FORRESTER®

A SPOTLIGHT ON SECURITY

The Key To Enterprise Hybrid Cloud Strategy

Executive summary

Modern IT organizations that take a holistic view of their IT infrastructure — including on-premises and cloud models — will be best positioned to combat security vulnerabilities. Today, organizations face more uncertainty than ever before. As cyberthreats increase in number and complexity, the need for secure digital availability is paramount. In turn, organizations struggle with adapting their infrastructure strategies to best support their clients and increasingly complex workloads, without sacrificing security.

In January 2020, IBM published a study it had commissioned with Forrester Consulting in September 2019, to evaluate how organizations develop and implement their IT infrastructure strategies. Forrester conducted an online survey of 350 global enterprise IT decision makers across industries to explore this topic. We found that organizations are creating hybrid cloud environments with various public cloud, hosted private cloud and on-premises infrastructure.

IT firms are addressing broad infrastructure investments to overcome security challenges of today and tomorrow.

Organizations are focused on not only providing for growing demands on existing IT infrastructure, but also ensuring security while expanding to new technologies.

58%
cite providing for growing demands on *existing* IT infrastructure as a top five priority this year.

56%
are expanding or implementing *new* infrastructure technologies this year.

77%
find *security* to be an important consideration when making an infrastructure purchase.
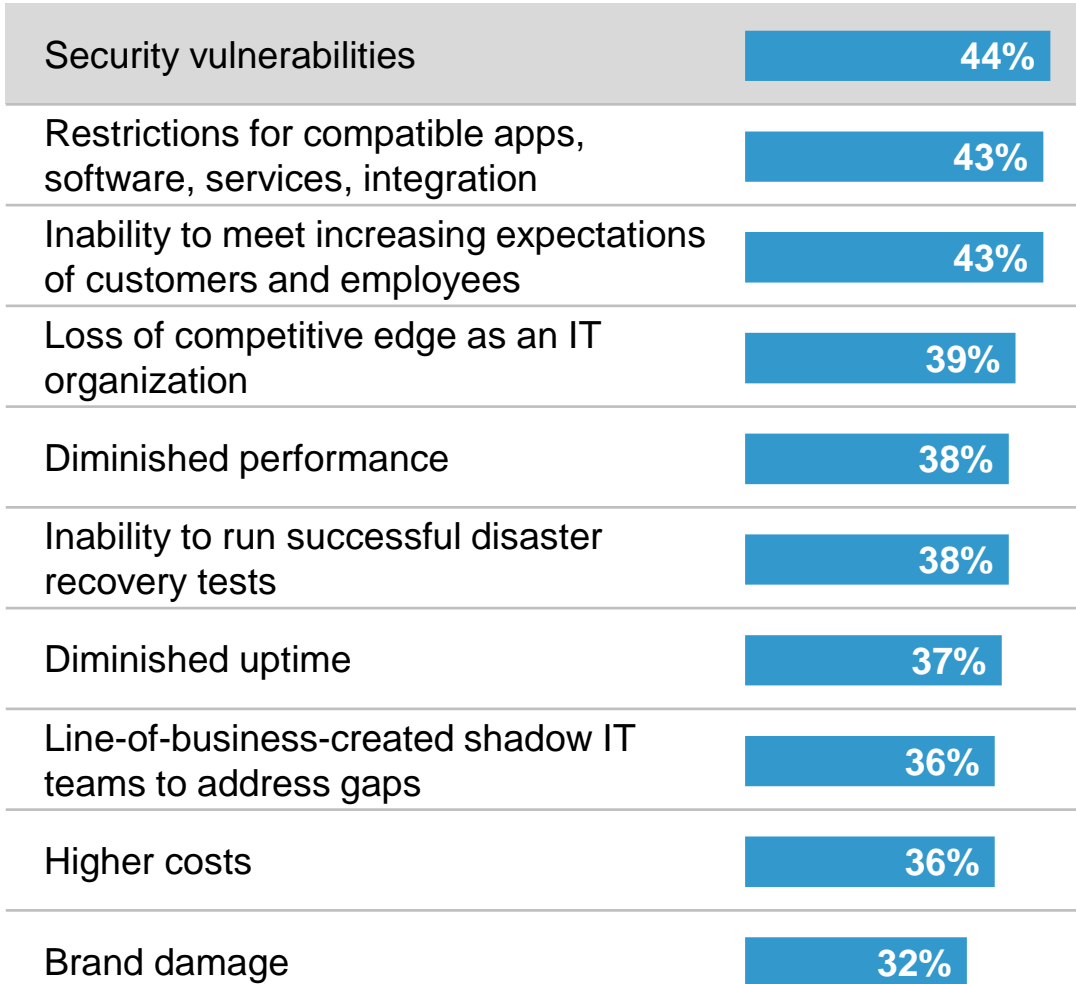
In times of uncertainty, with growing and shifting workloads, IT organizations must holistically address security when adapting their infrastructure.

Bolster security in the face of uncertainty by modernizing your firm's infrastructure strategy:

- Continuously refresh your strategy to protect against security vulnerabilities

- Maintain on-premises infrastructure as a player in your holistic security strategy

- Leverage on-premises infrastructure for improved security on critical workloads and applications

Top risks of delaying infrastructure refreshes

(Showing top 10, ranked 1 to 5)

Risk	Percentage
Security vulnerabilities	44%
Restrictions for compatible apps, software, services, integration	43%
Inability to meet increasing expectations of customers and employees	43%
Loss of competitive edge as an IT organization	39%
Diminished performance	38%
Inability to run successful disaster recovery tests	38%
Diminished uptime	37%
Line-of-business-created shadow IT teams to address gaps	36%
Higher costs	36%
Brand damage	32%

Base: Variable global decision makers for IT infrastructure environments
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, September 2019

Not keeping up with infrastructure refreshes introduces threats

38% of decision makers say their firms have faced failed disaster recovery tests following a delay in refresh.

61% have delayed a refresh of infrastructure a few times or more in the last five years.

Maintain on-premises infrastructure as a player in your holistic security strategy

Firms are continuing to diversify their infrastructure with nonpublic cloud platforms, including on-premises. On-prem infrastructure remains foundational and a critical part of a secure and resilient hybrid cloud strategy.

9/10

agree that on-premises infrastructure is a critical part of their firms' hybrid cloud strategies.
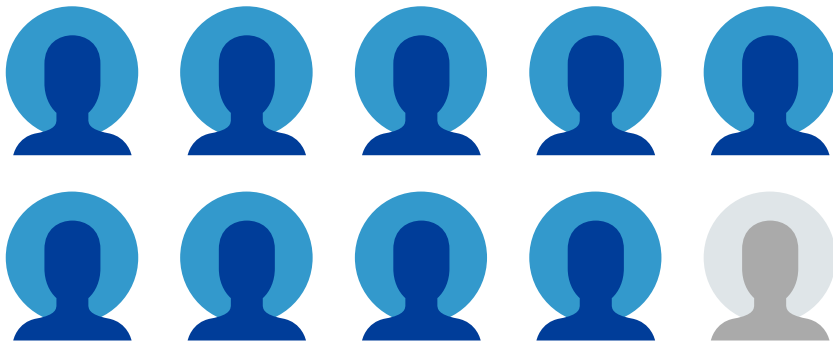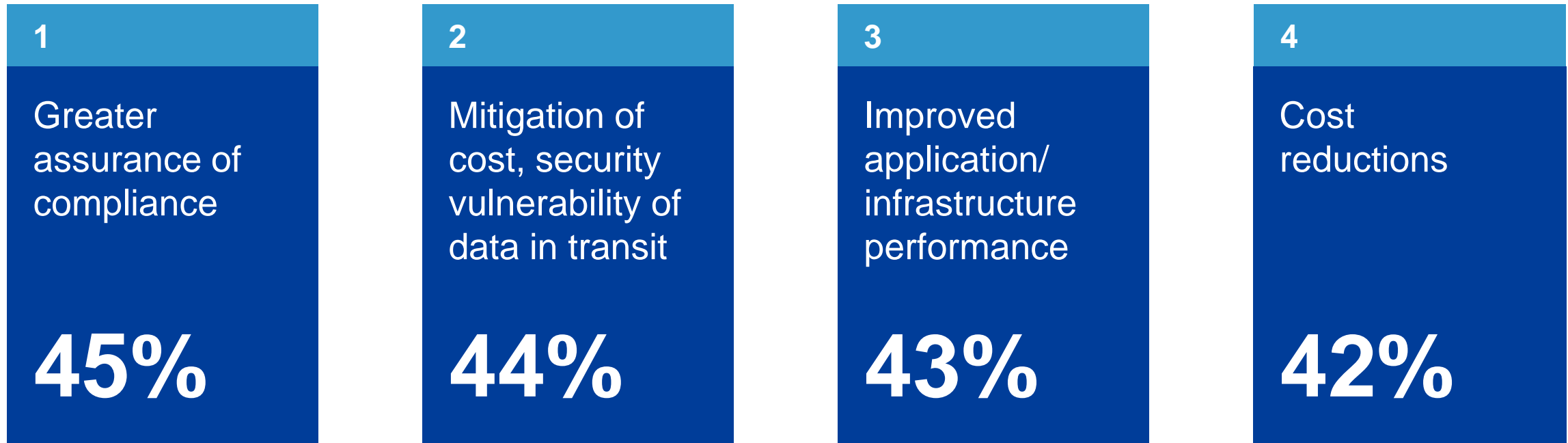
40%

say the public cloud's failure to meet **security needs** is a reason they maintain infrastructure outside of the public cloud platform.

Base: 350 global decision makers for IT infrastructure environments
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, September 2019

Leverage on-premises infrastructure for improved security on critical workloads and applications

Top ranked reasons for using on-premises resources for select workloads and applications:

1	2	3	4
Greater assurance of compliance	Mitigation of cost, security vulnerability of data in transit	Improved application/ infrastructure performance	Cost reductions
45%	**44%**	**43%**	**42%**

Base: 241 IT decision makers currently using public cloud
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, September 2019

Key recommendations

Prioritize infrastructure refreshes. Establish a clear, holistic infrastructure strategy that recognizes the continuing commitment to on-prem workloads and focuses on security issues as a primary driver of refresh decisions. Even firms struggling to survive in the pandemic should make security-related infrastructure refreshes a top priority.

Establish a data strategy to inform workload decisions — to promote security and performance. Avoid the trap of only considering costs when making workload decisions. Keep the impact of data location at the top of the list, tuning overall performance based on managing both security and latency issues through data and associated large workloads on the same platform.

Build an irrefutable business case. Performance is especially critical since it has significant impact on customer experience (CX) and brand perception. Executives who can't commit to complete refreshes can leverage subscription-based infrastructure refresh options to provide a more flexible future if their strategy changes.

Methodology

In this study, Forrester conducted an online survey of 350 global decision makers for IT infrastructure environments to evaluate how organizations develop and implement their infrastructure strategies. Survey participants included IT decision makers in infrastructure and operations, application management or maintenance, and/or software development. Questions provided to the participants asked about environments used for different workloads and investment in infrastructure. Respondents were offered a small incentive as a thank you for time spent on the survey. The study began in August 2019 and was completed in September 2019.