BROADCOM

Executive Summary

Cybersecurity in a Cloud-First World

As organizations increasingly shift to cloud-based infrastructures and services, they benefit from enhanced scalability and efficiency. However, this shift also introduces a critical dependency: When cloud security services go down, business operations and security controls likely go down with them. Executives today must confront a growing risk landscape where a single outage can disrupt security, impact customers, and damage brand reputation, and plan accordingly to ensure continuity of important security controls.

Why This Matters

Many essential cybersecurity functions—including identity and access management (IAM), threat detection, web filtering, and malware protection—now operate through the cloud. This means that when cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Oracle, or third-party security vendors in the realm of zero trust network access (ZTNA) and secure web gateway (SWG) experience downtime, organizations may lose visibility and control over critical security processes that affect end-user security, data security monitoring, and more.

Recent high-profile cloud outages have impacted everything from secure email access and endpoint protection to AI-driven healthcare services and financial data processing. These issues occur for a variety of reasons, ranging from provider misconfiguration to legitimate attacks. These incidents reveal just how exposed enterprises are to external disruptions—especially when no effective contingency plan is in place.

What's at Stake

The impact of cloud outages on security services can include:

Operational Downtime
Employees lose access to business-critical applications.

Revenue Loss
Interruptions in service can result in missed opportunities and regulatory fines.

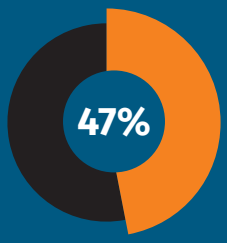
Brand Reputation
Customers and partners may perceive security failures as internal deficiencies, not third-party issues.

Security Gaps
Disruptions in IAM, SIEM, or firewall protection can open doors to cyber threats. In addition, many malicious sites and services are constantly targeting end users, and a disruption in content filtering and end-user security controls for site access, browser-based malware, and more can have a major risk impact.

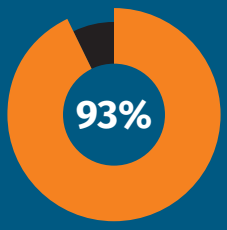
[1] "Top 10 Security Issues in Cloud Computing," www.veritis.com/blog/top-10-security-issues-in-cloud-computing/

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

The Rising Cost of Inaction



47% of data breaches in 2025 involved cloud-based systems.[1]



93% of enterprises report that downtime costs exceed $300,000 per hour.[2]

SANS | Research Program

What Executives Should Do Now

1. **Prioritize Cloud Resilience in Strategy and Budgeting**
   - Cloud continuity is now a core business concern, not just an IT issue.
   - Invest in disaster recovery (DR) and business continuity planning (BCP) that includes cloud security functions.
2. **Push for Multi-Cloud and Redundant Architectures**
   - Avoid vendor lock-in by diversifying cloud service providers.
   - Implement failover capabilities for critical security services like IAM, SWGs, and ZTNA.
3. **Ensure Regulatory Alignment**
   - Meet evolving compliance requirements (e.g., GDPR, DORA, NIST 800-53).
   - Conduct annual audits and testing to validate resiliency plans.
4. **Support Zero Trust and Cloud-Agnostic Solutions**
   - Zero trust architecture minimizes the blast radius of outages and attacks.
   - Choose security tools that can function across different cloud environments.
5. **Demand Visibility and Testing**
   - Require tabletop exercises, red team assessments, and automated failover tests.
   - Push SaaS vendors to provide better backup, logging, and recovery capabilities.

Looking Ahead: Building a Resilient Cloud Security Future

The future of cloud security continuity will be shaped by:

- **AI-powered resilience tools** to identify and mitigate threats faster
- **Edge and decentralized architecture** to reduce reliance on centralized services
- **Stronger government mandates** requiring cloud resilience

Bottom Line for Executives

Cyber resilience for cloud-based security services is no longer optional. Cloud service disruptions will always be on the horizon, but the consequences don't have to be calamitous. Executives must champion resilient cloud security architectures to ensure uninterrupted operations, protect brand integrity, and maintain customer trust. Your leadership in this area could mean the difference between business continuity and business crisis.