vade
FOR GOOGLE WORKSPACE

Sécurité de la messagerie de Google Workspace : Renforcez vos défenses

DÉPLOYEZ VADE AVEC L'ACCOMPAGNEMENT DE CLICKSECURE

ClickSecure

DÉPLOYEZ VADE AVEC L'ACCOMPAGNEMENT DE CLICKSECURE

Dans le paysage numérique actuel, où les cybermenaces évoluent à une vitesse vertigineuse, la sécurité des plateformes de collaboration en ligne est plus critique que jamais. ClickSecure, une entreprise leader dans le domaine de la cybersécurité, se distingue par sa capacité à offrir des solutions de sécurité de pointe qui protègent les entreprises contre les attaques les plus sophistiquées. Notre collaboration avec Vade nous permet d'intégrer une couche de sécurité robuste et intelligente à Google Workspace, offrant ainsi à nos clients une tranquillité d'esprit inégalée.

Pourquoi Google Workspace a-t-il besoin de sécurité renforcée ?

Google Workspace, anciennement connu sous le nom de G Suite, est utilisé par des millions d'entreprises à travers le monde pour la collaboration et la communication. Malgré sa popularité, les fonctionnalités de sécurité natives de Google Workspace peuvent être insuffisantes pour contrer les cyberattaques modernes.

La Solution ClickSecure : Sécurité renforcée par Vade

ClickSecure a choisi de s'associer à Vade, un pionnier dans le domaine de la sécurité prédictive, pour intégrer sa solution de pointe dans Google Workspace. Cette intégration offre des fonctionnalités avancées telles que :

- Filtration Email de Prochaine Génération
- Détection Intelligente des Menaces
- Réponse aux Incidents Automatisée
- Intégration avec les Systèmes Externes

Engagement envers la Sécurité et la Conformité :

ClickSecure s'engage non seulement à fournir une sécurité de premier plan, mais également à assurer que cette sécurité aide les entreprises à rester conformes aux normes réglementaires en vigueur. En choisissant ClickSecure, vous optez pour une approche proactive de la sécurité informatique, réduisant ainsi votre surface d'attaque et renforçant vos défenses contre les cybermenaces émergentes.

SOMMAIRE

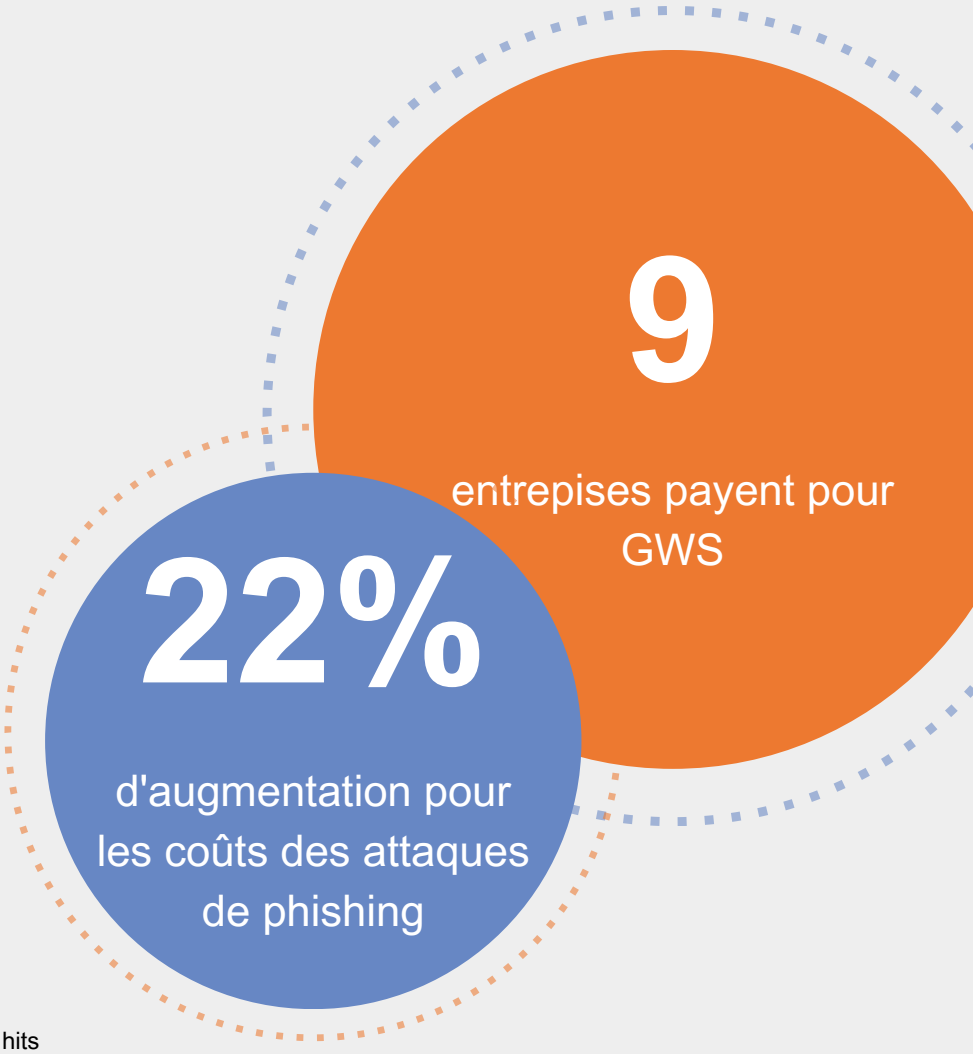
INTRODUCTION

Les suites de productivité sont devenues un outil professionnel essentiel. Plus de 70 % des entreprises en dépendent pour presque tous les aspects de leur activité, notamment la communication, la collaboration, la productivité, le stockage, etc.

Deux marques d'informatique dématérialisée se sont imposées comme les principaux fournisseurs de plateformes de productivité : Microsoft et Google. Si Microsoft reste la suite de productivité la plus populaire au monde, Google Workspace est également largement utilisé et continue de gagner des parts de marché. **En 2023, plus de 9 millions d'organisations payaient pour GWS, soit une augmentation de 80% depuis 2019.**[1]

Les suites de productivité sont conçues pour digitaliser le lieu de travail physique. Par exemple, les capacités de messagerie instantanée remplacent les communications physiques. Les vidéoconférences intégrées remplacent les réunions physiques, tandis que la somme combinée des applications fait de la proximité un luxe plutôt qu'une nécessité.

Bien que conçues pour l'efficacité et la productivité, ces plateformes n'ont pas pour priorité la sécurité. Des institutions respectées telles que Gartner ont appelé les entreprises utilisant des plateformes de productivité à compléter les fonctions de sécurité natives par des solutions dédiées proposées par des fournisseurs de cybersécurité tiers. Cette recommandation vise à lutter contre les menaces les plus avancées et les plus sophistiquées qui peuvent échapper à la détection des filtres de productivité.



1. Google Workspace, an office-software suite, hits 9 million paying organizations." Business Insider. 2023 March 14. https://www.businessinsider.com/google-workspace-9-million-paying-organizations-2023-3

Cependant, il semble que les organisations sous-estiment les vulnérabilités de ces plateformes et surestiment leurs capacités en matière de sécurité. Des études antérieures commandées par Vade ont confirmé cette position, bien que des recherches plus récentes soient nécessaires.[2]
Compte tenu de la réputation de Microsoft et de Google en tant qu'entreprises technologiques de premier plan, certaines entreprises pourraient accorder à la sécurité de ces plateformes une confiance plus grande qu'elle ne devrait l'être.

Il semble que les entreprises sous-estiment les vulnérabilités de ces plateformes et surestiment leurs capacités en matière de sécurité. Des études commandées par Vade dans le passé ont confirmé cette position, bien que des recherches plus récentes soient nécessaires.
Compte tenu de la réputation de Microsoft et de Google en tant qu'entreprises technologiques de premier plan, certaines entreprises pourraient accorder à la sécurité de ces plateformes une confiance plus grande qu'elle ne devrait l'être.

Il est clair que la dynamique du paysage des menaces encourage les hackers. Selon l'IC3, le coût des cyberattaques continue d'augmenter d'année en année. En 2023, les pertes subies par les victimes augmentaient de 22 % par rapport à 2022, toutes cybermenaces confondues.

Pourtant, pour les millions d'entreprises qui dépendent de Microsoft 365 et de GWS, la voie à suivre doit passer par la sensibilisation et l'action. Cela peut aider les entreprises à se protéger contre les menaces les plus sophistiquées du moment et éviter les impacts négatifs sur la continuité de leurs activités ou leur service.

2."The Time for MSPs is Now: SMB Cybersecurity Landscape Report 2022." Vanson Bourne. 2022.v

EMAIL : LE TALON D'ACHILLE DE GWS

L'email reste la principale forme de communication numérique dans le milieu professionnel. Pourtant, l'utilisation de ce canal essentiel va au-delà de la communication. Les utilisateurs s'appuient sur les emails pour :

- Gérer le calendrier et les invitations à des réunions.
- Partager et accéder à des fichiers.
- Accéder à d'autres applications de la suite de productivité.
- Utiliser un index consultable des conversations passées et des ressources numériques partagées.

L'**email joue un rôle prépondérant dans la hiérarchie des applications de GWS.** Son importance est à la fois définie par les caractéristiques de la plateforme et renforcée par le comportement des utilisateurs. L'email offre aux employés la facilité, la disponibilité et l'accès en temps réel qui en font le canal de communication numérique privilégié, que ce soit pour les travailleurs à distance, au bureau ou hybrides.[3]

Cependant, d'autres facteurs font de l'email un vecteur d'attaque particulièrement attrayant et productif pour les cybercriminels.

- L'email est également le moyen le plus direct pour les utilisateurs d'intéragir avec le monde extérieur. Il se trouve en première ligne de votre surface d'attaque.
- Le canal est géré par des humains vulnérables aux distractions, à une mauvaise hygiène cyber et aux erreurs.
- L'email est un centre de communication très actif - il envoie et reçoit de nombreux messages en permanence - ce qui augmente le risque de défaillance des mesures de sécurité.

"GWS est clairement une technologie puissante conçue pour la productivité, et non pour la sécurité."

3. Preferred communication method among office workers in the United States as of March 2023, by work location." Statista. 2023 August 24. https://www.statista.com/statistics/1407415/us-office-worker-top-communication-method-by-location/

LA SÉCURITÉ EMAIL DE GWS : LES RECOMMANDATIONS DE GARTNER

Dans ce contexte, la sécurité des emails doit être une priorité au sein de la plateforme GWS. Pourtant, les fonctions de sécurité natives de GWS laissent subsister des vulnérabilités critiques auxquelles les entreprises doivent remédier. Dans son Market Guide for Email Security 2023, Gartner reconnaît trois domaines dans lesquels les suites de productivité telles que GWS ne parviennent pas à fournir une protection adéquate :

1. Les attaques BEC et les scénarios mobiles.
2. Les menaces basées sur le texte, y compris les modèles de communication et les anomalies de style de conversation.
3. URL nécessitant une Computer Vision pour la détection.

À noter que **le coût des attaques BEC a atteint un niveau record, avec des pertes signalées s'élevant à 2,9 milliards de dollars (USD) au niveau mondial, selon l'IC3.**[4]
Entre-temps, Vade a détecté des attaques BEC plus sophistiquées, capables de contourner les protocoles d'authentification email qui complètent les capacités du GWS.

coût des cyberattaques en 2023

En outre, Gartner reconnaît également une limitation importante de GWS : l'intégration de l'intelligence email avec d'autres outils importants de cybersécurité. Il s'agit notamment de la gestion des informations et des événements de sécurité (SIEM) et des systèmes de détection et de réponse étendus (XDR), tous deux essentiels pour garantir une réponse et une investigation rapides en cas d'événements de sécurité et d'activité suspecte.

GWS est clairement une technologie puissante conçue pour la productivité, et non pour la sécurité. Plutôt que d'adopter GWS comme une plateforme tout-en-un, **les entreprises doivent adopter une approche "best-of-breed" et acquérir une alternative tierce qui complète leurs outils de sécurité.**[5]

4. Internet Crime Report 2023. Federal Bureau of Investigation. 6 March 2024. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report. pdf
5. "Top Email Security Predictions for 2024: How to Stay Ahead of Hackers." 2 November 2023. https://www.vadesecure.com/en/blog/2024-email-security-predictions

UNE APPROCHE COMPLÉMENTAIRE DE LA SÉCURITÉ NATIVE DE GWS

Une protection optimale et suffisante de GWS nécessite une solution de sécurité avancée, alimentée par l'IA. Celle-ci doit comprendre les éléments suivants.

Détection des menaces alimentée par l'IA

La détection des menaces alimentée par l'IA utilise à la fois l'apprentissage automatique et l'apprentissage profond pour analyser les menaces, en reconnaissant les modèles et les obscurcissements que l'analyse traditionnelle des URL ne peut pas faire. Il se compose de plusieurs fonctionnalités et capacités importantes, notamment :

Analyse instantanée des emails avant la remise

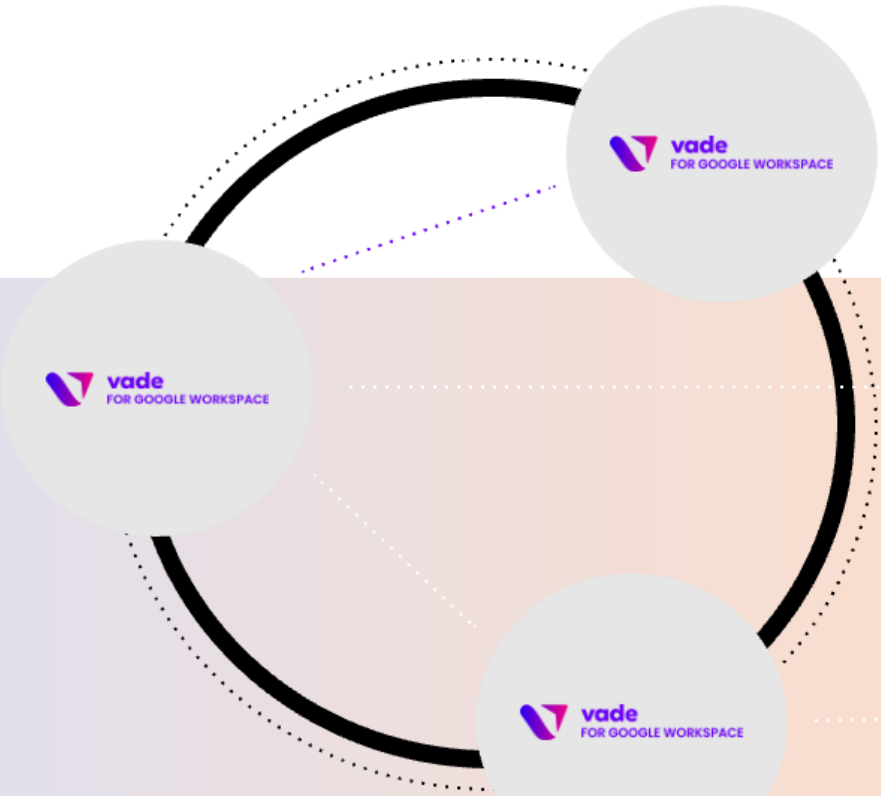
Les filtres de messagerie dotés d'une architecture "inline" analysent instantanément l'email avant de le délivrer dans la boîte de réception de l'utilisateur, et ce quasiment en temps réel. Contrairement à l'alternative basée sur l'API, les utilisateurs ne voient jamais un message potentiellement malveillant avant le filtrage. Parallèlement, cette architecture évite la mise en quarantaine des passerelles de messagerie et achemine les messages en temps quasi réel.

Algorithmes IA

Les algorithmes d'IA se présentent sous différentes formes et permettent de se défendre contre différents types de cybermenaces.

- Le **Machine Learning** analyse les éléments des emails, des liens, des pages web et des pièces jointes à la recherche de caractéristiques et de schémas uniques, tels que les redirections d'URL, le code obfuscé et les URL "bombes à retardement".

- Le **Computer Vision** analyse les images à la recherche de menaces, telles que les QR codes cachant des liens malveillants, les logos de marque manipulés et les images hébergées à distance.



- Les modèles de **Natural Language Processing** détectent les constructions grammaticales subtiles, les mots et les formulations qui caractérisent les attaques de spear-phishing.

- L'**IA générative** peut améliorer la capacité des modèles d'IA existants à détecter et à bloquer les menaces produites par l'IA générative, qui ne présentent souvent pas les signes d'alerte typiques des attaques produites par des sources humaines.

L'importance de l'humain et des données

L'intelligence et la précision de l'IA dépendent d'une alimentation continue en données statistiquement significatives, pertinentes et de qualité, provenant de moyens artificiels et humains. Dans le domaine de la sécurité des emails, cela se traduit par des informations en temps réel provenant du trafic d'email et des boîtes aux lettres protégées. Cela signifie également un flux constant de rapports d'utilisateurs, ainsi que des retours de data scientists et d'analystes de la cybersécurité. Ensemble, ces sources créent une boucle de rétroaction continue qui rend l'IA plus intelligente et plus performante.

Les capacités d'incident response

Pour construire un modèle de sécurité à plusieurs niveaux, les organisations ont besoin d'une technologie qui facilite une réponse précise et rapide aux incidents de sécurité. Cela inclut les capacités suivantes :

Automated remediation

Les nouveaux renseignements sur les emails peuvent révéler de nouvelles techniques d'attaque et de nouvelles menaces. Dans ce cas, les entreprises ont besoin de capacités de remédiation après livraison qui fonctionnent sans intervention humaine. La remédiation automatisée supprime les menaces nouvelles et émergentes des boîtes de réception des utilisateurs sur la base de nouveaux renseignements. L'IA est ainsi entraînée à devenir plus habile à détecter des menaces similaires à l'avenir lorsqu'elle les rencontrera, un modèle d'auto-apprentissage.

Manual remediation

Une réponse efficace aux incidents nécessite également la capacité à remédier manuellement aux emails, notamment en neutralisant les menaces et en normalisant les non-menaces. L'efficacité et la rapidité sont essentielles. Les emails qui nécessitent une correction doivent être rapidement localisés et simples à corriger.

THREAT INTEL AND INVESTIGATION

L'efficacité des activités de réponse aux incidents dépend de votre capacité à recueillir des informations sur les menaces et à mener des investigations sur l'ensemble de votre réseau. Outre les capacités de détection et de réponse, vous avez également besoin de solutions qui vous permettent d'analyser les menaces signalées par les utilisateurs, de recueillir des preuves médico-légales et d'intégrer les renseignements dans vos différents outils de cybersécurité.

Réponse aux incidents basée sur les utilisateurs
Les utilisateurs sont une source vitale de renseignements. C'est pourquoi vous avez besoin de solutions qui leur permettent de signaler facilement les emails suspects et qui permettent aux administrateurs de les examiner et d'y remédier en temps réel.

Analyse et inspection de fichiers en toute sécurité
Il est particulièrement important de télécharger et d'examiner en toute sécurité les menaces potentielles contenues dans les emails sans exposer vos administrateurs. Cela vous permet d'examiner les preuves médico-légales et de les utiliser pour comprendre la propagation potentielle des menaces dans votre réseau.

Intégrations avec SIEM, SOAR, XDR
L'email étant le principal vecteur d'attaque et la première source de renseignements sur les menaces, vous avez besoin de solutions qui intègrent vos journaux d'emails dans tout le système de gestion des informations et des événements de sécurité (SIEM), d'orchestration de la sécurité et de réponse automatisée (SOAR) ou de détection et de réponse étendues (XDR).

VADE FOR GOOGLE WORKSPACE

Vade for Google Workspace est une solution de sécurité de messagerie alimentée par l'IA pour Google Workspace qui bloque et corrige les menaces de messagerie avancées grâce à un puissant moteur d'IA qui attrape ce que Google ne voit pas. Le moteur d'IA de Vade apprend en permanence à partir d'une alliance de plus de 1,4 milliard de boîtes aux lettres protégées, de millions de rapports d'utilisateurs quotidiens et d'une équipe d'analystes en cybersécurité.

vade
FOR GOOGLE WORKSPACE

Vade for Google Workspace couvre la durée de vie de l'ensemble de l'email. Vade for GWS offre :

- Des couches de protection supplémentaires pour contrer davantage de menaces que Google seul.
- Une interface simplifiée et conviviale.
- Amélioration et précision de la classification du graymail
- Moins de faux positifs par rapport à Google.
- La visibilité, les outils et la technologie dont vous avez besoin pour réagir en cas de menace.
- Une boucle d'amélioration continue entre les utilisateurs et la technologie pour renforcer les deux.
- Des conditions permettant aux utilisateurs de participer plus efficacement à la boucle d'amélioration continue.

Fonctionnalités clés et caractéristiques

Anti-Phishing
Les algorithmes du Machine Learning et du Computer Vision effectuent une analyse comportementale, contextuelle et visuelle des emails et des pages web afin d'identifier les attaques de phishing.

Anti-Malware/Ransomware
Des algorithmes prédictifs et une analyse heuristique examinent les comportements et le code, identifiant les malwares et ransomwares dans les emails, les pièces jointes et les fichiers hébergés.

Anti-Spear Phishing
Les algorithmes de détection des anomalies et de traitement automatique du langage naturel identifient les tentatives d'usurpation d'identité et les modèles malveillants dans les emails de spear phishing.

Graymail Classification
Les emails de faible priorité, comme les notifications des réseaux sociaux et d'applications, encombrent les boîtes de réception des utilisateurs et nuisent à leur productivité. Vade classe les emails de faible priorité dans des dossiers Graymail pour que les boîtes de réception restent propres et que les utilisateurs restent concentrés.

Auto-remediation
Analyse en continu les boîtes aux lettres et supprime automatiquement les emails malveillants après leur distribution.

Threat Intel & Investigation
Triage et remédiation des emails signalés par les utilisateurs, déconstruction des emails et des pièces jointes, et injection des logs en live dans n'importe quel SIEM/SOAR/XDR.

Vade Remote Browser Isolation (RBI)
Il offre une protection complète contre les attaques de type "zero-day" qui proviennent d'un courriel et se déroulent via un navigateur.

À PROPOS DU GROUPE HORNETSECURITY

Vade est fière de faire partie du Hornetsecurity Group. Hornetsecurity est l'un des principaux fournisseurs mondiaux de solutions de sécurité, de conformité, de sauvegarde et de sensibilisation à la sécurité nouvelle génération basées sur le Cloud, qui aident les entreprises de toutes tailles dans le monde entier. Son produit phare, 365 Total Protection, est la solution de sécurité Cloud pour Microsoft 365 la plus complète du marché. Animé par l'innovation et l'excellence en matière de cybersécurité, Hornetsecurity construit un avenir numérique plus sécurisé et des cultures de sécurité durables grâce à son portefeuille primé. Hornetsecurity est présent dans plus de 120 pays grâce à son réseau international de distribution de plus de 12 000 partenaires et MSP. Ses services prémium sont utilisés par plus de 75 000 clients. Pour plus d'informations, visitez le site www.hornetsecurity.com.

ClickSecure

DÉPLOYEZ VADE AVEC L'ACCOMPAGNEMENT DE CLICKSECURE

Chez ClickSecure, nous comprenons que la sécurité de vos données et de vos communications est cruciale. Fondée par Thomas Délagrée, ancien Directeur des Systèmes d'Information (DSI), notre entreprise allie expertise technique pointue et relations de proximité pour offrir une protection adaptée à chaque client. En intégrant la solution de sécurité avancée de Vade pour Google Workspace, nous mettons à votre disposition une technologie innovante et en constante évolution, conçue pour anticiper et neutraliser les cybermenaces les plus sophistiquées.

Pourquoi choisir ClickSecure ?

- **Proximité :** Nous croyons en une relation directe et personnalisée avec chacun de nos clients, car comprendre vos besoins spécifiques est la clé pour vous fournir la meilleure protection possible.
- **Expertise :** Notre équipe d'experts utilise les technologies les plus avancées pour sécuriser vos environnements numériques, vous assurant une tranquillité d'esprit totale.
- **Engagement :** Chaque solution que nous proposons est le résultat d'un engagement profond envers la sécurité et l'efficacité, garantissant que vos activités peuvent se poursuivre sans interruption ni compromis.
- **Confiance :** Nous bâtissons des relations basées sur la confiance, ce qui nous permet de devenir un partenaire de sécurité fiable pour nos clients.
- **Innovation :** La technologie évolue rapidement, et nous aussi. Nos solutions sont toujours à la pointe de l'innovation, prêtes à faire face aux défis de demain.

Pour en savoir plus sur la manière dont ClickSecure peut protéger votre entreprise avec la solution de sécurité Vade pour Google Workspace, ou pour discuter de vos besoins spécifiques en matière de sécurité informatique, n'hésitez pas à nous contacter. Nous sommes là pour vous aider à naviguer dans le monde complexe de la cybersécurité avec confiance et expertise.

Contactez-nous aujourd'hui :
https://www.clicksecure.fr/contact/
01.87.76.25.79
contact@clicksecure.fr

Partenaires dans la sécurité, construisons ensemble un espace numérique sécurisé et dynamique pour votre entreprise.

ClickSecure