ENABLING SECURE CLOUD CONNECTIVITY

Create a Successful Cloud Strategy
with Reliable Connectivity Solutions

COMCAST
BUSINESS

TABLE OF CONTENTS

INTRODUCTION

Cloud computing has taken the IT industry by storm. According to recent reports, total revenues for public and private cloud hardware, software, and services amount to $180 billion annually, or 16% of the $1.1 trillion enterprise IT industry.[1] Given the flexibility, scalability, and cost efficiency of the cloud, it's hardly surprising that more and more organizations are contemplating the shift. Companies everywhere are trusting cloud environments to handle critical workloads and drive business success.

However, as cloud adoption grows rapidly, so does nervousness around security. As organizations move data-intensive applications off-premises and into the cloud, they expect these resources to perform seamlessly—as if they were inside the company's network—with no frustrating delays and no security loopholes. Businesses aren't willing to compromise on latency, reliability, or performance when deploying cloud-based solutions. For most companies, connecting over the open Internet isn't an acceptable option. They demand private, secure access to cloud providers as they build out their hybrid architectures.

That means increased pressure on IT decision-makers to make sure that their company's cloud architecture is secure, accessible, and efficient. As a result, IT professionals everywhere are looking for innovative ways to facilitate secure, direct access to private cloud environments. The answer lies in a solution that brings network security as well as the performance and scalability of Ethernet to the cloud—providing low-latency, secure, private access to mission-critical applications while effectively bypassing the Internet.

Spiceworks recently surveyed IT decision-makers to obtain insights into their expectations and concerns around managing data storage and cloud connectivity at their organizations. The survey explored their priorities and challenges related to managing growing volumes of data, deploying cloud connectivity solutions, and ramping up security across their network.

IT'S GETTING CLOUDIER

The cloud is growing 7 times faster than the rest of IT.[2]

THE DATA STORAGE CONUNDRUM

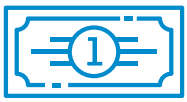
In today's data-driven world, companies are amassing more data than ever before. As they embrace trends such as big data, the Internet of Things (IoT), and analytics, they're forced to make sense of growing mountains of data. IDC forecasts that by 2025, the global data sphere will reach 163 ZB (a trillion gigabytes).[3] This will ultimately unlock unique user experiences and a new world of business opportunities. But to get there, IT pros must first determine the best way to store these staggering volumes of data.

As organizations transform their operations to meet today's digital needs, the question of where to store their data and applications becomes critical. IT pros know that when it comes to storing data, there is no "one-size-fits-all" solution. And in most cases, the decision between public and private cloud isn't a simple "this or that." Organizations have to weigh all of their options for managing workloads, including on-premises infrastructure, colocation facilities, private data center arrangements, and public cloud providers.

Many businesses view the public cloud as an option that provides affordable and flexible data storage. Yet, some worry that using a data center "somewhere" on the Internet puts their most sensitive data at risk. For some companies, it may also make sense to keep some of their data and workloads onsite, while moving the rest to a public cloud. Before deciding whether to store their structured and unstructured data in the cloud, on-premises, or a hybrid of both, IT decision makers typically analyze requirements in key areas, including:

Location of data storage

Security of data and applications



Cost

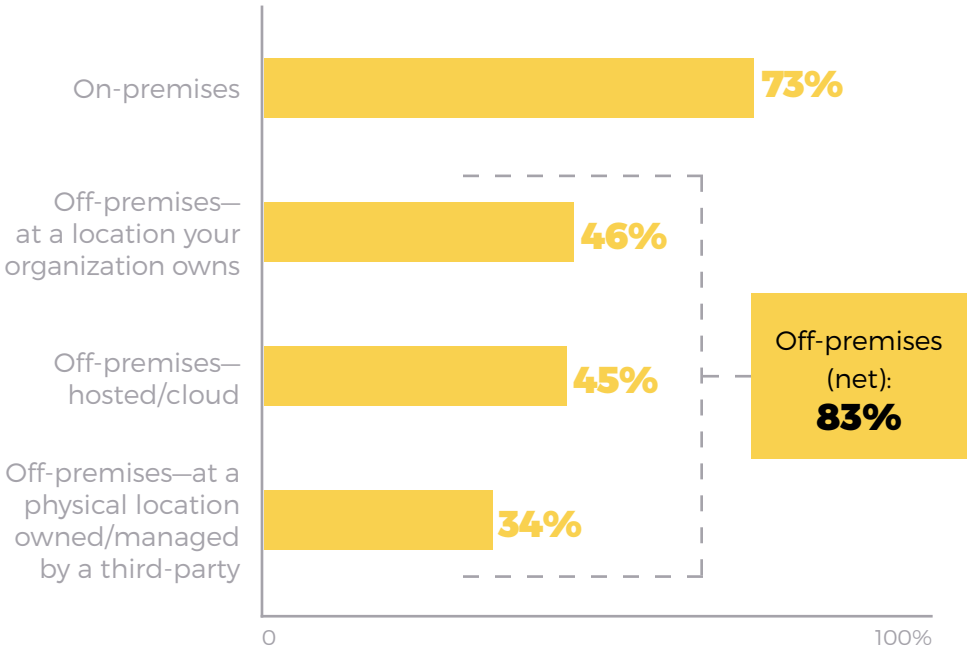
Level of control and flexibility needed

CLOUD VS. ON-PREMISES: FINDING THE RIGHT BALANCE

In the current IT landscape, computing resources that previously would have taken up rack space at on-premises data centers are increasingly being replaced by externally hosted or managed infrastructure residing with third-party providers. Most companies turn to their workload, security, and elasticity needs to dictate if they should store their data in a private, public, or hybrid cloud. Most studies—including the Spiceworks survey—suggest that less critical data is often transferred to a public cloud, while sensitive files frequently remain in a private cloud within the company.

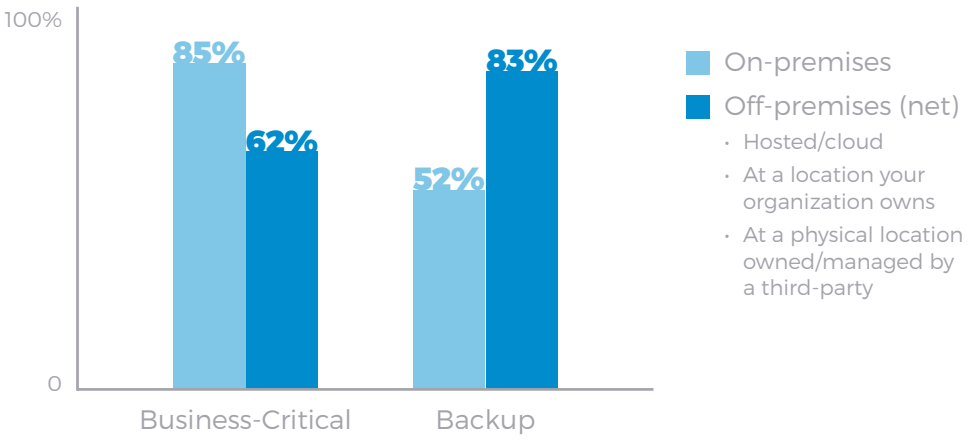
While an overwhelming majority (83%) of the Spiceworks survey respondents indicated that they are currently storing data off-premises—a large number (73%) reported still storing at least some data on-premises as well. Among those who store data off-premises, nearly half utilize company-owned locations (46%) and hosted or cloud options (45%), while about a third (34%) favor an off-premises location owned or managed by a third party.

CURRENT DATA STORAGE LOCATION



When asked about preferred locations for different kinds of workloads, most of the Spiceworks survey respondents suggested that backup data is more likely to be stored off-premises (83%)—split across company-owned, hosted/cloud, and third-party locations. Business-critical data, on the other hand, is highly likely to be stored on-premises (85%), even though a sizable portion admitted to storing critical data off-premises (62%).

STORAGE PREFERENCES FOR BUSINESS-CRITICAL VS. BACKUP DATA



While on-premises infrastructure is still a significant business reality, these numbers point to an ongoing shift to multi-tenant data centers (MTDC) and cloud solutions. More and more companies are turning to private cloud models, which gives them the additional flexibility to decide whether to store files on their own enterprise servers (on-premises) or in a data center of their choice. Among the survey respondents, at least half indicated that they rely on the cloud (public, private, or hybrid) to support workloads such as email, web hosting, content delivery, and file sharing.

A MASSIVE SHIFT TO THE CLOUD IS AFOOT

By 2018, 52% of all server racks in North America will be at cloud and colocation data centers.[4]

52%

SECURITY CONCERNS IN THE CLOUD

As businesses move more of their IT operations off-premises, they need to be able to connect to a range of different cloud services, securely and quickly. Many enterprises worldwide rely on VPNs to meet the connectivity needs of their businesses with adequate security, performance, and availability. As these businesses look to deploy cloud-based solutions more extensively, they expect a similar experience,

To that end, many enterprises depend on the Internet for cloud access. While the public internet certainly offers a convenient way to deliver cloud-based applications, it frequently doesn't meet the privacy and performance requirements of data-intensive enterprises.

For IT pros in particular, the Internet's questionable security is worrisome. Data protection is a nagging concern for system administrators and security managers. In today's volatile threat landscape, IT professionals are on the front lines at all times, battling major data leaks and developing suitable defenses. When it comes to ensuring seamless cloud connectivity, the surveyed IT pros singled out security as their greatest challenge.

TOP 5 CLOUD CONNECTIVITY CHALLENGES

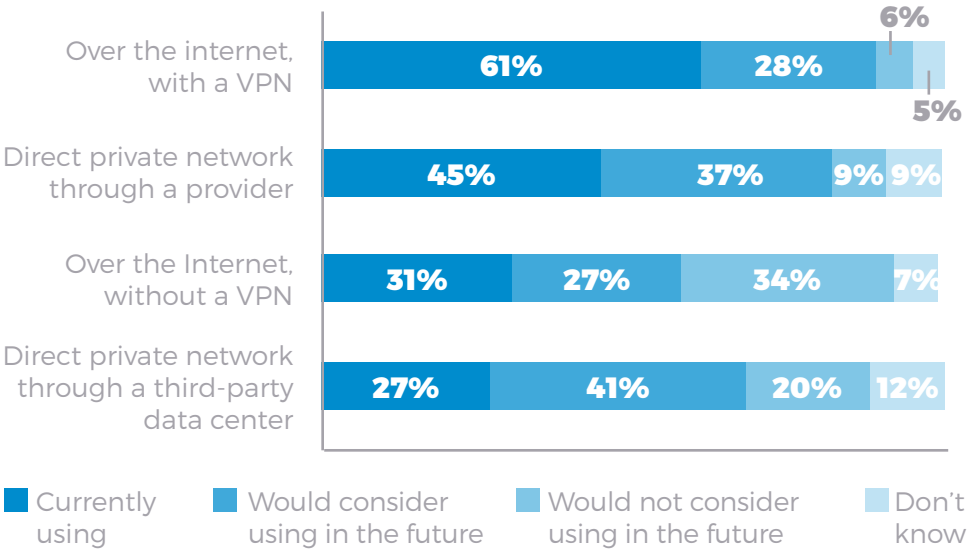
DIRECT AND PRIVATE: A BETTER WAY TO REACH THE CLOUD

To address security and performance concerns, some cloud providers have the capability to offer dedicated, private connectivity to the cloud. With private connectivity, organizations can benefit from isolation of traffic from the Internet, protecting critical corporate information and ensuring consistent, reliable speeds and quality of service. The additional security capabilities also help companies achieve or maintain compliance with stringent regulatory requirements.

With security concerns keeping IT pros up at night, private connectivity to the cloud sounds like a no-brainer. Yet, among the Spiceworks survey respondents, most organizations currently opt for the more traditional—and less secure—method to connect to the cloud, namely via VPN. The survey indicated that budget constraints, a lack of perceived need, and some amount of uncertainty around benefits were among the main reasons why some IT pros haven't yet adopted private connectivity to the cloud across their corporate network.

But a significant number—nearly half (45%)—currently use a direct, private network, either through a provider or a third-party data center. And this number is likely to rise steadily, with several others (37%) indicating that they are considering adopting that much safer option, going forward.

CLOUD CONNECTION STRATEGY



PRIVATE CONNECTIVITY BENEFITS

By replacing the open Internet with a direct, private connection, enterprises stand to gain significantly—in throughput, performance, and security. Private connectivity enables better reliability, faster speeds, lower latencies, and far higher security than typical Internet connections—all usually backed by a service level agreement (SLA). It's easy to connect a distributed ecosystem of employees, customers, and partners. Additionally, customers have the ability to take full advantage of the cloud's shared infrastructure and flexible pricing models for all their business needs.

Secure and Reliable: Private connections are dedicated to one organization, so the network bandwidth and latency remain inherently stable, increasing cloud reliability. In addition, the connections are significantly more secure, because no other users pass traffic across that network.

Optimal Performance: With private connectivity, organizations can ensure reliable, high-quality delivery of services and applications. In most cases, private connections via Ethernet allow for different streams of traffic to be separated by classes of service (CoS), ensuring that more latency-sensitive applications receive higher prioritization, resulting in a better end-user experience.

Easy Scalability: Private connectivity technologies are inherently scalable, giving organizations the ability to quickly, easily, and incrementally adjust bandwidth as their business needs shift. Private connections are particularly useful to organizations that have large data transfer requirements or those that conduct complex research and development initiatives across environments.

Efficient and Cost-effective: Data transfers via private connectivity are more cost effective than over the public Internet. The costs are predictable (for example, there are no unexpected peaks due to large transactions). In addition, network service providers that have already invested in pre-provisioned connectivity to a cloud exchange platform can pass on the savings—that is, they enable enterprises to connect to multiple cloud service providers using cost-effective price plans.

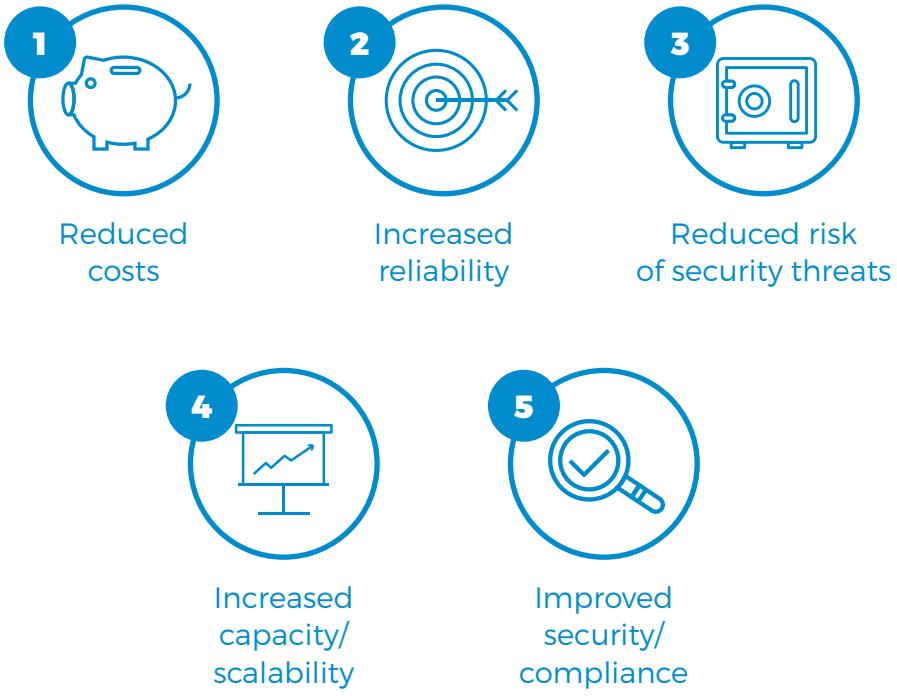
IT professionals increasingly recognize these benefits. According to the Spiceworks survey, they identified better performance, increased security, and higher availability as the top benefits of using a direct, private network to connect to the cloud.

ADVANTAGES: PRIVATE CONNECTIVITY TO THE CLOUD

WHAT TO LOOK FOR IN A CLOUD NETWORK PROVIDER

When evaluating cloud connectivity solutions, IT pros look for solutions that can help their organization create faster, more reliable, and more secure connections into their cloud ecosystem. What are the biggest drivers in their decision-making process? According to the Spiceworks survey, they value reduced cost savings, reliability, security, and scalability—among other key factors.

TOP 5 CAPABILITIES DESIRED IN CLOUD CONNECTIVITY SOLUTIONS



The best cloud connectivity solutions enable IT pros to balance cost-effectiveness with increased reliability and security. VPNs based on Multi-Protocol Label Switching (MPLS) can be a great way to connect to the cloud, since they allow enterprises to prioritize certain types of traffic and are more reliable and secure than the public Internet. However, MPLS VPNs require specialized skills, have limited flexibility, and are constrained by often-fluctuating bandwidth.

Ethernet solutions, in contrast to MPLS, have the advantage of lower cost, lower latency, easier scalability, more control over network routes, and better network management.[5] For many companies today, Ethernet is the preferred technology for integrating off-premises resources into an application delivery chain—enabling private network connections between select cloud services and their infrastructure—either on-premises or hosted in a colocation facility.

But how do you choose the right cloud network provider for your business? Look for a provider that can deliver Ethernet-based private cloud connectivity with:

- **Secure connections:** Direct, secure connections to the cloud provide better reliability, faster speeds, and lower latencies than typical Internet connections.
- **Lower costs:** The cloud's shared infrastructure enables new cost efficiencies and allows you to shift from CapEx to OpEx accounting.
- **Support for hybrid applications:** IT teams can build applications that span on-premises infrastructure and the cloud without conceding network performance.
- **Scalability:** Organizations can add compute/storage capacity and leverage the scale and economics of the public cloud without having to compromise on security.
- **Service level agreements:** Business leaders enjoy the peace of mind that comes with a network SLA—something that is unavailable with the open Internet.

CONCLUSION

Cloud-based solutions have taken center stage for modern businesses as they rapidly roll out innovative applications and services. Security, performance, and reliability remain key concerns when it comes to adopting cloud services or solutions. As a result, more and more IT pros are looking to deploy secure and reliable cloud network access via private connectivity.

The best cloud connectivity solutions facilitate fast, direct access to leading cloud environments nationwide. They bring the security, performance, and scalability of Ethernet to the cloud—providing low-latency, private access to mission-critical applications while effectively bypassing the Internet. The ideal providers deliver best-in-class security, reliability, and performance that businesses today need for their evolving cloud strategies and seamless connectivity requirements.

EXPLORE PRIVATE CLOUD CONNECTIVITY FROM COMCAST

LEARN MORE

COMCAST BUSINESS

ABOUT THE SURVEY

Comcast commissioned Spiceworks to conduct an online survey in October 2017. This survey targeted IT decision-makers, including IT directors, IT managers, and other IT staff, to understand current perceptions and practices around cloud connectivity. There were 150 respondents in the US, from a mix of organizations with 250 to 5,000+ employees, and representing a range of industries, including IT services, education, healthcare, manufacturing, and financial services.

Sources

[1] Bain and Company, Mark Brinda and Michael Heric, "Report: The Changing Faces of the Cloud," 2017

[2] International Data Corporation, "Worldwide Semiannual Public Cloud Services Spending Guide," 2017

[3] IDC, white paper sponsored by Seagate, "Data Age 2025: The Evolution of Data to Life-Critical Don't Focus on Big Data; Focus on the Data That's Big," 2017

[4] 451 Research Group, "Voice of the Enterprise Survey," 2016

[5] Telecom Brokerage Inc., "5 Ways Ethernet Edges Out MPLS," April 21, 2015