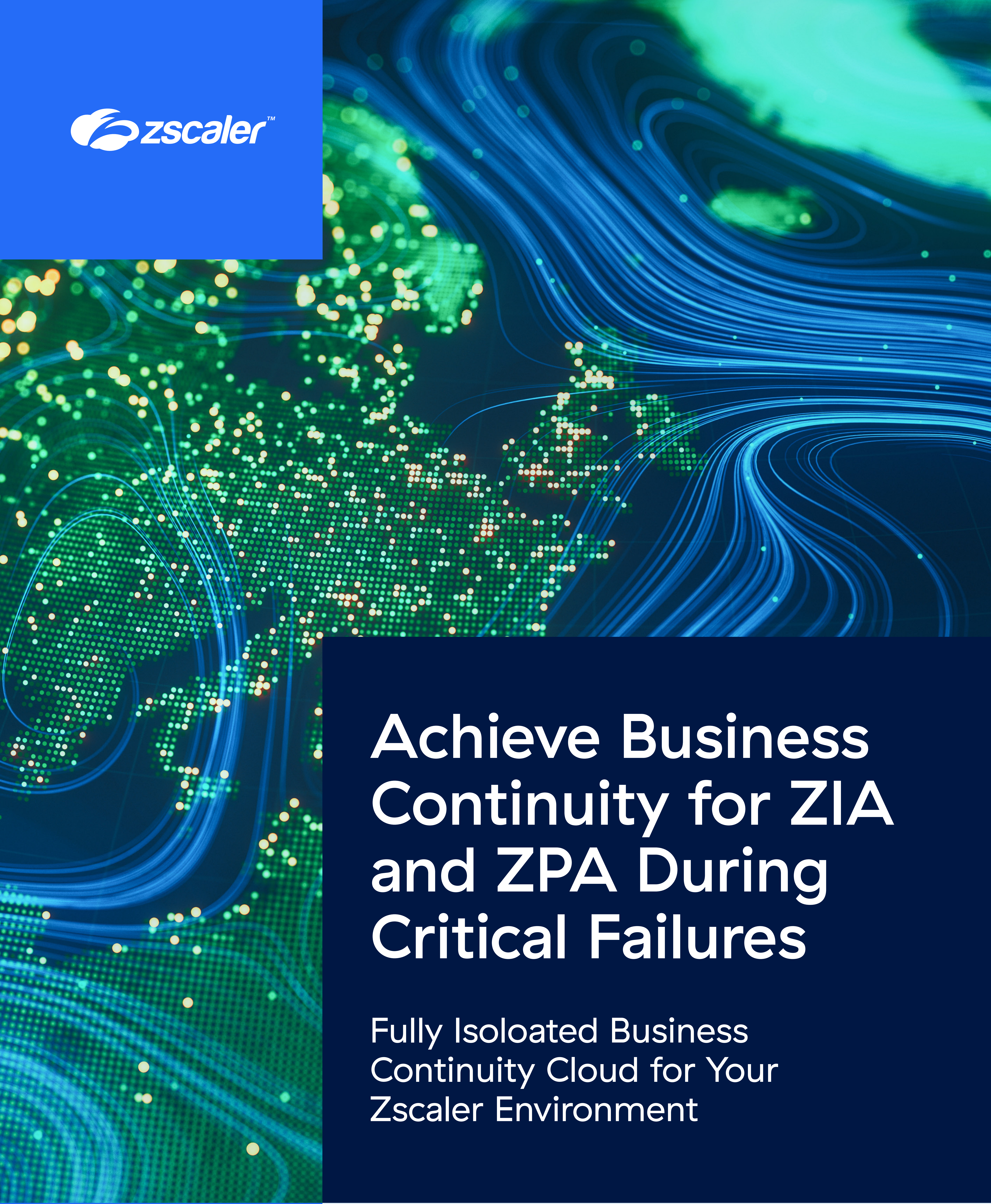


Achieve Business Continuity for ZIA and ZPA During Critical Failures

Fully Isoloated Business Continuity Cloud for Your Zscaler Environment

SOLUTION BRIEF

Introduction

SaaS or cloud native platforms are engineered for high availability; however, critical failures leading to large-scale outages, such as those caused by carrier failures or cyberattacks targeting global cloud infrastructure or major internet links, can severely impact revenue, customers, and employees instantaneously.

This necessitates rigorous business continuity and disaster recovery planning, arguably even more critical for SaaS than for on-premises applications. Regulations such as EU DORA, Australia CPS 230, and ISO 22301 underscore this requirement by mandating proof of service operability throughout widespread disruptions. To satisfy both business and compliance imperatives, organizations require failsafe controls that guarantee uninterrupted access, uncompromising security, and continuous compliance during any interruption.

Common Failure Scenarios Covered with the Zscaler Zero Trust Exchange Platform

In day-to-day operations, disruptions typically fall into three categories:

Component Failure

Small failure: Lowest impact on user experience and the business

Blackout

Complete data center/ network outage that halts ops and revenue

Brownout

Service degradation with intermittent connectivity or slow performance

Component Failure:

A single point of failure, such as a server, switch, disk array, or load balancer, can cause disruptions. For instance, major hyperscalers have encountered power supply failures that lead to the automatic shutdown of a small group of servers, thereby interrupting workloads in the affected area.

Blackout:

Unexpected power loss, whether due to weather, local or regional infrastructure failure, or sabotage, can have widespread effects across the internet. Major cloud infrastructure providers like Google Cloud, GitHub, and OpenAI have all experienced sudden outages, instantly disrupting service for millions of users.

Brownout:

Cloud hyperscalers like AWS, Azure, and Google Cloud have all encountered throttling incidents, resulting in partial disruptions. These disruptions manifest as degraded performance or intermittent connectivity, making them difficult to pinpoint and resolve. The fallout from these incidents has included increased latency, mandatory re-logins, and API timeouts across multiple zones for prolonged durations.

Resilient by Design: Built to Withstand Component Failures, Blackouts, and Brownouts

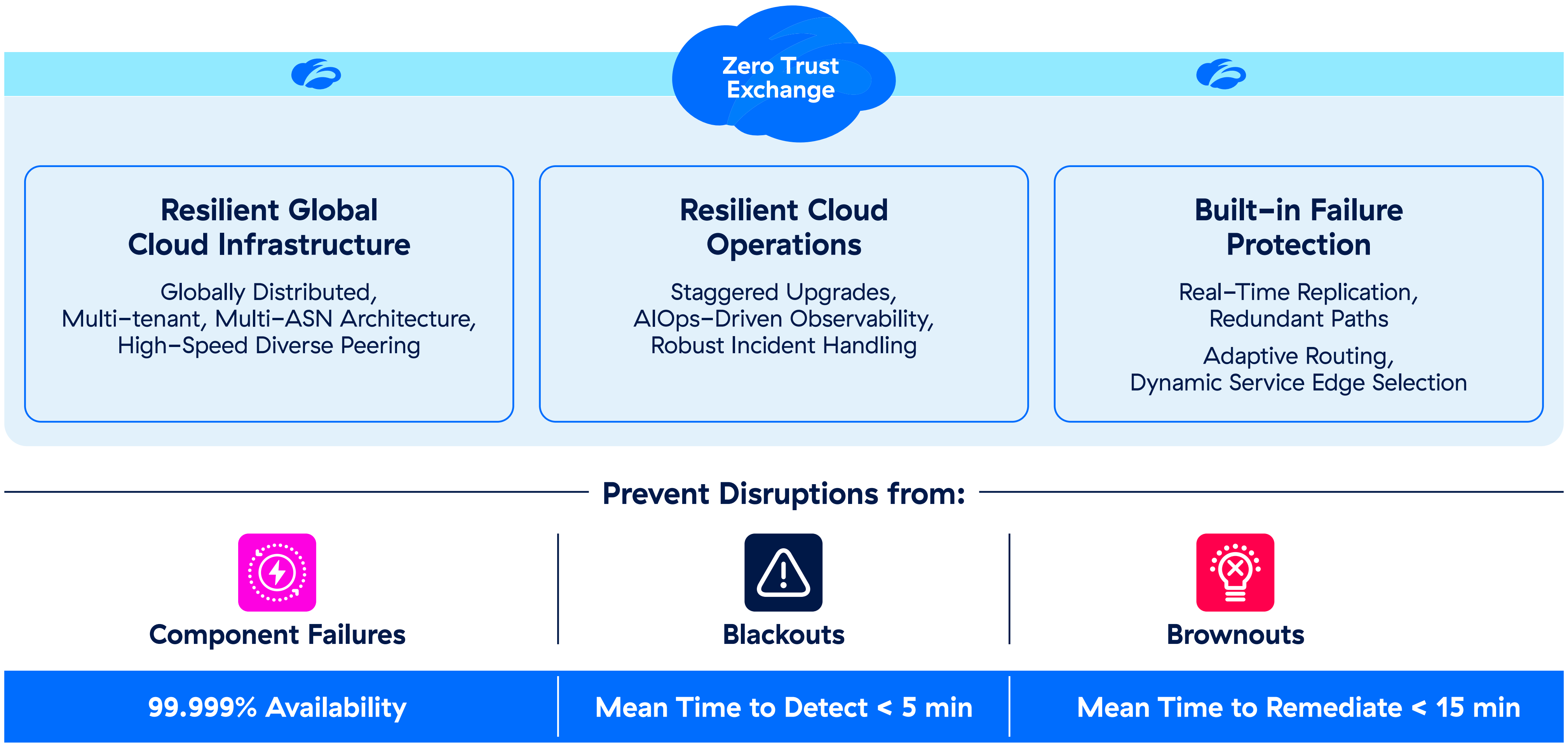
The Zscaler Zero Trust Exchange platform delivers uninterrupted security and connectivity—even when individual devices fail, networks slow, or entire regions go dark. Its globally distributed footprint, automated cloud operations, and built-in failure protections work together to maintain secure, low-latency access under any of these failure scenarios.

This approach to resiliency rests on three core pillars:

1. **Resilient Global Cloud Infrastructure:** Zscaler's cloud spans multiple autonomous system numbers (ASNs), automatically rerouting traffic around any regional or carrier outage. A true multitenant architecture shares capacity across its global footprint for instant scale, while extensive high-speed peering keeps users on the fastest, most available path and consistent security anywhere in the world.

2. **Resilient Cloud Operations:** Staggered upgrades with zero downtime, AIOps-driven observability and robust incident handling enable nonstop feature delivery and security enhancements essential for 24x7 operations.

3. **Built-In Failure Protection:** Real-time policy and session replication absorbs any node failure. Redundant paths with adaptive routing shift traffic in milliseconds, while dynamic service edge selection keeps every connection on the healthiest node to maintain availability and performance.



Zero Trust Exchange

Resilient Global Cloud Infrastructure

Globally Distributed,
Multi-tenant, Multi-ASN Architecture,
High-Speed Diverse Peering

Resilient Cloud Operations

Staggered Upgrades,
AIOps-Driven Observability,
Robust Incident Handling

Built-in Failure Protection

Real-Time Replication,
Redundant Paths

Adaptive Routing,
Dynamic Service Edge Selection

Prevent Disruptions from:

Component Failures	Blackouts	Brownouts
99.999% Availability	Mean Time to Detect < 5 min	Mean Time to Remediate < 15 min

The Zero Trust Exchange delivers exceptional resilience, guaranteeing 99.999% uptime through its SLA. This commitment ensures uninterrupted security and connectivity, even when faced with individual device failures, network slowdowns, or regional outages. This is achieved through a combination of its distributed global infrastructure, automated cloud operations, and integrated failure protections, which collectively provide secure, low-latency access in common failure scenarios.

Preparing for Events Beyond Zscaler's Regular Controls

Even the most robust platforms have limitations. Critical failures such as widespread cyberattacks, subsea cable damage, and global DNS failures are beyond any provider's control. A recent DNS error, for instance, caused a significant outage for a leading hyperscaler, impacting thousands of businesses. Therefore, planning for such extraordinary events is crucial for maintaining business continuity, security, and regulatory compliance.

Critical Failure:

While less frequent, nation-state cyberattacks, global infrastructure failures, and supply chain disruptions can have devastating consequences. For example, a recent faulty security update from a leading security vendor crippled millions of endpoints and nearly halted thousands of businesses. This incident not only led to lost revenue but also compromised security defenses, making companies vulnerable to a surge of cyberattacks, including spoofed websites, impersonation scams, and malicious ZIP files. Such events demand operational and security resilience that goes beyond simple redundancy, requiring strict isolation, rapid failover, and segmentation to ensure continuous operations and security during widespread crises.

Introducing Zscaler Business Continuity Cloud

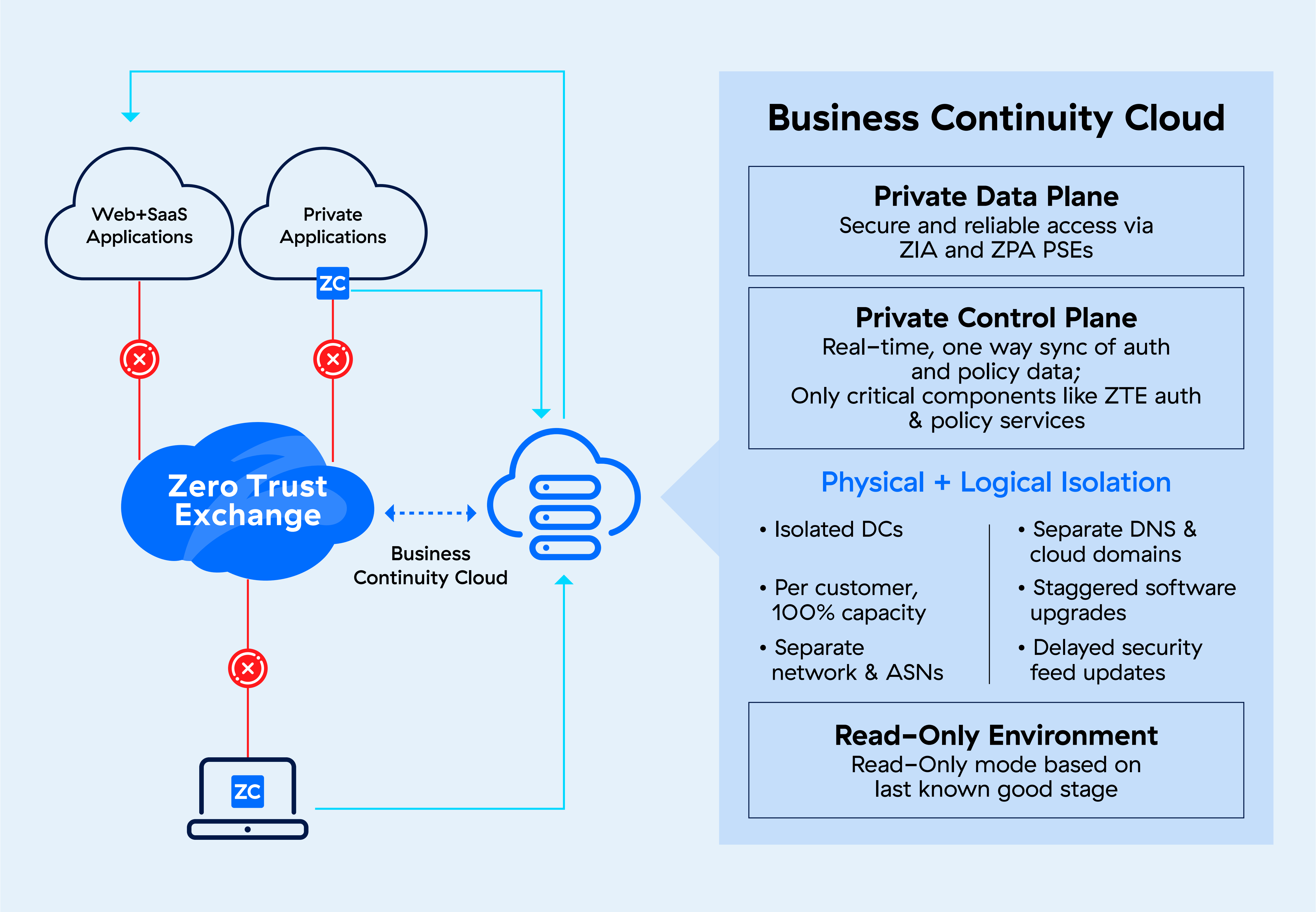
While Zscaler's cloud services are built with high resilience and disaster recovery capabilities, the Business Continuity Cloud (BCC) provides an added layer with customer specific backup instances that are isolated from the Zscaler's primary cloud, for maintaining operations during critical, large-scale disruptions. These events, such as global network outages, infrastructure failures, cyberattacks, sabotage, or DNS failures, often require specific backup instances beyond the scope of standard service-level agreements (SLAs). Delivering services beyond typical SLAs necessitates extra resources and specialized offerings not included in standard service packages.

Operating on infrastructure that is both physically and logically distinct from the Zero Trust Exchange platform, the BCC solution guarantees a fully redundant environment. Once a BCC instance is turned on, policies are synced in real time with the primary cloud instance and is maintained in read-only mode in the BCC instance. During an outage of the primary instance, an automated or a manual failover is triggered and the BCC instance takes over as the gatekeeper. The critical isolation of the BCC instance from the primary instance eliminates the shared-fate risk associated with a potential unavailability of the primary Zscaler service and enables customers meet demanding Recovery Time Objective (RTO) requirements. This approach is analogous to how enterprises deploy backup solutions in case the primary system fails, yet it delivers significantly more tangible benefits like consistent user experience and security posture, which are detailed later in this brief.

Leveraging Zscaler–managed private cloud infrastructure with dedicated, per–customer data and control planes, Business Continuity Cloud removes the need for administrators to maintain their own disaster recovery infrastructure. This eliminates the complexities of separate dashboards, additional end–user agents, different authentication services, and a completely different policy infrastructure, offering minimal zero trust and delivering an inconsistent end user experience.

Private Data Plane: Leverages Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) Private Service Edges for secure and reliable operations, even during critical failures.

Private Control Plane: Provides crucial features like authentication and configuration synchronization by incorporating essential components of the Zero Trust Exchange control plane into a dedicated private instance. This backup control plane is not a full replica of the primary control plane but offers running critical services like authentication and policy services etc.



Business Continuity Cloud

Private Data Plane
Secure and reliable access via ZIA and ZPA PSEs

Private Control Plane
Real–time, one way sync of auth and policy data;
Only critical components like ZTE auth & policy services

Physical + Logical Isolation

- Isolated DCs
- Per customer, 100% capacity
- Separate network & ASNs
- Separate DNS & cloud domains
- Staggered software upgrades
- Delayed security feed updates

Read–Only Environment
Read–Only mode based on last known good stage

Key Benefits:

High redundancy minimizes risk of downtime: Business Continuity Cloud ensures uninterrupted operations for customers by providing an infrastructure with a private control plane and a private data plane that are in a read-only mode, completely isolated from the Zscaler primary cloud. This critical separation prevents major failures from affecting the datacenters providing Business Continuity Cloud service, allowing customer employees to maintain productivity and ensure critical processes run smoothly, thereby minimizing downtime and any potential loss of revenue.

Deliver consistent user experience: With Zscaler Business Continuity Cloud, users avoid the re-login, downtime, and session interruptions common in multi-vendor environments. This seamless continuity minimizes the impact of critical failures on user productivity and experience.

Maintain security with zero trust: The Zscaler Business Continuity Cloud offers a streamlined approach compared to multi-vendor solutions. It maintains your existing security policies and application connectivity, ensuring continuous protection during outages and disruptions. This is achieved without the need for separate security policies, multiple logins, or additional endpoint agents, unlike the complexities often associated with a multi-vendor strategy.

Cost Savings and Simplicity: Eliminate complex, multi-vendor backup systems to reduce costs and streamline operations. This will improve end user experience, ensure consistent security policies, and remove the need for manual failovers.

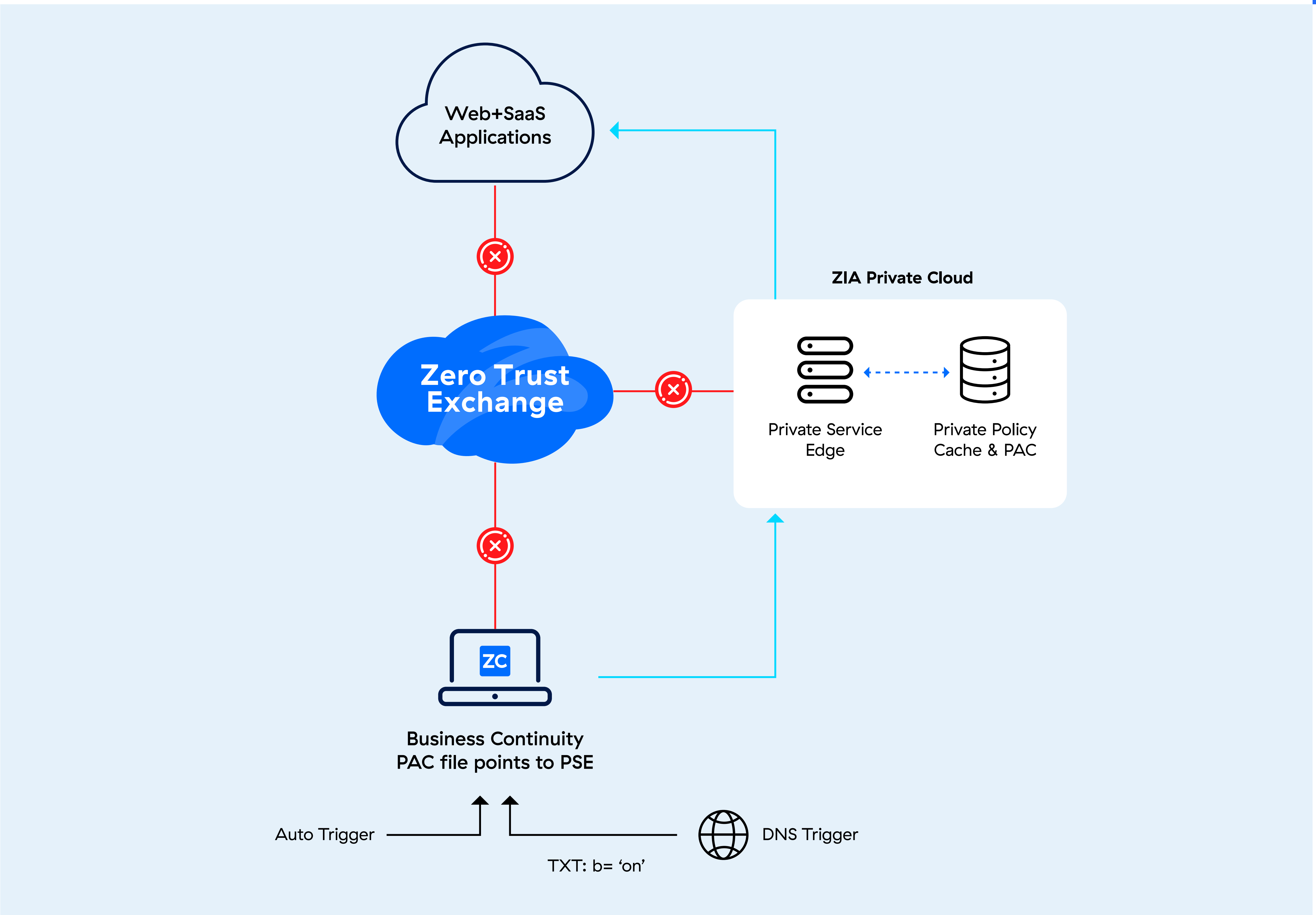
Compliance Assurance: Ensure continued adherence to regulatory requirements and SLA obligations like DORA, Australia CPS 230, and ISO 22301 even in the event of critical failures.

Business Continuity Cloud in Action

The Business Continuity Cloud guarantees the continuous availability of ZIA and ZPA services, even during critical failures when the Zero Trust Exchange is inaccessible or experiencing availability issues and customers cannot access their primary ZIA and ZPA instances. BCC constantly synchronizes policy and identity data with the Zero Trust Exchange, allowing it to seamlessly assume control of both the control plane and data plane within seconds of ZTE going down. This transition can be initiated automatically or manually by an administrator.

Business Continuity Cloud for ZIA

The Business Continuity Cloud comprises the following components responsible for enabling secure access to internet and SaaS applications, with ZIA.



- **ZIA Private Service Edge:** ZIA Private Service Edges (PSEs) are Zscaler-managed enforcement points. They replicate the Zero Trust Exchange to manage a customer specific traffic, providing comprehensive ZIA data and cyber protection services, similar to the Zero Trust Exchange.

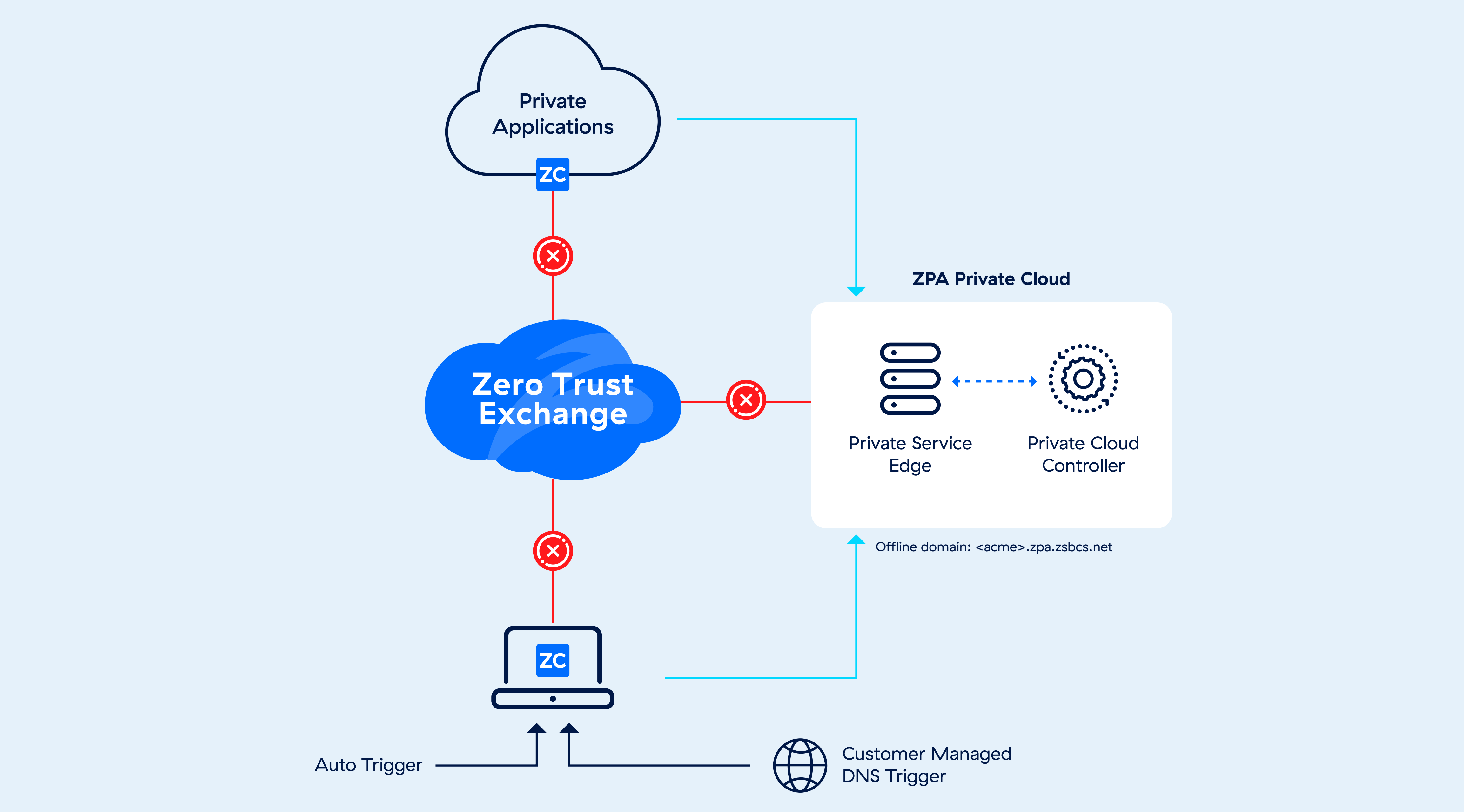
- **Private Policy Cache:** When operated with ZIA PSE, this cache provides:

  - **Local Configuration Proxy:** Delivers all security and access policies, even when the Zero Trust Exchange is unreachable.
  - **Continuous Sync:** Prefetches and updates the tenant's latest configurations from the Zero Trust Exchange during normal operations, ensuring the most recent updates are cached for any failover event.
  - **Read-Only:** This is a read-only instance, meaning no policy changes can be made locally.

- **Private PAC Server:** The Business Continuity Cloud offers global load balancing, which is both geographically and health-aware, across all its locations. It also hosts disaster recovery (DR) specific PAC files.

Business Continuity Cloud for ZPA

The Business Continuity Cloud comprises the following components responsible for enabling secure access to private applications, with ZPA.



- **ZPA Private Service Edge:** ZPA Private Service Edges (PSEs) maintain local control over traffic, authentication, and policy management. They achieve this by securely tunneling outbound-only TLS connections to private applications.

- **ZPA Private Cloud Controller:** The Business Continuity Cloud ensures secure application access even when the Zero Trust Exchange is unavailable. It achieves this by leveraging tenant-dedicated ZPA control plane components that work with Private Service Edges (PSEs) and App Connectors, performing the following key functions:

  - **Real-Time Sync:** Continuously synchronizes policies and configurations with the Zero Trust Exchange as updates are made on the ZPA Portal during normal times when the primary instance is up and running.
  - **Authentication:** Acts as the authentication endpoint, redirecting users to the existing Identity Provider (IdP) and validating SAML assertions.
  - **Global/Local Load Balancing:** Routes users to the closest, healthiest ZPA PSE.
  - **Log Streaming to SIEM:** Streams logs directly to a security information and event management (SIEM) system during outage detection, providing insights into user activity, App Connector status, and PSE performance.
  - **Read-Only:** This is a read-only instance, meaning no policy changes can be made locally.

User Experience with Business Continuity Cloud

When Business Continuity Cloud is active, the end user experience remains unaffected. This is due to three key factors:

1. **Seamless Session Transfer:** Users are automatically and seamlessly switched to a Business Continuity Cloud instance during critical failures. There is no need for re-login, even if a user is actively logged into ZIA and ZPA.

2. **Consistent Application Performance:** Users will not experience any performance degradation when accessing their applications through Business Continuity Cloud.

3. **No Agent Re-launch or Installation Required:** Since Business Continuity Cloud is a replica of the primary solution, user sessions are maintained, users do not need to re-launch existing agent applications or install new ones on their devices.

Operational Simplicity with Business Continuity Cloud

Business Continuity Cloud offers two methods for failover and failback: automated and manual.

1. **Automated Failover/Failback:** Zscaler Client Connectors and ZPA App Connectors continuously monitor their connection to the Zscaler Cloud. In the event of a connectivity loss, control and data connections for these connectors are automatically rerouted to the Business Continuity Cloud. Once connectivity is restored within seconds, traffic seamlessly returns to its standard path.

2. **Manual Failover/Failback:** Administrators can manually direct Client and App Connectors to the Business Continuity Cloud by updating a customer-managed DNS TXT record. Restoring the original DNS entry will then direct traffic back to the primary Zscaler instance once it is up and running.

Business Continuity Cloud Fault Isolation

Fault isolation is a cornerstone of Zscaler's Business Continuity Cloud, ensuring secure and uninterrupted application access during major outages or disruptions. Zscaler employs industry best practices, integrating both logical and physical fault isolation mechanisms to mitigate shared fate risk within the Zero Trust Exchange. Key strategies include:

1. **Isolated Infrastructure:** Separate private, per-tenant data and control planes are equipped with multiple safeguards to prevent the impact of failures or corruption.

2. **Physical and Network Plane Isolation:** Dedicated Disaster Recovery (DR) data centers operate on segregated racks, power, networks, and their own Autonomous System Number (ASN), completely isolated from the Zscaler Cloud for rapid cut-over.

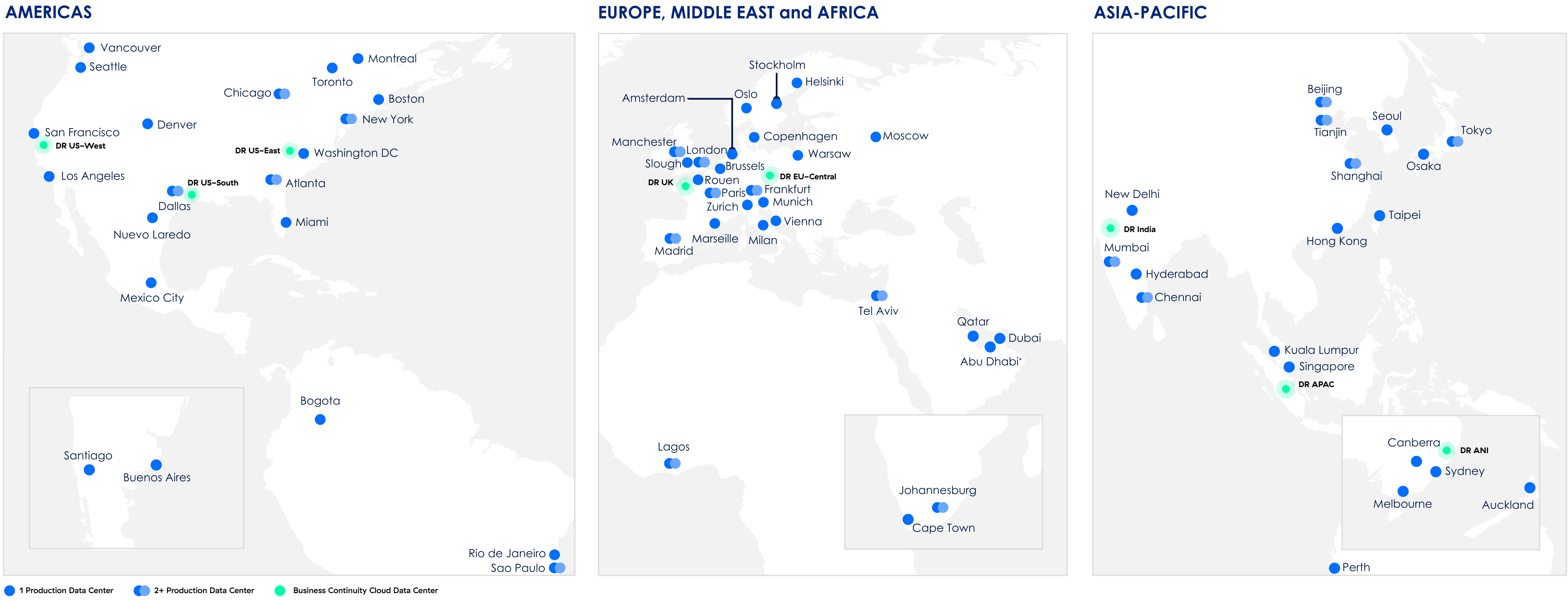
3. **Delayed Software Updates and Security Feeds:** Releases for the Business Continuity Cloud lag the Zscaler Cloud by one week, limiting exposure to new defects or supply chain threats.

4. **Priority Restoration:** Private infrastructure allows for faster updates and configuration changes, potentially accelerating service recovery.

5. **Isolated DNS Services:** A dedicated offline domain on separate DNS servers provides a customer-private entry point to the Business Continuity Cloud.

Business Continuity Cloud Regions

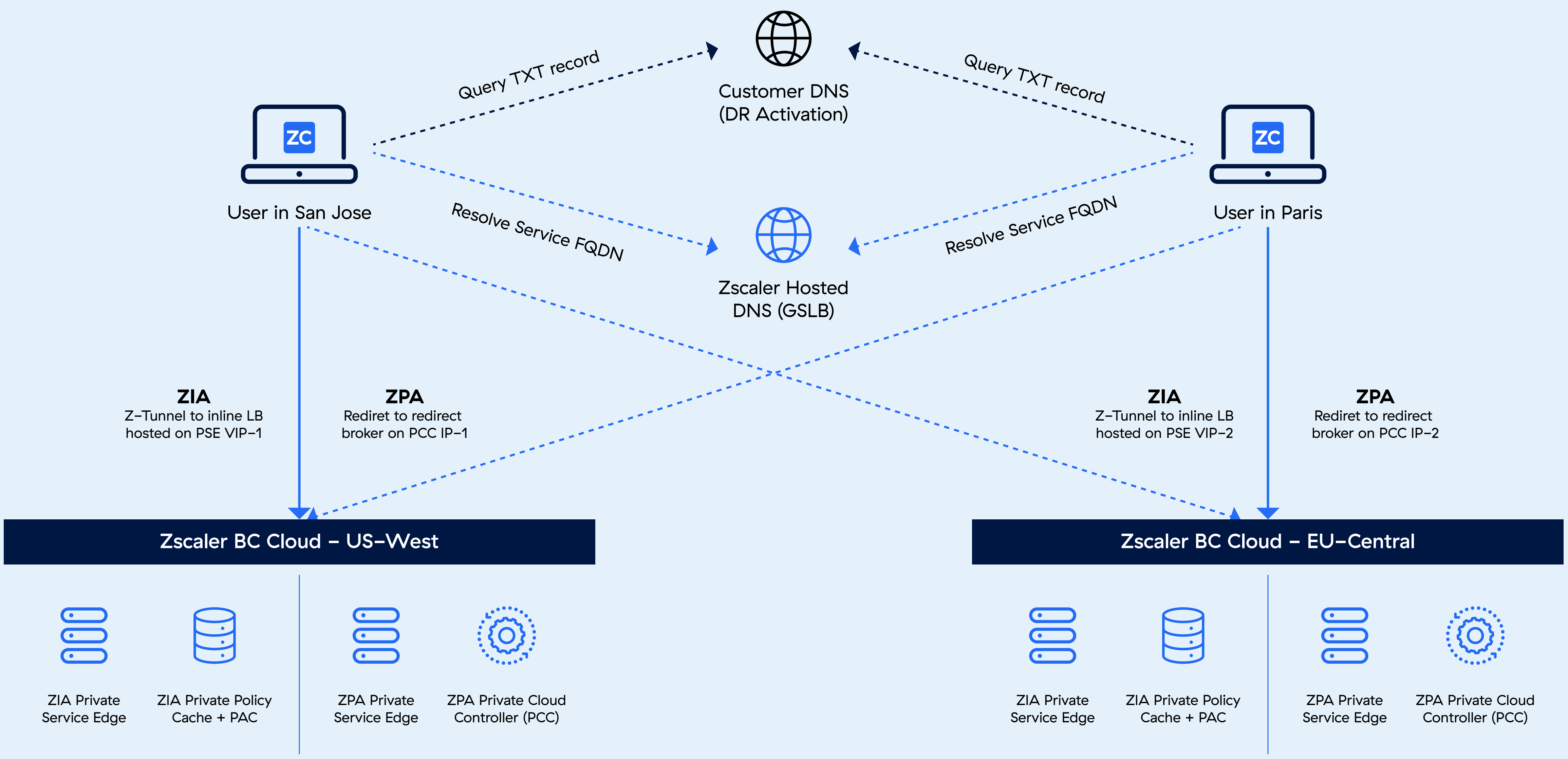
The Zscaler Business Continuity Cloud offers resilient and highly available access during major disruptions. It is strategically distributed across key global regions, as depicted in the graphic below, to ensure comprehensive coverage and continuous operation.



Business Continuity Cloud: Example Topology

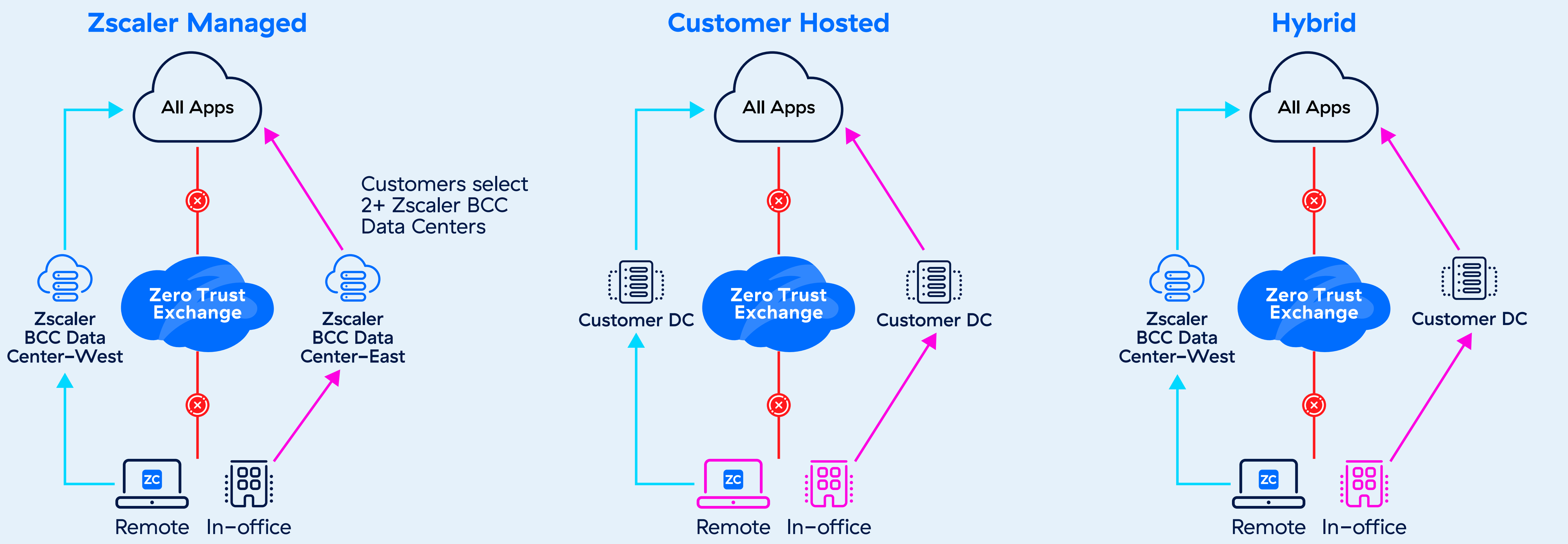
Each regional deployment of the Business Continuity Cloud (BCC) includes ZIA and ZPA private service edges, ZIA private policy cache with private PAC servers, and ZPA private cloud controllers. This architecture ensures consistent global performance, as exemplified by users in San Jose, CA connecting via the US-West BCC and users in Paris, France utilizing the EU-Central BCC, both with identical configurations.

The BCC architecture optimizes DNS management by resolving FQDNs through Zscaler-hosted DNS and handling customer-specific DNS queries. This streamlines service resolution and maintains connectivity even during network disruptions or regional challenges.


Query TXT record
Customer DNS (DR Activation)
Query TXT record
ZC
User in San Jose
ZC
User in Paris
Resolve Service FQDN
Zscaler Hosted DNS (GSLB)
Resolve Service FQDN
ZIA
Z-Tunnel to inline LB hosted on PSE VIP-1
ZPA
Rediret to redirect broker on PCC IP-1
ZIA
Z-Tunnel to inline LB hosted on PSE VIP-2
ZPA
Rediret to redirect broker on PCC IP-2
Zscaler BC Cloud – US-West
Zscaler BC Cloud – EU-Central
ZIA Private Service Edge
ZIA Private Policy Cache + PAC
ZPA Private Service Edge
ZPA Private Cloud Controller (PCC)
ZIA Private Service Edge
ZIA Private Policy Cache + PAC
ZPA Private Service Edge
ZPA Private Cloud Controller (PCC)

Business Continuity and Deployment Options

Business Continuity Cloud provides three deployment options. You can choose a fully managed service, where Zscaler handles all infrastructure, lifecycle management, and disaster recovery readiness. Second, a customer hosted model allows you to deploy ZIA and ZPA Private Service Edges within your own data centers. This self-hosted approach is particularly suitable if you currently use on-prem PSEs for zero trust access or to meet regulatory requirements and wish to integrate them seamlessly into your business continuity plan. Third, a hybrid model that allows you to have PSEs across both Zscaler hosted and customer managed options. This approach is suitable for customers who currently use on-prem PSEs but also have locations where cloud delivered option may be more suitable.



Suited for customers who want operational simplicity

Suited for customers who want to manage on-prem infrastructure

Suited for customers who want to manage on-prem but also have a cloud native options

Customer Approaches for Solving Business Continuity

Business continuity and resiliency are some of the most important topics our customers are interested in knowing about. Based on our conversations with many customer executives regarding their business continuity strategy, most of them have a plan established. These plans generally align with one of the following three approaches:

1. **Bypassing the Zscaler solution:** This approach constitutes a “fail-open” situation. It is often adopted by customers who prioritize immediate operational results and are willing to accept significant risks, including potential downtime, loss of business revenue, and the complete absence of a contingency plan. In this scenario, customers intentionally disable their Zscaler environment. Consequently, all user traffic flows directly to the internet and private applications (and vice versa) completely unchecked and without any form of authentication. It is critically important for these customers to immediately reconsider this strategy, as operating in this manner leaves their entire environment highly vulnerable to compromise.

2. **Utilizing a multi-vendor backup approach to address disruptions:** This is especially true with large enterprise customers who had a VPN or a firewall before they moved to a zero trust environment with Zscaler, or customers who want to have a similar solution from another SSE vendor as a backup. It is crucial for these customers to understand the implications of a multi-vendor strategy for backup. While it is highly resilient, customers should understand the operational overhead it requires, and the poor end user experience it delivers, as a result.

3. **Deploying Zscaler Business Continuity Cloud for comprehensive, zero trust business continuity:** Customers who have moved to Zscaler for delivering a zero trust environment for its users, get high resiliency as part of their services. However, they are looking to achieve high redundancy during critical failures, simplify their operations and deliver a consistent user experience are often the ones undertaking this approach.

The optimal choice will depend on your organization’s technical specifications, risk management priorities, and long-term resiliency goals.

“We trust Zscaler, but how do we stay secure and connected during a major outage?”
Business Continuity Cloud answers this by running on private, isolated planes that mirror the Zero Trust Exchange, keeping security and access intact.

Value Drivers	Bypass Zscaler Solution Fail-open for internet access, employees required on-prem for access to private apps	Multi-Vendor Backup/Redundancy Legacy on-prem firewalls/proxies, other SSE solutions for backup	Zscaler Business Continuity Cloud Secure access to all apps with full cyber and data security posture
Security Strength and Threat Mitigation	**• (Poor)** Internet connections are insecure with no inspection, prone to external and internal threats	**•• (Fair)** Relies on VPNs and firewalls, expanding attack surface and missing zero trust principles	**•••• (Excellent)** Maintains zero trust security for all apps with uninterrupted cyber and data protection
Reliability	N/A This is not applicable as there is no solution implemented	**•••• (Excellent)** Fully redundant, physically and logically isolated, may have management overhead	**•••• (Excellent)** Fully redundant, physically and logically isolated, fully managed
Operational Efficiency	**• (Poor)** Employees are required to be on-premises, which is not always possible, leading to productivity loss for remote employees and partners	**• (Poor)** Complex to manage with manual failover, multiple policy engines, multiple consoles, and multiple endpoint agents	**•••• (Excellent)** Fully managed Infrastructure, automated and manual options failover, same policy engine, same console and same endpoint agent
User Experience	**• (Poor)** Experience for internet access is good, but highly risky with minimal security controls, while experience for accessing private apps is bad, as employees are required to be in office	**• (Poor)** VPN backhaul latency, manual failover results in delayed access, agent swaps, full re-authentication to user sessions, and inconsistent policies disrupt workflows and productivity	**•••• (Excellent)** Seamless access with auto failover, session persistence, and local breakout. Users stay connected—no interruptions, no re-auth, and no workflow changes
Recovery Time Objective (RTO)	**(N/A)** This is not applicable as there is no solution implemented	**• (Poor)** Requires manual failover and solution switching, resulting in significant delays and extended recovery times	**•••• (Excellent)** Automated or admin-triggered, policy-based failover/failback keeps services up and meets strict RTOs during major incidents
Compliance	**• (Poor)** Exposes users to internet threats; high risk of losing sensitive information	**•• (Fair)** Risk is high with using VPNs and firewalls as there are limited controls for data protection and residency	**•••• (Excellent)** Meets all compliance and regulatory guidelines with data protection, data residency requirements

Conclusion

Zscaler has built the Zero Trust Exchange for maximum resilience and robust SLAs, drawing on over 15 years of experience delivering the industry's largest security cloud. This deep expertise also underpins the Business Continuity Cloud (BCC). The BCC is an isolated, separate instance from the Zero Trust Exchange, ensuring seamless operations and business continuity via dedicated, isolated infrastructure — all part of a unified Zscaler solution.

For Zscaler customers, the BCC is the superior choice for business continuity for the following three reasons, particularly for customers currently lacking a backup solution, or for customers using a multi-vendor approach for a backup:

- Deliver seamless end user experience during critical failures
- Maintains consistent security with same access and data security policies as defined in the primary solutions of Zscaler Internet Access and Zscaler Private Access
- Reduces operational complexity with automatic failover and not managing multiple vendors

To learn more, reach out to your Zscaler account manager, or go to ***zscaler.com.***

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

zscaler™

Zero Trust Everywhere