



Zscaler Resilience™

Continuité d'activité sans aucune interruption pendant les pannes totales, les baisses de la qualité de service réseau et les événements catastrophiques

La continuité d'activité est une préoccupation majeure des responsables informatiques

Notre façon de travailler a évolué, et avec ce changement, la continuité d'activité est devenue une priorité absolue pour les responsables informatiques. Désormais, ils doivent se concentrer sur la prévention des interruptions des services stratégiques et veiller au maintien de la productivité. Avec les outils, les processus et la technologie adaptés, les équipes informatiques peuvent rétablir rapidement et facilement toutes les fonctionnalités de leur entreprise, même en cas de sinistre.

La migration du stockage, de l'informatique et de la sécurité vers les services cloud a apporté aux entreprises des systèmes flexibles et évolutifs, une continuité d'activité optimisée, une réduction des coûts informatiques et une diminution de la complexité. Même avec ces avantages, les entreprises cherchent à optimiser la continuité d'activité face à des désastres tels que des catastrophes naturelles, des attaques physiques ou des menaces d'États-nations.

Zscaler Resilience désigne un ensemble complet de fonctionnalités de résilience qui garantit aux clients la continuité d'activité sans interruption en cas de pannes totales, de baisses de la qualité de service réseau et d'événements catastrophiques. Cette solution repose sur l'architecture avancée de Zscaler Zero Trust Exchange™ et est optimisée par notre excellence opérationnelle afin de garantir à tout moment une haute disponibilité et une facilité de maintenance à nos clients. Les capacités de reprise après sinistre de Zscaler contrôlées par le client, combinées à un ensemble robuste d'options de basculement, soutiennent les efforts de planification de la continuité d'activité des clients dans tous les scénarios de panne. Cet ensemble complet de capacités de résilience fait du cloud de sécurité Zscaler le cloud le plus sécurisé et le plus résilient du secteur.

Résilience cloud : pourquoi est-elle indispensable ?

Les chefs d'entreprise ont à cœur de fournir un environnement propice à une productivité

maximale. Les équipes informatiques doivent assurer la continuité d'activité et de productivité même lorsque des problèmes de connectivité, des événements de mise à l'échelle ou des défaillances de service perturbent l'activité normale de l'entreprise.

Le trafic des utilisateurs vers les applications stratégiques (SaaS, internes et privées) doit constamment être assuré pour garantir la continuité d'activité. Les interruptions peuvent résulter d'une panne du cloud ou de la connectivité aux applications. La résilience du cloud englobe à la fois la résilience au sein du cloud et la résilience vers le cloud.

Résilience du cloud

La résilience du cloud garantit que le cloud lui-même repose sur une infrastructure performante et dispose de processus opérationnels robustes pour les activités quotidiennes de l'entreprise. Le cloud Zscaler gère de manière autonome de nombreuses pannes mineures (panne de nœud, problèmes de disque, etc.) sans interaction du client, perte de connectivité ni baisse de performances. Nos systèmes matériels robustes spécialement conçus, avec une capacité de traitement et une redondance surdimensionnées, constituent la base d'une haute résilience.

Résilience vers le cloud

La résilience vers le cloud représente un aspect essentiel d'une solution complète de résilience cloud. La connectivité au cloud dépend de sa disponibilité et des moyens de connexion permettant aux utilisateurs d'accéder aux applications ou aux données. En cas d'interruption de l'accès au cloud, il est nécessaire de trouver un chemin alternatif et optimal vers les applications. Cette optimisation passe par un ensemble d'actions manuelles ou autonomes pouvant être appliquées pour faire face à des défaillances allant d'une baisse de performance réseau à une interruption totale. Zscaler Resilience est un ensemble complet de fonctionnalités qui assure une continuité d'activité ininterrompue pour tout type de défaillances, des pannes mineures aux pannes catastrophiques.

Garantir la résilience du cloud à travers des scénarios de défaillance

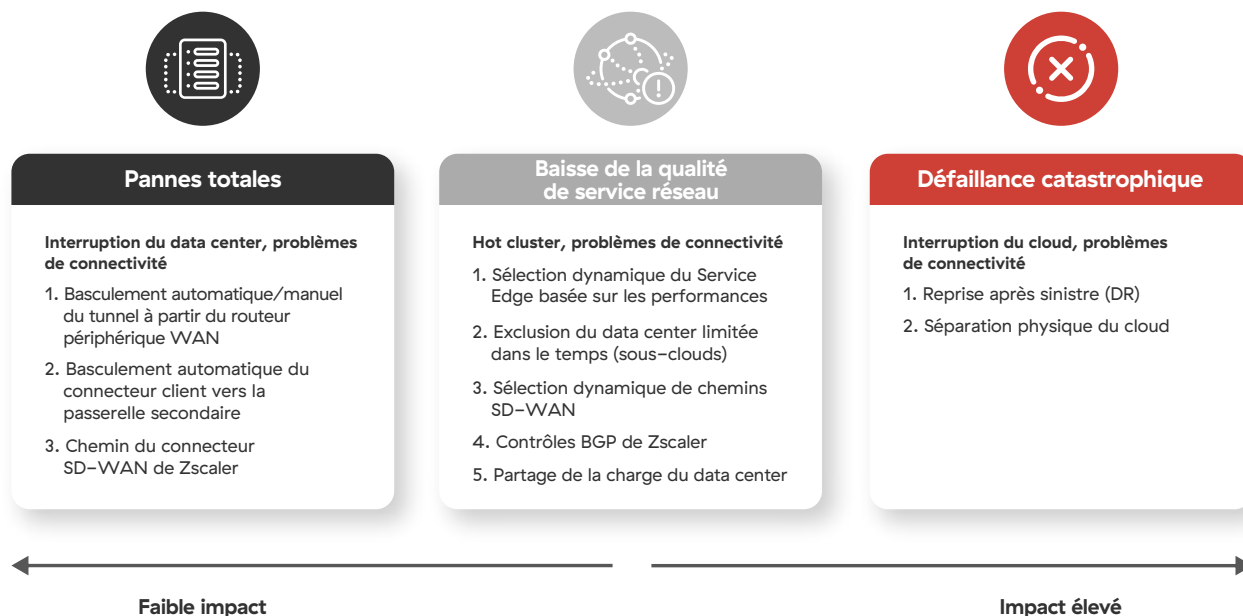


Illustration 1 : Plusieurs options de réponse aux scénarios de défaillance

Défaillances mineures

Les défaillances mineures sont notamment les problèmes de performances, de compatibilité et de fonctionnement ou de qualité qui ne sont pas des défaillances graves ni critiques. Les pannes de nœuds ou les problèmes de disque peuvent constituer les principales raisons des défaillances isolées. Les défaillances mineures surviennent le plus fréquemment et passent souvent inaperçues. Ces défaillances peuvent être responsables de ralentissements, de problèmes opérationnels et de la frustration des utilisateurs. L'architecture cloud résiliente et l'excellence opérationnelle de Zscaler peuvent contribuer à les éviter. Les défaillances mineures sont gérées en arrière-plan avec un minimum d'interaction avec le client, et en parallèle la continuité de la productivité est assurée.

Principaux avantages de Zscaler Resilience



Continuité d'activité avec une sécurité ininterrompue

Appliquez des politiques de sécurité critiques tout en accordant un accès Zero Trust à Internet, aux SaaS et aux applications privées, même en cas de sinistre.



Expériences fluides pour tous les scénarios de défaillance

Gérez sans peine les pannes totales, les baisses de la qualité de service réseau et les défaillances catastrophiques en exploitant l'architecture de pointe et l'excellence opérationnelle de Zscaler Zero Trust Exchange.



Réduction des coûts et de la complexité

Évitez les interruptions d'activité et les pertes de productivité causées par un manque d'accès aux applications critiques tout en éliminant les coûts de l'infrastructure de sauvegarde traditionnelle et les VPN sur site.

Panne totale

Les interruptions de service des data centers (par exemple, l'interruption de service en janvier 2022 du site d'Interxion de Londres) ou les graves problèmes de connectivité, tels que les interruptions de service des opérateurs/fournisseurs de transit, sont considérés comme des scénarios de panne totale au cours desquels les entreprises ne peuvent pas transférer le trafic vers le data center Zscaler affecté. Notre architecture redondante (data centers indépendants des opérateurs avec de multiples fournisseurs et des échanges Internet) est particulièrement efficace pour minimiser les pannes en cas de perte d'un opérateur et d'autres problèmes de connectivité. Quel que soit le temps de rétablissement, les clients sont dans l'impossibilité de bénéficier des services du data center touché.

Pour poursuivre leurs activités, ceux-ci doivent rediriger le trafic vers un data center Zscaler secondaire situé à proximité. Nous utilisons un mélange d'opérateurs et de fournisseurs de data centers pour atténuer efficacement les perturbations provenant de n'importe quel fournisseur donné, en garantissant que le data center secondaire sera disponible. Nous surveillons également et maintenons une capacité de réserve dans le data center afin de gérer une charge transitoire supplémentaire.

S'engager dans la continuité d'activité consiste à concevoir et à planifier les différents scénarios de défaillance possibles. Zscaler dispose d'une infrastructure de classe mondiale, conçue pour assurer une disponibilité totale.

Trafic provenant du bureau à l'aide d'un dispositif SD-WAN

Lors de l'envoi de trafic depuis un bureau à l'aide d'un dispositif de routage/SD-WAN, les clients doivent se conformer aux bonnes pratiques de déploiement de Zscaler en disposant d'un tunnel IPsec/GRE de secours prêt à être utilisé en cas d'indisponibilité du tunnel principal. Le déclenchement du basculement dépend des capacités du dispositif et de la conception du réseau. Par exemple, un SD-WAN avec deux circuits Internet peut basculer automatiquement vers le tunnel de secours sur un circuit secondaire lorsque le tunnel actif devient inaccessible ou dépasse un seuil de latence (avec les contrôles d'intégrité L7 activés). Avec des dispositifs plus rudimentaires, les clients doivent activer manuellement le tunnel de secours. Une fois que le data center principal est à nouveau opérationnel, il incombe au client de rétablir la connexion.

Trafic utilisant Zscaler Client Connector

Lors de l'envoi de trafic via Zscaler Client Connector, Zscaler contrôle les deux extrémités du tunnel et bascule automatiquement de la passerelle principale vers la passerelle secondaire à l'aide de la logique du fichier PAC du profil d'application. Zscaler Client Connector (ZCC) revient à la passerelle principale dès qu'elle est à nouveau accessible. Dans certains cas, les clients peuvent choisir de modifier manuellement les fichiers PAC pour déclencher un basculement.

Baisses de la qualité de service réseau

Ce type de défaillance consiste en une baisse involontaire ou inattendue de la qualité de service réseau. Une mauvaise gestion de la baisse de la qualité de service réseau peut s'avérer coûteuse, tant en termes de perte de revenus que de productivité. Si les utilisateurs signalent une baisse de la qualité de service réseau avant que l'équipe informatique ne la découvre et ne travaille à sa résolution, il peut en résulter une grande frustration des utilisateurs, ce qui aura pour effet de ralentir l'ensemble du système. Outre les méthodes utilisées pour résoudre les pannes totales, Zscaler aide à atténuer les baisses de la qualité de service réseau par d'autres moyens évoqués ci-dessous.

Sélection dynamique du Zscaler Service Edge basée sur les performances

Zscaler Client Connector choisit le chemin optimal entre le ZIA Service Edge principal et secondaire, indépendamment de la proximité géographique, en se basant plutôt sur l'état de chaque ZIA Service Edge, comme le montre l'illustration 2. Une connexion HTTP de bout en bout calcule la latence en envoyant continuellement des requêtes ping aux deux passerelles. Zscaler offre ainsi une sélection de data centers basée sur la latence afin de gérer efficacement les scénarios de baisse de la qualité de service réseau.

Exclusion du data center contrôlée par le client

Une autre façon de maintenir la continuité d'activité pendant les baisses de la qualité de service réseau consiste à sélectionner les data centers contrôlés par le client, comme le montre l'illustration 3. Lorsqu'un client rencontre des problèmes de capacité dans un data center, tels qu'un problème de peering d'application SaaS dans LAX (qui peut prendre des heures à résoudre),

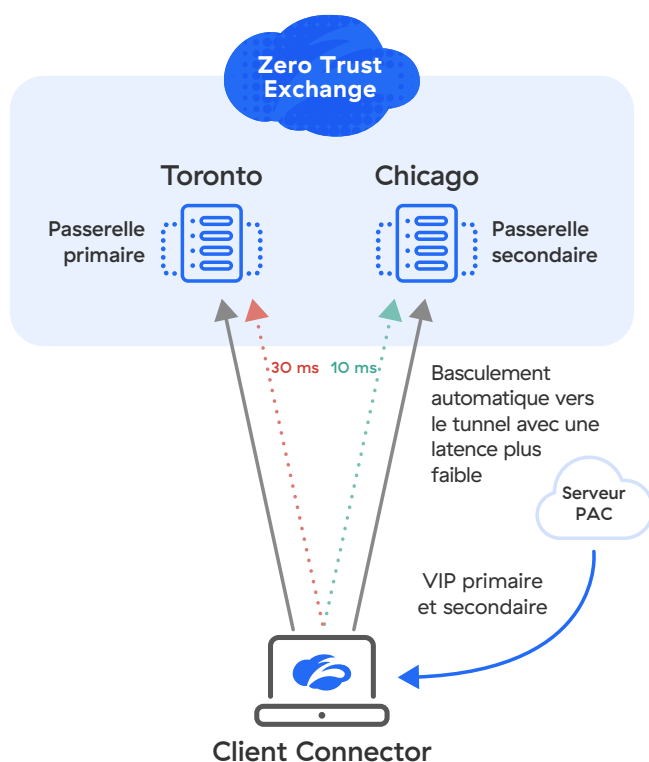


Illustration 2 : Sélection dynamique du Service Edge basée sur les performances

ce data center peut être exclu du sous-cloud dans le portail d'administration. Zscaler Client Connector récupère alors les nouvelles passerelles principale et secondaire, et établit un tunnel Z vers un nouveau data center. Cette exclusion du data center contrôlée par le client est limitée dans le temps et revient à la sélection initiale du data center après un délai prédéfini.

Basculement de tunnel à partir de dispositifs de routage sensibles aux baisses de la qualité de service réseau

Lors de l'envoi de trafic depuis un bureau à l'aide d'un dispositif de routage/SD-WAN sur lequel Zscaler n'a aucun contrôle direct, les options du client sont liées aux capacités du dispositif en périphérie. Par exemple, un routeur SD-WAN peut détecter une dégradation du service à l'aide d'algorithmes propriétaires basés sur des contrôles d'intégrité L7 des terminaux d'analyse Zscaler. Une fois qu'une baisse potentielle de la qualité est détectée, le dispositif SD-WAN peut basculer automatiquement vers un tunnel de secours sur la même liaison ou sur une liaison secondaire. Le dispositif revient au tunnel principal dès que les contrôles d'intégrité fournissent de meilleurs résultats.

Contrôles BGP de Zscaler

Notre architecture redondante, composée de data centers indépendants des opérateurs avec plusieurs fournisseurs et échanges Internet (IX), est hautement efficace pour minimiser les baisses de la qualité de service réseau, la congestion ou d'autres problèmes liés à un seul opérateur. Lorsque Zscaler CloudOps détecte qu'un FAI en amont fournit un routage sous-optimal, nous pouvons rediriger le trafic vers un FAI secondaire pendant que nous travaillons avec le FAI principal à la résolution du problème.

Partage de la charge des data centers de Zscaler

En cas de congestion du réseau ou d'autres problèmes de connectivité à un data center particulier, Zscaler peut rediriger de manière proactive les clients exécutant Zscaler Client Connector vers des data centers secondaires géographiquement proches sans recourir à une méthode statistique.

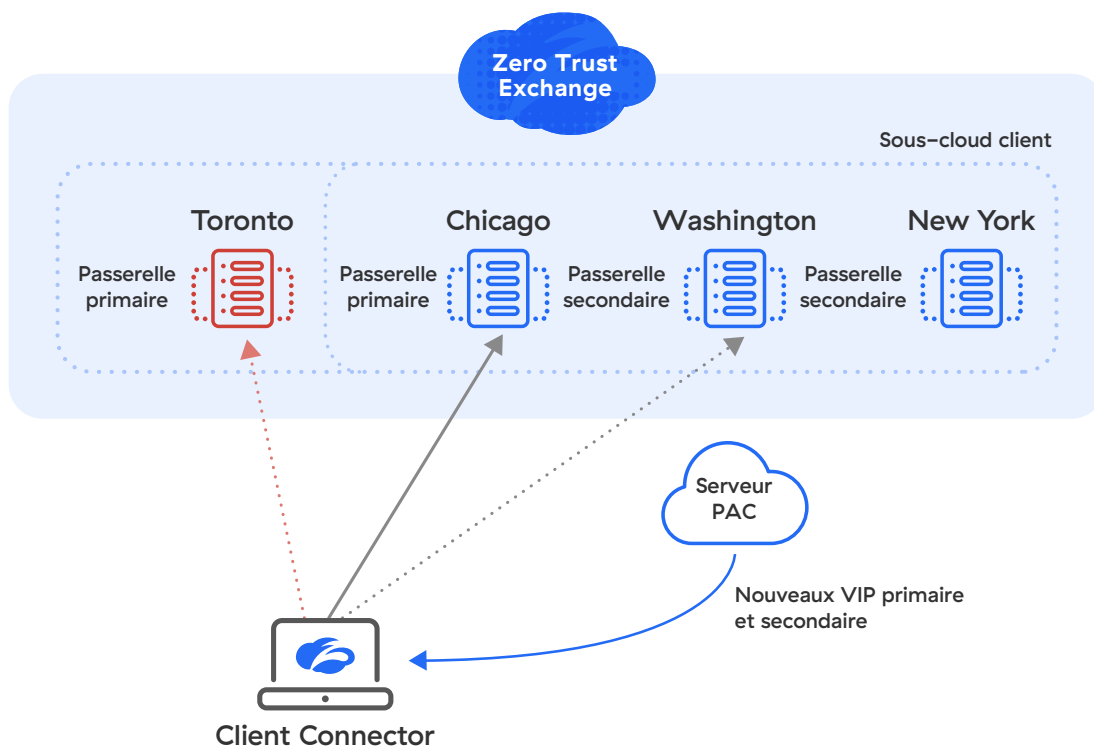


Illustration 3 : Exclusion du data center contrôlée par le client

Défaillances catastrophiques

Continuité d'activité Zscaler pour ZIA/ZPA

La continuité d'activité Zscaler pour le cloud assure aux utilisateurs un fonctionnement sans aucune interruption, garantissant qu'ils peuvent accéder aux applications stratégiques même pendant un événement catastrophique.

Les entreprises ont besoin d'un accès ininterrompu aux applications, sans compromettre la sécurité Zero Trust en cas de sinistre ou de dégradation de l'accès à l'infrastructure. De plus, de nombreux secteurs doivent se conformer à des normes réglementaires et de conformité en matière de continuité d'activité.

Pour répondre à ces besoins, Zscaler propose l'option d'un cloud privé de continuité d'activité qui permet aux entreprises de rester opérationnelles, même en cas d'événement catastrophique pouvant affecter le cloud public de Zscaler.

Si le cloud public de Zscaler est inaccessible ou indisponible, les clients peuvent passer en mode de continuité d'activité. Dans cet état, les politiques et l'authentification des utilisateurs continuent d'être appliquées par les services Zscaler, qui s'exécutent sur une machine virtuelle hébergée par le client.

Continuité d'activité pour ZIA

Afin de fournir un accès ininterrompu à Internet et aux applications SaaS, tout en restant en conformité, Zscaler offre la possibilité de basculer vers un cloud privé de continuité d'activité comprenant des ZIA Private Service Edges hébergés par le client et un cache de politiques privé.

Les Private Service Edges (PSE) assurent un traitement cohérent du trafic et prennent en charge des fonctionnalités telles que l'inspection du trafic et le pare-feu pour les utilisateurs qui exécutent Client Connector de Zscaler. En cas d'interruption, ces Private Service Edges sont pris en charge par un cache de politiques privé qui conserve une copie en cache de la configuration du client.

Pour les clients qui ne souhaitent pas déployer des fonctionnalités auto-hébergées, la solution de continuité d'activité standard de Zscaler permet un accès continu aux applications Web et SaaS en cas d'interruption. Les clients peuvent choisir l'une des trois options dans ce scénario :

Fail Open : accès Internet direct et sans restriction de sécurité

Predefined AllowList : accès illimité à un ensemble limité d'applications courantes

Fail Closed : accès à Internet bloqué pendant la durée de l'interruption

Continuité d'activité pour ZPA

Pour un accès ininterrompu aux applications privées pendant une interruption, les clients peuvent éventuellement choisir de déployer leur propre cloud privé de continuité d'activité, qui consiste en un groupement logique des composants suivants, chacun pouvant être déployé dans un groupe pour une redondance supplémentaire :

Private Cloud Controllers synchronisent en permanence la configuration et les politiques avec le cloud Zscaler.

ZPA Private Service Edges fournissent des fonctionnalités ZPA publiques dans l'environnement d'une entreprise.

App Connectors fournissent un accès sécurisé aux services privés.

Les récepteurs de journaux capturent les sorties de journaux d'autres composants.

En cas d'interruption catastrophique ou d'indisponibilité du cloud Zscaler, les utilisateurs se connectent automatiquement aux Private Cloud Controllers pour l'authentification et la redirection vers les ZPA Private Service Edges (PSE). Une fois connecté au PSE, le canal de contrôle et de données est associé au ZPA PSE.

Les Private Cloud Controllers, déployés sous forme de machine virtuelle, fournissent des fonctions essentielles en cas d'interruption :

- Redirection de l'authentification
- Redirection de l'utilisateur
- Service de diffusion des journaux
- Synchronisation de la configuration client
- Synchronisation des politiques client

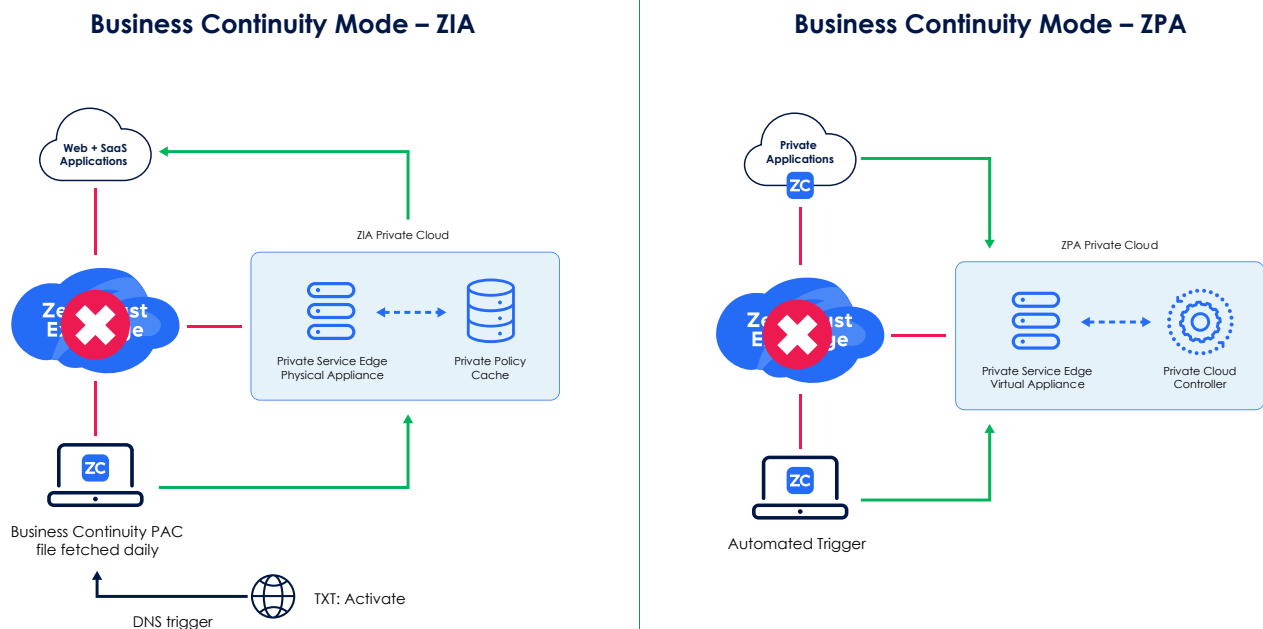


Illustration 4 : Clouds privés de continuité d'activité pour un accès à toutes les applications avec une posture de sécurité complète

Continuité d'activité pour les terminaux

Une autre situation susceptible d'entraîner des conséquences désastreuses pour une entreprise est l'impossibilité d'utiliser ses terminaux habituels (ordinateurs portables, ordinateurs de bureau, etc.) lorsqu'ils sont indisponibles pour quelque raison que ce soit : dysfonctionnement, perte ou compromission. Pour répondre à ce scénario, Zscaler Cloud Browser Isolation peut être déployé afin de fournir un accès sécurisé via un navigateur aux applications privées, Web ou SaaS à partir de terminaux non gérés (tels que BYoD), sans risque de perte de données.

Continuité d'activité de Zscaler, en conclusion

Une fois la fonctionnalité Zscaler Cloud restaurée, le produit peut reprendre son fonctionnement normal et tirer pleinement parti de la sécurité et de la connectivité Zero Trust fournies par Zero Trust Exchange. Zscaler Digital Experience détecte les défaillances mineures, les baisses de la qualité de service réseau et les pannes totales pour aider les clients à y remédier avant qu'elles n'affectent radicalement les utilisateurs. La plateforme Zscaler offre une flexibilité totale pour la continuité d'activité, assortie d'une sécurité inégalée et d'une expérience utilisateur fluide.

Zscaler Business Continuity, composante de la plateforme globale Zscaler, offre aux clients une redondance au sein de la plateforme sans avoir besoin de solutions tierces supplémentaires. Zscaler s'engage à fournir une expérience fluide et continue aux utilisateurs et aux équipes informatiques à la faveur d'investissements continus dans les solutions de résilience de Zscaler.

Principaux avantages des solutions de continuité d'activité de Zscaler

- Interruption minimale des opérations des clients lors d'un événement catastrophique
- Accès aux applications stratégiques même en cas d'événement catastrophique
- Fiabilité accrue de la solution pour l'accès aux applications avec Zscaler
- Économies de coûts grâce à une plateforme unique pour l'accès aux applications, aussi bien en fonctionnement normal qu'en cas d'interruption
- Économies potentielles en évitant les pertes de productivité dues aux interruptions pendant un sinistre

Pour les dernières informations concernant Zscaler Resilience, rendez-vous sur zscaler.com/fr/resilience.



À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur SSE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur zscaler.com/fr ou suivez-nous sur Twitter @zscaler.

©2024 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ et les autres marques commerciales répertoriées sur zscaler.com/fr/legal/trademarks sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.