

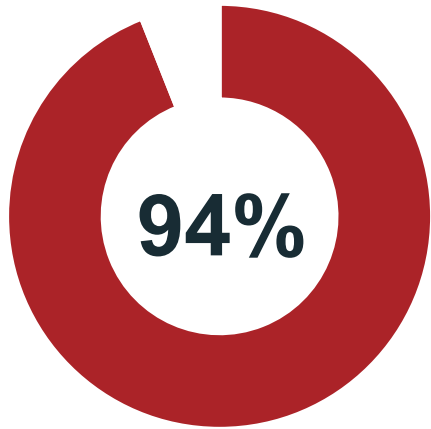
A nighttime cityscape with a network overlay of blue lines and dots. The city lights are visible in the background, and the network overlay is in the foreground. The text is overlaid on a red shape on the right side of the image.

VERITAS™

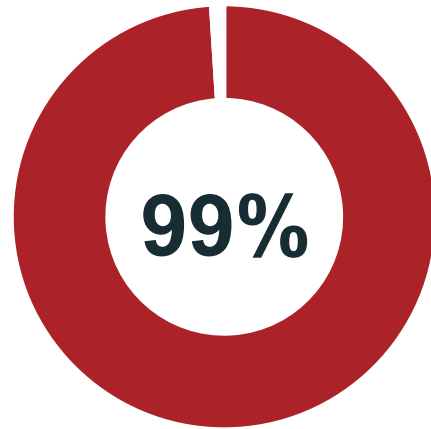
Securing Your Enterprise in a Multi- Cloud Environment Report

Cloud Overages Deep Dive

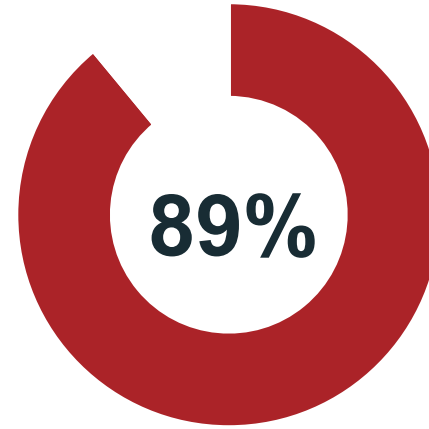
Overview of key findings



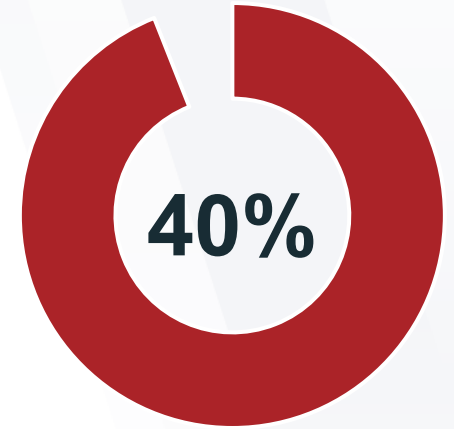
The vast majority of enterprises fail to stay within their cloud budgets.



That is in part because nearly all organizations incorrectly assume cloud service providers (CSPs) are responsible for protecting their assets in the cloud.



When they face ransomware attacks on their cloud data, which nine out of 10 organizations have, they realize they need more than the CSP-provided tools.

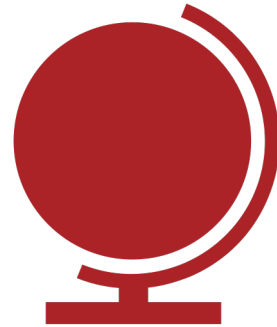


Failing to budget for proper data protection results in it being the most common source of unexpected cloud costs.

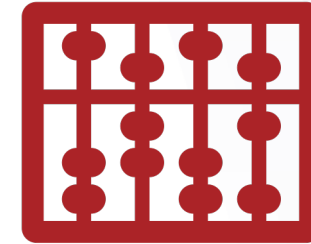
Methodology



Independent research
sponsored by Veritas
and carried out by
VansonBourne in
August and
September 2022.



Global scope
with respondents from
Australia, Brazil, China,
France, Germany, India
Japan, Singapore,
South Korea, UAE, UK
and the US.



1,500 respondents
in technology and IT
decision-maker roles.

A nighttime cityscape with a network overlay of blue lines and dots. The city lights are visible in the background, and the network lines are overlaid on the scene. A red shape is on the right side of the image.

Key Findings

The vast majority of enterprises fail to stay within their cloud budgets.



94%

of respondents reported that their organizations have incurred higher costs than originally anticipated when using a public CSP.

Those that overspent did so by an average of



43%

That is in part because nearly all organizations incorrectly assume CSPs are responsible for protecting their assets in the cloud.

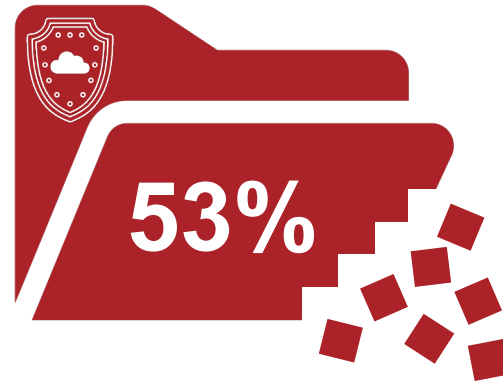


of respondents believed that their CSPs would be responsible for protecting some of their assets in the cloud. This is rarely the case as most CSPs make it very clear that while they are on the line to ensure the resiliency **of** their cloud, customers shoulder the responsibility for their data and applications **in** the cloud.

When they face ransomware attacks on their cloud data, they realize they need more than the CSP-provided tools for data protection.



of respondents said that their organizations have experienced ransomware attacks on their cloud environments.



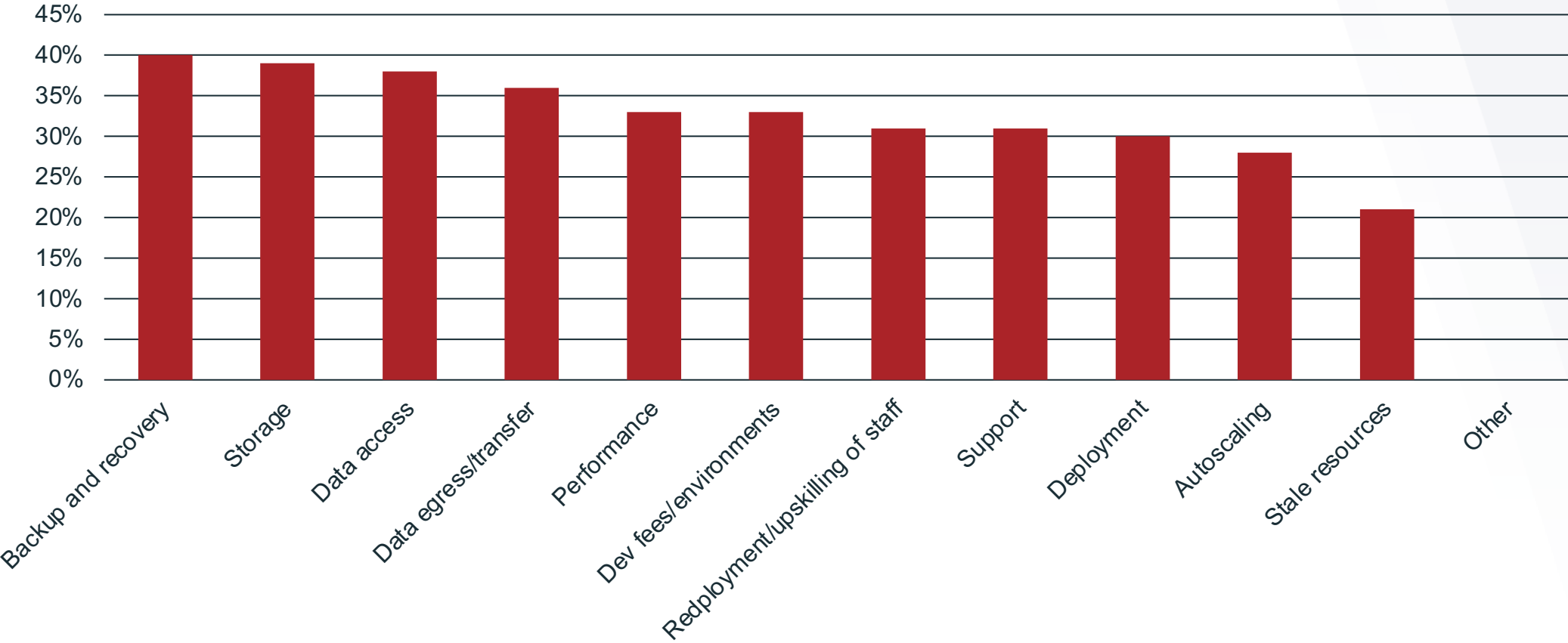
of respondents have lost data as a result of relying solely on backup tools built into solutions by their CSPs.



of respondents agreed that current offerings from CSPs fall short of their organizations' security needs.

Failing to budget for proper data protection results in it being the most common source of unexpected cloud costs.

In what areas did your organization experience additional costs when using a public cloud service provider?





Conclusion

Enterprises reap significant benefits from the cloud, but this research highlights the need for a better understanding of what organizations are actually buying from CSPs.

It is understandable to not budget for something that they think they are getting for free. However, by the time that IT leaders realize that there is something that they have overlooked, it is common that they have already lost data.

Therefore, if enterprises want to avoid asking for additional budget to cover cloud overspend, it is critical to factor in data protection right the start.



A nighttime cityscape with a network overlay. The city is illuminated with various lights, and a network of blue lines and dots is overlaid on the scene, suggesting a digital or data network. The city features a mix of modern and traditional architecture, with a prominent bridge in the background.

VERITAS™

Copyright © 2022 Veritas Technologies, LLC. All rights reserved.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.