Security: What to Look for in a UCaaS Provider

Zero Trust requires a scalable, standards-based security model

Q2-2021

Irwin Lazar
President and Principal Analyst
Metrigy

Table of Contents

Executive Summary

When COVID-19 first struck, many organizations rushed to deploy cloud-based Unified Communications-as-a-Service and video meeting solutions. But in the rush, security concerns were often overlooked, leading to potential risk from attack or unauthorized access to enterprise data.

Now that hybrid and remote work is here to stay, business, security, and IT leaders should reassess the security of their cloud-based applications. For example, they should ask if their applications offer End-to-End (E2E) encryption and support a Zero Trust security model.

As they evaluate their go-forward security strategies as part of a proactive collaboration security plan, IT leaders should:

- Incorporate cloud security provider assessments into a collaboration security approach
- Evaluate E2E implementation approaches, looking specifically for providers that are implementing the emerging Message Layer Security protocol to deliver E2E across multiple devices
- Assess the impact of E2E on available collaboration features
- Look for providers that offer the greatest flexibility for enterprise key management.

How Remote Work Has Changed Security

The COVID-19 pandemic has created an unprecedented shift in how and where people work. Going forward, work-from-home is likely to continue with just 12.4% of the 476 participating companies in Metrigy's global *Workplace Collaboration: 2021-22* research study planning to bring their employees back to the office full-time. Instead, the majority of employees will either work from home full or part time.

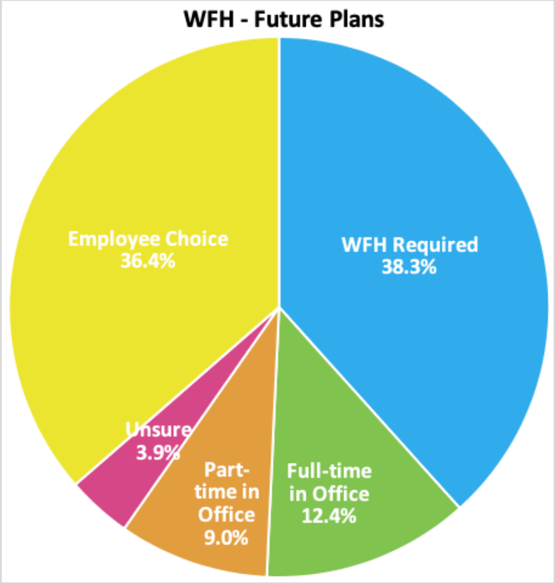

Figure 1: WFH - Future Plans

This change in employee location has fundamentally altered the enterprise communications and collaboration landscape. The shift to work-from-home drove a rapid acceleration in adoption of cloud-based applications including video conferencing and team messaging. In fact, 47.5% are using UCaaS for either their entire telephony needs, or in conjunction with a legacy on-premises platform as they complete their migration to the cloud. More than 50% have adopted cloud-based meeting platforms, and more than 80% say video conferencing is an important or critical business technology.

The WFH boom also has changed the paradigm for employee communications. Nearly 44% of participants report that phone usage is decreasing as employees shift to meeting apps, with video conferencing, for their 1:1 calls and group calls.

New Tools, New Security Needs

These rapid changes in both work location and collaboration applications have created significant challenges for those responsible for enterprise cybersecurity. Gone are the days in which most applications lived in the corporate-managed data center, accessed by endpoints solely connected to the enterprise network, or via VPN by a small number of remote employees. Now, IT leaders are faced with the reality that employees are using a wide variety of untested, and often unknown applications to meet, chat, and call one another. Even more importantly, IT and business leaders may lose control of data once it enters a cloud provider's domain. They have little visibility into how their providers store and maintain data, how it's encrypted, where it's kept, and what applications or processes may have access to it. Data stored by cloud providers, even if encrypted by the provider, may also be subject to requests for access from government entities without requiring customer approval or notification or at risk of access by rogue internal employees.

The State of Enterprise Collaboration Security

When it comes to dealing with WFH security threats, most organizations have a reactive approach, relying on VPNs to control user access to applications and enforcing application access policies at Internet connection points. However, using a VPN to connect to cloud-based apps adds additional cost, complexity, and delay by requiring voice and video traffic to be routed across the corporate WAN.

More recently, companies have shifted to split-tunnel approaches that enable home-based employees to directly connect to the cloud across their local Internet connections. This approach reduces delay, but it also creates new vulnerabilities as the user's devices can potentially become attack vectors should they become compromised.

Given the challenges with both VPNs and split-tunnel VPNs, it's not surprising that nearly one-third of our research participants say they consider security to be a primary challenge in supporting work-from-home.

Security Spend is Rising

In response to these challenges, approximately 55% of companies are increasing their spend on collaboration security in an effort to gain insight and control over risks. Among Metrigy's success group, defined as those with the highest ROI and/or productivity gains for their collaboration investments, nearly 75% are increasing security spending.

75%

of companies in Metrigy's research success group are *increasing collaboration security spending*

Figure 2 on the following page shows the difference in where the most successful companies are increasing spending, versus all participants. The number of successful companies increasing security spending is almost 20% higher than participating companies as a whole, indicating that higher spending on security results in more measurable success in using collaboration applications.

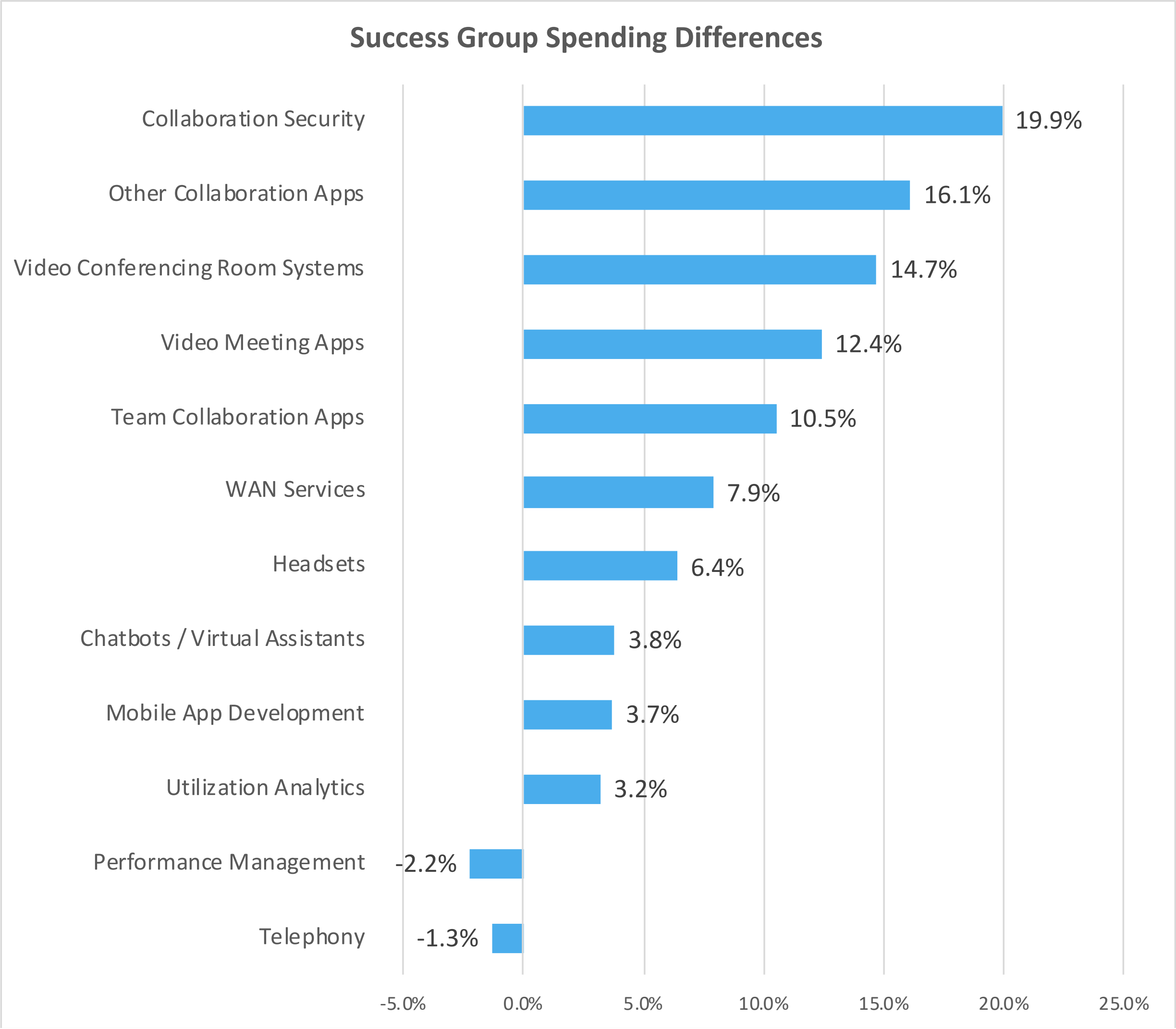

Figure 2: Success Group Spending Differences

Simply increasing spending on security isn't enough to address potential risks: Organizations need a proactive strategy that identifies threats and implements appropriate mitigation and monitoring measures. Today, just 40.8% of organizations have created a comprehensive workplace collaboration security strategy, and 54.2% have created one for their contact center. However, when analyzed further for workplace collaboration, 65.5% of successful companies have such an approach versus just 27.6% of our non-success group (those with below-average ROI or productivity gains for their collaboration investments.) (Please see Figure 3.).

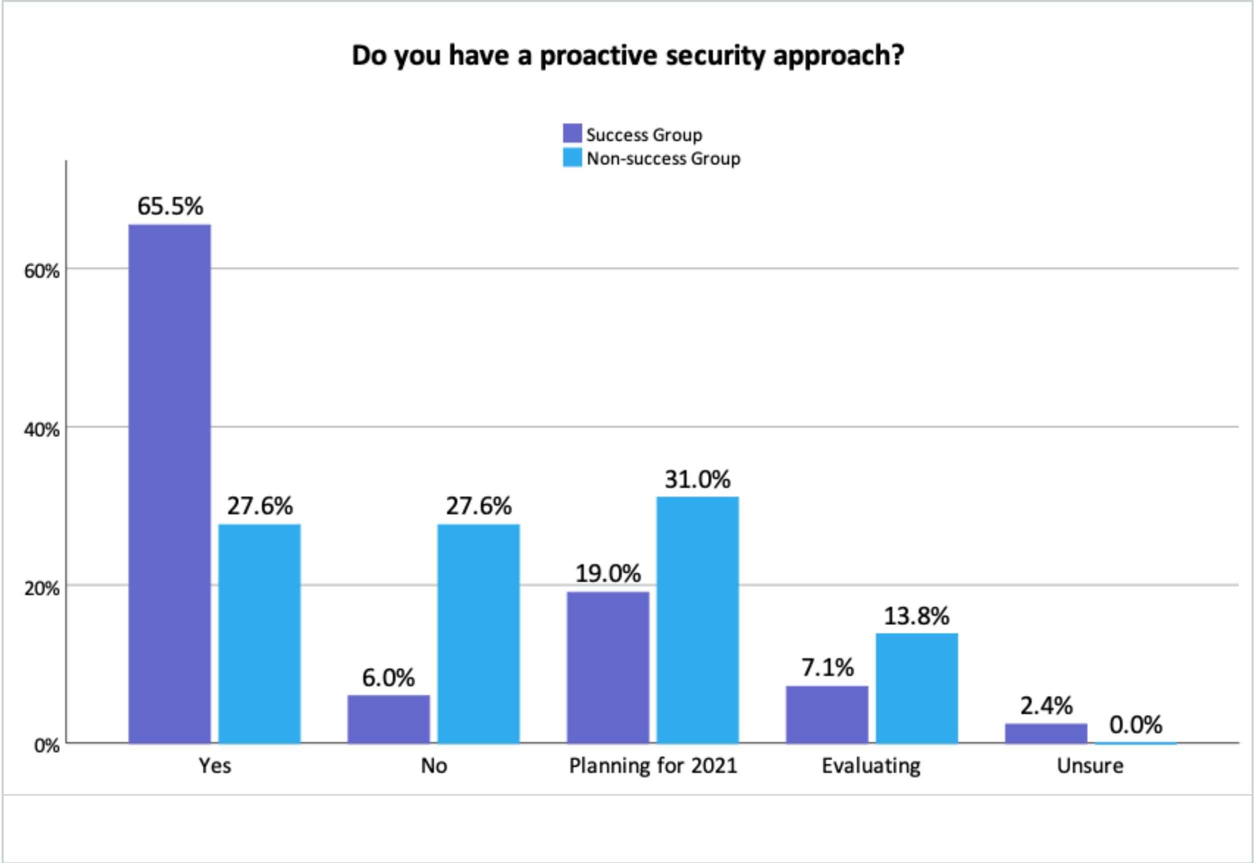

Figure 3: Do you have a proactive security approach?

The Benefits of End-to-End Encryption

Today, all calling, meeting, and team collaboration providers offer some level of encryption. Most often, sessions between endpoint and application servers are encrypted (i.e., "encryption in transit") and data stored on software clients and application services is encrypted, as well ("encryption at rest").

However, many providers do not guarantee end-to-end encryption as they need to decrypt customer data for a variety of purposes including to perform analytics, search indexing, transcription and translation, or to support other features.

This lack of end-to-end encryption means that not only are customers sharing data with their providers, but that those providers can potentially share that data with requesting government agencies, or that data is potentially vulnerable to an attack on the providers application servers or network infrastructure. To overcome these risks, the solution is to implement end-to-end encryption.

What is End-to-End Encryption?

Almost 41% of our research participants say that end-to-end encryption is a “must have” feature as they evaluate collaboration applications and services. But unfortunately, the market has delivered varying definitions of end-to-end encryption.

In a true E2E environment, the application service provider will have no ability to decrypt messages

End-to-end encryption means that only parties involved in a conversation (be it voice, video, or messaging) are able to decrypt messages sent between one-another. Only the customer holds access to the keys to decrypt their data.

E2E can apply to 1:1 audio / video / chat sessions, or multi-person calls, chats, or video conferences. It can also extend to cover additional applications and features including whiteboarding.

In a true E2E environment, the application service provider will have no ability to decrypt messages. Instead, decryption keys are only held by the customer. Therefore, E2E offers the highest level of data protection ensuring that an application provider has no ability to view customer data, nor share unencrypted data, nor risk having unencrypted data exfiltrated via attack.

As a growing number of companies adopt Zero Trust security models that are based on treating all endpoints, users, and application providers as untrusted, E2E enables the treating of application service providers as untrusted, as well.

Which E2E Approach is Best?

It’s important to understand that all E2E approaches are not the same. Significant differences continue to exist in the market in the way that vendors implement E2E, and in the features that they support when E2E is enabled.

For example, in most cases, enabling E2E for a video meeting service means that participants are not able to dial in to the meeting using a phone as the connection between the audio-conferencing gateway and the phone is not encrypted. Other capabilities, such as call recording and transcription, may not be supported when using E2E as they require the provider to be able to decrypt customer data to create transcripts. In addition, connecting into video meetings using legacy SIP or H.323 endpoints through gateways will generally not be supported because legacy endpoints will typically not support the same encryption standards as software clients.

Two Approaches to E2E

Providers wishing to offer E2E also have several architectural choices to pick from. They can build their own E2E implementation, ideally enabling third-party auditing to ensure a proper approach. Alternatively, two open-standards approaches exist: Signal Protocol and Message Layer Security.

Signal Protocol

Signal is an open-source protocol managed by The Signal Foundation. (https://signalfoundation.org). It has become a widely deployed protocol over the last few years but largely only for consumer messaging applications, like WhatsApp and Google Messenger, as well as the Foundation's own Signal app. The primary challenge in using Signal is that its key rotation approach is not well-designed for use in large group chats and is unable to guarantee forward secrecy (that is, protection against future compromise even if past conversations were hacked).

Key rotation involves the revocation and reissuance of new keys to avoid eavesdropping by someone who has through unauthorized means obtained decryption keys, or who should no longer be able to participate in a chat (e.g., a person who has left a company). Signal uses a broadcast reissuance method that potentially allows anyone who has successfully gained unauthorized access to a conversation to continue to decrypt messages. And it's E2E approach does not easily scale to large numbers of meeting or chat participants, potentially using multiple devices.

Message Layer Security (MLS)

To address the shortcomings of Signal, and to ideally eliminate the need for vendors to have to develop their own E2E implementations, several vendors began work on a new protocol. This led to the establishment by the IETF of the Message Layer Security protocol working group in 2018 (https://datatracker.ietf.org/wg/mls/) to enable E2E in conversations ranging from "two to thousands."[1]

As defined in the IETF informational draft document "draft-ietf-mls-protocol," MLS' key rotation approach enables infinite scale with unique key encapsulation for each endpoint, eliminating the risk of post-compromise access to past conversations and ensuring forward secrecy. MLS also provides features including integrity of messages, the ability to authenticate participant identity.

For example, in a scenario in which a user's mobile device is compromised, disabling messaging access from the device will prevent a hacker from both seeing past conversations prior to the last key rotation, future conversations from the device, and any user conversations on any other device.

[1] https://datatracker.ietf.org/doc/draft-ietf-mls-protocol/

MLS is rapidly emerging to become the de-facto standard for large-scale, end-to-end encryption of multimedia collaboration applications on any endpoint.

E2E: What to Look for in a UCaaS Provider:

Evaluating a UCaaS provider's encryption implementation is a critical function of a proactive collaboration security approach.

To successfully evaluate E2E implementations, organizations should:

1. Evaluate the underlying E2E protocol, ideally selecting a provider that has implemented, or is implementing MLS to ensure scalability for group conversations, to enable forward secrecy and post-compromise security
2. Ensure that the provider enables flexibility in enterprise key management to enable customers to choose the enterprise key management approach that works best for them to support Zero Trust
3. Ensure that the provider offers highly available services, ideally four 9's (99.99%) or better
4. Assess what features are available when E2E is implemented. A provider that can continue to deliver support for contextual search of chat or meeting transcripts, call recording and translation, and other value-added features when E2E is enabled provides an advantage over those who require that customers choose between E2E and advanced feature support
5. Consider supported devices. Ideally, providers will be agnostic and equally support E2E regardless of whether an end-user is using a company-provided device or a personal device or web browser
6. Review whether the provider has opened their E2E implementation to independent review by a trusted and well-known third party
7. Evaluate which endpoints support E2E. For example, are meeting room video conferencing systems, phones, or other peripherals supported?

Conclusions and Recommendations

End-to-end encryption is quickly becoming a core requirement to ensure security of enterprise communications and to support Zero Trust security models that control access to applications and data. Picking the right UCaaS provider requires careful evaluation of their security capabilities to ensure that they deliver protection against data loss, and that they provide end-to-end encryption to support Zero Trust security models.

However, not all E2E security approaches are alike, varying from home-grown approaches to those designed primarily for one-to-one conversations, to the more modern Message Layer Security (MLS) protocol specifically designed to provide scalable security for large numbers of conversation participants across multiple devices, web browsers, and software clients.

As they evaluate their go-forward security strategies as part of a proactive collaboration security plan, IT leaders should:

- Assess UCaaS provider security approaches, including support for end-to-end encryption, looking specifically for providers that are implementing MLS to deliver E2E across multiple devices
- Pay special attention to options for key management to ensure support for Zero Trust security
- Consider factors like guaranteed reliability and scale of E2E-supported applications.