2016 Private Cloud Resiliency Benchmarks

Based on exclusive data collected from over 100 enterprise cloud environments

Published by

CONTINUITY SOFTWARE

A first-of-a-kind analysis of private cloud resiliency

For the first time ever, we have a comprehensive set of data about private cloud resiliency, collected through automated scans of more than 100 enterprise environments performed over the past year.

The data shows there is room for concern. Most notably, downtime and security risks were found in each and every cloud environment tested; most of them had multiple downtime risks. A vast majority (82%) also had data loss risks.

This may not come as a surprise to those familiar with the inner workings of enterprise cloud infrastructure. With a growing level of the complexity, increasing interdependence among infrastructure components, and an escalating pace of change, keeping cloud infrastructure free of risky misconfiguration is becoming a challenge that most organizations fail to meet.

Unfortunately, these results are consistent with the reality we are experiencing across a wide range of industries and services.

In recent months, widespread and long-lasting infrastructure outages have grounded thousands flights and stranded hundreds of thousands of airline passengers in the United States; left millions of customers without telecommunication services in Australia; and withheld payments to scores of merchants worldwide.

But there is also good news in this report. The good news is that most risks lurking in the cloud infrastructure can be identified and corrected before they turn into a service disruption. Doing that requires a specialized set of processes and tools, but above all a mindset and strategy focused on early detection and remediation of risks.

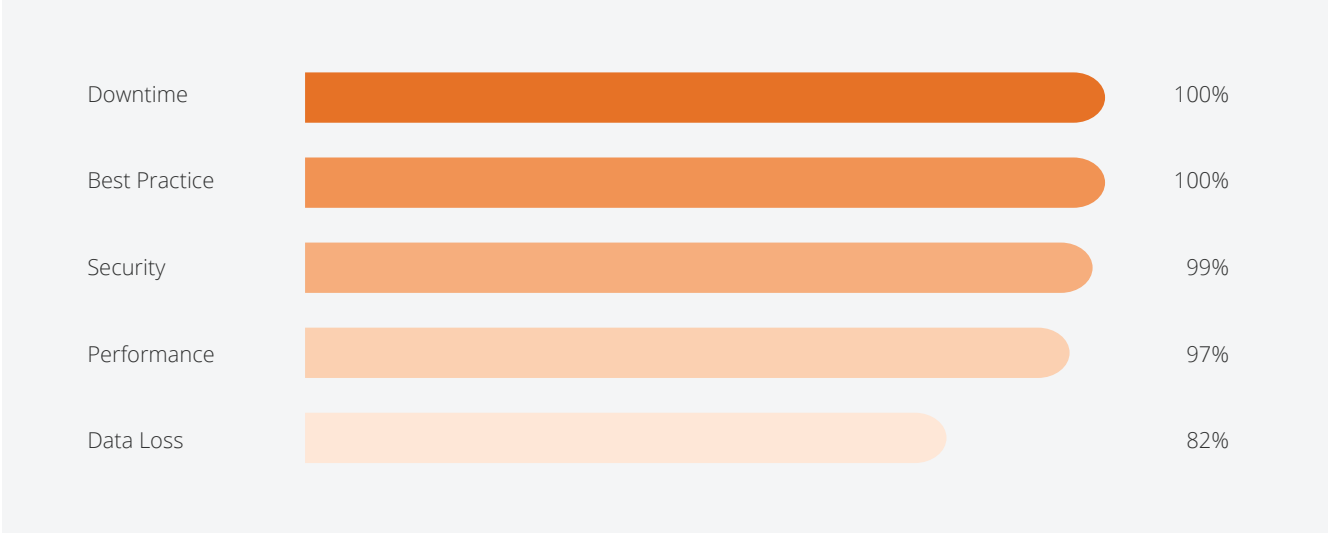
Following are some additional details based on the data uncovered in these private cloud infrastructure scans.

Risks Are Widespread

DOWNTIME RISKS WERE FOUND IN EVERY ENVIRONMENT TESTED

Downtime risks were found in every environment tested, and security and performance risks were found in **99%** and **97%** of the environments respectively.
As many as **82%** of the environments tested had some data loss risks as well.

Risk Impact Per Environment



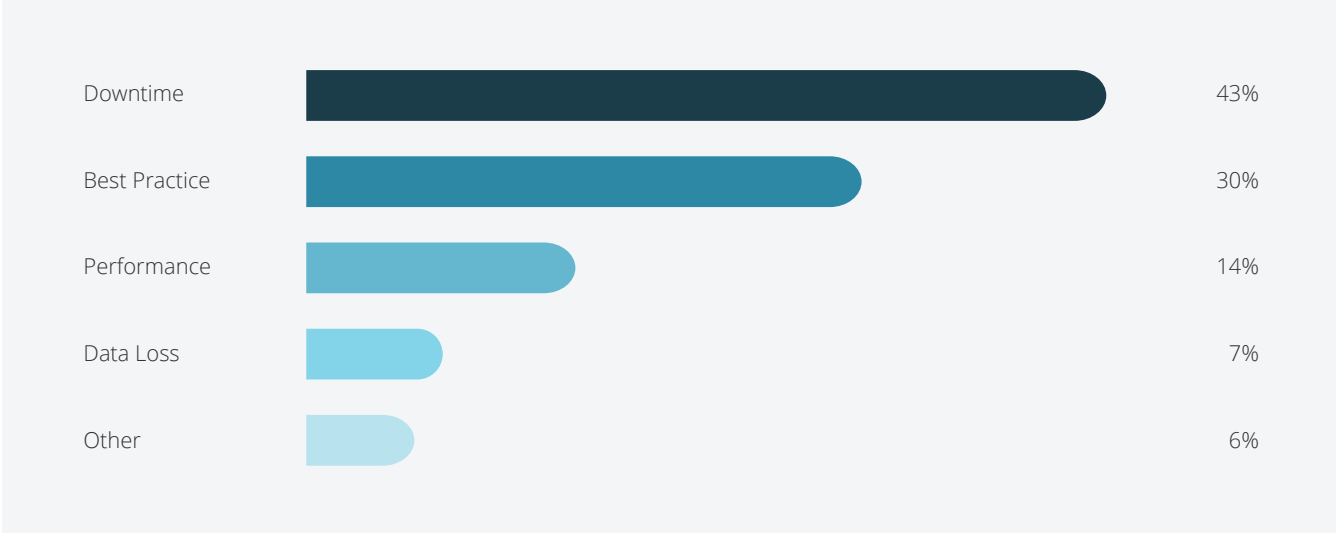
In how many of the environments did we find such risks?

Downtime Risks Are Most Common

DOWNTIME IS THE TOP RISK

Downtime is the top risk. **43%** of all risks detected are related to downtime, followed by best practices (**30%**), performance (**14%**) and data loss (**7%**).

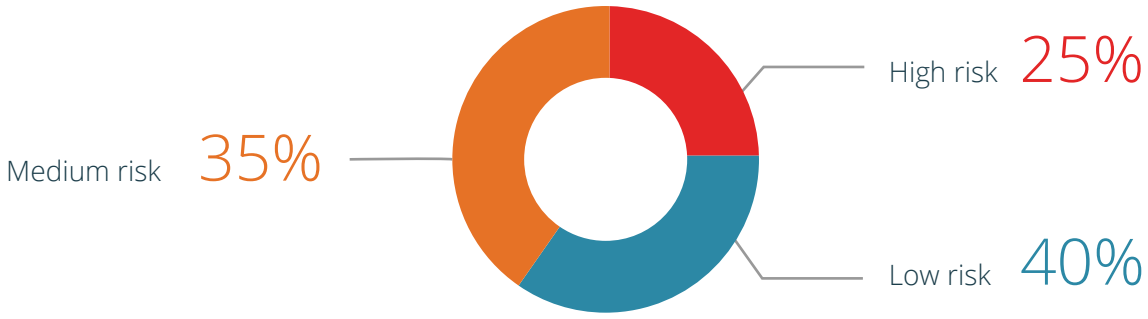
Risk Breakdown by Impact



Percentage of risks found across all scanned environments

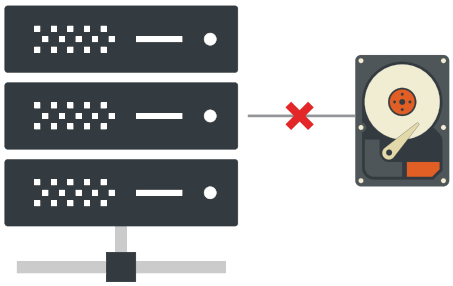
RISK BREAKDOWN BY SEVERITY

25% of the risks detected were defined as high level risks, 35% medium, and 40% are defined as low risk.



Top Risks

SOME OF THE TOP RISKS IDENTIFIED ACROSS THESE ENVIRONMENTS INCLUDE:



Configuration drifts between cluster nodes that will prevent HA failover. Examples for such discrepancies range from the most trivial – e.g., CD-ROM ISO file left mounted on a VM, but not accessible to all hosts in the cluster – to more complex ones – such as incorrect settings of affinity rules.

Virtual networking configuration errors that lead to VM isolation and downtime.
Examples include incorrect Virtual Machine Port Group configurations and resources misalignment between ESXi cluster hosts leading to a single point of failure.

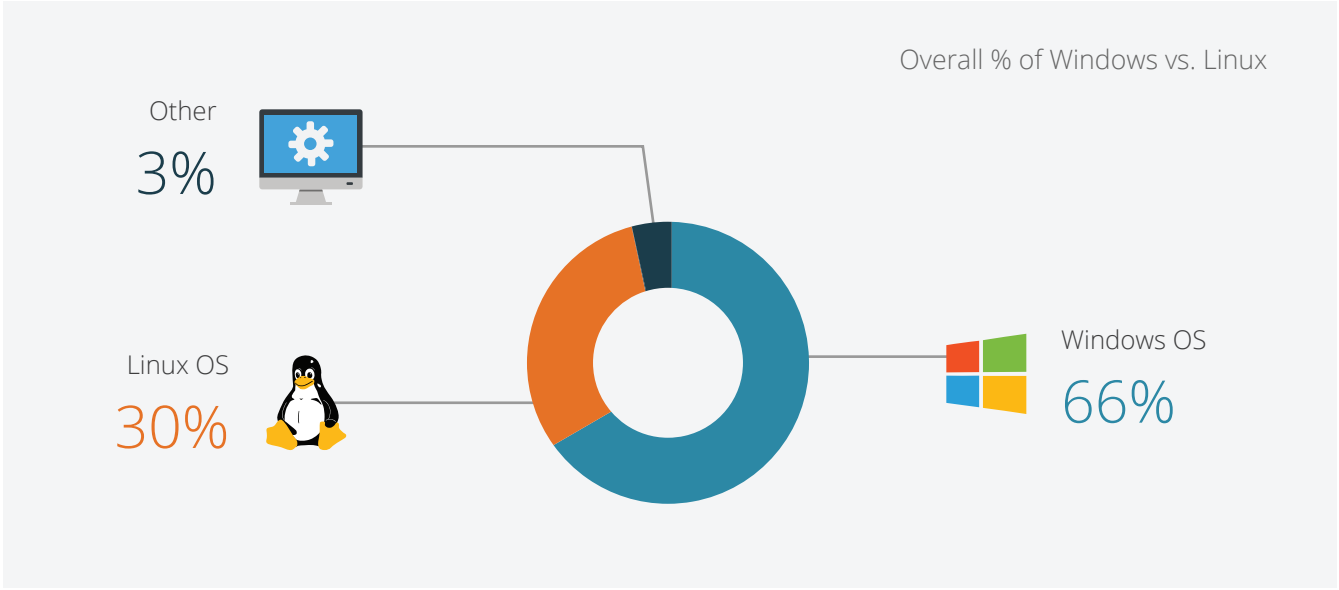
Incorrect storage setting leading to corrupt backups and data-store loss. Such risks can range from invalid CBT configuration to inconsistent LUN numbering and incorrect UUID setting.

What do these private cloud environments look like?

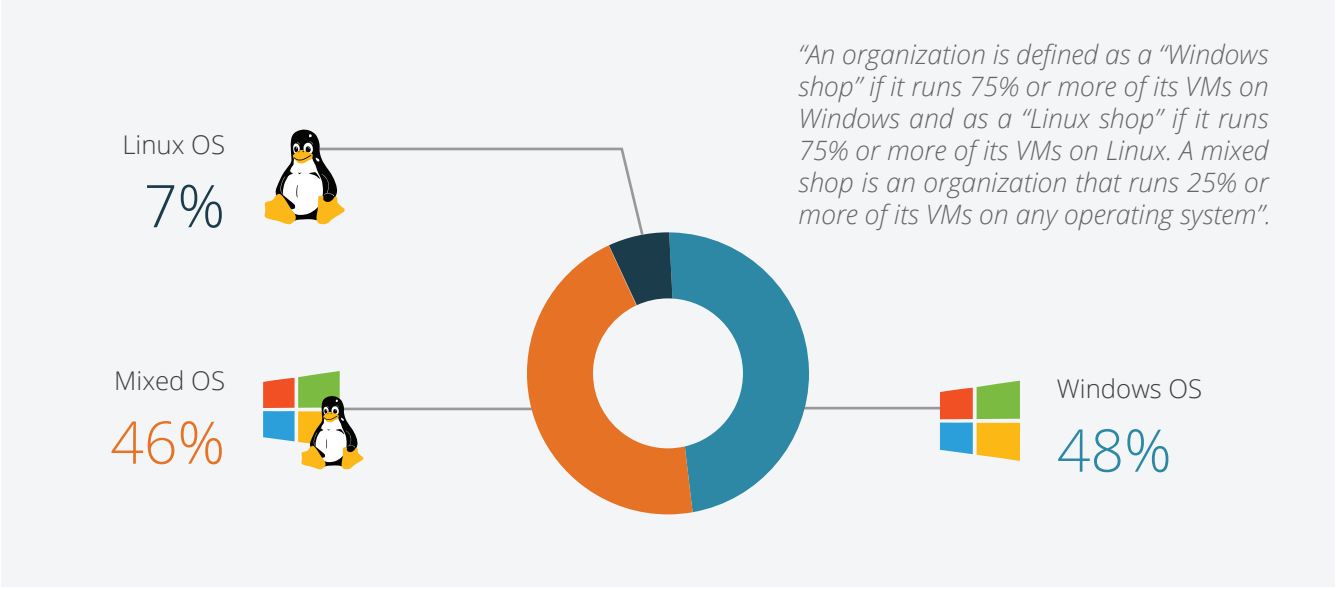
OPERATING SYSTEMS

48% of the organizations run their virtual machines on Windows compared to **7%** of the organizations that run on Linux. **46%** of the organization use a mix of operating systems.

VM Technology



Shop Type

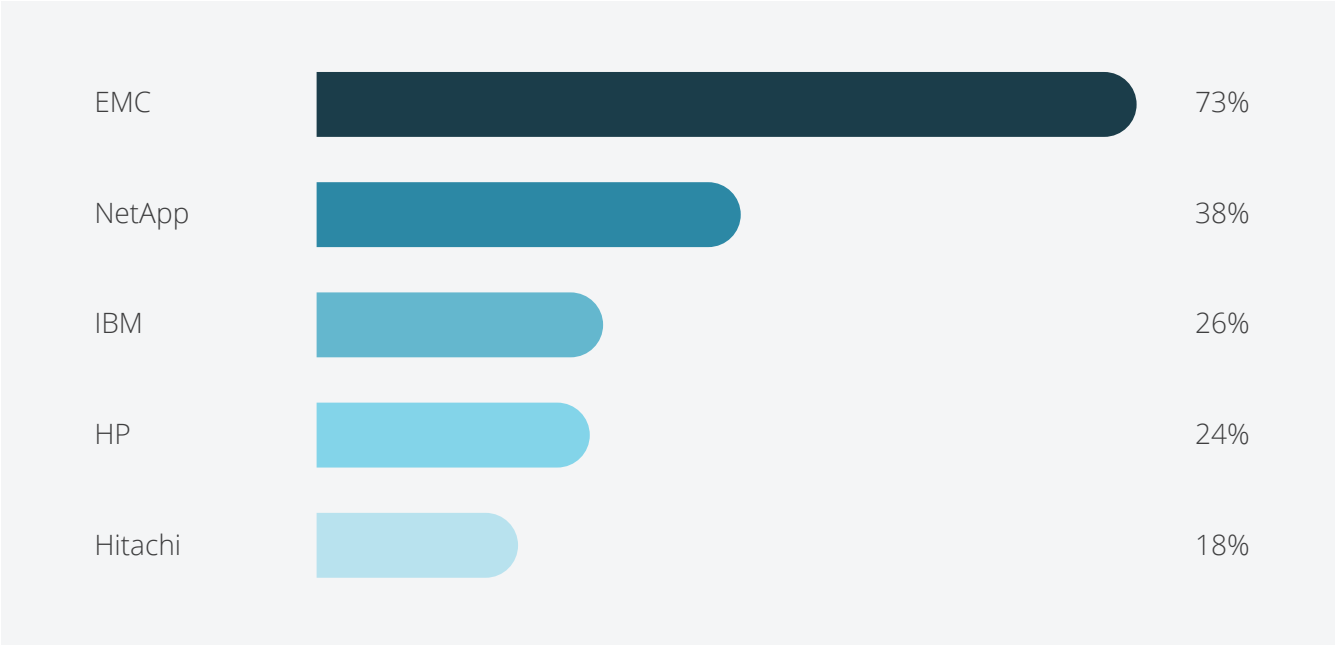


What do these private cloud environments look like?

STORAGE

Close to three quarters (**73%**) of the organization use EMC data storage systems. Other storage systems used include NetApp (**38%**), IBM (**26%**), HP (**24%**) and Hitachi (**18%**).

Storage Vendor



Which storage systems are in use within the organization?

What do these private cloud environments look like?

REPLICATION

27% of the organizations used replication for automated offsite data protection.

27%

ACTIVE-ACTIVE

12% of the organizations utilize active-active failover for continuous availability.

12%

MULTIPATHING

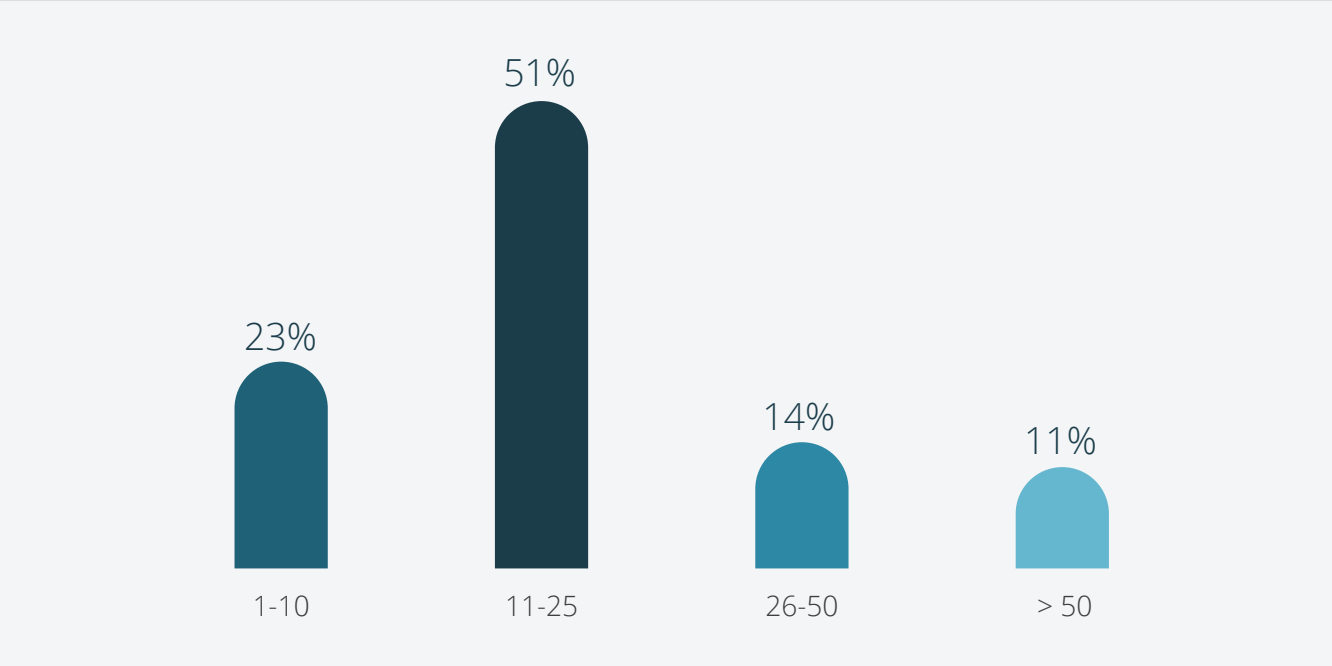
Almost all of the organizations (96%) use more than one physical path to transfer data between the host and the external storage device.

96%

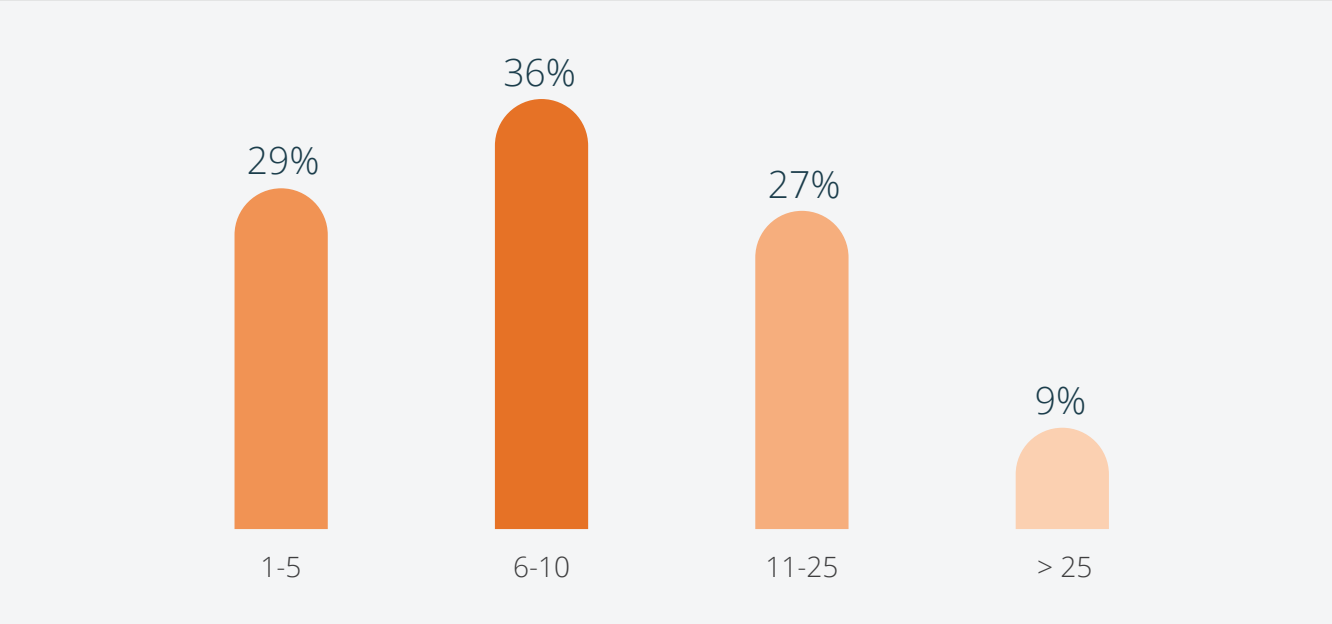
What do these private cloud environments look like?

VIRTUAL MACHINE ATTRIBUTES

VMs per host



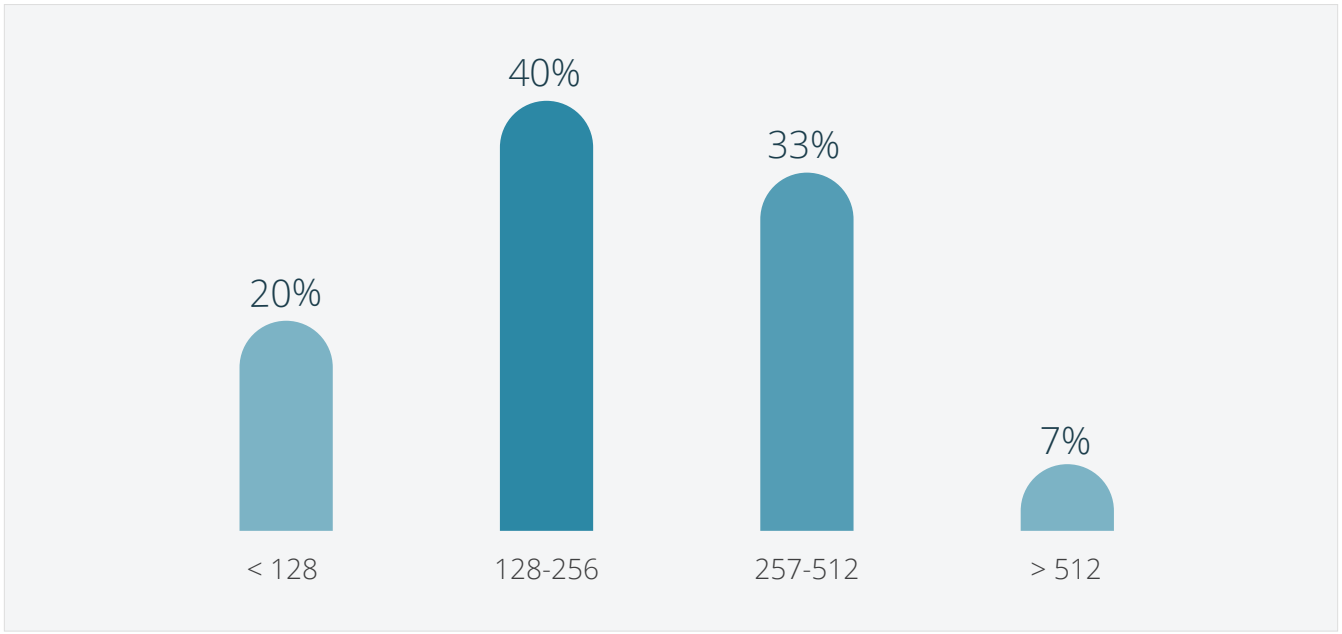
VMs per CPU



What do these private cloud environments look like?

VIRTUAL MACHINE ATTRIBUTES

Average Memory per Host (Megabyte)



ADDITIONAL RESOURCES

Survey

Cloud Resiliency Report

e-Book

The Agile IT Operations

Infographic

Shifting to Cloud Infrastructure

Don't let hidden misconfigurations put your critical systems at risk

Free VMware HealthCheck

START NOW