parametrix

Cloud Outage Risk Report 2024

Executive Summary

The number of ‘Critical’ cloud service interruption events among the three major public cloud providers – Amazon Web Services, MS Azure, and Google Cloud Platform – **rose of 18% in 2024**, and has increased by 52% in total since 2022.

The duration of ‘Critical’ events also continues to increase, **rising to 221.1 hours in 2024, up 18.7% since 2023**, and 51.3% since 2022.

The number of ‘Warning’ cloud service interruption events - those which affect the functionality of the service, but do not result in a complete service failure – has **fallen slightly, from 121 in 2023 to 111 in 2024.**

In 2024, as in 2023, cloud monitoring by Parametrix recorded **six cloud outage events that lasted more than ten hours each.** Together the downtime from just these six events totaled nearly 100 hours.

Google Cloud’s share of ‘Critical’ downtime hours increased by 57%, while that of MS Azure decreased by more than one fifth. Amazon Web Services again proved the most reliable of the big three.

Aggregate unavailability from ‘**Critical’ cloud service interruption events was up in 2024 for a total of 221 hours** (2023: 186 hours) during the 47 Critical interruptions (2023: 40).

Once again, **the majority of events by number and duration occurred in North America**, but significant ‘Critical’ interruptions also occurred in European, Asian, and other geographic areas.

Geographic split by hours of downtime is similar to that of 2023 and **North America’s share of downtime hours is around 60%.**

Human error continues to be the leading cause of service interruptions, and rose as their root cause from 53% of events in 2023 to 68% in 2024.

Fewer power incidents in 2024 (6 compared to 17 in 2023) led to **a significant reduction in disruptions to core services** like compute and storage.

In 2024, major service disruptions around the world reinforced the critical role of cloud infrastructure in business operations. Incidents like the global CrowdStrike outage in July, AWS's service disruption in the US-EAST-1 region, and Google Cloud's power failure in Frankfurt highlighted the growing systemic risks faced by enterprises dependent on digital supply chains. These large-scale events disrupted millions of businesses, intensifying the need for effective risk management tools and placing significant pressure on service providers to ensure accountability and address financial exposures.

As the digital economy continues to expand, new regulations like the EU's Digital Operational Resilience Act (DORA) are emphasizing the need for operational resilience. Organizations are now required to assess and mitigate risks from digital dependencies, including those linked to cloud service providers. With human error responsible for 68% of cloud outages in 2024, even the most advanced digital ecosystems are vulnerable.

The rapid adoption of generative AI has further accelerated demand for cloud services. The top three cloud providers invested $82 billion in infrastructure in Q3 2024 alone. While this growth fuels innovation, it also amplifies the risks of cloud outages, which can disrupt operations, diminish customer trust, and result in significant financial losses.

At Parametrix, we are dedicated to helping businesses navigate these challenges. Our advanced cloud monitoring system, which performed 14 billion tests across 317 data centers in 2024, delivers critical insights that empower organizations to manage their cloud risks effectively. Our cloud outage insurance solutions ensure companies can swiftly recover from service interruptions, protecting their operations, reputation, and financial stability.

As we look ahead, Parametrix remains committed to monitoring, analyzing, and insuring cloud outage risk in an increasingly digital world. We are grateful for your continued trust in our technology and expertise to protect digital operations and strengthen business resilience.

Jonathan Hatzor
Co-Founder and Chief Executive
Parametrix

Cloud Growth Soars

Organizations around the world are investing in cloud-based technologies that streamline their operations and deliver personalized customer experiences. **New technologies such as generative AI are driving an unprecedented reliance on cloud platforms.** As cloud usage soars, the public cloud market continues to boom.

Already more than half of business data is stored in the cloud, and more than half of computational workload is performed there.[1] Of that total, nearly half of all workloads and data now reside in the public cloud, where a third-party has delivered computing resources over the internet.[2] Further down the digital supply chain, third-party IT services such as SaaS providers, payment gateways, and customer relationship management systems are now mission-critical for many enterprises around the world.

This rapidly growing network of interconnected technologies dependent on cloud infrastructure presents new and far-reaching business risks. One of them is digital interruption: the threat that a fault up the line simply causes technology to stop working. That makes understanding and managing cloud outage risk, and its potential cascading impact, a new top priority for enterprises.

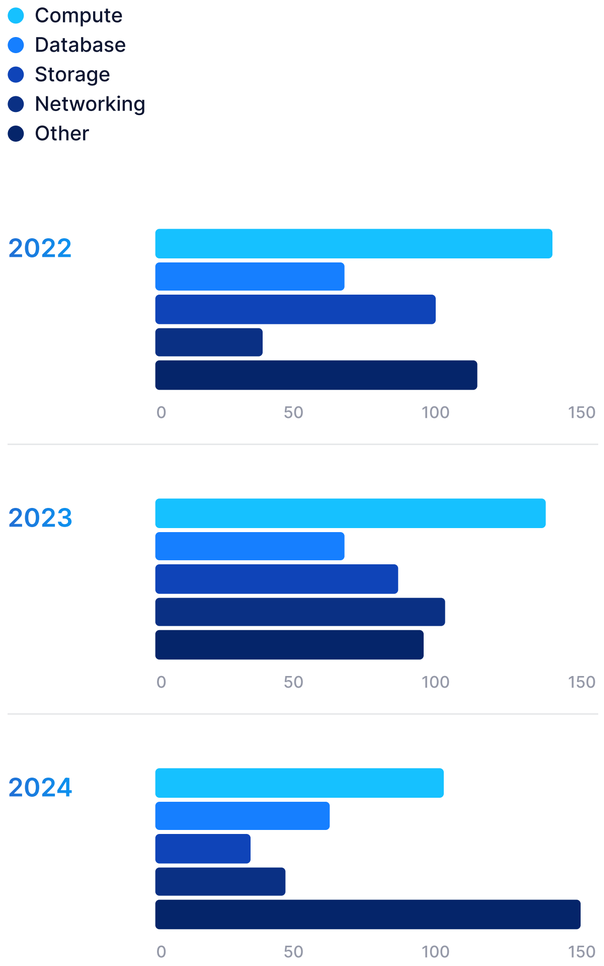
To keep up with the growth, the three biggest Cloud Service Providers (CSPs) – Amazon Web Services (AWS), Microsoft Azure (Azure), and Google Cloud Platform (GCP) – have increased their spending on cloud infrastructure. Together they spent $82.0 billion building the cloud in the third quarter of 2024 alone. **All in, total historical capital expenditure by the three tech giants could surpass $1 trillion in 2025.**[3]

As enterprises increasingly rely on cloud infrastructure, understanding its performance and availability is paramount. Serving as the backbone of today's digital supply chains, the cloud powers critical systems and interconnected technologies. However, its transformative potential also comes with financial complexities and vulnerabilities. Disruptions in availability can cascade through dependent systems, causing widespread operational and financial impacts. To thrive in this cloud-first era, organizations must prioritize managing cloud and digital interruption risks, ensuring efficiency, maximizing value, and maintaining the operational resilience of your digital supply chain.

1 https://info.flexera.com/cm-report-state-of-the-cloud-2024-thanks#centralization
2 https://spacelift.io/blog/cloud-computing-statistics
3 https://www.canalys.com/newsroom/global-cloud-services-q3-2024

New technologies such as generative AI are driving an unprecedented reliance on cloud platforms.

Figure 2:
Overall Duration of Critical Events (Hours), by Service Group



Cloud Outages 2024

Parametrix made 14 billion tests of 317 data centers operated by AWS, Azure, and GCP in 2024. **A trend of increased number and duration of 'Critical' cloud service interruptions continued** (Figure 1).

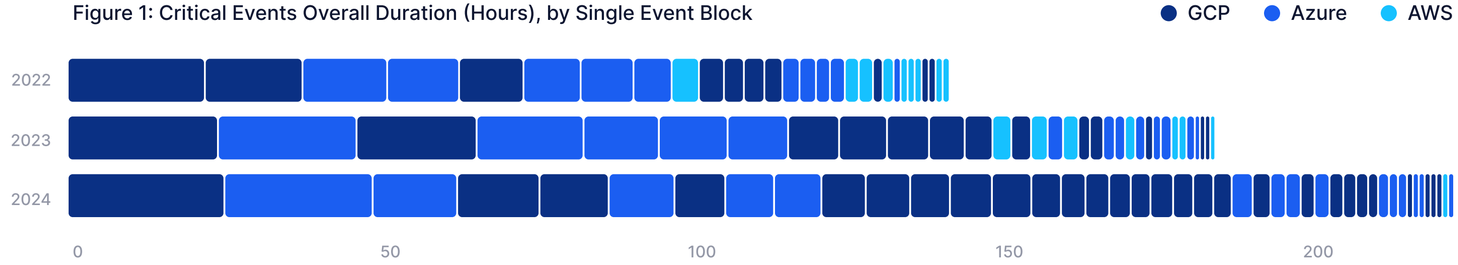
The number of 'Critical' downtime events - those which cause a complete shutdown of services or a significant service interruption, and have widespread impact on users - increased from 40 in 2023 to 47 in 2024, a rise of 18%. The metric is up by 52% from 31 in 2022. Meanwhile, the duration of critical events also increased. The total duration of critical events was 221.1 hours in 2024, up 18.7%, and 51.3% from 2022.

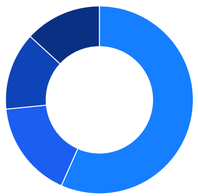
On a more positive note, the number of "Warning" events - those which affect the functionality of the service, but do not result in a complete service failure - fell slightly, from 121 in 2023 to 111 in 2024.

Parametrix monitors the functionality of CSPs' various services. **In 2024, the mix of cloud services affected by critical events changed.** The total number of hours that compute and database services were impaired fell by about one fifth. Storage and network services downtime fell even more, by almost 59.3% and 57.7% respectively.

These service improvements were offset by a dramatic increase in the duration of outages affecting all other services, which was up by more than half. **The findings reveal a trend of continuous improvement in the delivery of the four core services,** which - networking notwithstanding - have each suffered fewer hours of downtime year-on-year since 2022.

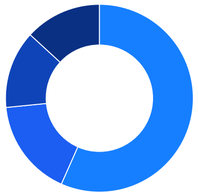
Figure 1: Critical Events Overall Duration (Hours), by Single Event Block





2022

- 43.5% North America
- 30.1% Europe
- 10.6% Asia
- 15.8% Rest of World



2023

- 56.7% North America
- 13.2% Europe
- 16.8 Asia
- 13.4% Rest of World

2024

- 61.5% North America
- 19.9% Europe
- 11.2% Asia
- 7.4% Rest of World

Figure 3:
Geographical Split, by Duration

Cloud Outages 2024

Power loss and physical infrastructure issues caused fewer issues in 2024, despite the many natural catastrophe events that occurred during the course of the year. **This resulted in a reduction of core services interruptions (compute, storage, database) for which the main root cause is Power loss.** This highlights the success of the cloud providers' physical risk management programs in ensuring the resilience of their data centers. The rise in "other" services includes many human error incidents, and factors such as new cloud regions and the ongoing addition of new cloud services such as artificial intelligence, serverless computing, edge computing, and advanced security solutions.

Human error remains the leading cause of outages by far. **In 2024 the three major public service providers blamed people's mistakes for more than two-thirds of all outages for which they revealed a cause**, up from just more than half in 2023. System overload and connectivity issues remained the second and third most common causes of downtime issues.

When analyzing the geographical split of interruptions, the number of events affecting globally managed services increased to 45 in 2024, up from 40 in 2023. Those which impacted users of North American cloud regions increased from 63 in 2023 to 85, while the number of events in Europe remained relatively steady, the duration of those events increased as shown in Figure 3.

Understanding Digital Supply Chain Risk

All systems are subject to occasional disruption. The fast-growing digital supply chain is no different. CSPs do everything they can to keep it flowing and maximize the reliability of their service delivery, but service interruptions occur despite their efforts. In July 2024, for example, a global IT outage left more than 8.5 million devices confronted with the “Blue Screen of Death.” The outage caused widespread business interruption around the world.

On 19 July 2024, leading cybersecurity provider, CrowdStrike, accidentally implemented a bad software update resulting in widespread outages around the world. It was not a cloud outage, but the cloud was fundamental to propagating and spreading the impact of the troublesome code which led to the interruption of so many computers and systems world-wide. It was the ‘contagion vector’ which spread the faulty programming.

Analyzing CrowdStrike

CrowdStrike gave the world a new appreciation of the potential scope of an outage event. **Parametrix's analysis estimated that the event cost the Fortune 500 companies (F500) alone $5.4 billion.** The largest direct financial loss was suffered by companies in the healthcare and banking sectors, which suffered more than half of the total loss. Yet they account for only 20% of Fortune 500 revenues. This disparity is due to the uneven impact of CrowdStrike on different business sectors.

Manufacturing, the largest sector by revenue, suffered an estimated loss of $36 million, which seems trivial compared to the sector's annual revenue of $3.4 trillion across 130 companies. However, the event cost the six F500 airlines approximately $860 million, or 33% of the group's total annual revenues. Delta Airlines alone reported a staggering $150 million loss due to the outage, **illustrating how significant operational disruptions to critical services can be, and how quickly digital supply chain risks can translate into real financial damage.**

The analysis concluded that:

- Traditional industries heavily reliant on physical computers experienced longer recovery times than those with cloud-based infrastructures
- The cloud acted as a "contagion vector" for the faulty code at the root of the CrowdStrike disruption
- The longstanding cyber risk management focus on the prevention of cyberattacks and other non-systemic disruptions was a catalyst for the CrowdStrike outage, since the management of risks arising from internal errors had been given much less priority
- Because the CrowdStrike outage impacted on-premises and cloud-based users alike, it does not provide a primary data point to model future cloud service provider outages
- The outage exclusively affected users of the Microsoft Windows operating system, while Linux users remained unaffected.
- Larger enterprises experienced the most significant impact, as they are more likely than small and medium-sized businesses to have adopted advanced cybersecurity solutions like CrowdStrike.

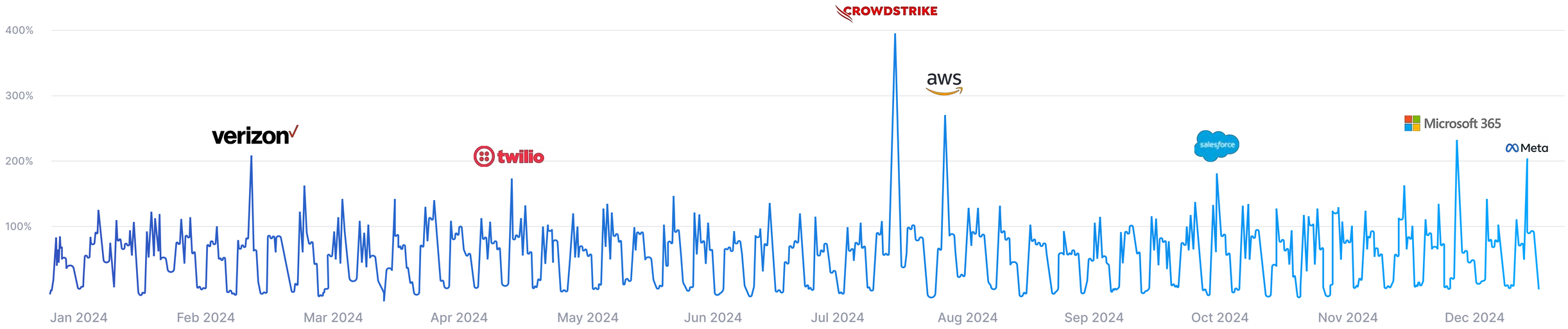
Beyond the cloud: monitoring the digital supply chain

This analysis was based on more than 54 billion data points collected by Parametrix to define the historical performance of cloud services. We also drew on our extensive expertise in system failures and business interruption losses, and direct monitoring of the real-time service availability of over 7,000 SaaS, PaaS and IaaS providers. Most notably in 2024, Parametrix closely monitored the global CrowdStrike outage. **Compared to the baseline for a regular working day, a 390% surge in the number of impacted companies was detected** (Figure 4).

This event recorded the highest daily incident count and the largest single-day spike of the year. Our analysis revealed that these widespread outages extend beyond large enterprises. **Smaller organizations also reported substantial service disruptions.** Unsurprisingly perhaps, notably fewer incidents were detected on weekends (less than 100) suggesting that major disruptions tend to surface during weekdays, when most organizations are actively operating.

The CrowdStrike event also revealed a high sensitivity to cybersecurity outages. Such events may be more disruptive than even a large-scale cloud provider failure in a single region. As organizations become more reliant on cybersecurity platforms, any lapse in these systems can have severe repercussions on day-to-day operations and revenue.

Figure 4:
Number of Companies Impacted, by Date



DORA Readiness

Another development that draws attention to evaluating the risk of cloud outages is DORA, the European Union's Digital Operations Resilience Act, which was implemented on 17 January 2025. DORA is intended to ensure that financial institutions can withstand, respond and recover from IT-related disruptions and cyber threats. While it obviously captures such companies based in the European Union (EU), its rules also extend to companies that provide services to European financial institutions or operate within the EU market.

The regulations require these organizations to address vulnerabilities and dependencies on digital systems, including third-party service providers like cloud platforms. Companies must be able to show that they have assessed the potential risks which lie within their digital supply chain, including the risks faced by their front-line suppliers, when those risks could impact the reporting company.

Recent outages impacting big banks like Capital One and Barclays in January 2025 further emphasize the importance of understanding digital supply chain risk. **These incidents highlight how disruptions to critical systems can ripple through financial operations**, reinforcing the need for DORA to ensure institutions have robust contingency plans and visibility into third-party dependencies.

Mapping exposure with DORA

DORA emphasizes **the need to identify, assess, and mitigate risks stemming from digital dependencies, including those tied to third-party service providers.** As financial institutions adapt to these new regulations, they must take a proactive approach to digital risk mapping.

A clear understanding of vulnerabilities, such as cloud outages and IT disruptions, is essential for compliance, operational resilience, and maintaining customer trust. By proactively addressing these challenges, financial institutions can strengthen their resilience, safeguard customer trust, and meet the stringent regulatory standards set by DORA.

Assessing Your Cloud-Risk Profile

Every company's cloud risk profile is unique. It is based on their sector, operations, location, cloud service provider/s, and risk mitigation efforts undertaken. Mapping your technological landscape and potential points of failure is essential to ensure your digital investments align with strategic objectives. Effective risk management must encompass robust strategies for monitoring, assessing, and mitigating risks.

By bridging the "business resilience gap," organizations will protect themselves against potential threats, optimize performance, and unlock the full potential of their investment. Thus, **understanding and managing systemic digital risk in the age of technological interdependence is crucial** to navigate and thrive in today's interconnected digital economy.

> **Understanding and managing systemic digital risk in the age of technological interdependence is crucial.**

5 Steps for Mapping Enterprise Cloud Risk Exposure

A comprehensive systemic cyber risk exposure map helps companies and their insurers identify potential vulnerabilities, assess the impact of different systemic cyber risk scenarios, and develop strategies for risk mitigation and transfer. It is a five-stage process.

1. Identify Critical Assets and Services

Start by identifying the assets and services that are essential to business operations. They include any data, applications, and infrastructure which, if disrupted, would have a significant operational or other impact on the normal course of business, or on reputation, finances, or other important areas.

2. Assess Vulnerabilities

Evaluate the vulnerabilities associated with each critical asset identified. These include:

- technical vulnerabilities (ie. outdated software),
- operational vulnerabilities (ie. inadequate backup and recovery processes), and
- external vulnerabilities (including dependence on third-party service providers)

3. Conduct Scenario Analyses

Simulate realistic events helps to understand the potential impact of different types of outages and attacks on operations and reputations. This could include an outage of a major cloud provider on a specific trading day, or a widespread malware attack that exploits a critical vulnerability present in specific systems.

4. Develop Mitigation Strategies

Develop and implement mitigation strategies that reduce these mapped risks. Such measures could include:

- investment in robust cybersecurity measures
- diversification of service providers
- preparation and testing of disaster recovery plans
- risk transfer through insurance

5. Monitor and Review

Digital risk is always evolving. It is essential to monitor the risk landscape continuously, and to regularly review the exposure map to ensure it remains up-to-date and relevant. A scheduled review should be conducted at least annually, in addition to impact reviews which follow major business or systems changes such as M&A activity or the implementation of major new systems infrastructure. In addition, it is essential to monitor the evolving threat by staying informed, updating risk assessments, and refining mitigation strategies.

Managing systemic cyber risk

To deal with systemic cyber risk effectively, organizations can adopt a three-step process:

- Develop a comprehensive understanding of the potential root causes of widespread cloud outage
  and malware incidents
- Identify where the root causes intersect
- Determine how the intersecting points could disrupt specific business operations

Pinpointing specific critical digital assets and evaluating individual vulnerabilities provides the basis for creation of a comprehensive exposure map. The deployment of robust mitigation strategies should be acknowledged in the map, which will highlight places where more action is needed.

The approach not only enhances resilience, but also lays the foundation for a sophisticated risk transfer framework using cyber insurance. Parametrix Analytics uses it to model and manage systemic cyber risk. We consider accumulations of cloud-related service delivery, and assess interdependencies between providers. That lets us create more accurate models which reflect the complexities of the current digital landscape.

For insurers, cloud services, including SaaS, PaaS, and IaaS, present two significant exposures:

1. Dependent Business Interruption (DBI)

Cloud-related DBI risk is analyzed by assessing criticality. How important are cloud services to the insured's delivery of their products and/or services to their customers? An online marketplace probably cannot operate without cloud services. If its payment systems go down, its operations will be severely impaired. Some entire sectors have unique, vendor-specific vulnerability profiles, because individual key service providers dominate a sector. For instance, ChangeHealthcare is crucial in the healthcare sector, and Amadeus is essential among airlines.

2. Third-Party Risk

Cloud-related TPL is analyzed by assessing data sensitivity. How much sensitive information does the service provider host or process? In many cases, it is an enormous quantity – again, as illustrated so starkly by the ChangeHealthcare cyberattack. In the event of a data breach, such exposures can subject insureds to significant third-party liability claims for compensation and damages.

Developing a comprehensive systemic cyber risk map enables organizations to not only mitigate systemic cyber risk but also transform them into strategic business advantages. Risk managers should work with their insurance broker, relevant insurers, and cyber specialists, leveraging their expertise to build resilience and unlock new opportunities.

Parametrix Cloud Stability Index

The Parametrix Cloud Stability Index **(PCSI), provides a benchmark of CSP performance for the year.** Based on the proprietary Parametrix Cloud Modeling System (PCMS), the Index assesses factors including the number of service interruption events per region, their relative severity, duration, and the broader impact of each incident.

The PCSI classifies stability into five grades, from “A” (scores of 0 to 20, representing the most stable regions) to “E” (scores of 80 to 100, reflecting the least stable regions). These scores represent relative performance during the measured period and are not projections of future risk or reflective of past years’ performance. The calculations power Parametrix’s risk modeling, product innovation, and cloud resilience consulting for clients and partners, supporting our mission to quantify and manage cloud risks.

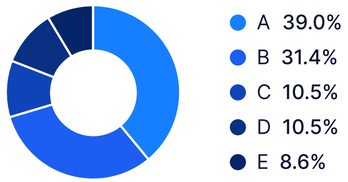


Figure 5: Market Leaders Percentage of Regions by Parametrix Cloud Stability Index Grades, 2022-2024

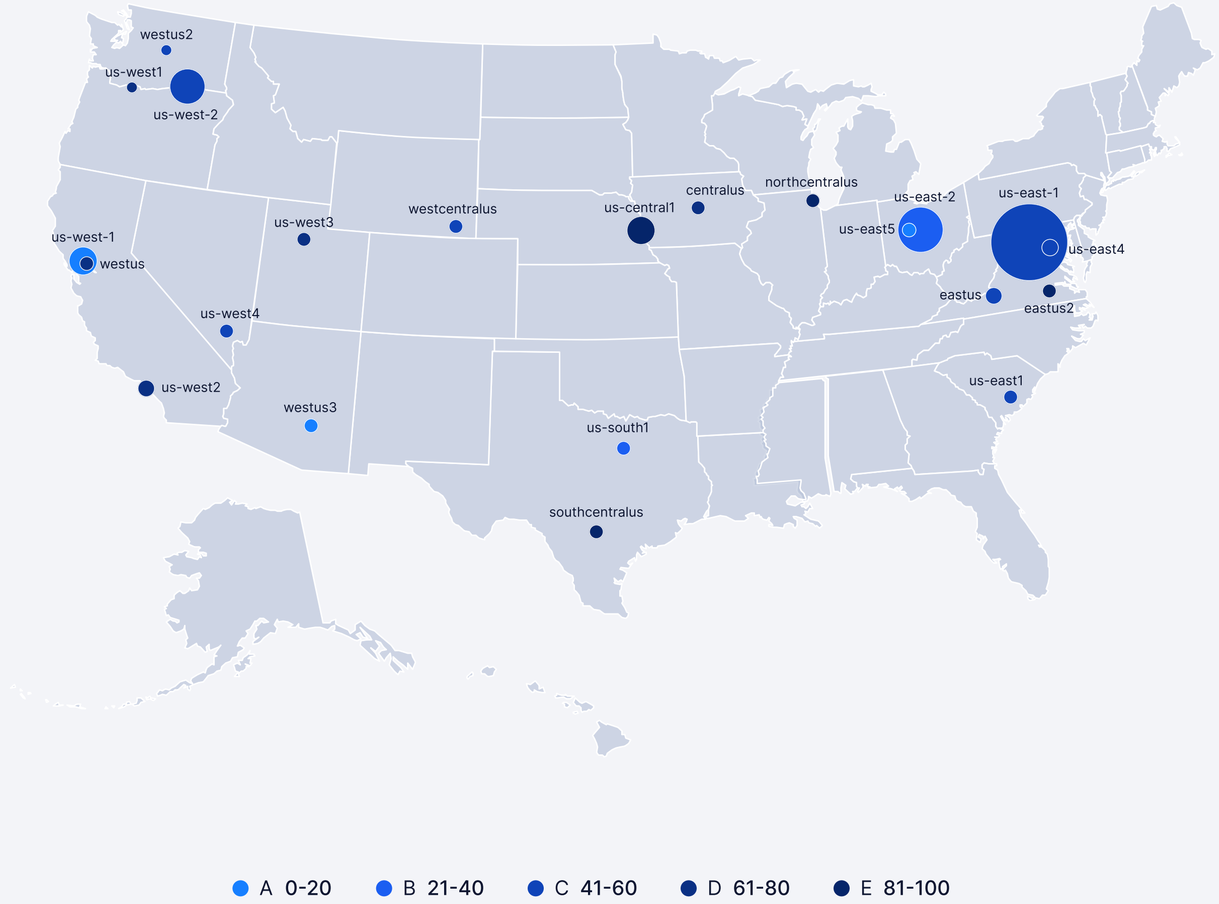


Figure 6: US Region Usage Level (Size) and Parametrix Stability Index (Color)

Event Analysis

Google Cloud

Start Date
2024-10-24

Duration
6h, 47m

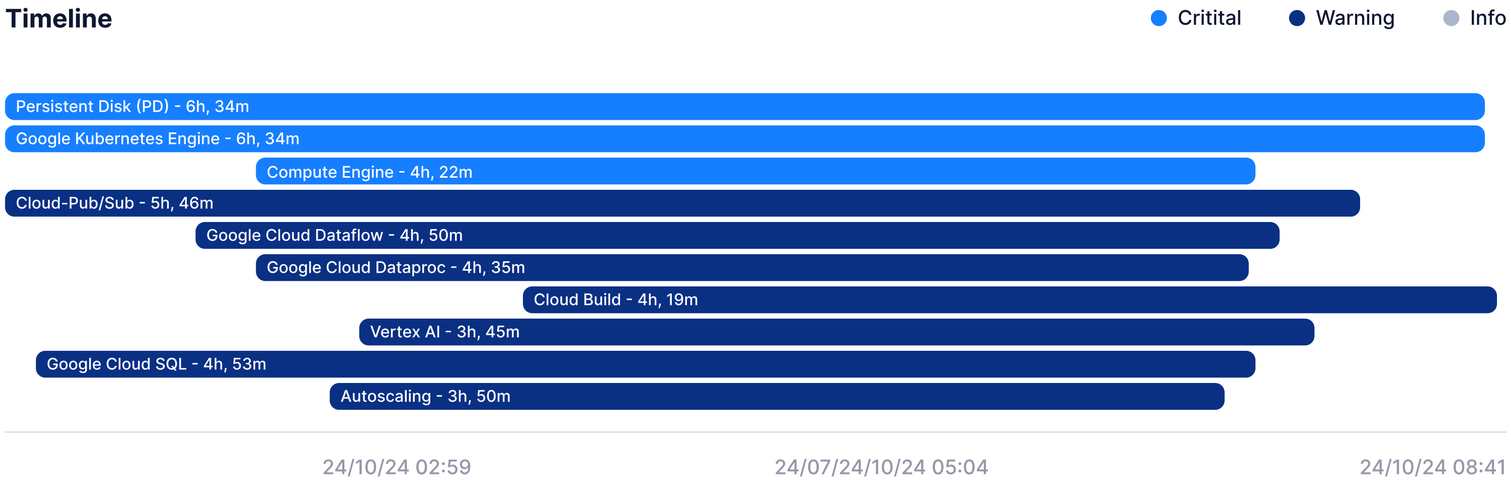
Cloud Region(s)
europe-west3 (Frankfurt)

Root Cause
Power Loss

User Impact
Compute Engine
Persistent Disk
Kubernetes Engine

On 24 October 2024, the only availability zone in Google Cloud's europe-west3 region in Frankfurt experienced a significant outage. The incident was caused by a power failure and subsequent cooling issues, leading to the shutdown of parts of the zone to prevent hardware damage. This resulted in degraded services for Compute Engine, Persistent Disk, and Kubernetes Engine, among others. This event demonstrates that even the issue in a single zone may impact services in a wider regional scope.

Timeline



Microsoft Azure

Start Date
2024-12-26

Duration
23h, 42m

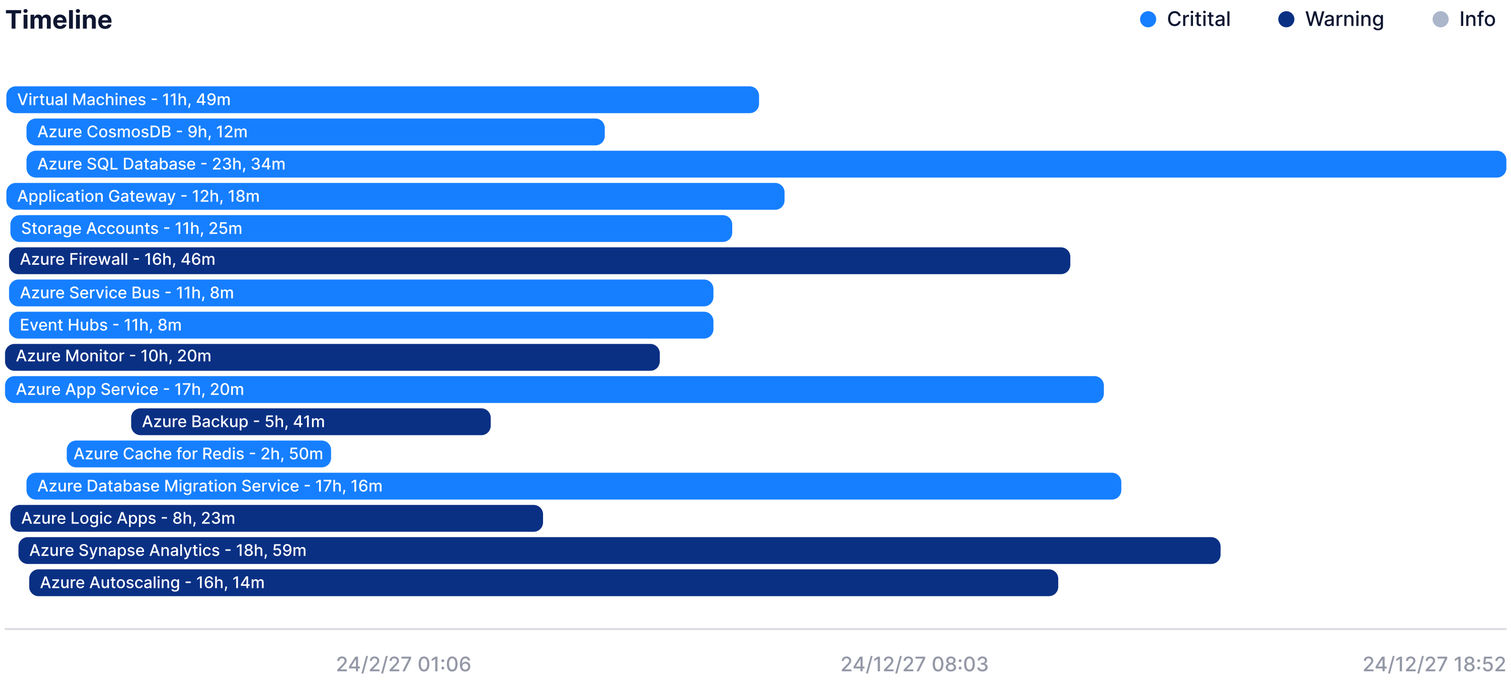
Cloud Region(s)
southcentralus (San Antonio)

Root Cause
Power Loss

User Impact
Virtual Machines
Storage
Databases
App Service
Application Gateway
Service Bus

A power loss triggered a cloud outage that disrupted Azure services, including Cosmos DB, and also affected Microsoft 365 and OpenAI in December 2024. While customers without resilience saw nearly a full day of downtime, those with resilience features in place experienced no disruption. This event highlights the critical trade off between cost and infrastructure resilience, emphasizing the importance of balancing stability with investment in cloud services.

Timeline



Amazon Web Services

Start Date
2024-07-30

Duration
6h, 47m

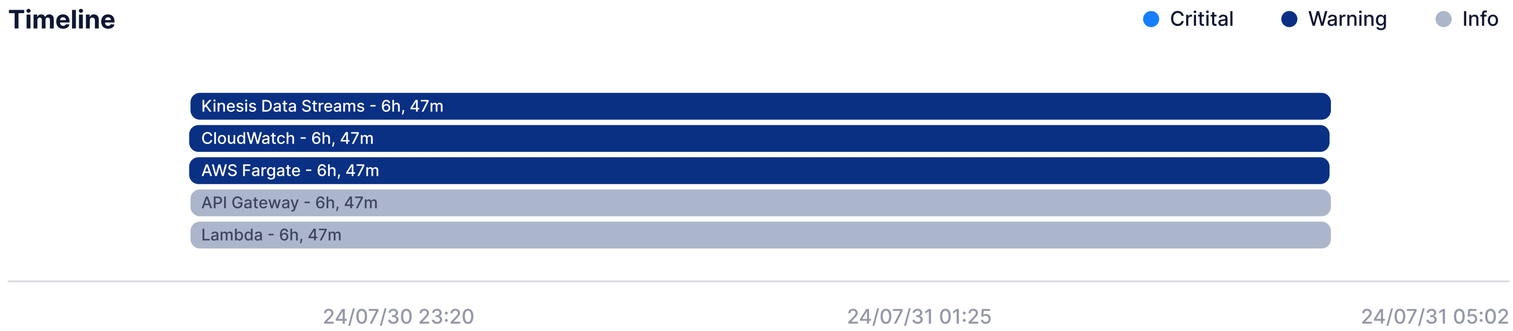
Cloud Region(s)
us-east-1 (N. Virginia)

Root Cause
Data processing issue within subsystem

User Impact
Kinesis Data Stream
CloudWatch
Fargate

On 30 July 2024, AWS experienced increased error rates and latencies for Kinesis APIs in the US-EAST-1 region, caused by increased contention in a Kinesis subsystem when processing incoming data. This issue caused downstream impacts on other services, including CloudWatch Logs (delayed log delivery and elevated errors), AWS Fargate (task launch failures), API Gateway, and Lambda (log-related errors). The mitigation efforts were initiated, though recovery progressed slower than expected. This issue demonstrates the interconnected nature of AWS services and the potential cascading effects of an underlying subsystem issue.

Timeline



parametrix

Parametrix is the leading provider of digital system interruption insurance solutions.
The company specializes in underwriting parametric insurance for digital business interruption risks, helping businesses protect against the costly impacts of downtime. Leveraging proprietary technology, Parametrix monitors and collects granular data on service performance and interruptions in order to assess risk accurately, provide instant insurance quotations, and streamline claims payments. Parametrix is a Managing General Agent and Lloyd's Coverholder whose policies are backed by major A-rated global insurers. The company is based out of New York.

www.parametrixinsurance.com

parametrix-insurance

info@parametrixinsurance.com