Zscaler Resilience™

Uninterrupted business continuity during blackouts, brownouts and catastrophic events

Solution Brief

Business continuity is top of mind for IT leaders

The way we work has changed, and with this shift, business continuity has become a top priority for IT leaders. Now, IT leaders must focus on preventing interruptions to mission-critical services and facilitate continued productivity as if it's business as usual. With the right tools, processes, and technology, IT teams can quickly and easily restore full functionality for their organizations, even in a disaster.

The move to cloud-delivered services for storage, computing, and security has brought organizations flexible and scalable systems, better business continuity, lower IT costs, and reduced complexity. Even with these advantages, organizations are looking to optimize business continuity in the face of disastrous events such as natural disasters, physical attacks, or nation-state threats.

Zscaler Resilience is a complete set of resilience capabilities that ensures uninterrupted business continuity for customers during blackouts, brownouts & catastrophic events. It is built on the advanced architecture of the Zscaler Zero Trust Exchange™ and enhanced by operational excellence to offer high availability and serviceability to customers at all times. Zscaler's customer-controlled disaster recovery capabilities, in combination with a robust set of failover options, support customers' business continuity planning efforts in all failure scenarios. This comprehensive set of resilience capabilities makes the Zscaler security cloud industry's most secure and resilient cloud.

Cloud resilience: Why is it necessary?

Business leaders are focused on providing an environment conducive to maximum productivity. IT teams must enable continuity of business and productivity even when connectivity issues, scaling events, or service failures disrupt normal business activity.

User traffic to mission-critical applications—SaaS, internal, and private alike—must always flow to ensure business continuity. Interruptions could stem from a breakdown in the cloud or in the connectivity to the applications. Cloud resilience encompasses both: resilience of the cloud and resilience to the cloud.

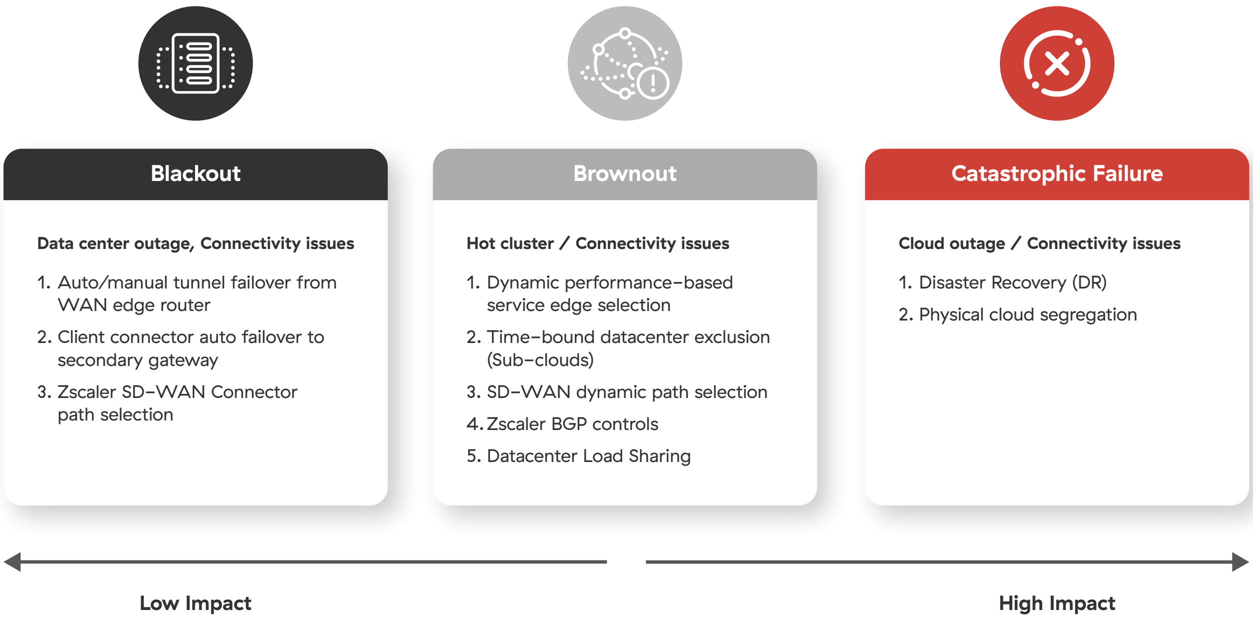
Resilience of the cloud

Resilience of the cloud ensures the cloud itself is built on an effective infrastructure and has strong operational processes for everyday business functions. The Zscaler cloud autonomously handles many minor failures (node crash, disk issues, etc.) without any customer interaction, loss in connectivity, or drop in performance. Our robust purpose-built hardware systems with over-provisioning of processing capacity and redundancy provide the foundation for high resilience.

Resilience to the cloud

Resilience to the cloud is an essential aspect of a comprehensive cloud resilience solution. Connectivity to the cloud depends on its availability and means to connect so users can reach applications or data. When access to the cloud is disrupted, there's a need to find an alternate, optimal path to applications. This optimization represents a collection of manual or autonomous actions that can be applied to address failures ranging from a drop in network performance to complete outages. Zscaler Resilience is a complete set of capabilities that ensures uninterrupted business continuity for any type of failures ranging from minor failures to catastrophic failures.

Ensuring resilience to the cloud across failure scenarios



Blackout

Data center outage, Connectivity issues

1. Auto/manual tunnel failover from WAN edge router
2. Client connector auto failover to secondary gateway
3. Zscaler SD-WAN Connector path selection

Brownout

Hot cluster / Connectivity issues

1. Dynamic performance-based service edge selection
2. Time-bound datacenter exclusion (Sub-clouds)
3. SD-WAN dynamic path selection
4. Zscaler BGP controls
5. Datacenter Load Sharing

Catastrophic Failure

Cloud outage / Connectivity issues

1. Disaster Recovery (DR)
2. Physical cloud segregation

Low Impact

High Impact

Figure 1: Multiple options to respond to failure scenarios

Minor failures

Minor failures include performance glitches, compatibility issues, and operational or quality issues that are not severe or critical failures, node crashes or disk issues could be the primary reasons for isolated failures. Minor failures occur most frequently and often go unnoticed. These failures can lead to slowdown, operational issues and user frustration. The resilient Zscaler cloud architecture and operational excellence can prevent them. Minor failures are managed in the background with minimal customer interaction while ensuring continued productivity.

Key Benefits of Zscaler Resilience

Business continuity with uninterrupted security

Apply critical security policies while granting zero trust access to internet, SaaS, and private apps, even during disasters.

Seamless experiences across all failure scenarios

Handle blackouts, brownouts, and catastrophic failures with ease by leveraging the best-in-class architecture and operational excellence of the Zscaler Zero Trust Exchange.

Reduced costs and complexity

Avoid business interruptions and productivity losses caused by a lack of access to critical apps while eliminating the costs of legacy backup infrastructure and on-premises VPNs.

Blackouts

Data center outages (e.g., the January 2022 outage at the Interxion London facility) or severe connectivity issues, such as carrier/ transit provider outages, are considered blackout scenarios in which organizations cannot forward traffic to the impacted Zscaler data center. Our redundant architecture—carrier-neutral data centers with multiple providers and internet exchange (IX)—is highly effective in minimizing outages in the event of single carrier loss and other connectivity issues. Regardless of the restoration time, the impact on our customers is the inability to further consume the services for the impacted data center.

To continue business, customers must redirect traffic to a secondary nearby Zscaler data center. We use a mix of carriers and data center providers to effectively mitigate disruptions from any given supplier, ensuring that the secondary data center will be available. We also over-provision and maintain spare capacity in the data center to support additional transient load.

> Embracing business continuity is about thinking through and planning for different possible failure scenarios. Zscaler's infrastructure is world-class that is designed to deliver 100% availability.

Traffic from the office using SD-WAN device
When sending traffic from an office using a routing/SD-WAN device, customers must follow Zscaler deployment best practices by having a backup IPsec/GRE tunnel ready to go when the primary one is unreachable. How failover is triggered depends on the device's capabilities and network design. For example, an SD-WAN with dual internet circuits could fail over to the backup tunnel on a secondary circuit automatically when the active tunnel becomes unreachable or exceeds a latency threshold (with L7 health checks enabled). With more primitive devices, customers would need to manually enable the backup tunnel. Once the primary data center is back up, it is the customer's responsibility to switch back.

Traffic using Zscaler Client Connector
When sending traffic using Zscaler Client Connector, Zscaler controls both edges of the tunnel and will automatically fail over from the primary to the secondary gateway using the App Profile PAC file logic. Zscaler Client Connector (ZCC) will revert to the primary gateway once it becomes reachable. In certain cases, customers can choose to manually modify the PAC files to trigger a failover.

Brownouts

An unintentional or unexpected drop in network service quality typically constitutes a brownout. Mismanaging a brownout can be costly, both in terms of lost revenue and productivity—if users are flagging a brownout before the IT team has discovered and begun working to resolve it, a great deal of user frustration can result, slowing everything down. In addition to the ways to address blackouts, Zscaler helps mitigate brownouts in other ways mentioned below.

Zscaler Dynamic Performance-Based Service Edge Selection

Zscaler Client Connector chooses the optimal path between the primary and secondary ZIA Service Edge irrespective of the geographical proximity, instead relying on the health of each ZIA Service Edge, as shown in figure 2. An end-to-end HTTP connection calculates the latency, by continuously pinging both gateways for latency. With this, Zscaler provides latency-based data center selection to tackle brownout scenarios effectively.

Customer-controlled data center exclusion

Another way to maintain business continuity during brownouts is through customer-controlled data center selection, as shown in figure 3. When a customer experiences capacity issues in a data center, such as a SaaS application peering issue in LAX (which could take hours to fix), that data center can be excluded from the subcloud in the admin portal. Zscaler Client Connector then fetches the new primary and secondary gateway and establishes a Z-tunnel to a new data center. This customer-controlled data center exclusion is time bound and returns to the original selection of data center after a pre-determined time.

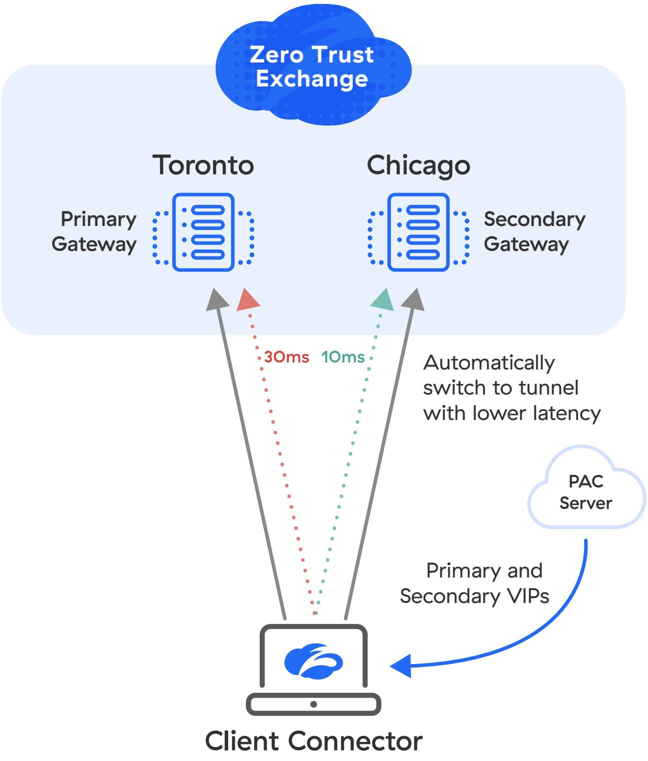


Figure 2: Dynamic performance-based Service Edge selection

Tunnel failover from brownout-aware routing devices

When sending traffic from an office using a routing/SD-WAN device over which Zscaler has no direct control, a customer's options are bound to the edge device's capabilities. For example, an SD-WAN router can detect service degradation using proprietary algorithms based on L7 health checks to Zscaler probe endpoints. Once a potential brownout is detected, the SD-WAN device can automatically failover to a backup tunnel on the same link or on a secondary link. The device will revert to the primary tunnel once the health checks provide better results.

Zscaler BGP controls

Our redundant architecture—carrier-neutral data centers with multiple providers and internet exchange (IX)—is highly effective in minimizing brownouts, congestion, or other issues with single carriers. When Zscaler CloudOps discovers that an upstream ISP gives suboptimal routing, we can reroute traffic through a secondary ISP while we work with the primary one to resolve the issue.

Zscaler data center load sharing

In the event of network congestion or other connectivity issues to a particular data center, Zscaler can proactively redirect clients running Zscaler Client Connector to secondary data centers in geo-proximity without using a statistical method.

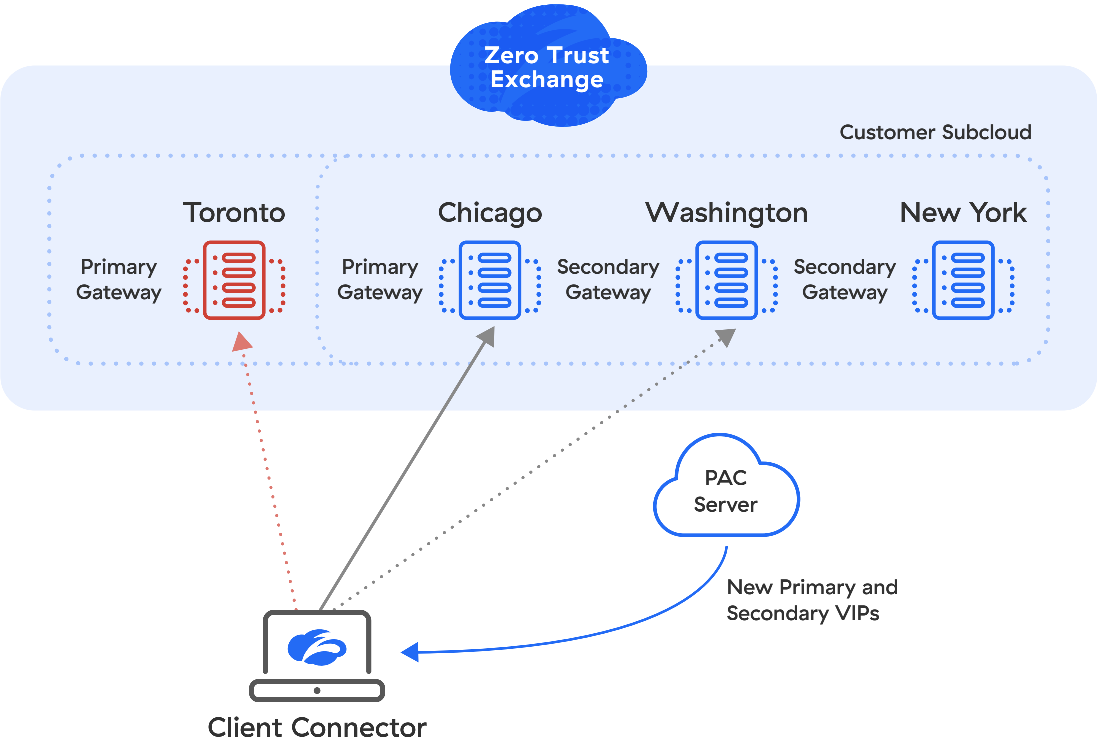


Figure 3: Customer-controlled data center exclusion

Catastrophic failures

Zscaler Business Continuity for ZIA/ZPA

Zscaler Business Continuity for the cloud provides uninterrupted operations for users, ensuring they can access mission-critical applications even during a black swan event.

Organizations need uninterrupted access to applications, without compromising zero trust security during disasters, or periods of degraded infrastructure access. In addition, compliance and regulatory standards for Business Continuity must commonly be met in many industries.

To meet these needs, Zscaler provides the option of a private business continuity cloud to keep organizations operational, even during a catastrophic event that may affect the Zscaler public cloud.

If the Zscaler public cloud is unreachable, or unavailable, customers can switch over to Business Continuity Mode. In this state, policies and user authentication continue to be enforced by Zscaler services, running on a customer-hosted virtual machine.

Business Continuity for ZIA

In order to provide uninterrupted access to the internet and SaaS applications, and remain compliant, Zscaler offers the ability to failover to a private business continuity cloud comprising customer-hosted ZIA private service edges, and a private policy cache.

The PSEs provide consistent traffic processing, supporting features such as traffic inspection, and firewall, for users running Zscaler's Client Connector. In an outage, these private service edges are supported by a private policy cache that holds a cached copy of the customer's configuration.

For customers who do not wish to deploy self–hosted capabilities, Zscaler's standard business continuity solution enables ongoing access to the web and SaaS applications in the event of an outage. Customers can choose one of three options in this scenario:

Fail Open: Unfettered internet access with no security restrictions

Predefined AllowList: Unrestricted access to a limited set of common applications

Fail Closed: All access to the internet is blocked for the duration of the outage

Business Continuity for ZPA

For uninterrupted access to private applications during an outage, customers can optionally choose to deploy their own private business continuity cloud, which are logical groupings of the following components, each of which can be deployed in a group for additional redundancy:

Private Cloud Controllers that continuously synchronize configuration and policies with the Zscaler cloud,

ZPA Private Service Edges that provide Public ZPA functionality in an organization's environment

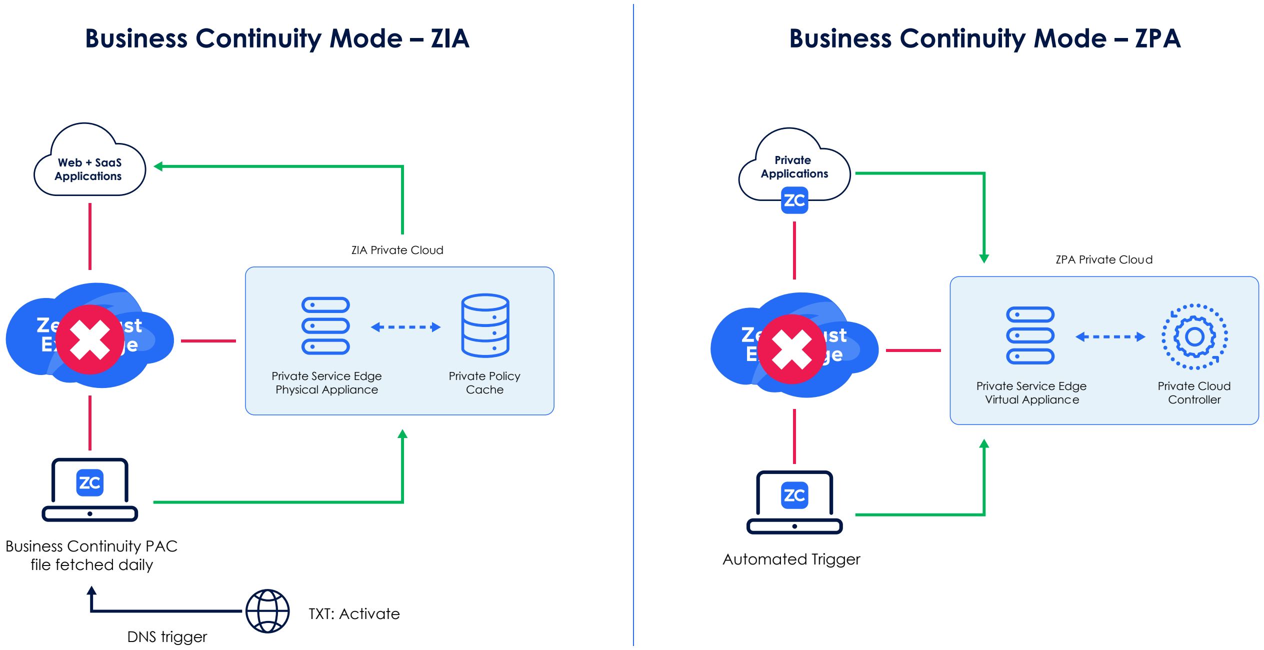
App Connectors for secure access to private services

Log receivers for capturing log outputs from other components

In the event of a catastrophic outage, or the Zscaler cloud becoming unreachable, users will automatically connect to the Private Cloud Controllers for authentication and redirection to ZPA private service edges. Once connected to the PSE, the control and data channel will be with the ZPA PSE.

The Private Cloud Controllers, deployed as a virtual machine, provide critical functions in an outage:

- Authentication redirection
- User redirection
- Log streaming service
- Customer configuration sync
- Customer policy sync



Business Continuity Mode – ZIA

Business Continuity Mode – ZPA

Figure 4: Private Business Continuity Clouds for Access to All Apps with Full Security Posture

Business Continuity for Endpoints

Another issue that can be catastrophic for an organization is an inability to use their regular endpoints (laptops, computers etc.) where those are unavailable for any reason: malfunctioned, missing, or compromised. To address this scenario, Zscaler Cloud Browser Isolation can be deployed to provide secure browser-based access to private, web or SaaS applications from unmanaged endpoints (such as BYoD), without risk of data loss.

Zscaler Business Continuity, In Conclusion

Upon restoration of Zscaler Cloud functionality, the product can return to normal operation to take full advantage of the zero trust security and connectivity provided by the Zero Trust Exchange. Zscaler Digital Experience detects minor failures, brownouts and blackouts to help customers address them before it drastically affects users. The Zscaler platform provides full flexibility for business continuity with unrivaled security and a seamless user experience.

Zscaler Business Continuity, as part of the overall Zscaler platform, provides customers with redundancy within the platform without the need for additional third party solutions. Zscaler is committed to providing a seamless, continuous experience for users and IT teams with continued investments into Zscaler resilience solutions.

Key benefits of Zscaler's business continuity solutions

- Minimal interruption to operations for customers during a catastrophic event
- Access to mission-critical applications even during a black swan event
- Increased solution reliability for application access with Zscaler
- Cost savings from having one platform to manage for application access both during normal operation and outage
- Potential savings by avoiding productivity loss due to gaps during a disaster

For the latest on Zscaler Resilience visit zscaler.com/resilience.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.