Enterprise Strategy Group™

The Hidden Cost of Cloud Complexity: How Automatic Rebuilds Save Time, Money, and Sanity

Torsten Volk | Principal Analyst

ENTERPRISE STRATEGY GROUP

MAY 2025

This eBook from Enterprise Strategy Group was commissioned by Commvault and is distributed under license by TechTarget,Inc.

Research Objectives

This research explores how organizations are evolving beyond traditional backup and recovery approaches to address the growing complexity of cloud-native applications. As configuration drift becomes increasingly problematic (affecting 82% of organizations), the distinction between simple restores and complete rebuilds has emerged as a critical consideration for maintaining business continuity. This study examines why IT leaders are now prioritizing rebuild capabilities as part of their resilience strategy, how rebuild processes differ from conventional recovery methods, and the significant resource implications these differences create for teams managing business-critical cloud applications.

THIS STUDY SOUGHT TO:

- **Assess** how organizations manage and rebuild cloud applications after outages, specifically measuring recovery timelines, IT resource allocation, and business impacts.
- **Understand** the operational and business challenges associated with cloud application rebuilds, focusing on the differences in tools, processes, and recovery strategies between multi-cloud environments and different application architectures.
- **Explore** the challenges, timelines, and resource requirements organizations face when rebuilding modern cloud applications after outages or security incidents.
- **Determine** the organizational structures, technological approaches, and resource requirements companies need for effectively restoring modern cloud applications.

Key Findings

Resource-intensive Disruptive Rebuilds: 40.6 Person-days per Incident

On average, organizations require 40.6 person-days to restore core functionality during complete rebuilds, with 41% reporting these incidents disrupt strategic initiatives.

PAGE 4

Enterprise Adoption: 47% of New Apps Are Cloud-native

Nearly half of all enterprise application development is now cloud-native, creating a hybrid reality where organizations must manage both modern and traditional architectures.

PAGE 9

Critical Configuration Drift: 82% Reported Problematic Changes

The dynamic nature of cloud environments creates significant configuration drift issues, with 82% of organizations reporting problematic levels of change that undermine recovery capabilities.

PAGE 12

Unified Protection Gap: 87% Want Cross-cloud Consistency

While 87% of organizations considered consistent resilience tools across cloud platforms critical or important, nearly 90% struggled with substantial variability in their current protection tools.

PAGE 15

Recovery Complexity Challenge: 49% Found Legacy Apps Easier

Organizations are nearly twice as likely to view backup and recovery as easier for legacy applications compared to cloud-native applications (49% vs. 26%), highlighting the technical challenges of microservices architectures.

PAGE 20

BACK TO CONTENTS

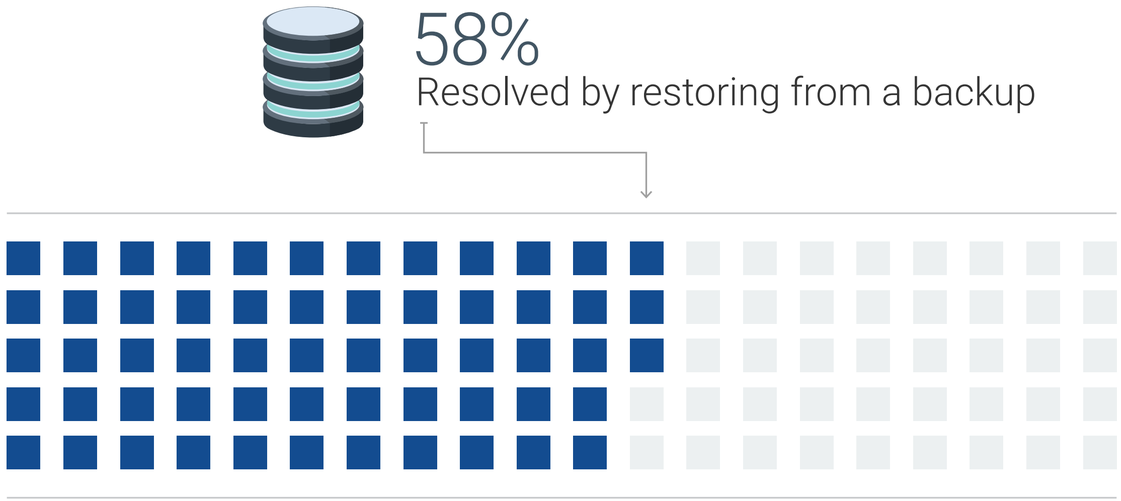
Resource-intensive Disruptive Rebuilds: 40.6 Person-days per Incident

On average, organizations require 40.6 person-days to restore core functionality during complete rebuilds of cloud applications, with 41% reporting these incidents disrupt strategic initiatives.

The Hidden Cost of Cloud Outages: Sacrificing Tomorrow's Innovation

The fact that, when disaster strikes, 42% of cloud application failures require a complete rebuild rather than simple backup illustrates the universal character of cloud-native resilience challenges. Infrastructure and network reconfiguration, application architecture mapping, code deployment and business logic restoration, and testing and validation of the entire restored application are substantial tasks that require significant time and manpower. By definition, resources used for rebuilding existing applications are unavailable for innovation, feature development, and other strategic initiatives that drive business growth. This creates a zero-sum scenario where operational recovery directly impedes digital transformation, creating an increasingly difficult tradeoff for organizations already struggling to balance maintenance with innovation.

Roughly what percentage of modern cloud app outages could be resolved by restoring from a backup vs. a complete rebuild?

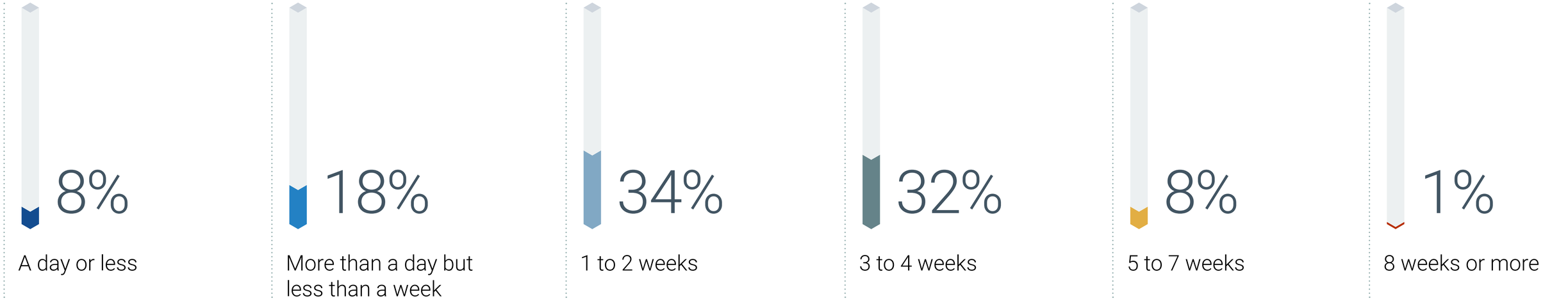


BACK TO CONTENTS

The Heavy Operational Burden of Cloud Application Rebuilds

Modern cloud application rebuilds extract a substantial operational toll from enterprise technology teams. On average, organizations require 40.6 person-days to restore core functionality during complete rebuilds. This significant resource allocation typically involves four or five specialized personnel (41% of cases) dedicating 50% to 74% of their productive capacity (62% of cases) over extended periods.

Approximately how much time do you think it would take your organization to reestablish core functionality when rebuilding a modern cloud application from scratch?



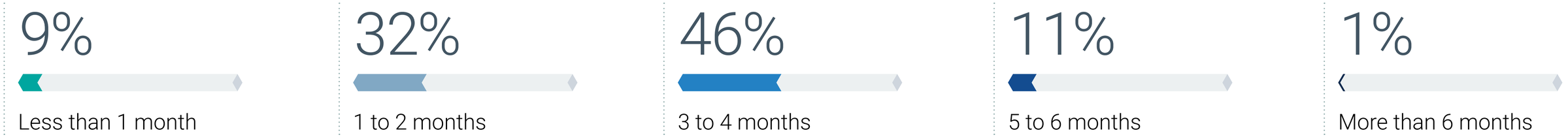
BACK TO CONTENTS

Financial Impact

For a typical organization experiencing ~9 complete rebuilds annually (out of ~21 total outages), the operational cost is substantial. At an average daily rate of $577 per specialist, these rebuilds represent approximately $210,836 in annual labor costs diverted from strategic initiatives to recovery efforts.

As cloud-native adoption accelerates, this operational tax represents a growing challenge for organizations pursuing digital transformation initiatives while maintaining business continuity commitments. With over 66% of organizations requiring at least a week to restore core functionality—and 78% needing more than a month for complete environment restoration—the business impact extends well beyond the immediate financial burden.

Approximately how much time do you think it would take your organization to reestablish the complete production environment when rebuilding a modern cloud application from scratch?



BACK TO CONTENTS

The Expanding Business Impact of Application Rebuilds

Application rebuild events create ripple effects far beyond immediate technical challenges, causing substantial business disruption. In fact, 41% of organizations expected to face disruption of strategic initiatives during rebuild periods, while 36% expected to experience direct revenue losses and 34% reported expecting negative customer experience impacts.

What business challenges would your organization expect to encounter during the application rebuild process for a business-critical modern cloud application?

49%
Increased stress on staff

41%
Disruption of strategic initiatives

36%
Revenue loss

35%
Customer churn

34%
Decreased customer satisfaction

33%
Loss of productivity by employee users

32%
Damage to brand

5%
None of the above

BACK TO CONTENTS

Enterprise Adoption: 47% of New Apps Are Cloud-native

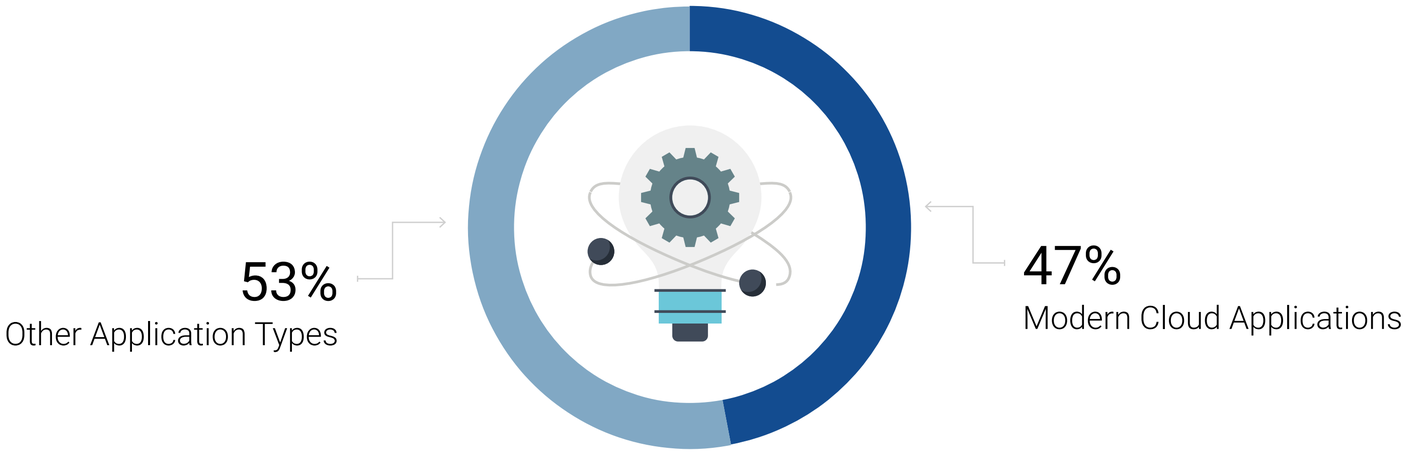
Nearly half of all enterprise application development is now cloud-native, creating a hybrid reality where organizations must manage both modern and traditional architectures.

Hybrid Environments Are the New Normal

Nearly half of all enterprise application development projects (47%) are now built on cloud-native principles. These apps ditch the traditional, monolithic code base in favor of loosely connected microservices—each of which could be owned by a different team, use its own specific tech stack, and follow its own release cadence.

Some of these microservices are built in-house, with others sourced from third-party vendors. This distributed architecture makes it easier to iterate fast and scale as needed, but it also introduces significant operational complexity, especially when the remaining applications still run on traditional, mostly monolithic architectures. This makes hybrid environments the new normal and highlights why it is so critical for organizations to have an operations strategy that spans both worlds.

Approximately what percentage of all your organization's application development projects today would you classify as modern cloud applications?



47%
of application development projects are cloud-native.

BACK TO CONTENTS

Cloud-native Means Business Critical

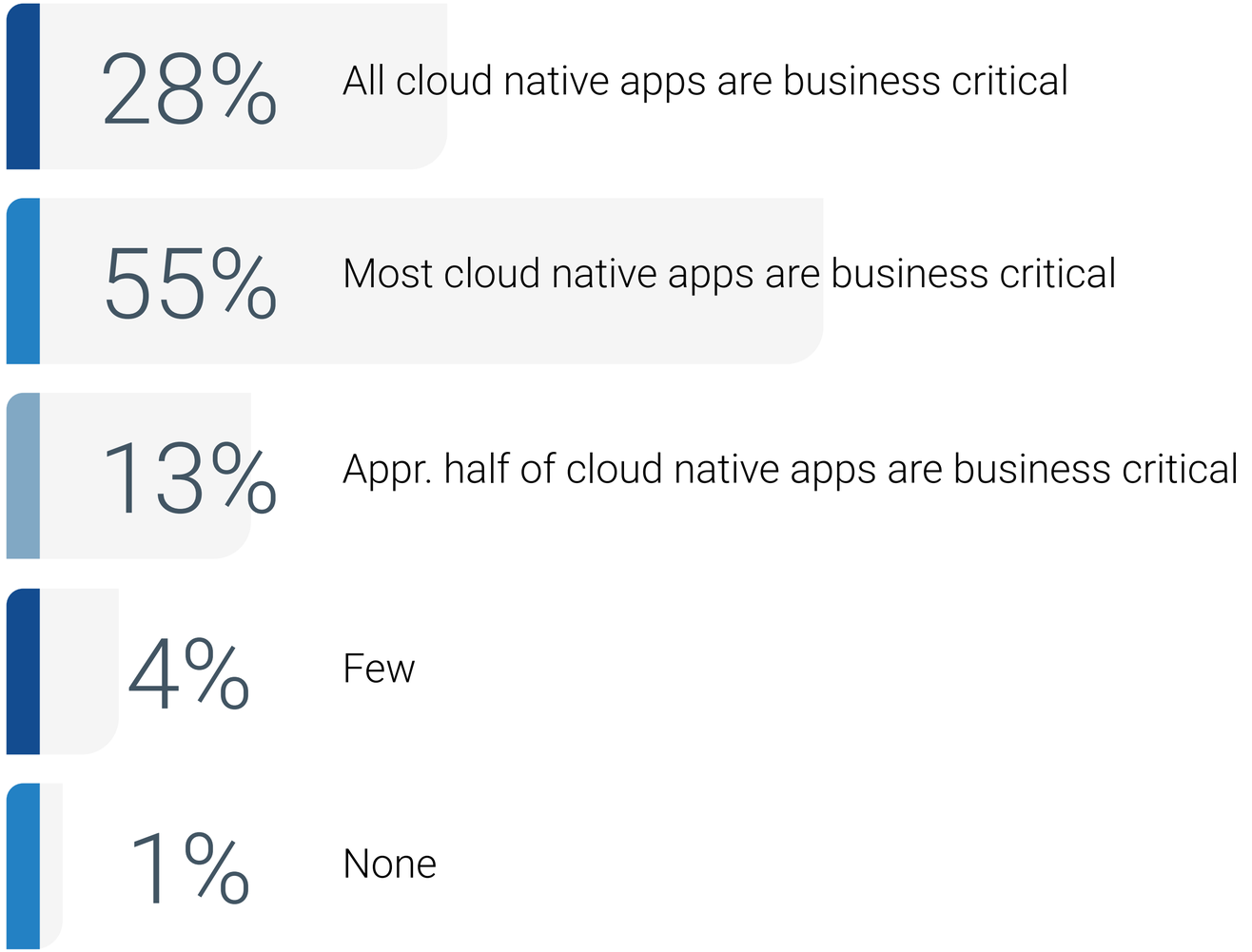
As development teams rapidly adopt cloud-native application architectures, organizations deem most of the resulting applications as business critical (~83%), with 28% of these organizations labeling all their cloud-native apps as essential to their business.

This high level of importance is underlined by 76% of organizations pushing code updates to cloud-native apps multiple times per week or more. This demonstrates that organizations are leveraging the advantages of cloud-native agility to quickly and continuously deliver business value based on changes in market demand.

~83%

say most or all cloud-native applications are business critical.

Approximately what proportion of your organization's modern cloud applications would you describe as business critical?

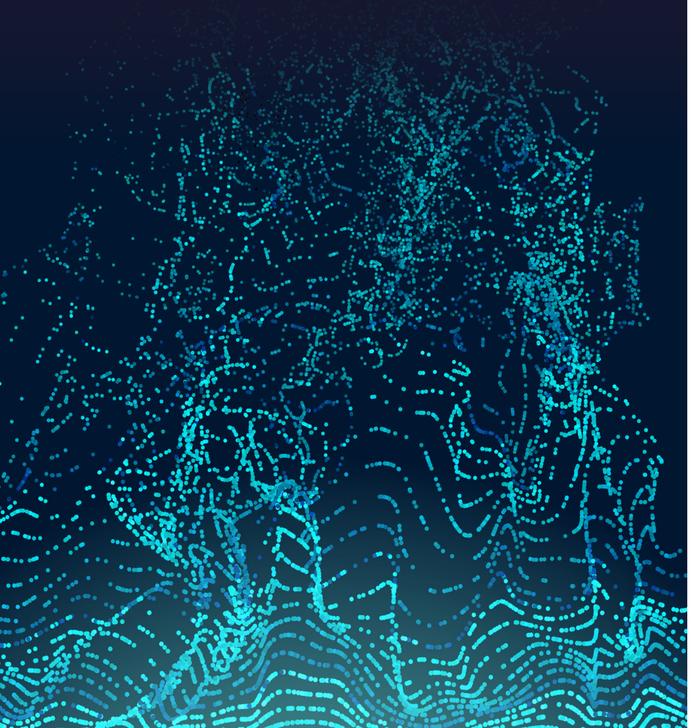


BACK TO CONTENTS

Critical Configuration Drift: 82% Reported Problematic Changes

The dynamic nature of cloud environments creates significant configuration drift issues, with 82% of organizations reporting problematic levels of change that undermine recovery capabilities.

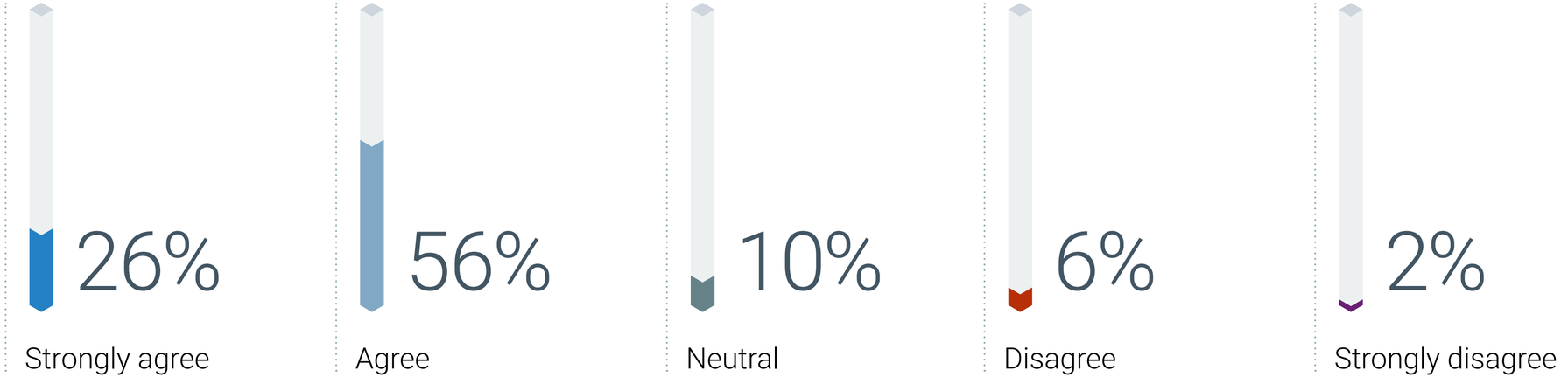
82% agreed: Configuration drift is a real problem



Configuration Drift Rears Its Ugly Head

Configuration drift is turning into a major operational headache for organizations going cloud-native. Eighty-two percent of teams said they are seeing it escalate to problematic levels across their modern cloud application stacks. This is due to cloud-native applications being composed of loosely coupled microservices, each of which constitutes a potential entry point for configuration changes that can adversely affect the resilience of the overall application. The process of validating the functionality of dozens of interconnected microservices, ensuring state consistency across data stores, and verifying network connectivity alone is a significant challenge.

Agree or disagree: The dynamic nature of our modern cloud applications creates a problematic level of configuration drift in our environments.



BACK TO CONTENTS

Configuration Drift Brings Hidden Risk

Configuration drift directly impacts the ability of organizations to recover applications from backup. Sixty-nine percent of respondents acknowledged that configuration drift is actively undermining their digital resilience posture.

The primary mechanism of this impact is the misalignment between production environments and backed-up states, creating significant recovery risk. When production configurations evolve independently from their backed-up counterparts, organizations face potentially extended recovery times or, in worst-case scenarios, failed recovery attempts that could lead to data loss or prolonged service disruptions.

Percentage of organizations that regularly encounter complications in digital resilience posture as a result of configuration drift:

Configuration drift **weakens digital resilience**

BACK TO CONTENTS

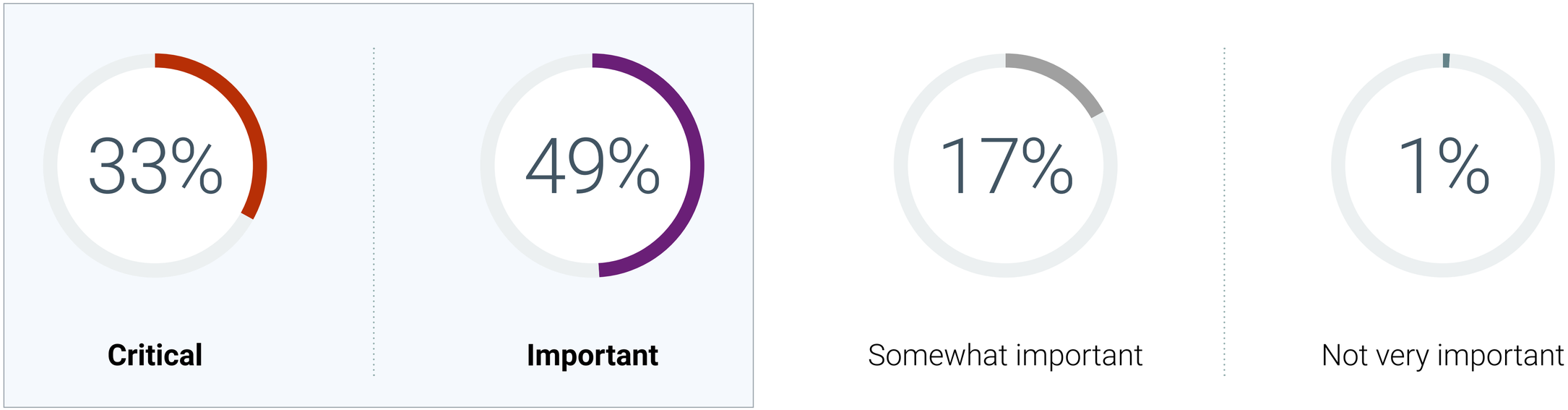
Unified Protection Gap: 87% Want Cross-cloud Consistency

While 87% of organizations considered consistent resilience tools across cloud platforms critical or important, nearly 90% struggled with substantial variability in their current protection tools.

Unified Protection Is Key

Eighty-two percent of respondents found it critical or important to have a common set of tools for backup and recovery of cloud-native and traditional applications. This strong preference reflects enterprise technology leaders' understanding that fragmented protection approaches increase operational complexity, elevate risk profiles, and create recovery blind spots across increasingly heterogeneous application portfolios. This becomes even more important for application environments consisting of a heterogenous mix of cloud-native and traditional applications.

When you think of digital resilience technologies (tools for backup, recovery, etc.), how important is consistency in tools and functionality across application types?



BACK TO CONTENTS

The Strategic Imperative for Cross-cloud Resilience

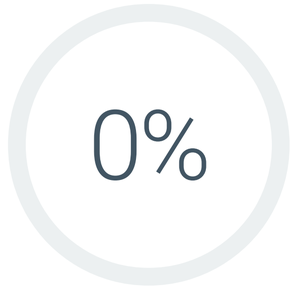
Enterprise technology leaders overwhelmingly recognize the strategic value of standardized protection approaches across heterogeneous cloud environments. Eighty-seven percent of organizations considered consistent resilience tools across cloud platforms either critical or important. This strong consensus reflects the operational reality of multi-cloud adoption, with 90% of surveyed organizations utilizing two or more cloud providers. As cloud-native architectures accelerate toward majority status, this preference underscores technology leaders' understanding that fragmented protection approaches create operational complexity, security vulnerabilities, and potential recovery blind spots that could compromise business continuity during critical incidents.

When you think of digital resilience technologies (tools for backup, recovery, etc.), how important is consistency in tools and functionality across cloud environments?

Critical

Important

Somewhat important



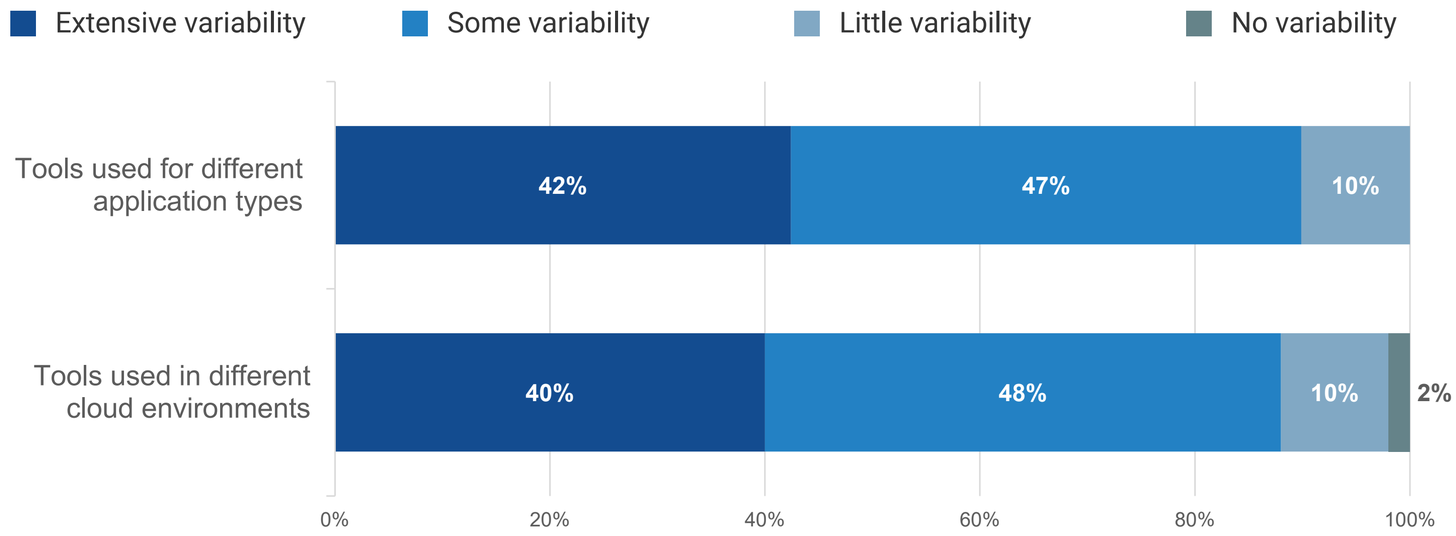
Not very important

BACK TO CONTENTS

The Implementation Reality Gap

The clear strategic preference for consistent recovery operations of cloud-native and traditional applications is not reflected in current implementation practices. Nearly 90% of surveyed organizations acknowledged substantial variability in the protection tools currently deployed across different application types and cloud environments. This fragmentation creates operational inefficiencies, specialized skill requirements, and potential resilience gaps. The disconnect between the recognized importance of tool consistency and today's fragmented implementation landscape represents a critical focus area for enterprise technology leaders pursuing comprehensive digital resilience strategies.

When invoking a complete application rebuild from scratch, how much variability exists (or would exist) in each of the following?



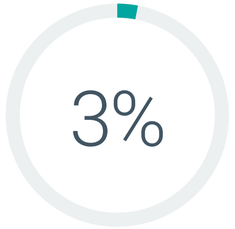
BACK TO CONTENTS

Forty-seven percent of organizations have implemented a bifurcated responsibility model, with separate teams managing on-premises applications and cloud environments.

The Operational Divide in Digital Resilience

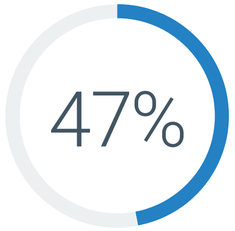
In today's enterprise technology landscape, a significant organizational pattern has emerged in how companies structure their digital resilience functions: 47% of organizations have implemented a bifurcated responsibility model, with separate teams managing on-premises applications and cloud environments. This reflects the technical and operational differences between traditional infrastructure and cloud-native architectures and creates potential coordination challenges across increasingly hybrid application portfolios.

Which of the following best describes your organization's structure for protecting and backing up cloud-hosted and on-premises applications?



Decentralized approach where individual teams are responsible for protecting and backing up their own applications

Separate teams manage on-premises applications and applications for each cloud provider (e.g., a different team for AWS, Azure, and GCP)



Separate teams manage on-premises applications and cloud applications (cloud workloads managed as a single group)

One team manages both on-premises and cloud applications across all providers

BACK TO CONTENTS

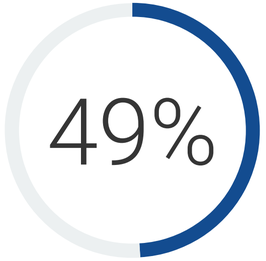
Recovery Complexity Challenge: 49% Found Legacy Apps Easier

Organizations are nearly twice as likely to view backup and recovery as easier for legacy applications compared to cloud-native applications (49% vs. 26%), highlighting the technical challenges of microservices architectures.

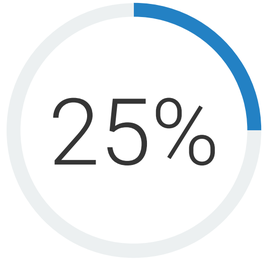
The Backup Complexity Divide: Legacy vs. Modern Cloud Applications

Organizations are nearly twice as likely to view backup and recovery strategies as easier to implement for legacy applications compared to modern cloud applications (49% vs. 26%). This striking disparity highlights how the dynamic, distributed nature of cloud-native architectures creates substantial resilience challenges despite their innovation advantages. The technical fragmentation, ephemeral components, and configuration drift inherent in modern architectures directly impact organizations' ability to establish consistent, reliable protection strategies across their application portfolios.

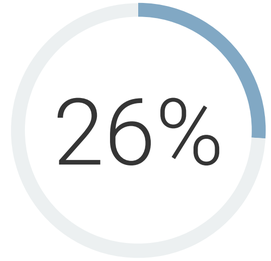
How would you compare the difficulty of developing and implementing an effective backup and recovery strategy for modern cloud applications vs. monolithic applications?



Easier for monolithic applications

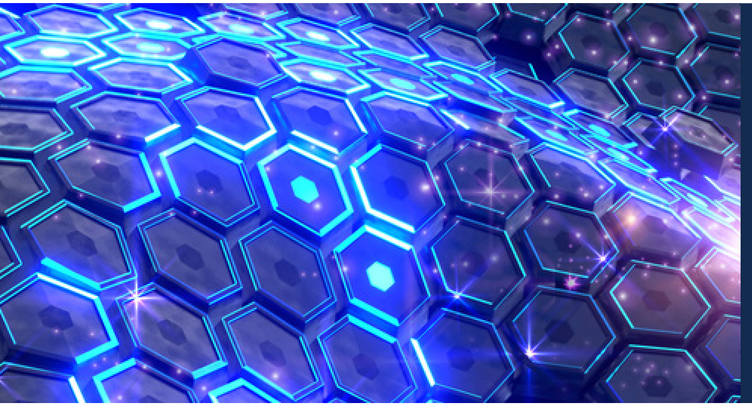


No perceived difference in difficulty



Easier for modern cloud applications

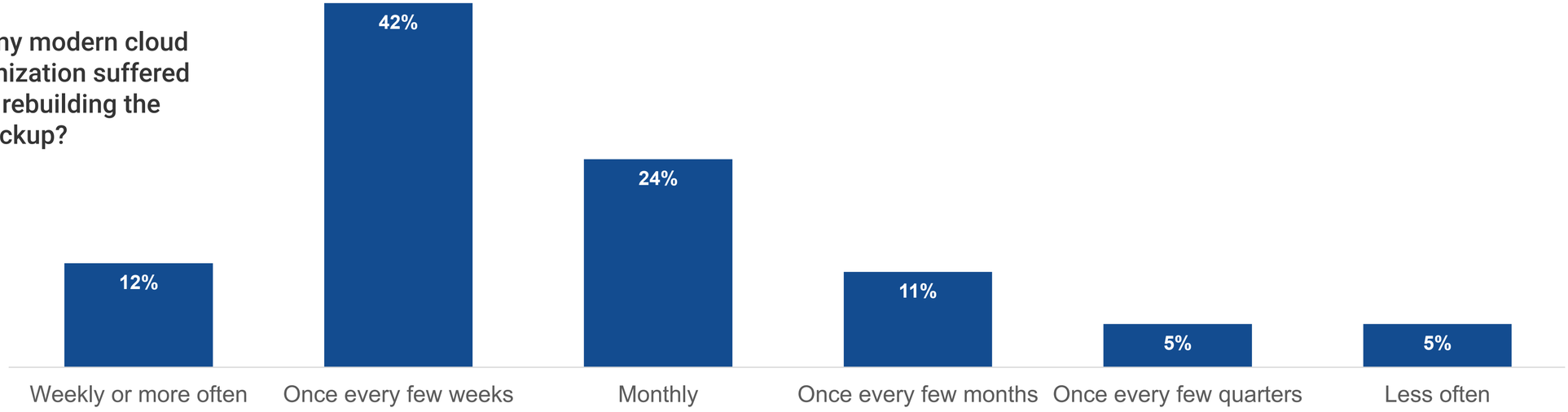
BACK TO CONTENTS



Cloud Application Outages Are the Rule, Not the Exception

Fifty-four percent of organizations reported experiencing cloud-native application outages every few weeks or even more frequently. In addition to their potential impact on revenue and reputation, these outages can place a significant strain on internal resources due to the complex and often resource-intensive rebuild process they trigger.

Over the past year, how often has any modern cloud application supported by your organization suffered from an outage that required either rebuilding the application or restoring it from a backup?



BACK TO CONTENTS

Commvault®

ABOUT

As the research shows, it takes time (40.6 days) to rebuild complex cloud-based applications completely, costing companies more than $200K annually in labor cost alone, never mind the reputational damage and lost revenue every time there's an outage. Being able to quickly get back to a minimal viable operating state is imperative.

Commvault can help.

Commvault is the gold standard in cyber resilience, helping more than 100,000 organizations keep data safe and businesses resilient and moving forward. Today, Commvault offers the only cyber resilience platform that combines the best data security and rapid recovery at enterprise scale across any workload, anywhere—at the lowest TCO.

Make your cloud data visible, recoverable, and resilient—across your workloads—all on a single pane of glass. Learn how Commvault solutions like Cloud Rewind can help you maintain continuous business operations.

LEARN MORE

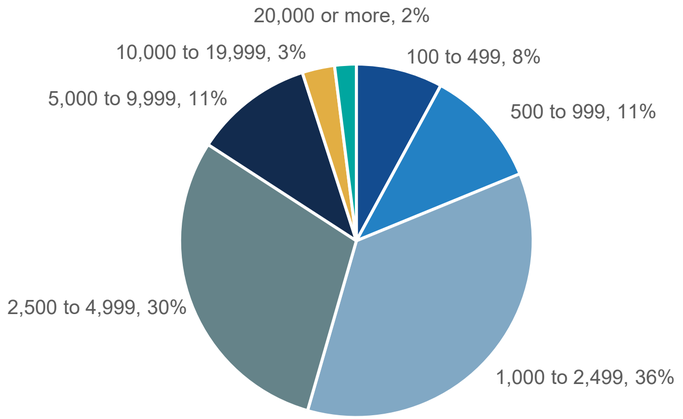
RESEARCH METHODOLOGY AND DEMOGRAPHICS

To gather data for this report, Commvault commissioned Enterprise Strategy Group to conduct a comprehensive online survey of IT (N=205) and application development (N=295) professionals from private- and public-sector organizations in North America (U.S. [N=150], Canada [N=25]), Western Europe (UK [N=75], Germany [N=50], France [N=50]), and the Asia-Pacific region (Australia [N=49], New Zealand [N=26], Singapore [N=75]) between January 21, 2025 and February 4, 2025. To qualify for this survey, respondents were required to be knowledgeable about application development and deployment processes at their organization as well as the solutions in place to ensure the resilience of internally developed applications. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

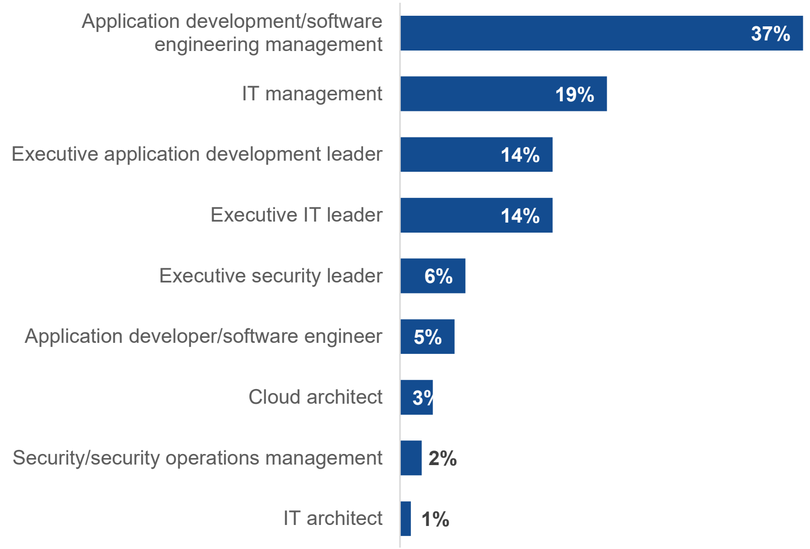
After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 500 respondents. The margin of error for a sample of this size is + or – 4 percentage points.

Note: Totals in figures and tables throughout this eBook may not add up to 100% due to rounding or organizations choosing more than one answer to select questions.

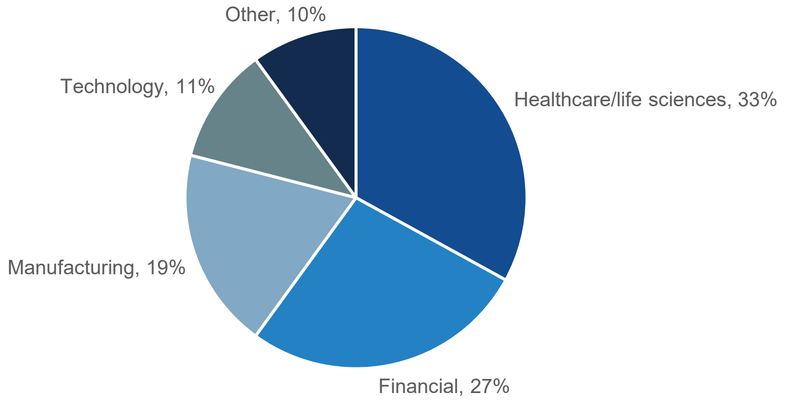
Respondents by Number of Employees



Respondents by Job Title



Respondents by Industry



BACK TO CONTENTS

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.