RESEARCH
Influence and insight
through social media

August 2018

As Collaboration Shifts to the Cloud, SECURITY REQUIRES A RETHINK

WHITE PAPER

Prepared by
Zeus Kerravala

ZK Research
A Division of
Kerravala Consulting

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

INTRODUCTION: THE CLOUD COMMUNICATIONS ERA HAS ARRIVED

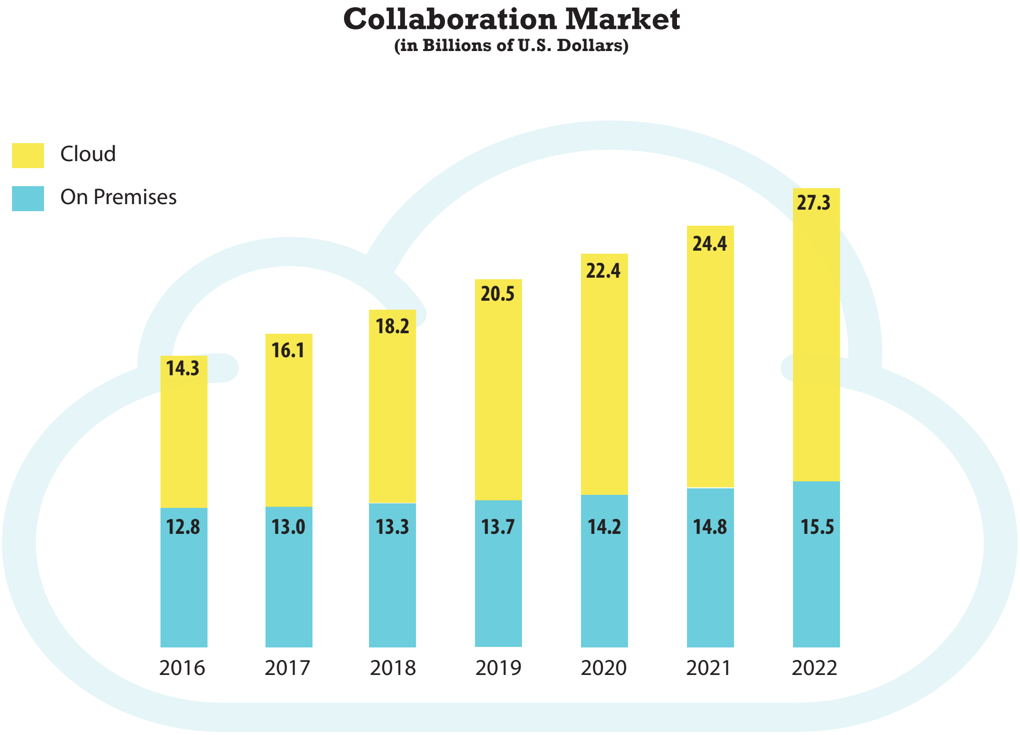
Communications technology has been around for decades and is deployed in companies of every size and in every industry vertical. Despite the ubiquity of on-premises infrastructure, businesses have been dumping legacy technology in favor of the cloud. The ZK Research 2018 Unified Communications and Collaboration Forecast shows that cloud communications technology is growing at six times the rate of legacy, on-premises systems (Exhibit 1).

There are many reasons for this shift, including the following:

The cloud is better aligned with mobile workers. On-premises systems were suitable for a workforce that was in the office most of the time. Today, almost half of the workforce spends a significant amount of time away from the office but still needs access to communications tools. The cloud enables "anywhere, anytime" access to communications and collaboration tools and is therefore ideally suited for the mobile workforce.

The cloud enables digital transformation. In the digital era, competitive advantage is based on a company's ability to make the best decision, with the right people involved, in as short a time as possible. On-premises systems limit the data and people that can be reached,

Exhibit 1: Cloud Collaboration Outpaces On-Premises Systems



ZK Research 2018 Unified Communications and Collaboration Forecast particularly by remote workers. Cloud-based collaboration tools enable geographically diverse teams to make decisions together more effectively.

The cloud enables faster innovation. The refresh rate of on-premises communication systems is measured in years. Now that most systems are software based, innovation can happen much faster. Because of the work required to upgrade solutions, businesses will often delay new versions, sometimes skipping them all together. This can cause organizations to miss entirely new features that could enable workers to be more productive. Also, many new features in communication systems, such as team collaboration, are only available via the cloud.

The cloud is one of the most transformative technologies of the past 20 years and is a core component of digital transformation.

There are many other reasons for the cloud's growth in popularity, including speed of deployment, lower capital costs and simplified IT operations. The cloud offers unprecedented agility, scale and elasticity, enabling enterprises to change the way they operate.

However, for every yin, there is a yang, and for all the benefits that the cloud offers, it does open the door to new security risks—and the problem is getting worse. The ZK Research 2018 Security Survey found that 90% of businesses have suffered at least one security breach, with 43% experiencing a breach in the past year. Security must be top of mind for businesses that are considering moving their collaboration tools to the cloud.

In this report, ZK Research investigates the security issues that arise when moving communications and collaboration tools to the cloud, highlights some myths regarding how to protect the business, and profiles Symphony Communication Services—a vendor that has taken a "security first" approach to cloud communications.

SECTION II: SECURITY CHALLENGES WITH CLOUD COMMUNICATIONS

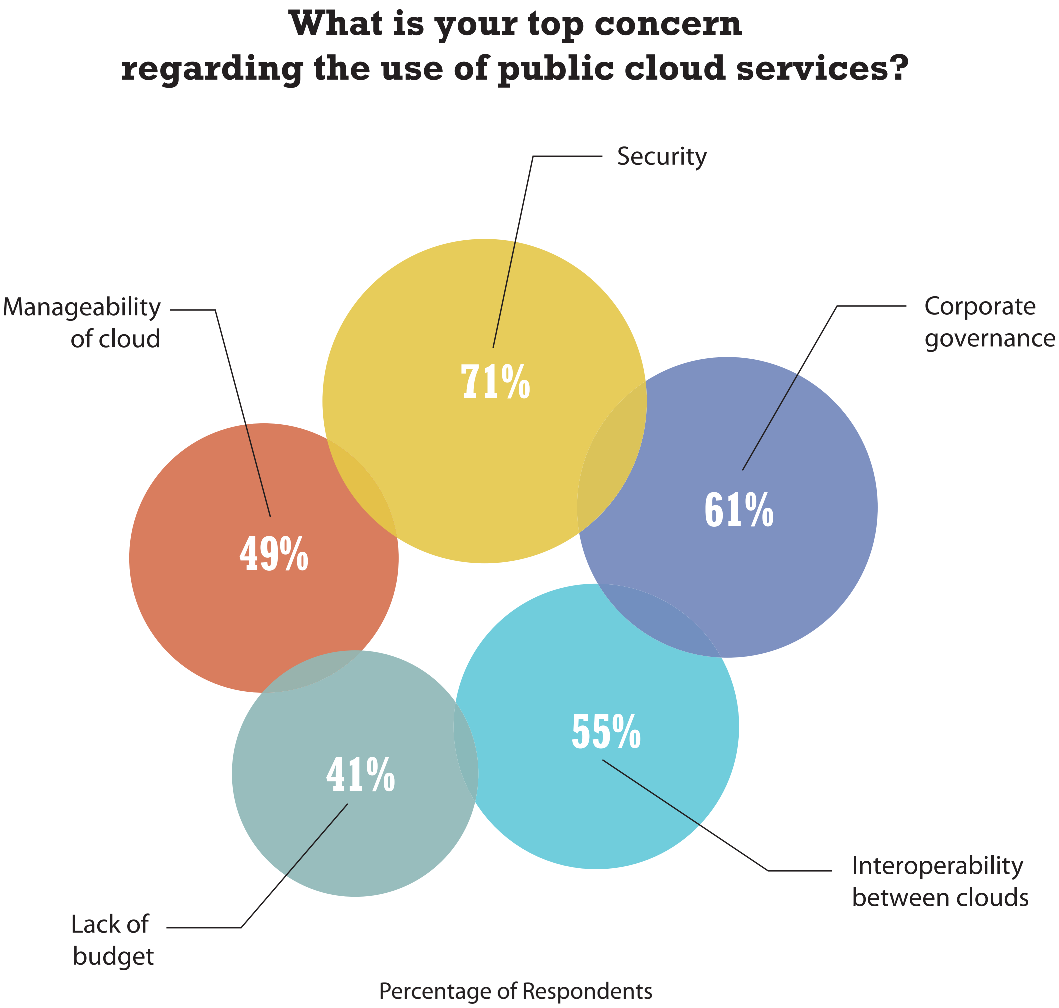
The cloud is one of the most transformative technologies of the past 20 years and is a core component of digital transformation. Regardless, many businesses have shied away from leveraging public clouds, primarily because of security concerns. In fact, the ZK Research 2018 Security Survey found that only 23% of businesses completely trust public cloud providers to protect their data. The same survey found that security concerns are the top inhibitor to cloud adoption (Exhibit 2). This isn't to say that cloud providers do not secure customer data—they do. But the level of security can vary greatly between offerings, so a healthy skepticism exists for good reason.

For businesses, protecting the company's information is of the utmost importance today, as each breach can cause brand damage, invoke lawsuits, increase customer churn and cost huge amounts of money. How much money? Based on interviews with customers and survey data, ZK Research has calculated the average cost of a breach in 2017 to be $3.5 million globally and $7.5 million in the United States—the highest of any nation.

With collaboration specifically, the stakes can be much higher, as teams often share sensitive information. Examples of such collaboration include a CEO sharing sensitive financial information

One would assume that if the traffic is encrypted both at rest and in transit, that is sufficient. The fact is, it's not.

Exhibit 2: Security Is the Top Concern Regarding Public Cloud Services



ZK Research 2018 Security Survey

with board members and a clinical team distributing patient records to another clinical team in a different location. Team collaboration applications are ideal for these use cases, but they can expose sensitive information to threat actors if the data is not protected.

One of the biggest challenges for businesses is trying to decipher how cloud providers secure data and whether that is enough. For example, on the security page of its website, one of the leading team collaboration vendors claims to conduct "data encryption in transit and at rest." One would assume that if the traffic is encrypted both at rest and in transit, that is sufficient. The fact is, it's not. Each time the data is transmitted and comes to rest, it is decrypted, moved to the next step in the process and then re-encrypted.

Although these gaps in encryption may seem small, the large data lakes owned by cloud providers make them an appealing target for hackers. There's an axiom in security that states that security is only as good as its weakest link—and the process of sending data from a user's device to the cloud includes many weak links. Each time the data is decrypted, it can be scraped, stolen, shared, used or hacked, sometimes by a disgruntled or dishonest employee of the cloud provider.

Another misleading security measure offered by cloud providers is allowing customers to "bring your own key." Again, logically, one would think bringing your own security keys is better than having them provided by the cloud provider—and that's true. But the bigger issue is where the keys are stored. Many cloud providers store security keys in their cloud, but this is akin to a bank offering to store a customer's ATM PIN on the same server as the customer's account data. A breach would give the threat actor access to both the data and the keys.

Finally, a lack of monitoring of and visibility into the cloud provider's operations makes it difficult for its customers to meet compliance requirements. This can be a significant problem in heavily regulated verticals and may mean the difference between being able to take advantage of the cloud or not.

Each time data is decrypted, threat actors have the ability to steal the data even if the decrypt/encrypt time is short.

SECTION III: RETHINKING SECURITY IN THE CLOUD ERA

Securing cloud communications and collaboration tools requires a complete rethink of both the problem and the solution.

Securing cloud communications and collaboration tools requires a complete rethink of both the problem and the solution. It's no longer sufficient to cobble together technologies and hope they adequately protect the business. To ensure the best possible security, chief information security officers (CISOs) should consider the following approaches:

Lower Reputational Risk

End-to-end encryption: This requires an understanding of how "end to end" security and "encryption in transit and at rest" differ. They might seem similar, but they are dramatically different. As mentioned earlier, with encryption in transit/at rest, the data is decrypted and re-encrypted a number of times. Each time this happens, there is the possibility of a breach. True end-to-end encryption involves the following actions:

- **Encryption at origin:** Encryption starts as soon as the user initiates the transmission of data.
- **Decryption at destination:** Content is never decrypted until it reaches the intended recipient. This protects against breaches that may occur when data is decrypted and then encrypted again.
- **Ownership and exclusive control of keys:** Businesses should have the ability to create their own keys. Just as important, the keys should be placed on a server located on their premises. If the cloud provider is breached, the data is unreadable without the keys. If the key server is hacked, there is no data to steal, as the keys and the data are stored in separate locations.

- **Changing the encryption keys:** The keys should be regularly changed to minimize the impact of a breach.

Security before transmission

- **User authentication:** Strong authentication tools are required to protect the business. The ZK Research 2018 Security Survey found that 81% of hacking-related breaches occur because of stolen or weak passwords. Two-factor authentication should be a matter of standard practice.
- **User authorization:** Workers should only have access to the data they need. Other content should be made invisible to them.
- **Mobile security:** Mobile devices are increasingly becoming the primary device for workers. Collaboration tools should assume "mobile first" and provide the necessary security.

Security during deployment: Administrator functions are required to control who can use the applications and bots. Ideally, the business would have a customized app marketplace where the apps are isolated in their own sandboxes.

Secure consumption: The messages initiated by the bots and the data generated by the application should be secured through strong encryption.

No compromise on speed and efficiency: On-site agents should provide REST APIs to quickly encrypt and decrypt data messages from in-house and third-party applications, bots and integrations. This will ensure that security doesn't get in the way and slow down the organization.

Ensure Data Ownership and Integrated Data Loss Prevention (DLP)

Data ownership: Customers need to own the data, not the cloud providers. This ensures that a nefarious individual at the service provider can't scrape and steal the data. Data ownership requires the following elements:

- Integrated DLP to enable the real-time parsing of messages and file attachments
- Policies to block content from leaving the customer's environment

Lower Compliance Risk

Real-time monitoring: This involves monitoring chat rooms and expression filters to promote active compliance with government regulations.

Granular entitlements: Entitlements should be set up both company wide and at the user level to control who can communicate with external participants, share files and use audio and video applications.

Segmentation: Information barriers between users and groups can be used to enforce company policies.

SECTION IV: SYMPHONY COMMUNICATION SERVICES—THE SECURE TEAM COLLABORATION PROVIDER

Symphony Communication Services is a highly secure, cloud-based team collaboration platform. The technology was initially built as an internal system by the financial firm Goldman Sachs and then later made into an independent company with funding from Goldman plus 14 other financial firms. Although there were other team collaboration tools on the market at the time, their lack of security was putting Wall Street firms at risk, so a more secure solution was needed.

The company's flagship product, Symphony Enterprise Tier, provides the following benefits:

Improved productivity: The application offers a complete set of real-time collaboration tools including persistent messaging, document sharing, screen sharing, audio/video conferencing and encrypted search.

Efficiency: Symphony has open APIs that enable software and application integrations and bots. Customers can use out-of-box integrations, or they can create their own bots and integrations to enable workflows that enrich and extend the user experience.

Rich mobile experience: All conversations, content and other information can be taken on the go through Symphony Mobile, which continually synchronizes with Symphony Desktop (Exhibit 3).

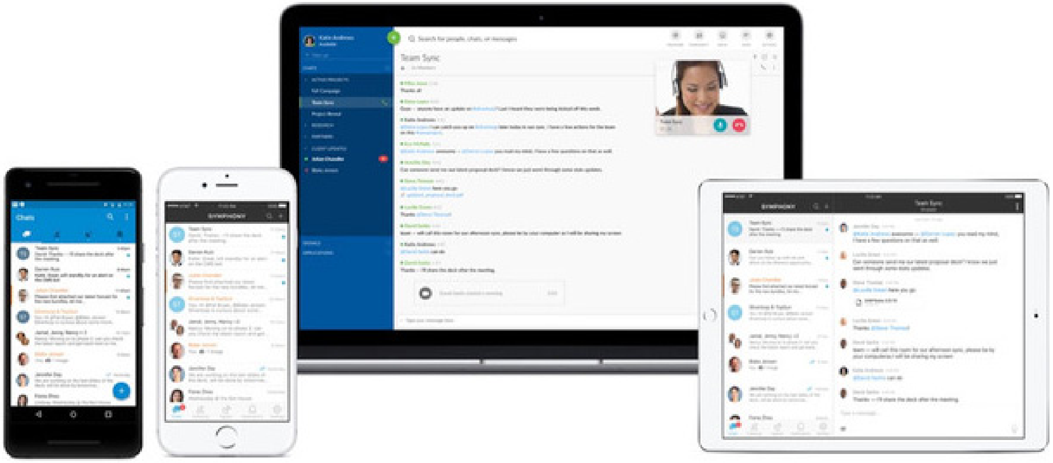
The heart of the Symphony solution is its best-in-class security.

The heart of the Symphony solution is its best-in-class security. The application was designed with security in mind instead of bolting it on afterward. The Symphony Enterprise Tier solution is built with end-to-end encryption, which enables individuals to collaborate with one another within their own company and between companies without fear of a breach or the data being stolen. Symphony offers a separate, fully independent, on-premises key management system where the unprotected keys never leave the customer premises. The proof of its best-in-class security comes from its customer base, which includes the world's premier financial services firms. The financial industry has some of the most demanding customers, and 16 of the world's 20 largest investment banks use Symphony.

In addition to end-to-end encryption, Symphony's "security first" approach includes the following features:

Policies based on international standards: ISO 27001 is the basis of Symphony's information security policies. It's one of the most demanding and stringent security standards.

Exhibit 3: Symphony Desktop and Mobile Are Kept in Lockstep



Symphony Communication Services, 2018

Hardened system: Symphony has conducted extensive penetration testing as well as source code and vulnerability scanning to harden the software stack.

Certifications: SOC 2 Type II and SOC 3 certifications are used to demonstrate the robustness of Symphony's security controls.

Compliance-specific features: Symphony has included several features to help security-conscious organizations comply with internal and industry mandates, including the real-time monitoring of chat rooms and expression filters, granular entitlements and application segmentation. Symphony supports the creation of information barriers between users and groups to enforce corporate communication policies. Customers can also export their content for archiving and electronic discovery. All of this can be controlled through a robust administrator portal.

Integrated data loss prevention: Symphony automates the process of scanning messages and attachments to ensure content is not hijacked.

In addition to secure enterprise collaboration, the Symphony Enterprise Tier application includes the following features:

Trusted Global Directory: Customers can expand their network of contacts using an integrated global directory that includes individuals both inside and outside the organization while maintaining the highest levels of security and compliance.

Persistent chat: The application includes one-on-one or group chat with drag-and-drop document sharing and screen sharing.

Content marking: Important messages or data can be "marked" through the use of hashtags (#), cashtags ($) and mentions (@).

Streamlined workflows: Actions can be assigned, progress tracked and alerts handled through the use of third-party applications, bots and other integrations.

SECTION V: CONCLUSION AND RECOMMENDATIONS

In today's competitive business environment, where new, agile companies are disrupting industries almost overnight, the speed of decision making is key to sustaining market leadership. Those businesses that can become dynamic, distributed organizations will lead their respective industries, while those that cannot will rapidly become irrelevant and struggle to survive. This has put communications and collaboration tools, particularly team collaboration, front and center as they facilitate better, faster decision making.

Collaboration technology continues to evolve faster than ever. Combined with an increasingly mobile workforce, this has put an emphasis on cloud-based communications. The cloud delivers faster innovation and a better mobile experience with an affordable pay-as-you-go model, enabling all businesses to have access to the latest features and applications.

However, as powerful and transformative as the cloud is for collaboration, there is a dark side to the cloud—security. Workers use team collaboration tools to send private messages, store sensitive documents and make key business decisions, making them a prime target for threat actors. Team collaboration has become a top initiative for business and IT leaders, but they must focus more on ensuring the application offers best-in-class security. This is likely obvious to decision makers in regulated verticals, such as healthcare and financial services, but is something all businesses should consider. Collaboration applications hold a tremendous amount of sensitive information, and therefore security must be top of mind.

Collaboration applications hold a tremendous amount of sensitive information, and therefore security must be top of mind.

To help organizations choose the right team collaboration tool, ZK Research makes the following recommendations:

Understand the difference between point encryption and end-to-end encryption. Most vendors claim to encrypt both in transit and at rest. As explained earlier, this is not enough. Challenge the vendor and ask if the data is encrypted and decrypted each time it is transmitted and comes to rest. If it is, that's not end-to-end encryption, and it can easily be breached.

Put data in the cloud but not the keys. Collaboration applications generate massive amounts of data, and it's much more effective to store it in the cloud. However, the encryption keys should not be stored in the cloud along with the data. Choose a vendor that provides an on-premises key management server to minimize the likelihood of a breach.

Research security and compliance certifications. Independent opinions can be valuable in validating a vendor's claim to offer best-in-class security. Ask the vendor for its security certifications and compliance standards, and look for ones like SOC 2, Privacy Shield Framework and General Data Protection Regulation (GDPR) compliance.

CONTACT

zeus@zkresearch.com

Cell: 301-775-7447
Office: 978-252-5314