Sécurité : que rechercher chez un fournisseur UCaaS

Le Zero Trust exige un modèle de sécurité évolutif basé sur les standards du marché.

T2-2021

Irwin Lazar
Président et analyste principal
Metrigy

Table des matières

Synthèse

Au début de la pandémie de COVID-19, de nombreuses entreprises se sont ruées sur les solutions cloud de communications unifiées en tant que service (UCaaS) et de visioconférences. Mais dans la précipitation, elles ont souvent négligé les questions de sécurité, s'exposant à un risque d'attaque ou d'accès non autorisé à leurs données.

Maintenant que le travail hybride est devenu la nouvelle norme, les chefs d'entreprise ainsi que les responsables de la sécurité et informatiques ont tout intérêt à ré-évaluer la sécurité de leurs applications cloud, notamment en s'assurant que leurs outils intègrent le chiffrement de bout en bout (ou E2EE pour End-to-End Encryption), et un modèle de sécurité dit « Zero Trust ».

Pour ce faire, les responsables informatiques devraient évaluer leurs stratégies de sécurité dans le cadre d'un plan de collaboration proactif. Les bonnes pratiques comprennent notamment :

- une approche collaborative de la sécurité, intégrant des évaluations de la sécurité des fournisseurs cloud ;
- l'évaluation de plusieurs approches d'implémentation de l'E2EE en se concentrant sur les fournisseurs ayant adopté le protocole émergent MLS (Message Layer Security) pour déployer l'E2EE sur plusieurs terminaux ;
- une analyse de l'impact de l'E2EE sur les fonctions de collaboration disponibles ;
- le choix d'un fournisseur offrant une flexibilité maximale en termes de gestion des clés de sécurité de l'entreprise.

L’impact du télétravail sur la sécurité

La pandémie de COVID-19 a bouleversé nos modes et lieux de travail. Et tout porte à croire que le télétravail s'ancre durablement dans nos nouvelles habitudes : ainsi, 12,4 % seulement des 476 entreprises ayant participé à l’étude mondiale de Metrigy « *Workplace Collaboration: 2021-22* » entendent faire revenir leurs collaborateurs au bureau à temps plein, alors que la majorité des employés travailleront désormais à distance au moins une partie du temps.

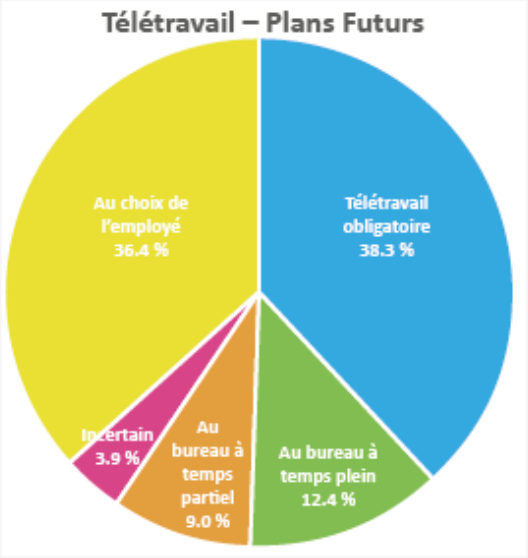

Figure 1 : Télétravail - plans futurs

Cette évolution du lieu de travail a fondamentalement modifié les modes de communication et de collaboration. Le passage au télétravail a en effet accéléré l’adoption d’applications cloud, notamment de visioconférences et de messagerie d’équipe. Pas moins de 47,5 % des entreprises interrogées ont recours aux UCaaS soit pour tous leurs besoins de téléphonie, soit en complément d’une plateforme existante dans le cadre de leur migration vers le cloud. Elles sont plus de 50 % à utiliser des plateformes de réunions en ligne basées sur le cloud, et plus de 80 % à affirmer que les visioconférences constituent une technologie importante, voire déterminante, pour leur activité.

L’essor du télétravail est aussi à l’origine d’un changement dans les habitudes de communication des employés. Près de 44 % des participants rapportent ainsi une baisse de leur utilisation du téléphone au profit d’applications de visioconférences, qu’ils utilisent pour communiquer avec une ou plusieurs personnes.

Nouveaux outils, nouveaux besoins en matière de sécurité

Conséquence de ces changements rapides en termes de lieu de travail et d'applications de collaboration : les responsables de la cybersécurité des entreprises font face à des défis majeurs. À présent, la majorité des applications n'est plus abritée dans un centre de données géré en interne et accessible uniquement par des terminaux exclusivement connectés au réseau de l'entreprise, ou par un petit nombre d'employés distants via un VPN. Les responsables informatiques doivent maintenant composer avec des employés utilisant une foule d'applications, non testées et souvent peu connues, pour se réunir, échanger des messages et s'appeler. Le risque pour les chefs d'entreprises et responsables informatiques : perdre le contrôle des données une fois celles-ci saisies dans le giron d'un fournisseur cloud. Difficile de savoir précisément comment leurs fournisseurs enregistrent et conservent leurs données, quelles méthodes de chiffrement ils utilisent, où les données sont stockées et quels processus ou applications peuvent y accéder. Même si les fournisseurs cloud chiffrent les données qu'ils enregistrent, celles-ci peuvent faire l'objet de demandes d'accès de la part d'instances gouvernementales sans que l'accord ou la notification du client soit nécessaire, ou risquer de finir entre les mains d'employés mal intentionnés.

Le niveau de sécurité des systèmes de collaboration en entreprise

Pour faire face aux risques pour la sécurité induits par le télétravail, la plupart des entreprises adoptent une stratégie réactive : elles utilisent des VPN pour contrôler l'accès des utilisateurs aux applications et édictent des règles en matière d'accès aux applications sur les points de connexion à Internet. Mais utiliser un VPN pour se connecter à des applications cloud est synonyme de coûts supplémentaires, de complexité accrue et de perte de temps en raison du nécessaire transfert du trafic audio et vidéo via le WAN (réseau de télécommunication privé) de l'entreprise.

Plus récemment, certaines entreprises sont passées au « split tunneling », une méthode permettant aux personnes en télétravail de se connecter directement au cloud via leur connexion Internet locale. Si cette solution permet de limiter la perte de temps, elle crée aussi de nouvelles vulnérabilités, car les terminaux d'un utilisateur peuvent devenir des vecteurs d'attaques.

Vu les risques liés aux VPN et au split tunneling, il n'est guère étonnant que près d'un tiers des participants à notre enquête affirme considérer la sécurité comme l'une des principales difficultés liées au télétravail.

Les dépenses de sécurité sont en hausse

Face à ces écueils, environ 55 % des entreprises augmentent leurs dépenses dans la sécurité de la collaboration en vue de mieux cerner et limiter les risques. Parmi tous les participants à l'étude de Metrigy qui enregistrent le retour sur investissement et/ou les gains en productivité les plus élevés au titre de leurs investissements dans la collaboration, **75 % environ augmentent leurs dépenses dans la sécurité**.

La figure 2, à la page suivante, montre les domaines dans lesquels les entreprises les plus performantes augmentent leurs dépenses. Le nombre d'entreprises performantes augmentant leur budget de sécurité est près de 20 % supérieur à celui de toutes les entreprises participantes, ce qui prouve qu'investir davantage dans la sécurité accroît la réussite mesurable liée à l'utilisation d'applications de collaboration.

75 %

des entreprises les plus performantes de l'étude de Metrigy *augmentent leur budget alloué à la sécurité de leurs outils de collaboration.*

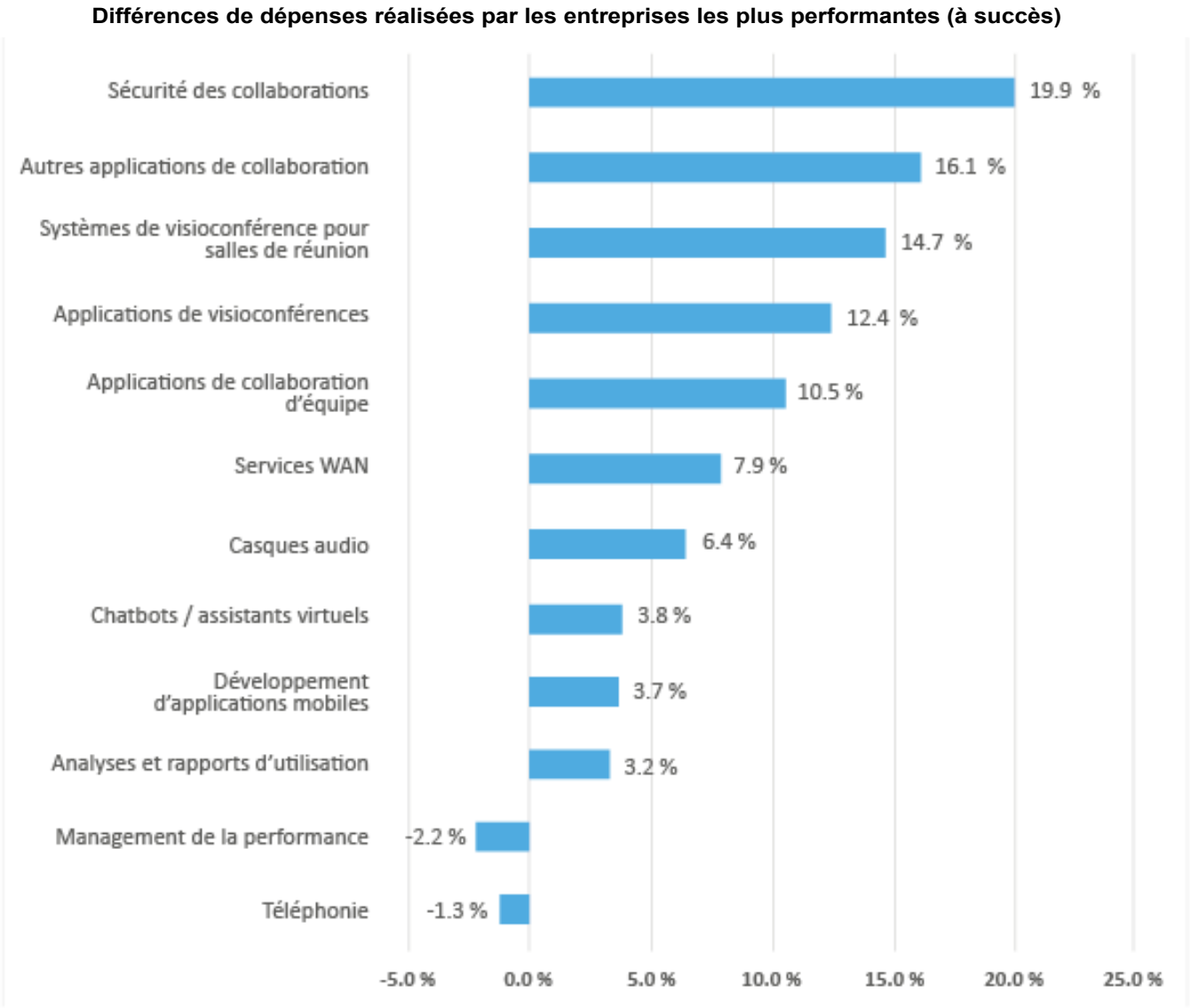

Figure 2 : Différences de dépenses réalisées par les entreprises les plus performantes (à succès)

Il ne suffit pourtant pas d'accroître ses dépenses dans la sécurité pour réduire les risques : les entreprises doivent adopter une stratégie proactive pour identifier les menaces et adopter des mesures de limitation et de surveillance adéquates. Aujourd'hui, 40,8 % seulement des entreprises ont mis au point une stratégie complète en matière de sécurité de la collaboration professionnelle, et 54,2 % d'entre elles l'ont fait pour leur centre de contact. Toutefois, une analyse plus poussée de la collaboration au poste de travail révèle que 65,6 % des entreprises les plus performantes adoptent ce type d'approche, contre seulement 27,6 % de celles qui affichent un ROI ou des gains de productivité inférieurs à la moyenne au titre de leurs investissements dans des solutions de collaboration. (Voir figure 3)

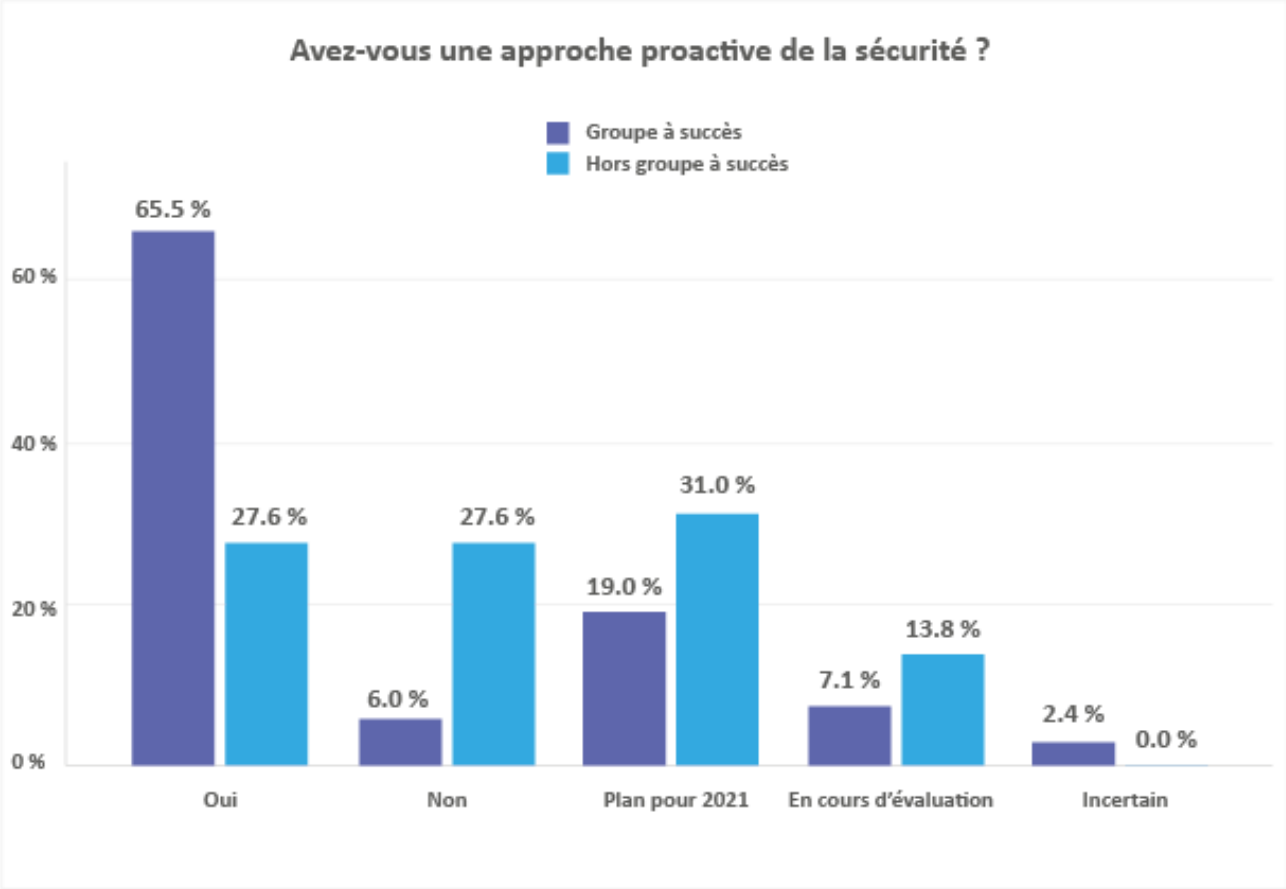

Figure 3 : Avez-vous une approche proactive de la sécurité ?

Les avantages du chiffrement de bout en bout

À l'heure actuelle, tous les fournisseurs de solutions de téléphonie, de visioconférences et de collaboration d'équipe offrent un certain niveau de chiffrement. Le plus souvent, les sessions entre un terminal et les serveurs des applications sont chiffrées (chiffrement en transit), tout comme les données stockées sur les clients logiciels et les services applicatifs (chiffrement au repos).

Pour autant, certains fournisseurs ne garantissent pas le chiffrement de bout en bout, car ils doivent déchiffrer les données de leurs clients à des fins notamment d'analyses, d'indexation de recherches, de transcription, de traduction, ou de prise en charge d'autres fonctionnalités.

Or, sans chiffrement de bout en bout, non seulement les clients partagent leurs données avec leurs fournisseurs, mais ces derniers peuvent aussi potentiellement partager ces données avec des instances gouvernementales l'exigeant. Pire encore : ces données peuvent faire l'objet d'attaques ciblant les serveurs applicatifs ou l'infrastructure réseau de ces fournisseurs. La solution, pour surmonter ces risques : passer au chiffrement de bout en bout.

Qu'est-ce que le chiffrement de bout en bout ?

Pour près de 41 % des participants à notre enquête, le chiffrement de bout en bout constitue un critère clé dans le choix d'une application ou d'un service de collaboration. Mais malheureusement, tous les acteurs du marché n'ont pas la même définition de ce concept.

Dans un véritable environnement d'E2EE, le fournisseur de services applicatifs ne peut pas déchiffrer les messages.

Avec le chiffrement de bout en bout (E2EE), seules les parties impliquées dans une discussion (que ce soit par téléphone, vidéo ou messagerie) sont capables de déchiffrer les messages qu'elles s'échangent. Seul le client a accès aux clés permettant de déchiffrer ses données.

L'E2EE peut s'appliquer aux sessions audio, vidéo et par chat entre deux personnes ou plus. Il peut aussi être étendu pour couvrir d'autres applications et fonctionnalités, y compris le tableau blanc virtuel.

Dans un véritable environnement d'E2EE, le fournisseur de services applicatifs n'a pas la possibilité de déchiffrer les messages. Seul le client détient les clés nécessaires au déchiffrement. L'E2EE constitue donc le niveau ultime de protection des données : il garantit que le fournisseurde l'application ne peut ni consulter les données du client, ni partager des données non chiffrées, ni risquer d'exfiltrer des données non chiffrées via une attaque.

Alors qu'un nombre croissant d'entreprises adoptent des modèles de sécurité Zero Trust consistant à ne traiter aucun terminal, utilisateur ni fournisseur d'applications comme fiable, l'E2EE permet d'en faire autant des fournisseurs de services applicatifs.

La meilleure méthode d'E2EE ?

Il faut bien comprendre que toutes les approches du chiffrement de bout en bout ne se valent pas. Il existe encore des différences importantes sur le marché dans les modalités de mise en œuvre des fournisseurs et dans les fonctionnalités prises en charge avec l'E2EE.

Ainsi, le plus souvent, quand un service de visioconférences prend en charge l'E2EE, ses utilisateurs ne peuvent pas rejoindre une réunion en se servant d'un téléphone, la connexion entre la passerelle audio et le téléphone n'étant pas chiffrée. D'autres fonctionnalités, comme l'enregistrement et la transcription des appels, peuvent ne pas être proposées en parallèle de l'E2EE, car elles exigent que le fournisseur déchiffre les données du client pour créer les transcriptions correspondantes. De plus, il est généralement impossible de rejoindre des visioconférences à l'aide de terminaux SIP

ou H.323 existants via des passerelles, les terminaux existants n'étant généralement pas compatibles avec les mêmes standards de chiffrement que les clients logiciels.

Deux approches de l'E2EE

Les fournisseurs souhaitant offrir le chiffrement de bout en bout doivent choisir parmi différentes architectures possibles. Ils peuvent développer leur propre implémentation E2EE, si possible en autorisant les audits de tiers pour garantir une approche optimale. Mais ils peuvent aussi opter pour un des deux standards ouvert : le protocole Signal, ou le protocole MLS (« Message Layer Security »).

Le protocole Signal

Signal est un protocole en open source géré par The Signal Foundation. (https://signalfoundation.org). S'il s'est largement répandu ces dernières années, il reste principalement utilisé pour des applications de messagerie grand public telles que WhatsApp et Google Messenger, ainsi que pour l'application propre à The Signal Foundation, également appelée Signal. Son principal défaut réside dans le fait que sa méthode de rotation des clés n'est pas adaptée à une utilisation dans des chats impliquant de nombreux participants, et n'est donc pas capable de garantir la confidentialité persistante (c'est-à-dire la protection des données contre des risques futurs quand des discussions passées ont été piratées).

La rotation des clés consiste à créer de nouvelles clés pour éviter l'interception des échanges par une personne ayant obtenu des clés de déchiffrement par un moyen détourné, ou par une personne qui ne devrait plus être capable de participer à un chat (par exemple une personne qui aurait quitté une entreprise). Signal utilise une méthode de création de nouvelles clés par diffusion permettant en principe à toute personne ayant réussi à accéder à une discussion sans y être autorisée à continuer de déchiffrer les messages. De plus, son approche de l'E2EE ne peut pas s'étendre à un grand nombre de participants à une réunion ou à un chat susceptibles d'utiliser plusieurs terminaux.

Le protocole MLS (Message Layer Security)

Afin de pallier les défauts de Signal et, si possible, de faire en sorte que les fournisseurs n'aient pas besoin de développer leurs propres systèmes d'E2EE, plusieurs fournisseurs ont entrepris d'élaborer un nouveau protocole. Ainsi, l'IETF a créé en 2018 le groupe de travail du protocole Message Layer Security (https://datatracker.ietf.org/wg/mls/) afin d'appliquer l'E2EE à des discussions impliquant « entre deux personnes et des milliers »[1].

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

Comme l'indique le projet de document à visée informative de l'IETF « draft-ietf-mls-protocol », l'approche de rotation des clés du protocole MLS garantit une évolutivité infinie moyennant une encapsulation unique des clés pour chaque terminal, ce qui empêche tout risque d'accès non autorisé à des discussions passées et, ainsi, garantit la confidentialité persistante. Le protocole MLS fournit aussi des fonctionnalités telles que l'intégrité des messages, c'est-à-dire la possibilité de vérifier l'identité des participants.

Ainsi, en cas de piratage du terminal mobile d'un utilisateur, la désactivation de l'accès à la messagerie depuis le terminal empêchera le pirate informatique d'accéder aux discussions menées avant la dernière rotation des clés, aux discussions futures qui seront menées depuis ce terminal et à toute discussion menée par l'utilisateur sur un quelconque autre terminal.

En pleine expansion, MLS est en passe de devenir la nouvelle norme pour le chiffrement de bout en bout à grande échelle des applications de collaboration multimédia sur n'importe quel terminal.

E2EE : les caractéristiques d'un fournisseur d'UCaaS compétent

Les entreprises soucieuses d'adopter une approche proactive de la sécurité de la collaboration doivent impérativement évaluer la méthode de chiffrement mise en œuvre par les fournisseurs d'UCaaS.

Pour que cette évaluation soit parlante, il leur faut :

1. examiner le protocole d'E2EE sous-jacent, si possible en sélectionnant un fournisseur mettant en œuvre le MLS pour permettre son extension à des discussions de groupe, afin de garantir la confidentialité persistante et la sécurité post-compromission ;
2. s'assurer que leur fournisseur garantit une gestion flexible des clés de sécurité, permettant à leurs clients de choisir la méthode de gestion des clés qui leur convient le mieux pour appliquer un modèle Zero Trust ;
3. vérifier que le fournisseur propose un très haut niveau de disponibilité, si possible « quatre neuf » (99,99 %) voire plus ;
4. déterminer les fonctionnalités prises en charge avec l'E2EE : un fournisseur capable de continuer à garantir la recherche contextuelle dans un chat ou une transcription de réunion, l'enregistrement d'un appel, une traduction ou toute autre fonctionnalité à valeur ajoutée sera plus intéressant que ses concurrents obligeant leurs clients à choisir entre l'E2EE et la prise en charge de fonctionnalités avancées ;
5. examiner les terminaux pris en charge : l'idéal est d'opter pour un fournisseur garantissant l'E2EE quel que soit le terminal de l'utilisateur final, qu'il s'agisse d'un appareil fourni par une entreprise, d'un terminal personnel ou d'un navigateur Web ;
6. se renseigner pour savoir si le fournisseur a soumis sa méthode d'E2EE à l'audit indépendant d'un tiers réputé et de confiance ;
7. consulter la liste des terminaux compatibles avec l'E2EE : les systèmes pour salles de visioconférence, téléphones ou autres périphériques, par exemple, sont-ils pris en charge ?

Conclusions et recommandations

Le chiffrement de bout en bout est en passe de devenir déterminant pour la sécurité des communications des entreprises et pour soutenir les modèles de sécurité Zero Trust gérant les accès aux applications et aux données. Pour choisir le bon fournisseur d'UCaaS, il convient d'évaluer soigneusement ses fonctionnalités en matière de sécurité afin de s'assurer qu'il garantit une protection adéquate contre la perte de données et un chiffrement de bout en bout compatible avec des modèles de sécurité Zero Trust.

Néanmoins, toutes les méthodes de mise en œuvre de l'E2EE ne se valent pas : certaines se limitent aux discussions entre deux personnes, tandis que d'autres, plus modernes, à l'instar du protocole MLS, sont conçues spécifiquement pour offrir une sécurité pouvant s'étendre à un grand nombre de participants sur de multiples terminaux, navigateurs Web et clients logiciels.

Les responsables informatiques ont donc tout intérêt à évaluer leurs stratégies de sécurité dans le cadre d'un plan de collaboration proactif en :

- évaluant les approches de sécurité des fournisseurs d'UCaaS, notamment la prise en charge du chiffrement de bout en bout, en se concentrant sur ceux qui déploient le protocole MLS pour garantir l'E2EE sur plusieurs terminaux ;
- étant particulièrement attentifs aux options de gestion des clés pour garantir la sécurité Zero Trust ;
- tenant compte de facteurs tels que la fiabilité garantie et le caractère évolutif des applications prenant en charge l'E2EE.
