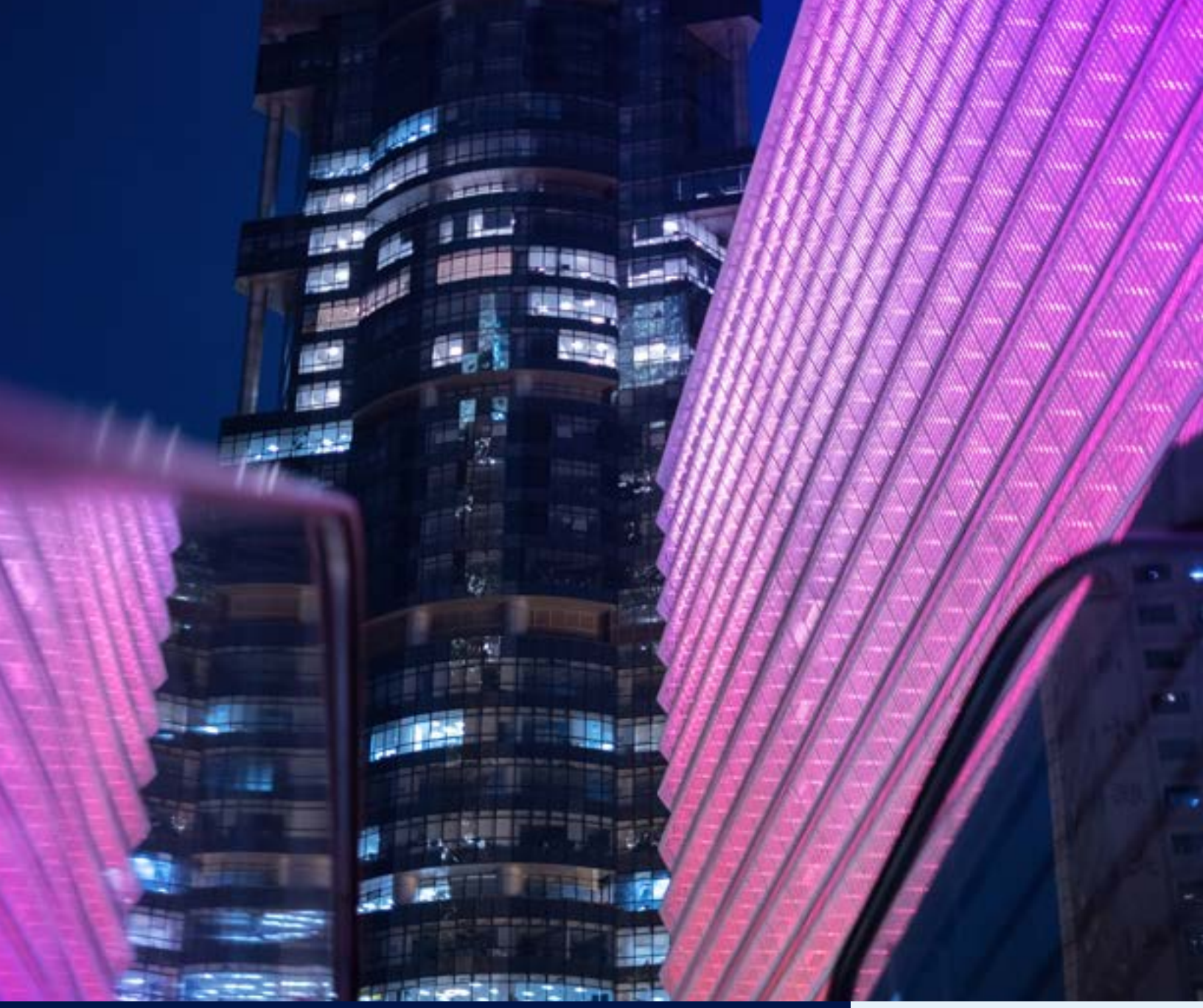

Zscaler Resilience™

Continuità operativa senza interruzioni durante blackout, brownout e della qualità ed eventi catastrofici

PANORAMICA SULLA SOLUZIONE

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

Il nostro modo di lavorare è cambiato e, di conseguenza, la continuità operativa è diventata una priorità assoluta per i responsabili IT. Questi ultimi, infatti, oggi devono concentrarsi sulla prevenzione delle interruzioni dei servizi critici per il business e favorire la continuità della produttività, al fine di consentire alle aziende di continuare a operare come di consueto. 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, una 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 garantisce ai clienti una continuità operativa ininterrotta durante blackout, cali di tensione ed eventi catastrofici. Si basa sull'architettura avanzata di Zscaler Zero Trust Exchange™ e si avvale di un'eccellenza operativa che consente di offrire ai clienti un'elevata disponibilità e facilità di manutenzione in ogni momento. Le funzionalità di disaster recovery di Zscaler, gestite dal cliente e abbinate a un solido set di opzioni di failover, supportano le attività di pianificazione della continuità operativa dei clienti in tutti gli scenari di guasto. Questo set completo di funzionalità 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 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 aziendale, 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.

Resilienza del cloud
La resilienza del cloud garantisce che il cloud stesso sia basato su un'infrastruttura efficace e disponga di solidi processi operativi per supportare le funzioni aziendali quotidiane. Il cloud di Zscaler gestisce in autonomia numerosi guasti minori (crash dei nodi, problemi del disco, ecc.) senza necessitare di interazioni con il cliente né comportare perdite di connettività o cali delle prestazioni. I nostri solidi sistemi hardware appositamente progettati, con overprovisioning della capacità di elaborazione e ridondanza, gettano le basi 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 di connessione, per consentire agli utenti di raggiungere applicazioni o dati. Quando l'accesso al cloud viene interrotto, è necessario trovare un percorso alternativo e ottimale per le applicazioni. Questa ottimizzazione è data da un insieme di azioni manuali o autonome che possono essere intraprese per affrontare guasti che possono andare da un calo delle prestazioni della rete a interruzioni totali. Zscaler Resilience è un set completo di funzionalità che garantisce una continuità operativa senza interruzioni di fronte a qualsiasi tipo di guasto, dai guasti minori a quelli di natura catastrofica.

Garantire la resilienza al cloud in tutti gli scenari di guasto

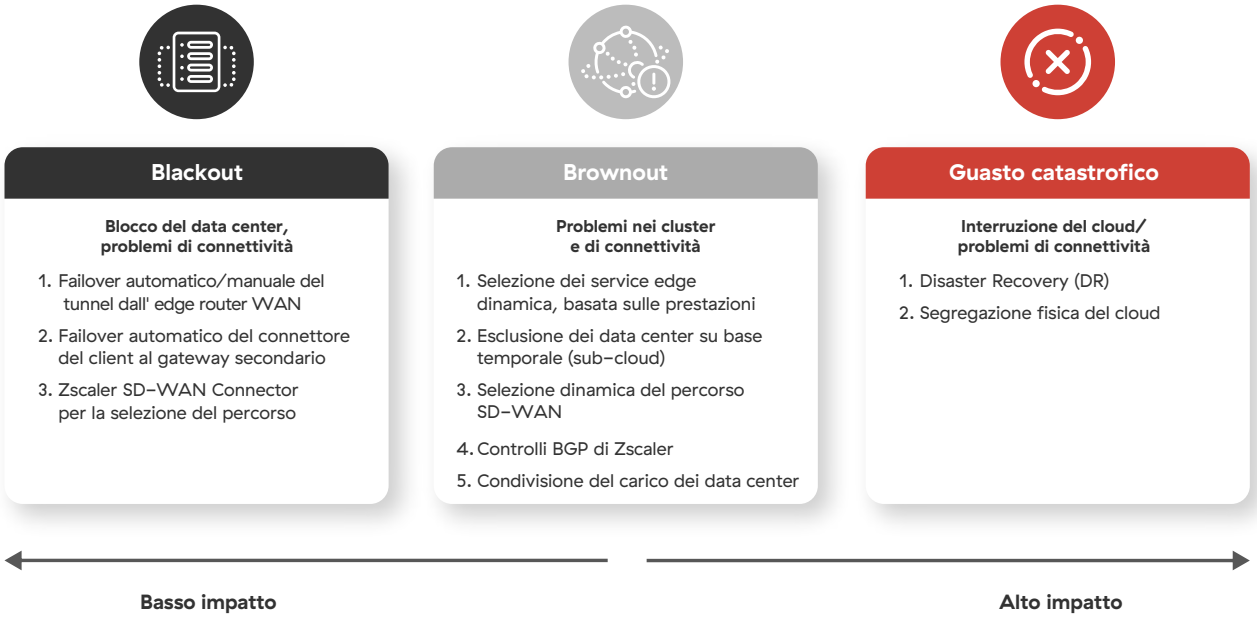

Figura 1: diverse opzioni per rispondere agli scenari di guasto

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

La continuità operativa con una sicurezza costante

Applica le policy di sicurezza critiche garantendo al tempo stesso un accesso zero trust a Internet, SaaS e app private, anche durante eventi catastrofici.

Esperienze senza interruzioni in tutti i possibili scenari di guasto

Gestisci con facilità blackout, cali di tensione e guasti legati a eventi catastrofici sfruttando l'architettura migliore della categoria e l'eccellenza operativa di Zscaler Zero Trust Exchange.

Riduzione di costi e complessità

Evita le interruzioni dell'attività e le perdite di produttività causate dalla mancanza di accesso alle app critiche per il business eliminando al tempo stesso 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'overprovisioning 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
Se il traffico viene inviato da un ufficio utilizzando un dispositivo di routing/SD-WAN, i clienti dovranno seguire le best practice di distribuzione di Zscaler predisponendo un tunnel IPsec/GRE di backup pronto per essere utilizzato quando quello primario non è raggiungibile. Il modo in cui verrà attivato il failover dipenderà dalle capacità del dispositivo e dalla progettazione della rete. Ad esempio, una SD-WAN con circuiti Internet doppi potrebbe eseguire automaticamente il failover sul tunnel di backup di un circuito secondario quando il tunnel attivo risulta irraggiungibile o supera una data soglia di latenza (con i controlli di integrità L7 abilitati). Se si adottano dispositivi più basici, i clienti devono abilitare manualmente il tunnel di backup. Una volta ripristinato il data center primario, sarà responsabilità del cliente ripristinare la configurazione precedente.

Traffico tramite Zscaler Client Connector.
Se il traffico viene inviato tramite Zscaler Client Connector, Zscaler controlla entrambi i lati del tunnel ed esegue automaticamente il failover dal gateway primario a quello secondario utilizzando la logica del file PAC in App Profile. Zscaler Client Connector (ZCC) tornerà al gateway primario non appena risulterà nuovamente raggiungibile. In alcuni casi, i clienti possono scegliere di modificare manualmente i file PAC per attivare un failover.

Brownout

Un calo involontario o inaspettato della qualità del servizio di rete è dato, in genere, da un brownout. Gestire male un brownout può essere costoso, sia in termini di mancati ricavi che di produttività: la segnalazione di un brownout prima che il team IT lo abbia rilevato e abbia iniziato a lavorare per risolverlo può generare notevole frustrazione negli utenti, comportando un rallentamento a livello generale. Oltre alle modalità di gestione dei blackout, Zscaler aiuta a mitigare i brownout anche attraverso i seguenti metodi.

Funzionalità di selezione dinamica del service edge basata sulle prestazioni di Zscaler
Zscaler Client Connector seleziona il percorso ottimale tra lo ZIA Service Edge primario e quello secondario, indipendentemente dalla prossimità geografica, basandosi sullo stato di ciascun ZIA Service Edge, come mostrato nella figura 2. Una connessione HTTP end-to-end calcola la latenza, e per calcolarla effettua continuamente il ping su entrambi i gateway. In questo modo, Zscaler offre una selezione del data center basata sulla latenza per affrontare efficacemente gli eventuali cali di tensione.

Esclusione del data center controllata dal cliente
Un altro modo per preservare la continuità operativa durante i cali di tensione consiste nella selezione del data center controllata dal cliente, come mostrato nella figura 3. Quando un cliente riscontra problemi di capacità in un data center, come un problema di peering dell'applicazione SaaS in LAX (che potrebbe richiedere ore per essere risolto), il data center in questione può essere escluso dal subcloud nel portale di amministrazione. 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 di natura temporanea e, dopo un periodo di tempo predeterminato, si ritornerà al data center originario.

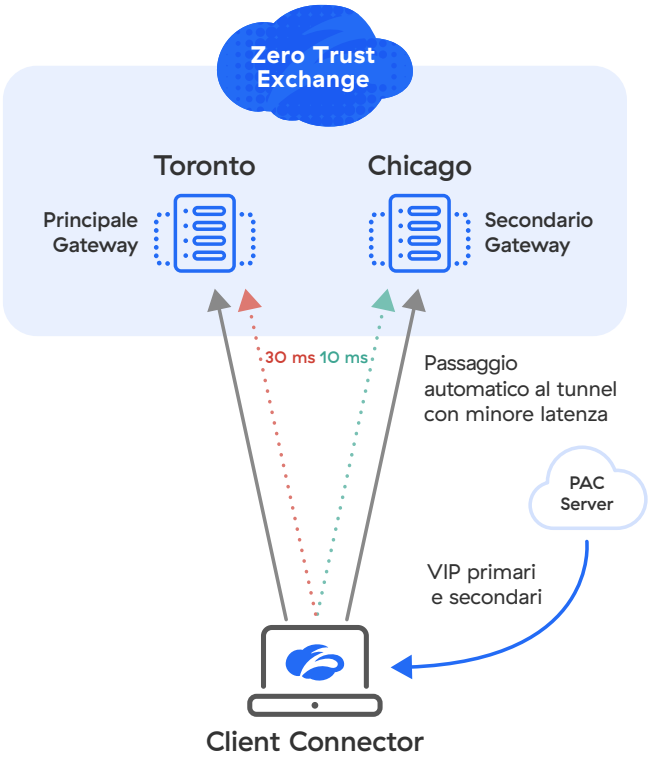

Figura 2: selezione dinamica dei service edge in base alle prestazioni

Failover del tunnel dai dispositivi di routing sensibili al brownout
Quando il traffico viene inviato da un ufficio utilizzando un dispositivo di routing/SD-WAN su cui Zscaler non ha alcun controllo diretto, le opzioni a disposizione del cliente sono vincolate alle capacità del dispositivo all'edge. Ad esempio, un router SD-WAN può rilevare la riduzione del servizio utilizzando algoritmi proprietari basati sui controlli di integrità L7 per gli endpoint di probing di Zscaler. Una volta rilevato il potenziale brownout, il dispositivo SD-WAN può eseguire automaticamente il failover su un tunnel di backup sullo stesso collegamento o su un collegamento secondario. Il dispositivo tornerà al tunnel primario non appena i controlli di integrità forniranno risultati migliori.

Controlli BGP di Zscaler
La nostra architettura ridondante, costituita da data center carrier-neutral con numerosi provider e Internet Exchange (IX), è altamente efficace nel ridurre al minimo cali di tensione, congestioni o altri problemi con singoli carrier. Se Zscaler CloudOps individua un routing inefficiente da parte di un ISP upstream, il traffico viene deviato su un secondo ISP, consentendoci di intervenire con il provider principale per correggere l'anomalia.

Funzionalità di Zscaler di condivisione del carico dei data center
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.

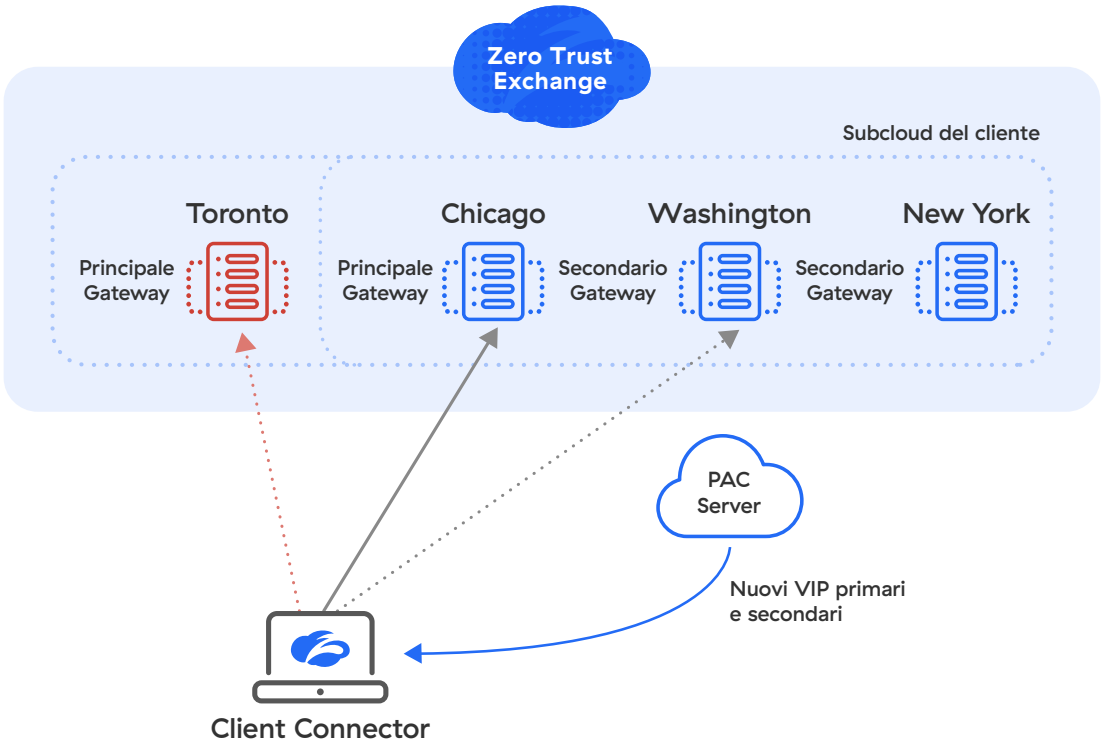

Figura 3: esclusione dei data center controllata dal cliente

Guasti catastrofici

Zscaler Business Continuity per ZIA/ZPA

Zscaler Business Continuity per il cloud offre agli utenti un'operatività ininterrotta, garantendo l'accesso alle applicazioni fondamentali per il business anche in caso di eventi imprevisti.

Le organizzazioni necessitano di un accesso ininterrotto alle proprie applicazioni, senza però compromettere la propria sicurezza zero trust, anche in caso di eventi imprevisti o periodi di riduzione dell'accesso all'infrastruttura. Inoltre, in molti settori è necessario rispettare standard normativi e di conformità per la continuità operativa.

Per soddisfare queste esigenze, Zscaler offre la possibilità di accedere a un cloud privato per la continuità operativa, in modo da garantire l'operatività delle organizzazioni anche durante un evento catastrofico che potrebbe avere ripercussioni sul cloud pubblico di Zscaler.

Se il cloud pubblico di Zscaler non è raggiungibile o disponibile, i clienti possono passare alla Business Continuity Mode. In questo stato, le policy e l'autenticazione degli utenti continuano a essere applicate dai servizi Zscaler presenti su una macchina virtuale ospitata dal cliente.

Business Continuity per ZIA

Per garantire un accesso ininterrotto a Internet e alle applicazioni SaaS e preservare la conformità, Zscaler offre la possibilità di eseguire il failover su un cloud privato per la continuità operativa, che comprende ZIA Private Service Edge ospitati dal cliente e una cache privata di policy.

I PSE offrono un'elaborazione coerente del traffico, supportando funzionalità come l'ispezione del traffico e un firewall per gli utenti che utilizzano Client Connector di Zscaler. In caso di interruzione, i private service edge sono supportati da una cache privata di policy che conserva una copia della configurazione del cliente memorizzata nella cache.

Per i clienti che non desiderano implementare funzionalità in self hosting, la soluzione di continuità operativa standard di Zscaler consente l'accesso continuo alle applicazioni web e SaaS in caso di interruzione. In questo scenario, i clienti possono scegliere una di queste tre opzioni:
Fail Open: accesso a Internet illimitato senza restrizioni di sicurezza
Lista di elementi consentiti predefinita: accesso illimitato a un set limitato di applicazioni comuni
Fail Closed: l'accesso a Internet risulta bloccato per tutta la durata dell'interruzione

Continuità aziendale per ZPA

Per un accesso costante alle applicazioni private durante un'interruzione, i clienti possono facoltativamente scegliere di implementare il proprio cloud privato per la continuità operativa, costituito da raggruppamenti logici dei seguenti componenti, ognuno dei quali può essere distribuito in un gruppo per aumentare ulteriormente la ridondanza:
Private Cloud Controller che sincronizzano continuamente la configurazione e le policy con il cloud Zscaler
ZPA Private Service Edge che forniscono funzionalità ZPA pubbliche nell'ambiente di un'organizzazione
App Connector per l'accesso sicuro ai servizi privati
Ricevitori di log per l'acquisizione degli output dei log da altri componenti

In caso di interruzioni di natura catastrofica o di irraggiungibilità del cloud Zscaler, gli utenti si collegheranno automaticamente ai Private Cloud Controller per l'autenticazione e il reindirizzamento agli ZPA private service edge. Una volta effettuato il collegamento al PSE, il canale per il controllo e i dati sarà con lo ZPA PSE.

I Private Cloud Controller distribuiti come macchine virtuali forniscono funzioni critiche in caso di interruzione:

- Reindirizzamento dell'autenticazione
- Reindirizzamento dell'utente
- Servizio di trasmissione dei registri
- Sincronizzazione della configurazione del cliente
- Sincronizzazione delle policy del cliente

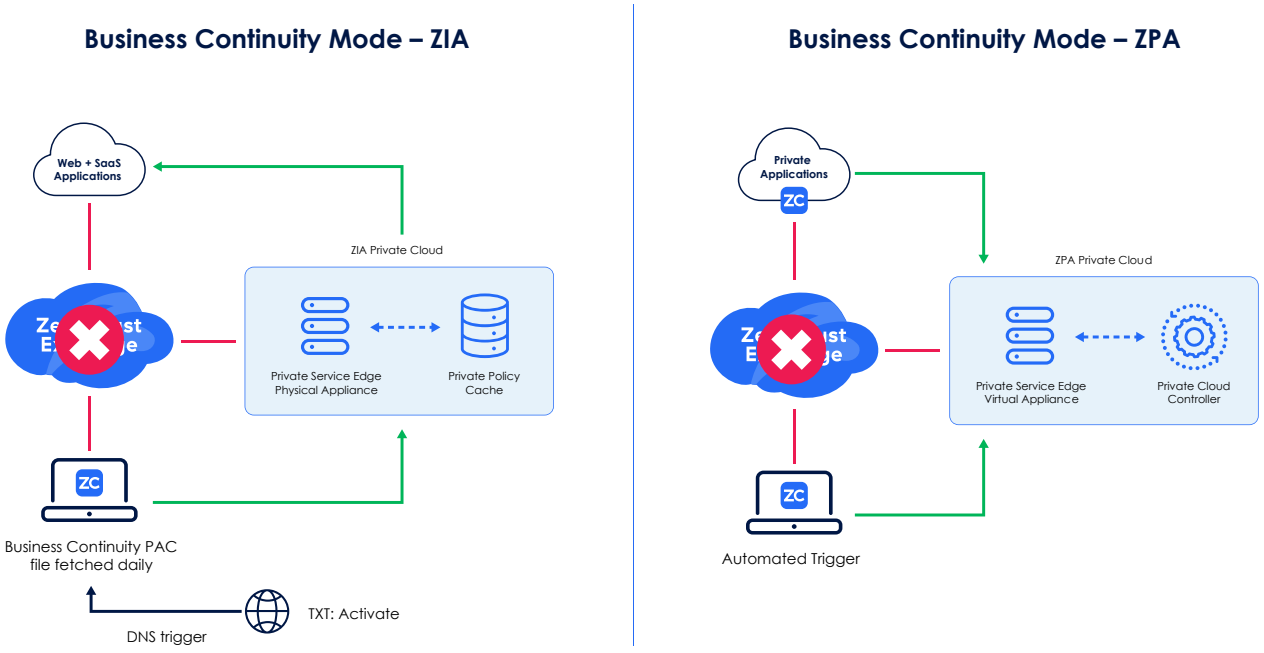

Figura 4: cloud privati per la continuità operativa per accedere a tutte le app in totale sicurezza

Business Continuity per gli endpoint

Un altro problema che può rivelarsi catastrofico per un'organizzazione è l'impossibilità di utilizzare i propri endpoint abituali (laptop, computer, ecc.) quando questi, per un qualsiasi motivo, non risultano disponibili perché malfunzionanti, inaccessibili o compromessi. Per affrontare questo scenario, è possibile implementare Zscaler Cloud Browser Isolation per fornire un accesso sicuro basato su browser ad applicazioni private, web o SaaS dagli endpoint non gestiti (come BYOD), senza il rischio di perdere i dati.

Zscaler Business Continuity – Conclusione

Al ripristino della funzionalità del cloud Zscaler, 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 Business Continuity, parte integrante della piattaforma Zscaler, garantisce ai clienti ridondanza senza la necessità di aggiungere altre soluzioni di terze parti. Zscaler si impegna a fornire un'esperienza fluida e senza interruzioni agli utenti e ai team IT, investendo costantemente nelle soluzioni di resilienza di Zscaler.

I principali vantaggi delle soluzioni di continuità operativa di Zscaler

- Interruzione minima delle operazioni per i clienti durante un evento catastrofico;
- Accesso alle applicazioni critiche per il business anche al verificarsi di un incidente imprevisto;
- Maggiore affidabilità della soluzione nel 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 caso di interruzioni;
- Risparmi potenziali, evitando i cali di produttività dovuti a eventuali interruzioni durante un evento catastrofico.

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

zscaler™ | Experience your world, secured.™

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