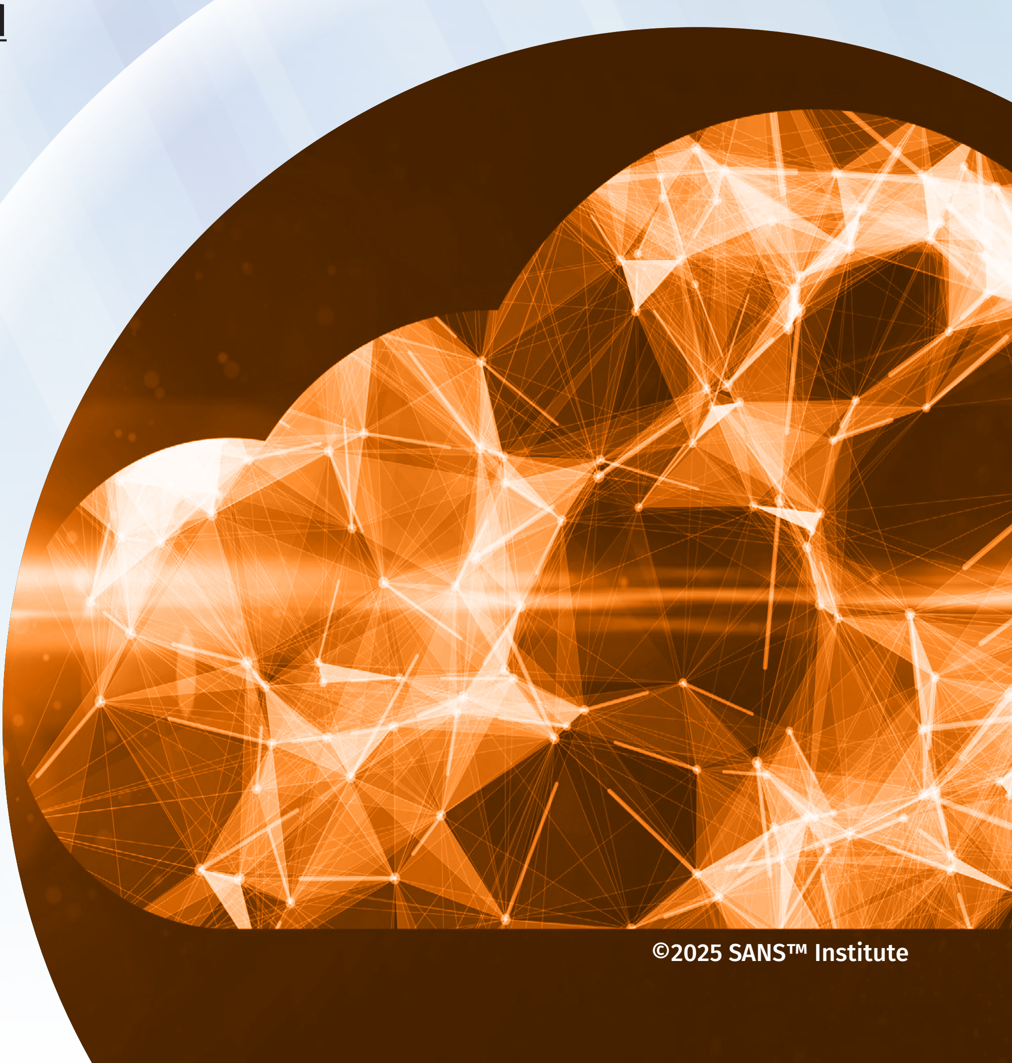
SANS | Research Program

WHITE PAPER

Resiliency and Business Continuity in the Cloud Era

Written by **Dave Shackleford**

May 2025



BROADCOM®

Introduction

As organizations continue migrating their IT infrastructures and security functions to the cloud, the need for robust disaster recovery (DR) and business continuity strategies has never been greater. Cloud-based security controls provide scalability and operational efficiency, but they also introduce dependencies that can lead to catastrophic failures when cloud service providers (CSPs) experience outages.

The reality of cloud service disruptions and their impact on cybersecurity functions highlight the importance of resilient cloud security planning. Organizations today need to look at regulatory requirements, key continuity strategies, and best practices for maintaining security controls during disruptions, with a new emphasis on how cloud services could potentially fail (especially those that provide important security functionality). By implementing a multicloud approach—not only to deployments but also to security resiliency, zero trust security principles, and proactive incident response—organizations can enhance their stability and responsiveness when cloud failures inevitably occur.

Cloud Service Outages and Cybersecurity Risks

The shift to cloud-based services is nearly universal, with businesses leveraging cloud platforms for computing, storage, and security operations. From endpoint protection to SIEM, many organizations have offloaded critical security functions to cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. However, this dependency creates a significant risk: when CSPs experience downtime, security operations can be severely affected. Key cybersecurity services, such as secure web gateway controls, identity and access management (IAM), threat detection, and firewall enforcement, are often rendered inoperable during an outage, leaving businesses exposed to cyber threats.

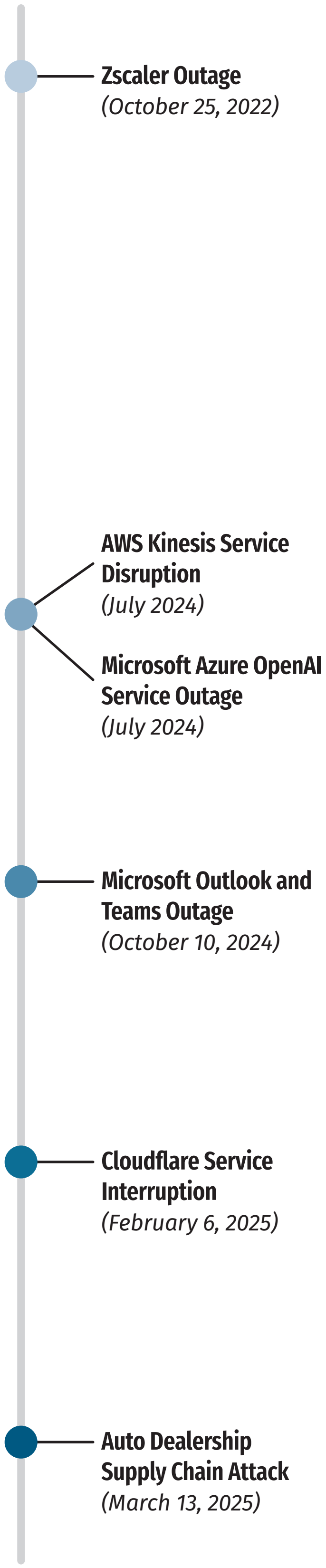
Today, this issue has grown even more concerning, as many organizations rely on cloud-based services and third parties for cybersecurity capabilities beyond the traditional PaaS/IaaS environments (such as cloud-based IAM services, cloud firewalling and zero trust, and cloud protection for end user browsing and internet access). Today, a vast number of enterprises rely on cloud services to provide security controls for end users such as:

- **Site content filtering and categorization—**Many organizations have shifted their content management controls into the cloud to control access to websites based on URLs to prevent users from accessing malicious or inappropriate content and to enforce bandwidth restrictions on streaming services. Internet traffic is either prevented or granted access based on URL category, site risk scoring, users, groups, or machines.
- **Application control—**Application control in the cloud supports web security policies based on users to identify, block, or limit usage of web applications and widgets. This ensures that the data being used by and shared between applications is private and secure.
- **Malware protection—**Especially in the age of ransomware and web-based malware delivery, cloud malware protection services often support both signature-based and behavioral monitoring of web traffic to detect drive-by downloads and other advanced malware targeting browsers and user endpoints.
- **HTTPS inspection—**Many cloud security solutions support HTTPS inspection of traffic, scanning TLS encrypted traffic passing through the gateway. Gateways using HTTPS inspection decrypt the traffic with the sender's public key, inspect and protect, then re-encrypt the content to send back to the sender. Specific traffic types can be excluded for privacy reasons as well.
- **Data loss prevention—**With an increasing emphasis on cloud applications and data for many end users, many cloud security services increasingly support data loss prevention (DLP) policies to detect and prevent unauthorized transfer of data to/from online sites and services. With more compliance regulations requiring DLP today, these controls becoming unavailable could be a significant issue.

- **Remote browser isolation (RBI)—**Increasingly, cloud security services provide end users with a browser sandbox that prevents malware and execution of other browser-borne threats from executing on the actual end user device.
- **Zero trust network access (ZTNA)—**ZTNA services are often implemented to replace traditional VPNs, providing remote access to on-premises applications and services for users, along with strong authentication, access controls, and behavioral monitoring.

Although this list is a starting point, it's no secret that organizations of all types and sizes are using more cloud services all the time for critical cybersecurity controls. What would happen if the current platforms and services in use for the above security capabilities were down or disabled for an extended length of time? With this increased use of cloud services comes a dark side: a disturbing dependence on cloud applications and services that may significantly impair continued business function if they fail. In 2025, there's no shortage of major cloud outage scenarios to highlight our increasing dependence on cloud services overall. Some of the more notable recent cloud provider outages include:

- **Zscaler outage (October 25, 2022)—**Zscaler suffered a significant outage that lasted for close to four hours, leading to a loss of connectivity for many users and leaving them unprotected from a wide array of online threats.
- **AWS kinesis service disruption (July 2024)—**AWS experienced a disruption in its Kinesis data streaming service within the us-east-1 region. The incident lasted nearly seven hours, causing API slowdowns and errors. This disruption had widespread effects, particularly on logistics and financial services that rely on real-time data streaming.
- **Microsoft Azure OpenAI service outage (July 2024)—**Microsoft Azure OpenAI services faced a global outage across multiple regions, lasting over 20 hours. The disruption stemmed from a routine operation that inadvertently disabled critical code components, affecting businesses dependent on AI-driven tools.
- **Microsoft Outlook and Teams outage (October 10, 2024)—**Microsoft experienced outages impacting Outlook, Teams, and Office 365 services. The disruptions were attributed to a potential memory management issue.
- **Cloudflare service interruption (February 6, 2025)—**Cloudflare experienced a 59-minute outage affecting multiple services, including its R2 object storage. The incident caused failures in operations dependent on R2, impacting services like Stream, Images, Cache Reserve, Vectorize, and Log Delivery.
- **Auto dealership supply chain attack (March 13, 2025)—**Although not explicitly a cloud service failure, a third-party supply chain attack from a shared third party used in the auto dealership industry highlights web-distributed malware that could prey on consumers who are left unprotected by critical security services outages delivered via the cloud (such as the Zscaler outage mentioned previously).


Zscaler Outage
(October 25, 2022)
AWS Kinesis Service Disruption
(July 2024)
Microsoft Azure OpenAI Service Outage
(July 2024)
Microsoft Outlook and Teams Outage
(October 10, 2024)
Cloudflare Service Interruption
(February 6, 2025)
Auto Dealership Supply Chain Attack
(March 13, 2025)

There are innumerable examples of cloud service provider outages—and they all beg the question: Have we become overly reliant on cloud provider infrastructure? If so, should we consider designating these large service providers as critical infrastructure globally? So far, although there hasn't been any distinct signal from government agencies worldwide that might indicate this designation is imminent, it's been debated for close to a decade as we've shifted many traditional in-house applications, services, and infrastructure to third-party environments. If we're just talking about losing access to email, collaboration services, or file shares for a relatively short period of time ("short" being relative, of course), then marking even the largest cloud service providers as critical infrastructure is likely unwarranted, no matter the inconvenience and disruption.

However, the largest providers are now hosting IoT platforms, payment processing for global financial organizations, and healthcare patient data processing and application integration. Take, for example, Azure Health Data Services, used by large organizations such as Humana, SAS, and others to process healthcare patient and research data. AWS is increasingly targeting the energy sector with AWS for Energy solutions that include oil exploration and drilling models, petroleum production monitoring, and many other options. The automotive industry now can take advantage of Google Cloud's Connected Car Telemetry Platform to collect and coordinate data from self-driving vehicles and those with telemetry reporting for speed, location, camera footage, and more. Recent updates to the EU's Digital Operational Resilience Act (DORA) state that financial institutions need full resilience coverage in service providers for information communications technologies (ICT), which includes cloud providers and security-oriented services hosted in a cloud model.

The processing power of the cloud will continue to attract new technology models and use cases, and it's inevitable that critical infrastructure industries will determine that the risk of relying on third-party services like IaaS and PaaS clouds is lower than building and maintaining in-house workloads and applications. For now, though, organizations of all types should double down on disaster recovery and business continuity planning (DR/BCP) for their most important cloud workloads and application scenarios. These incidents emphasize the need for proactive cloud resilience planning to ensure continuous security operations.

Getting back to the security-specific services we are seeing in the cloud, it's important to note what may happen when a service fails. When a cloud security service outage occurs, organizations may lose access to essential capabilities, such as:

- **IAM—**If authentication services are disrupted, users may be locked out or unauthorized users could gain access.
- **Threat detection and response—**SIEM and endpoint detection and response (EDR) tools may fail, leaving networks vulnerable.
- **Firewall and DDoS protection—**Cloud-based security enforcement mechanisms can be rendered ineffective, exposing systems to attacks.
- **Secure web gateway (SWG)—**In the age of zero trust, many end users now access the internet through a cloud service vs. a traditional on-premises gateway, meaning content filtering, DLP, and malware protection are solely handled in the cloud. If these controls are unavailable, users may be prevented from accessing many internet sites or could alternately be enormously vulnerable to a vast range of threats online.

Another major challenge is the potential cost. For a number of enterprises, maintaining redundant cloud instances is expensive. Running full security stacks across multiple cloud providers requires significant investment, making resilience planning a balancing act between cost and risk. To this point, it's actually important to prioritize and select the most relevant and common security controls that many organizations need from a cloud service, and for many organizations, those services are focused on end users (browser controls, content filtering, application and protocol inspection, and data security).

The Business Impact: Why Resilient Cloud Security Planning Is Essential

As more organizations start to rely on cloud-based security services, they may face a number of possible disruptions and resilience challenges if providers experience issues. Cloud service disruptions can lead to:

- **Revenue loss—**If core security systems fail, businesses may face data breaches, regulatory fines, or ransomware attacks. Imagine that most or all employees cannot log in or access critical sites and applications needed for business.
- **Operational downtime—**Critical security functions being unavailable can lead to prolonged service disruptions. This can lead to customer delays, partner-related issues, and lost productivity. This is a classic DR/BCP scenario that now may hinge on cloud services.
- **Reputation damage—**Customers and partners lose trust in businesses that suffer security failures. Although it seems to make sense that organizations could point to providers and third-party services, when cloud services fail and organizations are affected, they look bad in the eyes of their own customers.

For security and operations teams, the stress of cloud disruptions can be personal. When services and cloud functions go down, cybersecurity and cloud engineering and operations professionals may need to work around the clock to restore operations. The thought of an extended outage "keeps security leaders up at night," as they face immense pressure to protect sensitive data. Here's the problem, though: With the shared responsibility model, there are often scenarios where IT and security teams cannot do anything at all to rectify the situation and need to look elsewhere.

Given the unpredictability of cloud failures, organizations must design cloud security solutions with built-in redundancies, including:

- **Failover mechanisms—**Automatic switching to backup environments in case of failure. For most cloud security controls, this has been completely nonexistent.
- **Multicloud strategies—**Reducing reliance on a single CSP. Again, most organizations are heavily reliant on a single cloud security service in one or more ways.
- **Offline security options—**Maintaining on-premises security capabilities for worst-case scenarios. At the risk of being pessimistic, many enterprises don't have a plan to fall back to their original model of security. Once the move to a cloud-based service is complete, the previous platforms (firewalls, proxies, web and content gateways, etc.) may be wholly decommissioned if specific use cases do not require on-premises security.

The increasing reliance on cloud services for cybersecurity controls has underscored the need for robust cloud resilience strategies. Here are several statistics highlighting this necessity:

- In 2025, 47% of all data breaches targeted cloud-based systems, marking a 5% increase from the previous year.[1]
- Gartner reports that through 2025, 99% of cloud security failures will result from human error, emphasizing the critical need for comprehensive training and stringent access controls.[2]
- As of late 2022, approximately 90% of cybersecurity risks remained uninsured, highlighting a significant gap in risk management strategies.[3]
- Data loss and leakage are primary concerns for 71% of organizations utilizing cloud services, underscoring the importance of implementing robust data protection strategies.[4]

In addition, SANS has seen that although most businesses use cloud-based security controls, few have failover strategies. According to a variety of polls collated by Queue IT, 93% of enterprises report downtime costs exceeding $300,000 per hour.[5] In short, the numbers don't lie, and we need to look at how reliant we are on cloud services that could easily lead to major business loss or issues if they go down. These statistics collectively highlight the pressing need for organizations to bolster their cloud resilience to effectively manage and mitigate the evolving landscape of cybersecurity threats.

Regulatory and Compliance Considerations for Business Continuity Planning

Although no one wants to build their cloud security programs and resiliency measures and models around compliance, the sad truth is that regulators increasingly mandate that organizations implement robust cloud security continuity measures. Some of the current compliance requirements and best practice recommendations include:

- **NIST 800-53 & 800-171—**Requires contingency planning for cloud-based security controls
- **GDPR—**Mandates data protection and breach response capabilities, even during cloud outages
- **CISA Cloud Resilience Guidelines—**Calls for multicloud and offline security backup strategies
- **DORA—**Requires all financial institutions to have resilient and redundant ICT, which includes cloud services

[1] "Top 10 Security Issues in Cloud Computing," www.veritis.com/blog/top-10-security-issues-in-cloud-computing

[2] "Is the Cloud Secure?" October 2019, www.gartner.com/smarterwithgartner/is-the-cloud-secure#

[3] "Cloud Reassurance: A Framework to Enhance Resilience and Trust," January 2024, https://carnegieendowment.org/research/2024/01/cloud-reassurance-a-framework-to-enhance-resilience-and-trust?lang=en

[4] "Top 10 Security Issues in Cloud Computing"

[5] "The Cost of Downtime: IT Outages, Brownouts & Your Bottom Line," April 2025, https://queue-it.com/blog/cost-of-downtime

Even organizations that don't have specific compliance requirements are choosing to align with industry frameworks and best practices. To that end, organizations are changing their strategies around cloud security services to incorporate some of the following:

- **Maintaining security logs even during outages—**Although audit trails and operational logs should be collected anyway, this is becoming more of a DR issue than we've seen previously.
- **Ensuring IAM and other critical cybersecurity solutions function redundantly—**This can be a huge headache and a costly option. Nonetheless, with the shift away from on-premises control models, organizations need to think about single points of failure more than ever.
- **Conducting annual disaster recovery testing—**This should be done no matter what! All organizations should be building and testing DR playbooks that incorporate cloud service providers, especially those playing critical roles in day-to-day business requirements. For a number of security services, this will fall into the top tier of priority for DR/BCP recovery functions.

Failing to align cloud continuity strategies with regulations can result in legal repercussions and financial penalties. This is still evolving at present, but it's a good idea for most enterprises to get ahead of the situation and prepare for cloud security service redundancy.

Maintaining security logs even during outages

Although audit trails and operational logs should be collected anyway, this is becoming more of a DR issue than we've seen previously.

Ensuring IAM and other critical cybersecurity solutions function redundantly

This can be a huge headache and a costly option. Nonetheless, with the shift away from on-premises control models, organizations need to think about single points of failure more than ever.

Conducting annual disaster recovery testing

This should be done no matter what! All organizations should be building and testing DR playbooks that incorporate cloud service providers, especially those playing critical roles in day-to-day business requirements. For a number of security services, this will fall into the top tier of priority for DR/BCP recovery functions.

Key Strategies for Cybersecurity Business Continuity in Cloud Environments

For many organizations, there's never been a lot of focus on redundancy in the cloud (or certainly not enough). With so many recent outages and downtime concerns, that's changing. Some strategic considerations include:

- Instead of creating a replica of cloud infrastructure in a different availability zone or region within the same provider's environment, consider a replica to fail over to a second provider's cloud, if possible. Complexity and cost may increase, so look for a vendor that could provide a failover service at a fraction of full price.
- Invest in backup solutions or disaster recovery as a service (DRaaS) providers that can replicate and store cloud workload and application data externally to the primary cloud services in use.
- Push SaaS vendors to offer more flexible and accessible backup options through API integration, where possible.
- Despite all the benefits of cloud services, perform a thorough business impact analysis (BIA) for all major cloud applications (particularly SaaS, which can't easily be replicated elsewhere) to ensure that organizational risk tolerance is aligned with cloud usage.

For organizations already invested in a multicloud architecture, this can sometimes lead to a diversified security service model across multiple providers. For proper resilience in these scenarios (which are increasingly common), look to spread security operations across different CSPs, preventing a single failure from crippling business operations. Best practices include:

- **Distributing security workloads—**Are there optimal failover and distributed options available that aren't cost prohibitive?
- **Maintaining hybrid security operations—**Although keeping critical security controls operational on-premises may not be ideal, this may be a viable workaround for some capabilities. Many organizations plan to operate a hybrid security architecture model for the foreseeable future.
- **Using cloud-agnostic security tools—**Ensuring security solutions work across multiple cloud environments is an important architectural consideration regardless, but having options to shift into if a regional or localized failure occurs makes a lot of sense.

As part of many cloud security service strategies, organizations are adopting zero trust security services in the realm of identity management, access management, and more. This can definitely help to minimize risk by continuously verifying trust at every access point, and includes some of these key control aspects:

- **Context-aware access controls—**Even during a cloud failure, adaptive authentication ensures users meet strict verification conditions.
- **Microsegmentation—**This prevents lateral movement in case security controls go down.
- **Least privilege access—**Reducing access rights mitigates the impact of security outages.

Zero trust initiatives can touch a vast array of end users, so it's really important to plan for a failover and backup scenario. In other words, if all of your employees are using a central gateway to access resources, and this gateway fails, what do you do? What secondary gateway can you point them to? In the age of cloud, this is a shockingly common problem—no secondary gateway is provisioned at all! One thing that can help organizations recognize gaps in cloud security resilience is to simulate cloud failures to test their capabilities. Essential practices include:

- **Tabletop exercises—**Running simulations of cloud outages
- **Automated failover testing—**Ensuring backup security systems activate as expected
- **Red team assessments—**Identifying weaknesses in cloud security continuity plans

In addition, for organizations looking to build and maintain a resilient cloud security infrastructure, some other considerations include:

- **Automating compliance monitoring—**Ensure audit logs are collected even during disruptions.
- **Performing regular cloud risk assessments—**Identifying potential weaknesses in cloud security strategies should be a regular practice, especially with the pace of cloud service updates.
- **Engaging with auditors—**Keeping up with evolving security and business continuity needs is a chore, but auditors and regulators can help to inform cloud and security teams about best practices and specific requirements.

Conclusion: The Future of Cyber Resilience in Cloud-Driven Businesses

Cloud adoption will continue to accelerate, making cybersecurity resilience a business-critical priority. The future of cloud security continuity will be shaped by:

- **AI-driven security resilience—**AI-enhanced cybersecurity tools will detect and mitigate failures faster.
- **Decentralized cloud security models—**Businesses will adopt edge security and decentralized cloud architectures.
- **Stronger regulatory requirements—**Governments will impose stricter mandates on cloud resilience.

Organizations that proactively implement multicloud security strategies, zero trust models, and robust disaster recovery plans will be best positioned to withstand cloud failures and maintain security operations in the face of disruptions. By prioritizing resilient cybersecurity architecture, businesses can protect their assets, reputation, and customers—even when the cloud goes down.

Sponsor

SANS would like to thank this paper's sponsor:

BROADCOM®