Secure Video Collaboration:

How to Ensure Security of Your Cloud Video Conferencing Solution

FROST & SULLIVAN

A Frost & Sullivan White Paper

Sponsored by Lifesize

contents

INTRODUCTION

In the past few years, cloud computing has taken off in a big way. Large enterprises as well as small and mid-sized businesses are benefiting from the adoption of the latest communications and collaboration technologies in the cloud with no upfront investment. The adoption of cloud-based video conferencing has multifaceted benefits. Organizations are able to immediately eliminate heavy CAPEX costs and IT management of hardware and software, while simultaneously having flexibility of procuring services on demand with greater scalability. The pay-as-you-consume option has extended the reach to anyone who wants to implement video conferencing for productivity enhancements and cost-savings.

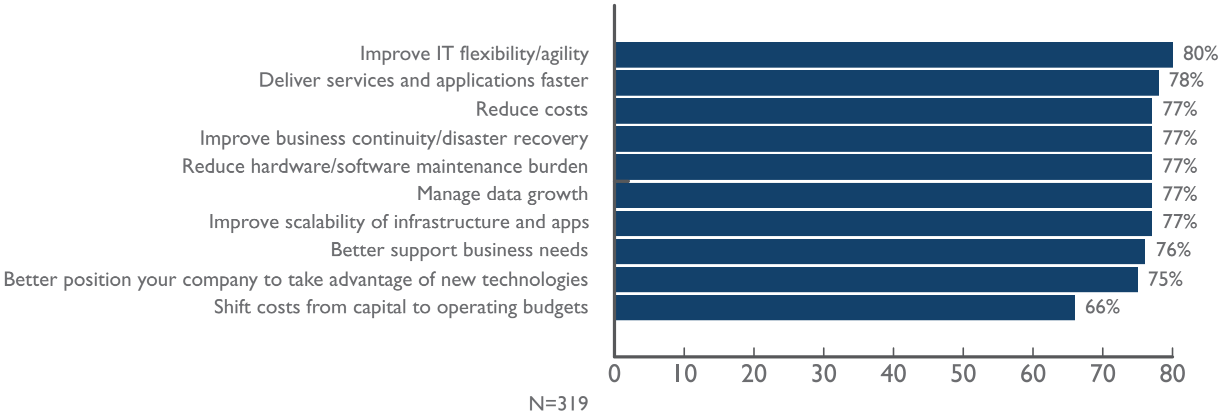
Despite momentous benefits, cloud computing has its own set of challenges that must be addressed. The primary concern that many enterprises and end users have is related to security, especially data protection and privacy and loss of control. This article discusses the several challenges associated with security for cloud-based video conferencing and how organizations can remove these barriers by adopting solutions that implement security as a key tenet.

THE SECURITY CHALLENGE

Video conferencing has become vital to thousands of organizations that seek not only productivity enhancements and sustained competitive advantage, but also greater profitability through reduced operating costs. Businesses have a lot of good reasons to implement video conferencing in the public cloud. The chief drivers include both short-term tactical objectives and longer-term strategic goals. The tactical drivers, such as shift to OPEX and reduced management burden, address the growing needs of resource-constrained IT managers. The strategic drivers, such as increased agility and supporting changing business needs, reflect the top-of-mind concerns for IT leaders focused on transformation. Though the benefits are insurmountable, several enterprises have held off on cloud video conferencing adoption due to concerns with security and control.

Annual surveys conducted by Frost & Sullivan of IT decision-makers show that while the cloud decision is being supported by a plethora of drivers, there exists a high level of concern regarding aspects of security in public cloud services. Exhibit 1 below lists the percentage of public cloud users, from a recent Frost & Sullivan survey, who indicated the drivers that were "very important" to their decision to choose cloud for certain workloads in their organization. While many factors weighed into the decision, the cost and budget factors that have dominated the list in the past are now joined by criteria that address broader business challenges.

Exhibit 1: Key Criteria Listed as "Very Important" to the Cloud Decision

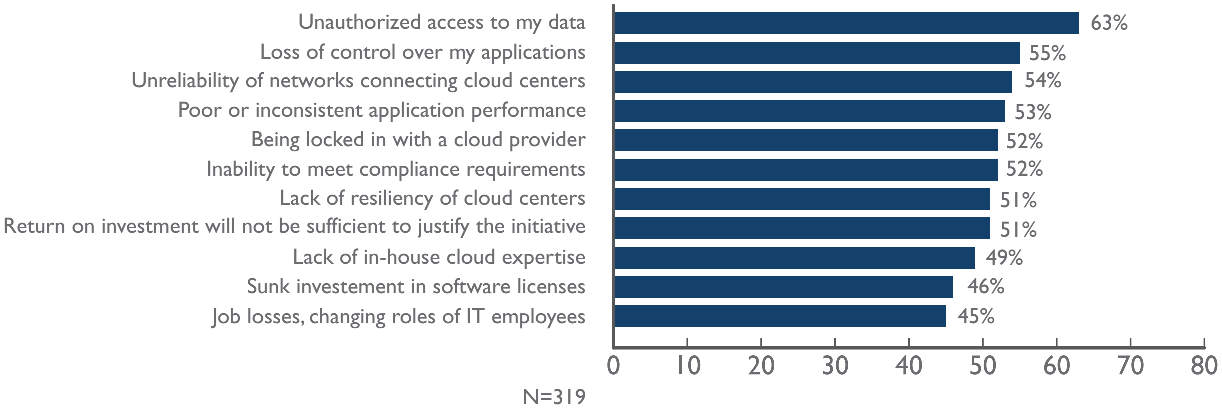


Source: Frost & Sullivan

In the same survey, respondents cited the familiar objections related to security and control as the key factors contributing to the decision not to entrust a workload to the public cloud (Exhibit 2).

Since cloud services let users connect with anyone over any device, this means that some of the calls are conducted over the public Internet. As a result, users have concerns around how they can protect their data and applications that reside in a shared public cloud that has no defined boundaries.

Exhibit 2: Key Restraints Listed as "Very Important" to the Decision Not to Use the Cloud



Source: Frost & Sullivan

MOBILITY COMPOUNDS SECURITY CHALLENGES

The emergence of Bring-Your-Own-Device (BYOD) and Bring-Your-Own-Application (BYOA) is a key trend that has resulted in landmark shifts in how business users acquire and consume productivity apps. While employees are happier and more productive if they are allowed to use their own devices and applications, BYOD and BYOA bring huge security challenges for IT. A proliferation of user-driven devices and applications results in more attempts to connect untrusted devices to the corporate network.

As a result of the massive growth in the number of applications, devices, as well as the variety of networks that connect to corporate databases, maintaining security of intra- and inter-company collaboration has become an increasingly daunting task. If the chosen cloud solution lacks the necessary layers of security and access control, organizations are not only putting their corporate networks at risk, but also the underlying data they share. Customer databases and applications could be accessed or compromised from an unsecured device. Lost or stolen devices and the potential for viruses and other malware to infect corporate assets are valid concerns. These issues require additional security measures across multiple access points, including mobile devices, applications, and networks.

TOP SECURITY CONSIDERATIONS

During a video conference, sensitive information and data travels across internal and external public and private networks where it's susceptible to security violations.

The key aspects of cloud security that are top of mind for video conferencing customers include:

- ***Information Protection*** – A multi-tenant video conferencing cloud shares applications and resources, which presents inherent risks. Video conferencing cloud providers must take all required steps to protect the integrity of the data and information being exchanged before, during, and after the meeting.

- ***Privacy*** – Service providers must ensure that all critical customer data (credit card numbers, for example) is masked or encrypted and that only authorized users have access to sensitive information. Moreover, users' digital identities and credentials must be protected, along with any data that the provider collects about customer activity in the cloud.

- ***Physical security*** – Cloud video conferencing service providers must ensure the physical security of the data centers and the IT hardware against unauthorized access and theft as well as ensure redundancy and failover to minimize the possibility of service disruption.

- ***Endpoint Integrity*** – As video conferencing services originate in the cloud and are then used on-premises, the security, compliance, and integrity of the endpoints involved must be part of any security consideration.

- ***Identity and Access Management*** – Users have multiple access points. Local, remote, and mobile users need easy access to video conferencing services with strong authentication controls that do not compromise their identities.

THE LIFESIZE ALTERNATIVE

While the challenges with video conferencing security are multifold, several next-generation cloud services are taking the right steps to tighten the security and to alleviate customer fears. Lifesize Cloud, a cloud video service that enables easy-to-use and reliable video meetings, document sharing and audio calls over any device, has taken customers' security concerns seriously. Delivered over the IBM and Amazon cloud backbone and deployed in global data center locations, Lifesize Cloud delivers the resiliency, capacity, and global connectivity that business users seek.

A comprehensive security strategy must architect security into the people, processes, and technologies of the cloud service. Lifesize has taken a multifaceted approach to enable secure video collaboration.

- ***Encryption*** – All communication among Lifesize Cloud users is fully encrypted with enterprise-class 128-bit AES (Advanced Encryption Standard) encryption for media and TLS (Transport Layer Security) encryption for signaling. At no point in the system can a Lifesize administrator get access to the media. It is not stored or recorded anywhere.

- ***Data Center Security*** – An important security consideration for cloud service customers is to find out about the hosting centers used by the provider. Lifesize Cloud customers are assured of system performance, reliability, resiliency, and security over the IBM and Amazon Cloud backbones. Additionally, every data center and network location is regularly audited and hardened against physical intrusion.

- ***Authentication*** – The connection between the Lifesize Cloud and Lifesize Icon systems is authenticated through https at provisioning. Registrations are secured via TLS. Each user only has one account, which they can use to be logged in simultaneously across all of their devices. When they receive a call, they can answer on the device of their choice.

- ***Firewall/NAT Traversal*** – Users don't need to place devices outside the firewall to enable communications through Lifesize Cloud. Lifesize Cloud lets users keep the apps and meeting room video systems behind the firewall and manages the traversal through authenticated servers.

- ***Data Storage*** – The only user-related data Lifesize Cloud stores are the full name of the user, email address, password, phone, physical address and company name. Passwords are encrypted in the database and no clear text passwords are stored in the cloud.

- ***Billing*** – Lifesize leverages its partners for channel sales; therefore, no user billing information is stored in its systems.

- ***Account Security*** – Users must be vigilant about how passwords are assigned, protected and changed in a cloud service. Lifesize sends an authentication email before activating an account. Each account (admin and users) is secured with a password. Passwords and authentication are encrypted, which is what customers would expect in a secure cloud service.

- ***Meeting Security*** – Lifesize Cloud allows users to add a passcode to secure their meetings, which provides an added level of security for gaining entrance to a meeting. Additionally, during a meeting, any participant can be easily removed from the call.

- ***Service Availability*** – Lifesize Cloud is operated in secure IBM data centers globally, ensuring redundancy and failover. In case of disruption, the calls are routed to another available server. Since the systems are backed up, IT ensures that user configurations are protected and up to date.

- ***Business Continuity and Disaster Recovery*** – If there is a catastrophic event at a data center or network POP, all Lifesize users immediately fail over to another data center. The service becomes available through a different physical data center location and a user simply redials and the call connects.

> “We have offices in New York and San Francisco, so being able to communicate internally over video is much better than voice alone. Data security is always a big concern when working in the cloud. We cover some very proprietary issues in those conversations, and if that data were leaked it could be detrimental to our business. One thing we really like about Lifesize is that we have control over the endpoints that are used to transmit our video calls. All of our video calls are encrypted by Lifesize, so that greatly increases our comfort level. We would not use Lifesize if that encryption feature wasn’t built into the product. Lifesize was also quick to show us other things we could do to enhance our security, like how to better configure our firewalls for video conferencing.
>
> -Trevor Hicks, Director of Technology,
> Wetherby Asset Management”

> “
>
> The typical concerns around security and teleconferencing–such as authentication and encryption–quickly evaporated after converting to Lifesize Cloud. We're especially confident because the service let us keep our meeting room video systems behind our firewall, while it managed the traversal through its authenticated servers. It both drastically simplified, and vastly improved, the way we connect with hundreds of employees across our remote AdRoll offices. Now, even our most non-technical staff is able to start and run meetings without the assistance from IT.
>
> - Steve Latour, Director of IT
> AdRoll
>
> ”

CONCLUSION

Businesses are moving to the cloud at an accelerated pace. According to Frost & Sullivan research, 50% of US businesses are now using public cloud services–more than three times as many as a year ago. Video conferencing, often prone to complex and costly solutions, is becoming a key application that is migrating to the cloud.

As with any other technological shift, customers should carefully evaluate all benefits and risks when adopting cloud video conferencing services. IT, which is constantly moving forward by taking advantage of new technologies and processes in the cloud, expects security to be built into the DNA of a cloud video conferencing service. A holistic security framework is becoming a table stake in the decision-making process for most organizations that are adopting public cloud services for greater efficiencies and cost considerations.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Colombo
Delhi/NCR
Detroit

Dubai
Frankfurt
Houston
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Miami

Milan
Mumbai
Moscow
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai

Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

Silicon Valley

331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio

7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London

4 Grosvenor Gardens
London SW1W 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041