattaforma Zscaler offre la massima flessibilità per supportare la continuità operativa, fornendo una sicurezza senza eguali e un'esperienza utente senza interruzioni.

Zscaler Resilience fa parte della piattaforma completa, e offre ai nostri clienti ridondanza senza la necessità di ricorrere a servizi esterni aggiuntivi. Zscaler si impegna a fornire un'esperienza fluida e senza interruzioni agli utenti e ai team IT, investendo costantemente nelle soluzioni Zscaler Resilience.

I principali vantaggi di Zscaler Disaster Recovery

- Interruzione minima delle operazioni dei clienti durante un evento catastrofico;
- Accesso alle applicazioni mission-critical, anche durante un evento imprevisto; • Maggiore affidabilità della soluzione per consentire l'accesso alle applicazioni con Zscaler;
- Risparmio sui costi, grazie alla possibilità di gestire un'unica piattaforma per l'accesso alle applicazioni, sia durante il normale funzionamento che in DR
- Risparmi potenziali, evitando i cali di produttività dovuti a eventuali interruzioni durante un evento catastrofico.

Per scoprire le ultime novità su Zscaler Resilience visita zscaler.it/resilience.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita di dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata sul SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it