Élaborer une stratégie de sécurité pour la collaboration au travail

La nécessité d'une approche proactive

T2 2023

Irwin Lazar
Président et analyste principal
Metrigy

Sommaire

Résumé

La collaboration au travail évoluant à un rythme particulièrement soutenu, les équipes chargées de la sécurité, notamment des systèmes d'information (CSO/CISO), sont plus que jamais confrontées à des problématiques de contrôle et d'achat raisonné d'applications. La multiplication des applications de collaboration, les nouvelles fonctionnalités applicatives qui génèrent leur propre contenu et permettent le partage d'informations entre participants à une réunion ou à une discussion instantanée, l'intégration croissante des communications unifiées, des centres de contact et des fonctions fournies par API, sans parler de l'essor du travail hybride et à distance avec un accès aux applications de n'importe où, sont autant de défis à relever.

Dans ce contexte, les dirigeants d'entreprise, les responsables des technologies de l'information et de la sécurité doivent mettre en œuvre une stratégie de sécurité proactive afin de minimiser les risques de perturbations et de perte de données. La sécurité ne peut plus être considérée comme un acquis. Une approche adéquate de la sécurité passe par une évaluation des exigences dans ce domaine, un investissement si nécessaire dans des outils tiers et le recours à des fournisseurs d'applications de collaboration qui ont fait la preuve de leur engagement en matière de sécurité.

Metrigy recommande aux équipes de direction de travailler avec les responsables de la sécurité et des systèmes d'information afin de :

- Documenter les applications et fonctionnalités collaboratives utilisées au sein de l'entreprise et évaluer le risque de perte de données
- Élaborer une stratégie de sécurité proactive avec l'aide des équipes de sécurité des informations et de collaboration, mais aussi d'autres domaines comme les RH ou la gestion des réseaux
- Élargir les stratégies de sécurité en prenant en compte les centres de contact et les plateformes de communication en tant que service (CPaaS)
- Investir dans des plateformes de sécurité tierces pour centraliser et renforcer les contrôles de sécurité et de conformité mis en place par les fournisseurs d'applications de collaboration
- Passer en revue ce que proposent les fournisseurs d'applications en matière de sécurité et de conformité, notamment leurs certifications et les fonctionnalités de sécurité disponibles

Des défis croissants en matière de sécurité

La collaboration au travail s'est profondément transformée durant ces dernières années. La pandémie de COVID-19 a été le déclencheur d'un extraordinaire essor du travail à distance ou hybride et a poussé les entreprises à adopter toujours plus d'outils permettant aux équipes virtuelles ou géographiquement dispersées de communiquer et de collaborer, quel que soit leur localisation physique.

Le travail à distance s'est installé pour durer. Selon l'étude *Workplace Collaboration: 2023-24* menée par Metrigy auprès de 440 organisations dans le monde entier, seulement 25,2 % des entreprises prévoient de faire revenir leurs employés sur leur lieu de travail à plein temps. Pour la grande majorité d'entre elles, les options de travail à distance, hybride ou flexible vont perdurer.

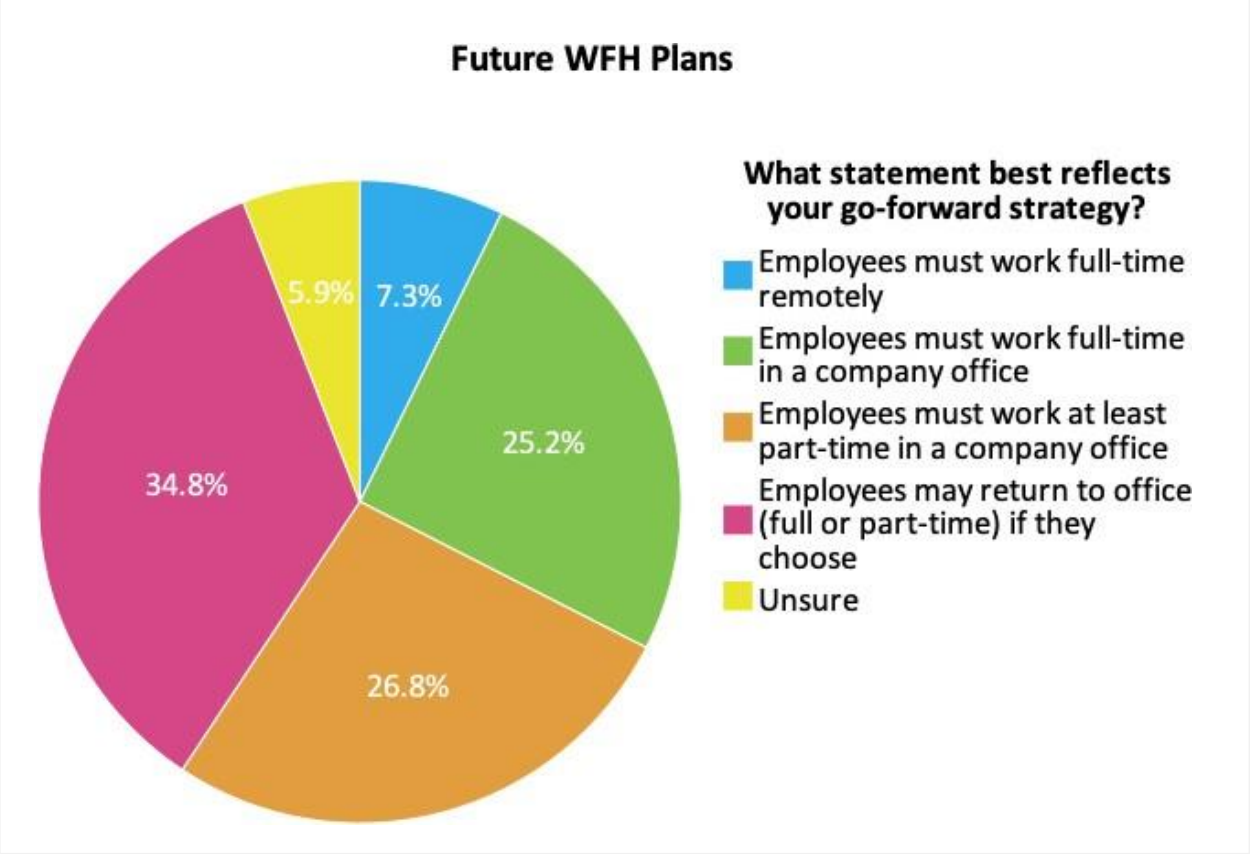

Figure 1 : Les évolutions envisagées du travail à distance

Ces évolutions dans l'organisation du travail se traduisent par de nouveaux défis à relever en matière de sécurité, de conformité et de gouvernance. Les employés n'utilisent plus un nombre limité d'applications centralisées et administrées à partir du centre de données de l'entreprise. L'environnement collaboratif d'aujourd'hui est généralement basé sur le cloud et les échanges, aussi bien au sein de l'entreprise qu'avec l'extérieur, se font par le biais d'une myriade d'applications et d'outils (courrier électronique, messagerie d'équipe, visioconférences, tableaux blancs virtuels, etc.).

Les applications elles-mêmes génèrent des données sous la forme d'enregistrements, de transcriptions et, plus récemment, de notes et d'évaluations créées par IA.

Avec la dispersion et la complexité croissante de l'environnement de collaboration, les incidents de sécurité se multiplient. Près de 15 % des participants à notre étude ont ainsi déclaré avoir subi au moins un incident de sécurité lié à la collaboration en 2022, deux fois plus qu'en 2021.

Pour protéger les données, la réputation et les activités d'une entreprise, ses dirigeants et ses responsables des systèmes d'information et de la sécurité doivent adopter une approche proactive qui identifie et limite les risques et avoir recours à des applications dotées de contrôles de sécurité alliant rigueur et flexibilité.

L'influence grandissante des équipes de sécurité

Compte tenu des défis croissants en matière de sécurité et de la multiplication des attaques, dont certaines ont fait grand bruit, via le cloud ou des services largement utilisés par le grand public, il n'est guère étonnant que les équipes de sécurité soient plus que jamais impliquées dans la prise de décision en matière de collaboration au travail. Parmi les participants à l'étude, un peu plus de la moitié ont indiqué impliquer des spécialistes internes de la sécurité, de la conformité et de la gouvernance dans leurs décisions d'achat de solutions collaboratives.

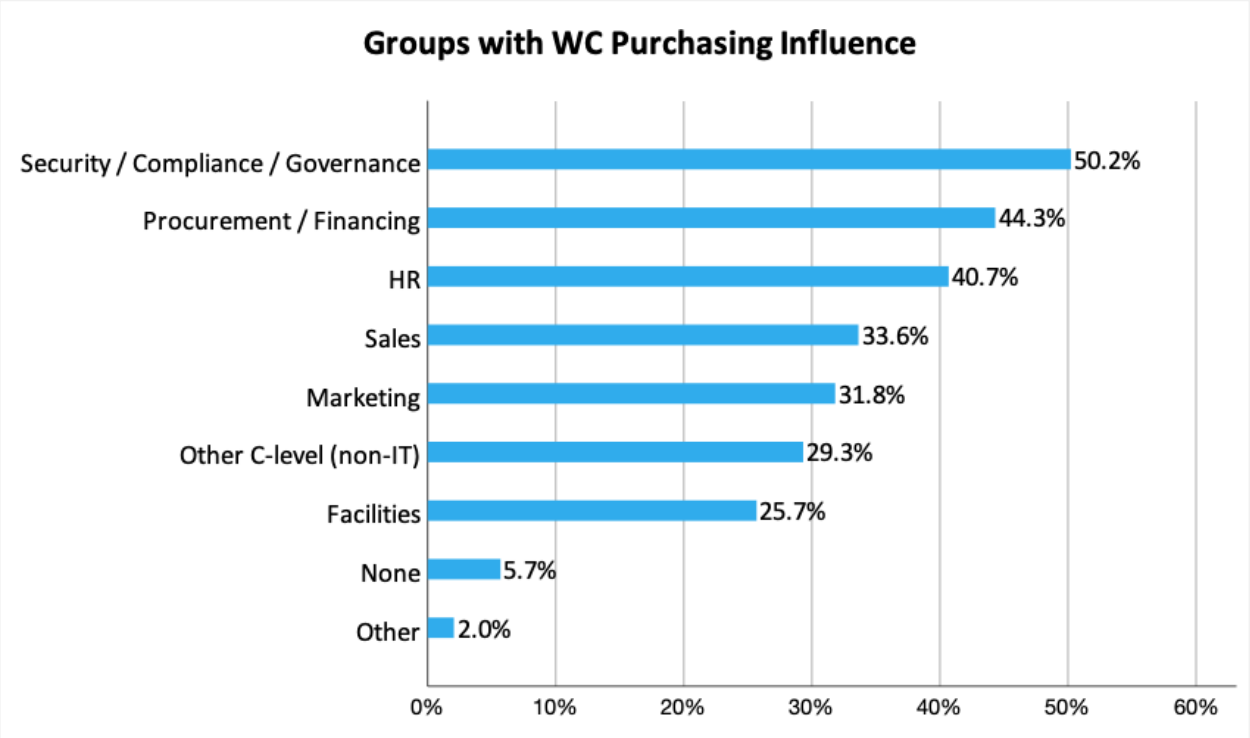

Figure 2 : Groupes impliqués dans les décisions d'achat de solutions collaboratives

En outre, près de 55 % des entreprises ayant constaté le niveau de retour sur investissement le plus élevé pour leurs dépenses en matière de collaboration ont intégré des experts de la sécurité et de la conformité dans la prise de décision.

Préparer l'évaluation des solutions de collaboration en matière de sécurité

Actuellement, les organisations ont une approche mixte de la sécurité de la collaboration au travail. Selon notre étude, l'équipe CISO/CSO est responsable de tout ou partie de la stratégie de sécurité de la collaboration dans près de 50 % des entreprises, tandis que dans près de 48 % d'entre elles, la équipes de collaboration portent la responsabilité de la sécurité. Dans certaines entreprises, les responsabilités sont partagées entre les équipes de sécurité, de collaboration et d'autres fonctions informatiques comme la gestion des réseaux ou celle des identités et des accès.

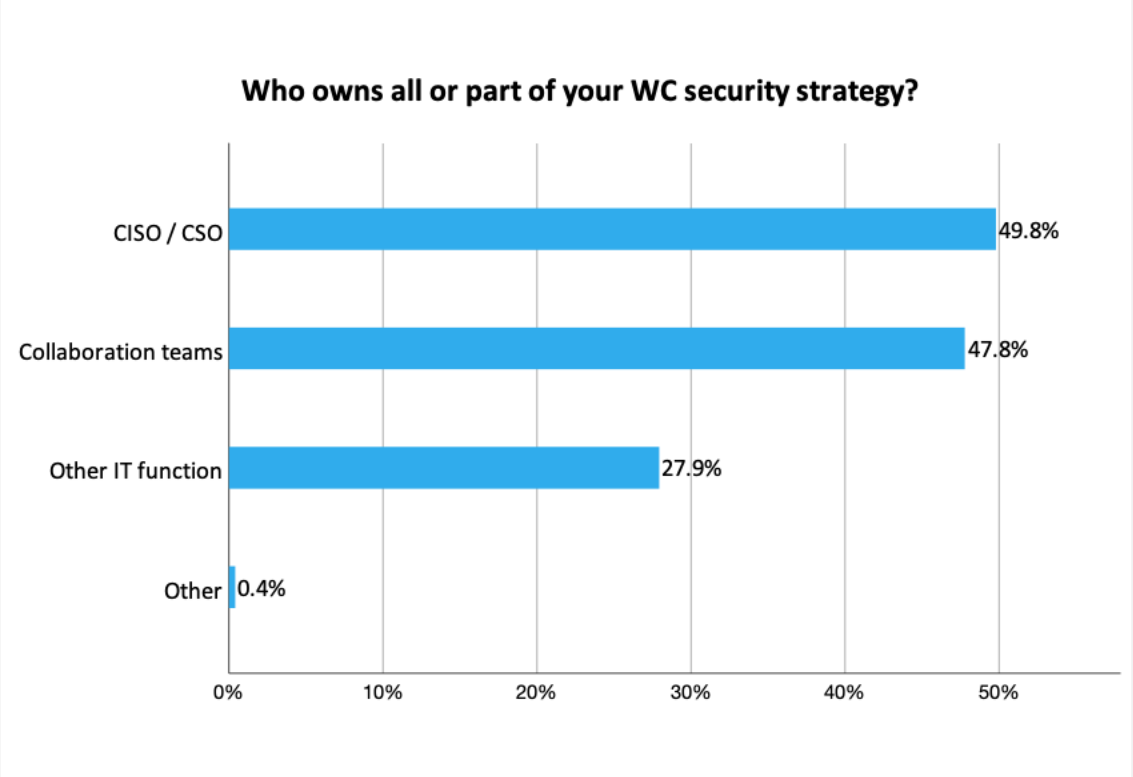

Figure 3 : Qui porte la responsabilité de la stratégie de sécurisation de la collaboration dans votre entreprise ?

Les équipes de sécurité ne sont pas impliquées dans la stratégie de sécurité de la collaboration dans près de 40 % des entreprises. Un chiffre préoccupant pour diverses raisons. Elles peuvent manquer d'informations sur les déploiements d'applications collaboratives et sur leurs usages, et orienter des décisions d'achat sans véritablement comprendre les besoins.

Elles doivent aussi connaître les tendances en matière de déploiement d'applications dans les entreprises modernes. Par exemple, parmi les participants à notre étude, près de 76 % prévoient de faire converger, ou font déjà converger, les plateformes de centre de contact et de collaboration vers un seul fournisseur. L'organisation doit donc être en mesure d'évaluer le niveau de sécurité fourni par une solution unifiée, et de définir des règles en fonction des risques, afin de protéger les données de l'entreprise et des clients.

Au-delà de l'ajout d'un centre de contact, près de 60 % des entreprises ont désormais recours à des services de communication en tant que service (CPaaS) proposés par leurs fournisseurs de solutions de collaboration ou d'autres fournisseurs. Selon notre étude, 25,5 % d'entre elles prévoient d'utiliser des services CPaaS d'ici fin 2023. Ce mode de fonctionnement génère de nouveaux défis pour les équipes de sécurité, qui doivent comprendre comment seront utilisés les services basés sur des API, quels sont les risques potentiels et comment limiter ces risques. Selon l'étude 2023 *Advanced API & CPaaS Development* menée par Metrigy auprès de 440 entreprises dans le monde entier, la sécurité constitue le principal défi à relever, 46,5 % d'entre elles réalisant des audits de sécurité réguliers et 44,6 % mettant en œuvre un processus d'authentification des API.

Élaborer une stratégie de sécurité proactive

Cela peut sembler évident, mais la première étape de l'élaboration d'une stratégie proactive de sécurité de la collaboration au travail est ... l'élaboration d'une stratégie proactive de collaboration au travail. Malheureusement, malgré la multiplication des menaces et des applications utilisées, la majorité des entreprises que nous avons interrogées dans le cadre de notre étude n'en ont toujours pas. Seules 37 % d'entre elles ont déclaré avoir mis en place une stratégie de sécurité proactive qui évalue les applications et les fonctionnalités utilisées, détermine les risques, et définit et met en œuvre des politiques de sécurité. Dans notre groupe des entreprises ayant constaté le meilleur retour sur investissement pour leurs dépenses en matière de sécurité, le pourcentage est beaucoup plus élevé, avec 42,4 % des répondants disposant d'une stratégie de sécurité proactive. Près de 19 % des entreprises interrogées prévoient de mettre en place une telle stratégie en 2023, tandis que 12,3 % d'entre elles réfléchissant à en élaborer une.

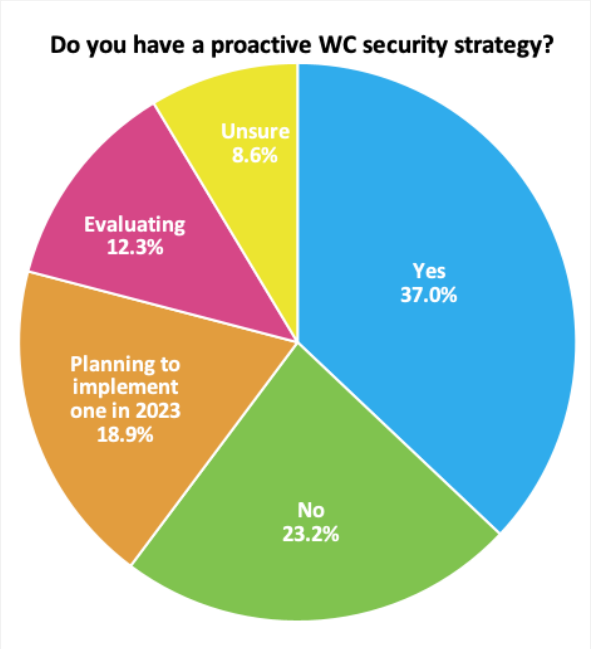

Figure 4 : Avez-vous mis en place une stratégie de sécurité proactive pour la collaboration au sein de l'entreprise ?

Différentes approches peuvent être adoptées, mais les finalités restent les mêmes :

- Protéger les applications contre les menaces internes et externes
- S'assurer que les employés ne divulguent pas, délibérément ou par inadvertance, des données potentiellement sensibles par le biais d'applications de courrier électronique, de messagerie ou le partage de fichiers
- Veiller au respect des exigences réglementaires appropriées
- Évaluer les fournisseurs d'applications de collaboration en fonction de leur capacité à assurer des fonctionnalités comme le chiffrement de bout en bout, avec un accès zéro confiance aux données. Leurs certifications et leurs pratiques en matière de sécurité doivent aussi être passées en revue
- Veiller à ce que les applications et les appareils soient toujours à jour au niveau logiciel et micrologiciel
- Prévoir un accès à distance sécurisé aux applications, avec le recours à un VPN, au chiffrement ou à des contrôles de sécurité appropriés dans le cas d'un accès direct au cloud

Les pare-feux et les passerelles de niveau application (ALG) sont les éléments de protection les plus couramment déployés dans le cadre d'une stratégie de collaboration sécurisée, comme le montre la figure 5 ci-dessous.

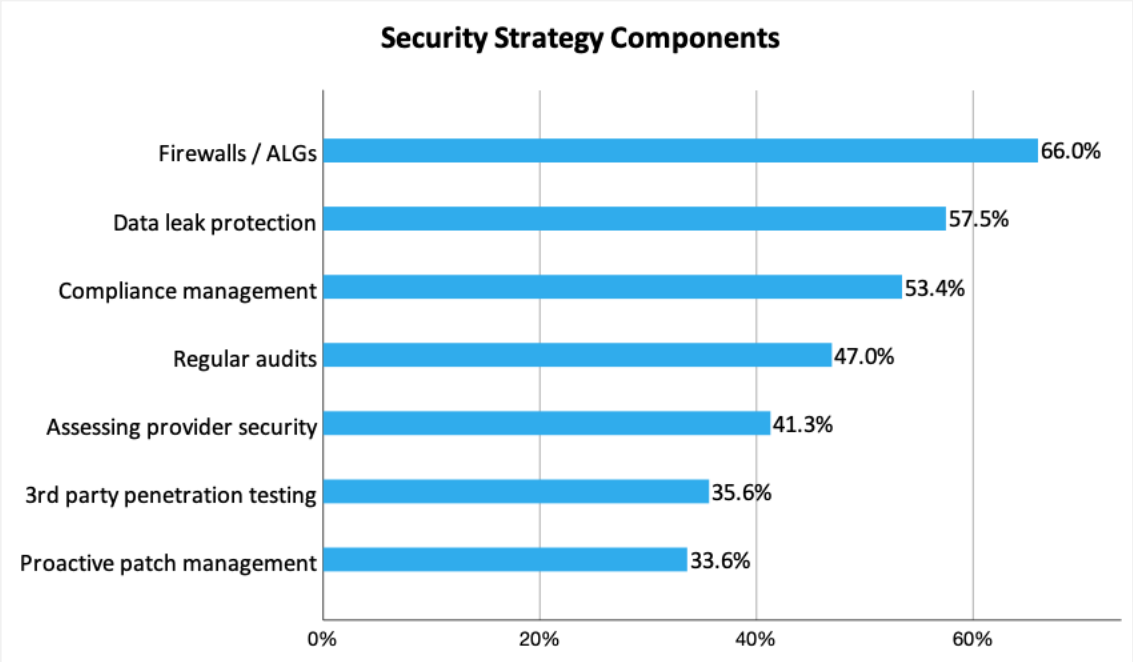

Figure 5 : Composantes de la stratégie de sécurité

Le rôle des plateformes de sécurité tierces

Pour soutenir leur stratégie de sécurité proactive, près de 26 % des organisations interrogées ont eu recours à des plateformes de sécurité tierces spécifiquement conçues pour protéger les applications de collaboration au travail, les centres de contact et autres applications de communication. Utilisés en complément des contrôles natifs proposés par les fournisseurs de logiciels et de services, ces outils mettent à disposition des responsables des systèmes d'information et de la sécurité les capacités dont ils ont besoin pour établir et appliquer des politiques cohérentes entre différentes applications et dans l'ensemble de l'organisation.

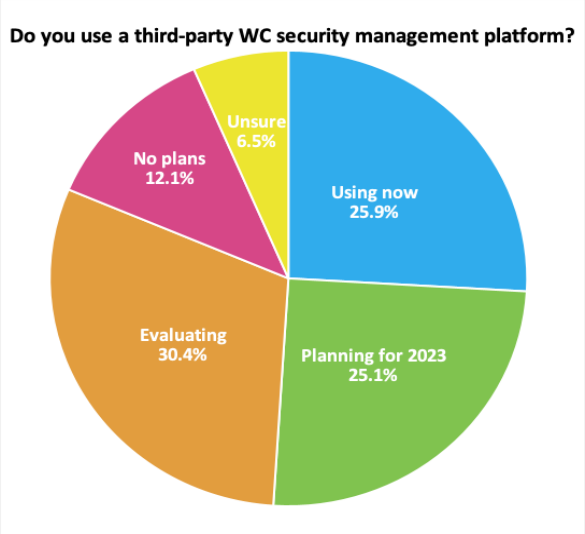

Figure 6 : Avez-vous recours à une plateforme de gestion de la sécurité pour la collaboration au travail ?

Sans la possibilité d'établir et d'appliquer les contrôles de sécurité nécessaires, les entreprises peuvent être contraintes de désactiver certaines fonctionnalités de collaboration, ce qui nuit à une communication de qualité entre les membres d'équipes géographiquement dispersées.

Selon notre étude, 19,4 % des entreprises ont désactivé certaines composantes de ces outils de collaboration pour des raisons de sécurité. Les fonctionnalités les plus souvent désactivées sont l'accès d'invités aux espaces de travail, les tableaux blancs virtuels, la messagerie d'équipe, la possibilité de chatter en cours de réunion, et l'enregistrement et la transcription des réunions.

Un grand nombre de fournisseurs proposent des plateformes pour sécuriser les différentes composantes de la collaboration au travail, comme le montre la figure 7 ci-dessous.

Vendor	Features
AudioCodes	Voice and endpoint security
Checkpoint	Email, file, DLP, archiving, compliance
LeapXpert	Messaging security
Oracle	Voice security
Proofpoint	Collaboration app security
Ribbon	Voice security
Safeguard Cyber	Messaging security and compliance
Smarsh	Compliance and archiving
Theta Lake	Compliance, risk identification, and DLP enforcement
Unisys (formerly Unify Square)	Collaboration app security and policy enforcement
Virsae	Collaboration app security

Figure 7 : Exemples de fournisseurs et de fonctionnalités de sécurité

Le déploiement de plateformes de sécurité tierces répond à différents objectifs, comme le montre la figure 8 ci-dessous. L'identification et l'atténuation des menaces arrivent en tête de ces objectifs, suivis par l'application de politiques de sécurité et la sécurité des communications vocales (en particulier pour les plateformes de communications unifiées et de centres de contact).

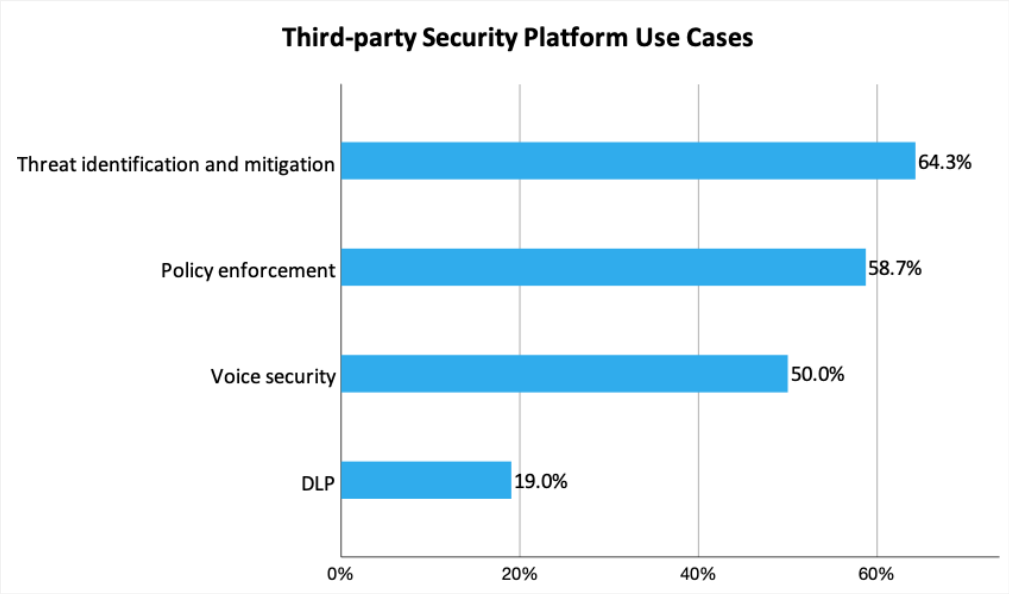

Figure 8 : Objectifs du recours à des plateformes de sécurité tierces

Le recours à des plateformes de sécurité tierces pour la collaboration au travail est financé par divers départements. Les équipes CISO/CSO sont le principal financeur dans près de 41 % des entreprises, suivies par les équipes de collaboration (26,2 %). Dans un peu plus de 18 % des entreprises, les équipes RH financent l'achat de plateformes de sécurité, souvent pour assurer la protection des informations permettant une identification personnelle et pour répondre à des exigences de conformité comme l'archivage et l'application de politiques RH.

Évaluer les capacités des fournisseurs en matière de sécurité

Tous les fournisseurs d'applications de collaboration n'offrent pas les mêmes garanties en matière de sécurité. La plupart d'entre eux proposent au minimum un chiffrement des données stockées et en transit, mais certains vont plus loin. Pour s'assurer que les contrôles de sécurité disponibles répondent à leurs besoins, les responsables des systèmes d'information et de la sécurité doivent évaluer leurs fournisseurs dans différents domaines, notamment :

- Le chiffrement de bout en bout et la confiance zéro : Le chiffrement de bout en bout garantit, si nécessaire, que le fournisseur de services n'a pas la possibilité de déchiffrer les communications sans l'accord du client. Environ 41 % des participants à notre étude considèrent le chiffrement de bout en bout comme une fonctionnalité indispensable pour les communications sécurisées et sensibles.

- Les certifications et capacités en matière de sécurité : Les contrôles de sécurité appropriés, par exemple liés au RGPD, aux normes ISO27001, ISO27017, ISO27018 et ISO22301, aux règles PCI, SOC 2+ et 3 ou HITRUST doivent pouvoir être mis en œuvre.
  Les certifications nationales doivent aussi être prises en compte. Les fournisseurs qui ont pris le temps et fait l'effort d'obtenir ces certifications démontrent leur engagement en faveur de la sécurité des opérations
- Le DevSecOps : Les entreprises doivent avoir mis en place des contrôles appropriés pour sécuriser le code tout au long du processus de développement.
- Les contrôles pour l'application des politiques : Le client doit pouvoir mettre en œuvre des contrôles granulaires sur l'accès aux applications et aux données, la disponibilité des fonctionnalités, la participation aux réunions, le délai d'inactivité, l'accès externe à la messagerie et la prise en charge des fonctions de sécurité comme l'authentification unique et l'authentification multifactorielle.
- La protection de la voix : De telles mesures incluent par exemple la protection contre les attaques par hameçonnage, la prise en charge des contrôles STIR/SHAKEN pour limiter les appels indésirables et le masquage des numéros et le respect des exigences de conformité pour les appels d'urgence.
- Les contrôles pour les appareils mobiles : Il peut s'agir d'une intégration avec des systèmes de gestion des appareils mobiles pour la distribution d'applications, ou de la possibilité de s'assurer que les appareils mobiles répondent à des normes minimales pour exécuter une application de collaboration.
- La conformité et la gouvernance : Le fournisseur peut par exemple proposer des fonctionnalités de capture et d'archivage de données provenant de diverses applications dans un entrepôt commun, souvent en s'appuyant sur un fournisseur de conformité tiers.

Conclusions et recommandations

Avec le travail hybride et l'adoption rapide de fonctionnalités de collaboration autrement que par la voix, les problématiques de sécurité revêtent une importance grandissante. La protection des utilisateurs, des données et de la réputation de l'entreprise passe par la nécessaire mise en place d'une stratégie proactive qui s'appuie sur des contrôles de sécurité natifs, des plateformes tierces et une évaluation rigoureuse des capacités du fournisseur de services de collaboration en matière de sécurité. Les responsables informatiques ont donc tout intérêt à :

- Documenter les applications et fonctionnalités collaboratives utilisées au sein de l'entreprise et évaluer le risque de perte de données
- Élaborer une stratégie de sécurité proactive avec l'aide des équipes de sécurité des informations et de collaboration, mais aussi d'autres domaines comme les RH ou la gestion des réseaux.
- Élargir les stratégies de sécurité en prenant en compte les centres de contact et les plateformes de communication en tant que service (CPaaS)
- Investir dans des plateformes de sécurité tierces pour centraliser et renforcer les contrôles de sécurité et de conformité mis en place par les fournisseurs d'applications de collaboration

- Passer en revue ce que proposent les fournisseurs d'applications en matière de sécurité et de conformité, notamment leurs certifications et les fonctionnalités de sécurité disponibles

---