L'ARCHITECTURE DE L'EXFILTRATION SILENCIEUSE : ENQUÊTE SUR LA SURVEILLANCE SYSTÉMIQUE DANS L'ÉCOSYSTÈME CORPORATIF MODERNE

Chapitre 1 : Introduction et Grille de Lecture Stratégique

La transformation numérique des entreprises, accélérée par l'adoption massive du travail hybride, a engendré une mutation profonde des menaces pesant sur le patrimoine informationnel industriel. Si la cybersécurité traditionnelle se focalise encore majoritairement sur les intrusions externes malveillantes — rançongiciels, attaques par déni de service, ou menaces persistantes avancées (APT) — une réalité plus insidieuse s'est installée au cœur même des infrastructures légitimes. Nous définissons ce phénomène comme l'**Exfiltration Silencieuse**.

Contrairement à l'exfiltration hostile, qui implique une rupture des défenses, l'exfiltration silencieuse opère via les canaux de communication et de production autorisés, chiffrés et contractuellement validés par l'entreprise. Elle repose sur la collecte systémique de métadonnées, de télémétrie comportementale et de contenus propriétaires sous couvert d'optimisation de service, d'amélioration de l'expérience utilisateur et, plus récemment, d'entraînement de modèles d'intelligence artificielle.

Cette enquête se propose de déconstruire les mécanismes de cette surveillance en appliquant une grille de lecture tridimensionnelle, indispensable pour saisir la portée réelle du risque d'espionnage industriel au XXIe siècle.

1.1 Le Triptyque de la Vulnérabilité Structurelle

L'analyse de l'environnement technologique actuel révèle trois vecteurs de force convergents qui, ensemble, rendent les frontières de l'entreprise poreuses.

1.1.1 La Télémétrie Hypertrophiée et l'Économie de la Métadonnée

Le premier pilier est technologique. Les outils de collaboration (Microsoft Teams, Slack, Zoom) et de développement (VS Code, GitHub) ne sont plus des logiciels passifs. Ils sont devenus des capteurs actifs, générant des flux continus de télémétrie vers les éditeurs. Cette télémétrie ne se limite plus aux rapports d'erreurs techniques ; elle englobe désormais l'analyse comportementale (qui parle à qui, à quelle fréquence, sur quels sujets), la structure

sociale de l'organisation et la nature des projets de développement.[1] L'avènement de l'IA générative a exacerbé cette soif de données, transformant chaque interaction utilisateur en potentiel point de donnée pour l'entraînement de modèles globaux ou propriétaires.[3]

1.1.2 L'Extraterritorialité Juridique : CLOUD Act et FISA 702

Le second pilier est juridique. La majorité des infrastructures critiques utilisées par les entreprises occidentales (et mondiales) sont sous juridiction américaine. L'interaction entre le *Foreign Intelligence Surveillance Act* (FISA), spécifiquement sa section 702, et le *CLOUD Act* crée un cadre légal permettant aux agences de renseignement américaines d'accéder aux données stockées par des fournisseurs de services américains, indépendamment de la localisation physique des serveurs (même situés en Europe).[5] Pour une entreprise européenne de défense ou de haute technologie, cela signifie que la souveraineté de ses données est compromise dès lors qu'elles transitent par un cloud hyperscaler américain, exposant ses secrets industriels à une interception légalisée sous prétexte de sécurité nationale étrangère.[7]

1.1.3 La Convergence Actionnariale : L'Influence de BlackRock et Vanguard

Le troisième pilier est financier. Une analyse de la structure capitalistique des géants technologiques révèle une concentration inédite de la propriété. Les gestionnaires d'actifs comme BlackRock et Vanguard détiennent des parts significatives et souvent dominantes simultanément chez Microsoft, Salesforce (propriétaire de Slack), Zoom, Alphabet (Google), Amazon, et les fournisseurs de sécurité comme Zscaler ou CrowdStrike.[9] Cette "propriété commune" aligne les intérêts de l'ensemble de l'écosystème sur la maximisation de la valeur actionnariale, qui dépend aujourd'hui de la capacité à exploiter les données pour l'IA. Elle favorise une standardisation des politiques de confidentialité permissives et décourage une concurrence réelle sur la protection de la vie privée, créant un consensus de marché favorable à l'extraction de données.[12]

Chapitre 2 : Les Outils de Collaboration comme Vecteurs de Renseignement

Les plateformes de communication unifiée (UCC) constituent le système nerveux des organisations modernes. Elles transportent la voix, la vidéo, le texte et les fichiers, rendant leur analyse prioritaire pour tout acteur cherchant à comprendre la stratégie interne, les hiérarchies réelles et les projets confidentiels d'une cible.

2.1 Microsoft Teams : L'Omniscience du "Graph" et la Surveillance Managériale

Microsoft Teams, avec ses 320 millions d'utilisateurs actifs mensuels recensés en 2024, domine le marché de la collaboration.[14] Son intégration profonde dans l'écosystème Microsoft

365 en fait un outil de surveillance d'une puissance inégalée, alimentant le "Microsoft Graph", une cartographie dynamique de toutes les activités humaines au sein de l'entreprise.

2.1.1 De la Productivité à la Surveillance Comportementale : Viva Insights et Adoption Score

L'évolution la plus marquante de Teams est le passage de la simple métrique technique à l'analyse comportementale via des outils comme *Viva Insights* et le *Microsoft Adoption Score* (anciennement Productivity Score).[1] Ces outils agrègent des trillions de signaux quotidiens pour noter et analyser la "productivité" des employés.[2]

Analyse de la Menace :

Pour un analyste en espionnage industriel, l'accès à ces rapports — que ce soit via une compromission de compte administrateur ou une interception de flux — fournit une vue radiographique de l'entreprise cible.

- **Identification des Cibles de Recrutement (HUMINT) :** L'analyse de sentiment et de "bien-être" intégrée dans Viva Insights permet d'identifier les employés en situation de burnout, désengagés ou isolés.[16] Ces profils constituent des cibles privilégiées pour des approches d'ingénierie sociale ou de recrutement par des concurrents.
- **Cartographie des Projets Critiques :** L'analyse des fréquences de réunions, des heures de travail atypiques et des graphes d'interaction permet de déduire l'existence de projets secrets (ex: fusion-acquisition, lancement de produit) bien avant leur annonce publique. Une intensification soudaine des échanges entre le département juridique et la R&D, visible via la télémétrie Teams, est un indicateur fort d'un dépôt de brevet imminent ou d'un litige.
- **Le Risque de l'Agent Boss :** Microsoft promeut le concept de "l'agent boss" et des firmes frontières gérées par des équipes hybrides humain-IA.[2] Cela implique que les décisions managériales seront de plus en plus basées sur des données algorithmiques opaques, dont les biais ou les manipulations pourraient déstabiliser une organisation.

2.1.2 Télémétrie Réseau et Signature des Flux

Au-delà de l'analyse sémantique, Teams génère une empreinte réseau spécifique via le *Call Quality Dashboard* (CQD) et le *Real-Time Analytics* (RTA).[18] Ces outils de diagnostic sont conçus pour aider les administrateurs IT, mais ils centralisent des données sensibles.

- **Exposition des Données de Localisation et d'Infrastructure :** Le RTA fournit en temps réel les adresses IP des participants (internes et externes), leur localisation géographique, le type de connexion (filaire, Wi-Fi, 4G/5G) et les détails matériels des périphériques (casques, caméras).[20]
- **Flux "Direct IP" et Risques P2P :** Dans certaines configurations, Teams établit des connexions média pair-à-pair (P2P) directes entre les clients pour optimiser la latence, contournant les serveurs centraux pour le flux média.[21] L'analyse de paquets (PCAP) de

ces flux révèle les adresses IP réelles des terminaux, même derrière un VPN d'entreprise si le "split tunneling" est activé pour optimiser le trafic Teams (pratique recommandée par Microsoft). Cela permet à un attaquant externe de cartographier l'architecture réseau interne et d'identifier les passerelles critiques.[23]

2.2 Zoom : La Controverse de l'Entraînement IA et la Persistance des Données

Zoom, bien que challenger face à Teams, reste un outil critique pour les communications inter-entreprises. Son histoire récente est marquée par des tensions répétées autour de l'utilisation des données pour l'entraînement de l'IA.

2.2.1 L'Incident des Conditions de Service de 2023-2024

La controverse majeure de 2023-2024 a mis en lumière la volonté des plateformes de s'approprier le contenu des utilisateurs. Les conditions d'utilisation (ToS) de Zoom avaient été modifiées pour accorder à l'entreprise un droit perpétuel et mondial d'utiliser le "contenu client" pour entraîner ses modèles d'IA.[4]

Bien que Zoom ait dû rétropédaler face au tollé général, en affirmant que le contenu audio/vidéo ne serait pas utilisé "sans consentement", l'analyse forensique des fonctionnalités actuelles comme *Zoom AI Companion* (anciennement Zoom IQ) montre une réalité plus nuancée.[25]

- **Traitement Obligatoire dans le Cloud :** Pour fournir des résumés de réunion, des chapitrages intelligents et des analyses de sentiment, le flux audio/vidéo doit être déchiffré et traité par les serveurs de Zoom ou de ses partenaires (comme OpenAI ou Anthropic).[26] Il n'existe pas de traitement local (Edge AI) pour ces fonctions lourdes.
- **Le Consentement Illusoire :** Les mécanismes d'activation de ces fonctionnalités sont souvent basés sur un opt-in de l'hôte, qui s'impose aux participants. Un invité externe (partenaire, sous-traitant) participant à une réunion Zoom où "AI Companion" est actif voit ses paroles analysées et potentiellement stockées sous forme de résumé textuel dans le cloud de l'hôte, échappant ainsi à son propre contrôle de données.[28]

2.2.2 Analyse des Flux et Signature Métadonnée

L'analyse technique du trafic Zoom révèle l'utilisation massive de protocoles UDP propriétaires et d'inspection ICMP pour la gestion de la qualité.[30] Contrairement au trafic HTTPS standard, les flux vidéo chiffrés laissent transparaître des motifs de trafic (Traffic Analysis) qui permettent de déduire l'activité :

- **Fingerprinting des Réunions :** La taille et la fréquence des paquets peuvent permettre de distinguer une présentation (partage d'écran statique, flux audio dominant) d'une discussion animée (flux vidéo et audio variables).
- **Vulnérabilités Historiques et Vecteurs d'Attaque :** Zoom a un historique de

vulnérabilités critiques, notamment l'exposition de données via des URL de réunion prédictibles ou non sécurisées.[31] L'utilisation récente de malwares imitant les invitations Zoom (campagnes de phishing sophistiquées utilisant l'IA) démontre que la confiance implicite accordée à la "marque" Zoom est un vecteur d'entrée pour l'espionnage.[32]

2.3 Slack : La Mémoire Non Chiffrée et le Risque de la Supply Chain

Slack (propriété de Salesforce) diffère de Teams et Zoom par sa nature asynchrone et sa persistance. Il agit comme une archive vivante de la connaissance de l'entreprise, souvent moins formelle et donc plus riche en informations contextuelles sensibles.

2.3.1 Le Défaut de Chiffrement de Bout en Bout (E2EE)

Une vulnérabilité structurelle majeure de Slack est l'absence de chiffrement de bout en bout par défaut pour la majorité des plans. Slack conserve les clés de déchiffrement des données au repos, ce qui signifie techniquement que l'éditeur (et par extension toute entité légale ayant juridiction sur lui, comme via le CLOUD Act) peut accéder au contenu des messages, fichiers et canaux privés.[34] Seule l'option "Enterprise Grid" avec le module EKM (Enterprise Key Management) offre un niveau de contrôle supérieur, mais elle reste rare et coûteuse.

2.3.2 L'Exfiltration via les Applications Tierces et l'IA

L'incident de sécurité impliquant *Salesloft Drift* en 2025 illustre parfaitement le risque d'exfiltration via la chaîne d'approvisionnement logicielle (supply chain).[36] Des tokens d'authentification compromis dans un chatbot tiers intégré à Slack ont permis l'exfiltration de données clients sensibles (contacts, détails de comptes) chez de multiples victimes, dont des entreprises technologiques majeures.

- **Risque d'Intégration :** Chaque application ajoutée à un espace de travail Slack (Jira, Google Drive, chatbots RH) augmente la surface d'attaque. Ces applications disposent souvent de droits de lecture étendus sur les canaux publics et privés.
- **Entraînement des Modèles Globaux :** La politique de confidentialité de Slack concernant l'IA a suscité des inquiétudes légitimes. Bien que Salesforce affirme ne pas entraîner ses LLM génératifs sur les données clients, des modèles de "recherche et d'intelligence" (autocomplete, ranking) utilisent des données agrégées.[3] Le processus d'opt-out pour ces modèles "globaux" est complexe et bureaucratique (email à l'admin), ce qui suggère une stratégie de collecte par défaut (opt-out vs opt-in).
- **L'Affaire Disney :** La fuite massive de 1,1 To de données internes de Disney en 2024, exfiltrées via Slack par le groupe "NullBulge", confirme que Slack est devenu une cible prioritaire ("soft target").[38] Les attaquants ont accédé non seulement aux messages mais aussi aux fichiers de stratégie, aux codes sources et aux données financières, démontrant que la compromission d'un espace Slack équivaut à la compromission de la mémoire institutionnelle de l'entreprise.

Tableau Comparatif des Risques de Surveillance UCC

Vecteur	Mécanisme de Surveillance Principal	Risque Juridique (US)	Risque Technique	Indicateur de Compromission
Microsoft Teams	Analyse comportementale (Viva Insights), Graph	Élevé (FISA/CLOUD Act)	Exposition IP directe (P2P), Télémétrie massive	Trafic anormal vers vortex.data.microsoft.com
Zoom	Analyse de contenu via AI Companion (transcriptions)	Élevé (CLOUD Act)	Fingerprinting de trafic chiffré, Phishing ciblé	Flux UDP vers IPs non-Zoom, exploitation de vulnérabilités
Slack	Archivage persistant non-E2EE, Apps tierces	Élevé (Propriété Salesforce)	Exfiltration via tokens d'apps tierces (OAuth)	Exportations massives de données, accès via IPs inconnues

---

Chapitre 3 : Les Plateformes de Développement comme Canaux de Fuite de Propriété Intellectuelle

Si les outils de collaboration capturent les intentions stratégiques, les environnements de développement intégrés (IDE) et les forges logicielles capturent le savoir-faire technique pur : le code source, les algorithmes propriétaires et les configurations d'infrastructure. L'analyse de VS Code et GitHub révèle une architecture propice à la fuite de capital intellectuel.

3.1 Visual Studio Code : Le Cheval de Troie de l'Environnement de Développement

VS Code n'est plus un simple éditeur de texte ; c'est une plateforme connectée, modulaire et hautement télémétrique. Sa domination du marché en fait le standard de fait, mais aussi le vecteur d'exfiltration le plus sous-estimé.

3.1.1 Télémétrie Granulaire et Profilage Technique

La documentation officielle de VS Code détaille trois niveaux de télémétrie : rapports de crash, erreurs et données d'usage.[39] C'est la catégorie "usage" qui présente un risque d'intelligence économique.

- **Signature Technologique :** Microsoft collecte des données sur les langages utilisés, les bibliothèques importées, la durée des sessions d'édition et les types de fichiers ouverts. Pour un analyste, ces métadonnées permettent de reconstituer la "stack" technologique d'une cible. Une augmentation soudaine de l'activité sur des fichiers .rs (Rust) ou des bibliothèques de cryptographie post-quantique signale un virage stratégique R&D bien avant la sortie d'un produit.
- **Processus d'Arrière-Plan :** VS Code maintient des processus actifs qui communiquent avec les serveurs Microsoft même en l'absence d'activité utilisateur apparente. Ces processus (mises à jour, vérification d'extensions, synchronisation de paramètres) créent un bruit de fond réseau qui peut masquer des canaux d'exfiltration plus malveillants.[39]

3.1.2 Les Tunnels Distants : Contournement du Périmètre

La fonctionnalité *Remote Tunnels* de VS Code Server permet aux développeurs d'accéder à leur environnement de travail depuis n'importe quel navigateur via les serveurs de relais Microsoft (tunnels vscode.dev).[42]

- **Évasion de Pare-Feu :** Ces tunnels initient des connexions sortantes (outbound) vers l'infrastructure Microsoft, contournant ainsi les règles de pare-feu traditionnelles qui bloquent les connexions entrantes. Cela crée une porte dérobée persistante au cœur du réseau de développement, accessible via une simple authentification GitHub/Microsoft.
- **Risque d'Exfiltration Latérale :** Un attaquant compromettant un compte GitHub développeur peut utiliser ces tunnels pour pivoter dans le réseau interne, accéder au code source et l'exfiltrer sans déclencher d'alertes IDS conventionnelles.

3.2 GitHub Copilot : La Pompe Aspirante Algorithmique

GitHub Copilot, alimenté par les modèles OpenAI et intégré nativement dans l'écosystème Microsoft, représente un changement de paradigme : le code n'est plus seulement stocké, il est "compris" et traité par une IA tierce.

3.2.1 Le Mécanisme d'Exfiltration Contextuelle

Pour fournir des suggestions pertinentes, Copilot ne se contente pas d'analyser la ligne de code active. Il prélève et transmet le "contexte" environnant : les lignes précédentes et suivantes, les fichiers ouverts dans les onglets adjacents, et potentiellement des structures de projet entières.[43]

- **Fuite de Secrets et de Logique Métier :** Ce contexte peut contenir des commentaires expliquant des algorithmes secrets, des clés API "hardcodées" temporairement, ou des données clients utilisées pour des tests. Ces informations quittent le périmètre sécurisé

de l'entreprise pour être traitées par les serveurs d'inférence de Microsoft/OpenAI. Bien que Microsoft affirme que les données des clients "Business" ne sont pas retenues pour l'entraînement [44], elles transitent néanmoins en clair (déchiffrées) dans la mémoire des GPU d'inférence.

- **Vulnérabilité au "Prompt Injection" :** Des recherches ont démontré la faisabilité d'attaques par injection de prompt indirecte. Un attaquant peut placer du code malveillant invisible (ex: dans des commentaires ou des fichiers markdown) dans un dépôt open-source. Lorsqu'un développeur d'entreprise ouvre ce dépôt avec Copilot, l'IA peut être manipulée pour exfiltrer des variables locales ou des secrets vers un serveur tiers via des requêtes générées automatiquement.[43]

3.2.2 Le Phénomène du "Vibe Coding" et la Perte de Contrôle

L'essor du "Vibe Coding" — l'utilisation de l'IA pour générer du code par des non-experts — aggrave le risque.[32] Les développeurs juniors ont tendance à copier-coller des blocs entiers de code propriétaire ou de données sensibles dans les interfaces de chat de l'IA pour obtenir de l'aide au débogage, alimentant directement les modèles avec de la PI critique. L'absence de garde-fous stricts (comme des politiques DLP empêchant le collage de code dans le navigateur) transforme ces outils d'aide en canaux de fuite massifs.

Chapitre 4 : L'Infrastructure de Sécurité Cloud comme Point de Compromission Unique

Le modèle de sécurité "Zero Trust" a paradoxalement conduit à une centralisation extrême du trafic via des plateformes SSE (Security Service Edge) comme Zscaler, Cloudflare ou Palo Alto Networks. Ces acteurs, censés protéger l'entreprise, se retrouvent en position d'intercepteurs universels ("Man-in-the-Middle").

4.1 Zscaler et l'Inspection SSL : Le Dilemme de la Confiance

Zscaler intercepte, déchiffre et inspecte la quasi-totalité du trafic web et applicatif de ses clients pour détecter les menaces.[46]

4.1.1 La Controverse de l'Entraînement IA sur les Logs (2025)

En 2025, une polémique a éclaté suite aux déclarations du CEO de Zscaler concernant l'utilisation de "trillions de signaux" et de logs complets pour entraîner leurs modèles d'IA défensive.[48]

- **Les URLs comme Vecteurs de Fuite :** Les logs de proxy contiennent les URLs complètes visitées par les utilisateurs. Dans le web moderne, les URLs contiennent fréquemment des paramètres sensibles : tokens de session, identifiants de documents (ex: Google Docs, SharePoint), requêtes de recherche interne, et parfois même des données

personnelles en clair.

- **L'Illusion du "Data Containment" :** Zscaler a tenté de rassurer en évoquant le concept de "Data Containment" [48], affirmant que les données clients ne servent pas à entraîner les modèles partagés. Cependant, la frontière technique entre "métadonnée d'entraînement" (utile pour l'IA) et "donnée confidentielle" (URL complète) est poreuse. Si l'IA apprend à reconnaître des "comportements anormaux" en analysant des structures d'URL spécifiques à une entreprise, elle a *de facto* ingéré une partie de la connaissance de cette entreprise.

4.1.2 Centralisation des Clés et Risque Systémique

Pour inspecter le trafic chiffré, Zscaler agit comme une Autorité de Certification (CA) intermédiaire, émettant des certificats à la volée.[50] Cela signifie que Zscaler possède les clés privées permettant de déchiffrer tout le trafic de ses clients.

- **Cible de Haute Valeur :** Cette architecture fait de Zscaler une cible irrésistible pour les services de renseignement. Une seule injonction FISA ou une compromission de leur infrastructure de gestion de clés donnerait accès au trafic clair de milliers d'entreprises mondiales simultanément.[51] C'est la définition même d'un Point de Défaillance Unique (SPOF) pour la confidentialité mondiale.

4.2 Les "Data Clean Rooms" : Le Blanchiment de Données B2B

Les partenariats stratégiques entre Salesforce, AWS, Google Cloud et Snowflake autour des technologies de "Data Clean Rooms" (DCR) institutionalisent le partage de données inter-entreprises.[52]

- **Partage de Données "Sans Copie" :** Les DCR permettent de croiser des bases de données clients (CRM, comportementales) sans échanger les fichiers bruts, via des requêtes fédérées. Si cela protège la donnée brute, cela permet néanmoins de construire des profils d'identité extrêmement précis par croisement.
- **Ré-identification et Espionnage :** Pour un acteur capable de corréler ces croisements (via une présence dans le capital de tous les acteurs, comme BlackRock), la capacité de ré-identification des individus ou des stratégies commerciales est immense.[55] Les DCR normalisent la circulation de la donnée client hors du silo de l'entreprise, augmentant la surface d'exposition aux réquisitions légales ou aux fuites par inférence.

Chapitre 5 : L'Étau Juridique et Financier

L'infrastructure technique décrite ci-dessus ne flotte pas dans le vide. Elle est ancrée dans un cadre juridique spécifique (le droit américain) et pilotée par une logique financière précise (la concentration actionnariale).

5.1 La Mécanique de l'Extraterritorialité : FISA 702 et CLOUD Act

L'analyse juridique confirme que la protection des données européennes hébergées par des fournisseurs US est largement illusoire face aux impératifs de sécurité nationale américains.

5.1.1 La Section 702 du FISA : L'Espionnage Légalisé

La section 702 du *Foreign Intelligence Surveillance Act* permet au gouvernement américain de cibler les communications de personnes non-américaines situées hors des États-Unis pour obtenir du "renseignement étranger".[7]

- **Définition Extensive du Renseignement :** La notion de "renseignement étranger" ne se limite pas au terrorisme. Elle inclut les informations nécessaires à la conduite des "affaires étrangères" des États-Unis. Cela couvre potentiellement les négociations commerciales stratégiques, les politiques énergétiques européennes, ou les avancées technologiques concurrentes (aérospatial, nucléaire, IA).[8]
- **Application aux Fournisseurs Cloud :** Les entreprises comme AWS, Microsoft, Google, Zoom et Salesforce sont des "fournisseurs de services de communication électronique" au sens du FISA et doivent obtempérer aux demandes d'interception, souvent accompagnées d'ordres de non-divulgation (Gag Orders).[57]

5.1.2 Le CLOUD Act : La Fin de la Souveraineté Territoriale

Le CLOUD Act (2018) a explicitement levé les obstacles juridiques à l'accès aux données stockées à l'étranger. Il oblige les fournisseurs US à livrer les données qu'ils contrôlent, peu importe où elles sont stockées (Dublin, Francfort, Paris).[58]

- **Conflit de Lois :** Ce texte place les filiales européennes des géants de la tech dans une position intenable : violer le RGPD (en transférant des données sans base légale adéquate) ou violer la loi US. L'histoire et la jurisprudence montrent qu'elles choisissent systématiquement la conformité avec leur maison mère américaine.[6]

5.2 L'Influence Normalisatrice de BlackRock et Vanguard

L'analyse de l'actionnariat institutionnel révèle pourquoi cette architecture de surveillance ne rencontre que peu de résistance de la part du marché.

5.2.1 La Propriété Commune (Common Ownership)

BlackRock et Vanguard sont les premiers actionnaires de Microsoft, Apple, Amazon, Alphabet, Salesforce, Zoom, et Zscaler.[9]

- **Alignement Stratégique :** Ces investisseurs ont un intérêt direct à ce que les données circulent librement entre ces plateformes pour alimenter l'économie de l'IA, qui est le principal moteur de croissance de leur portefeuille. Ils n'ont aucun intérêt à ce que Microsoft (qu'ils possèdent) protège trop fortement les données contre Zscaler (qu'ils possèdent aussi) ou contre Salesforce (idem).[10]

- **Gouvernance des Données :** Les votes de ces grands fonds lors des assemblées générales s'alignent généralement avec le management sur les questions de gouvernance, bloquant souvent les résolutions d'actionnaires activistes demandant plus de transparence sur les droits de l'homme ou la confidentialité des données.[12] Ils sont les architectes silencieux d'un écosystème où l'exfiltration de données vers l'IA est la norme par défaut.

Chapitre 6 : Synthèse et Recommandations Stratégiques

L'enquête démontre que l'entreprise moderne opère, souvent à son insu, au sein d'une architecture de surveillance intégrée. La "productivité" offerte par les outils SaaS se paie par une transparence totale vis-à-vis des éditeurs américains, de leurs actionnaires, et par extension, de l'appareil de renseignement des États-Unis. L'exfiltration n'est pas une anomalie ; c'est le modèle d'affaires.

6.1 Indicateurs Forensiques pour les Équipes SOC

Pour détecter cette exfiltration silencieuse, les équipes de sécurité doivent surveiller des signaux faibles spécifiques :

- **Anomalies Volumétriques SSL :** Surveiller les volumes de données sortants vers les domaines de télémétrie connus (vortex.data.microsoft.com, telemetry.zoom.us, events.stats.slack.com) en dehors des heures ouvrées.
- **Flux UDP/P2P Suspects :** Détecter les connexions UDP persistantes vers des IP résidentielles ou non identifiées (hors des plages officielles des fournisseurs), signes potentiels de tunnels ou de flux média détournés.[24]
- **Activité de Processus Fantômes :** Identifier les processus liés à VS Code ou Slack consommant des ressources CPU/Réseau alors que l'application est supposée être inactive.[41]

6.2 Recommandations de Contre-Mesures

Face à ce constat, une stratégie de "Souveraineté de Combat" est nécessaire :

1. **Ségrégation des Environnements Critiques :**
   - Interdire l'usage des outils SaaS grand public (Teams, Slack, Copilot) pour les projets classifiés ou de R&D sensible.
   - Déployer des environnements de développement isolés ("air-gapped" ou sans accès internet direct) pour le code source critique.
2. **Maitrise du Chiffrement (BYOK/HYOK) :**
   - Exiger des solutions permettant le "Bring Your Own Key" (BYOK) ou "Hold Your Own Key" (HYOK) où les clés de chiffrement sont stockées dans des HSM (Hardware

Security Modules) contrôlés par l'entreprise, rendant les données illisibles pour le fournisseur cloud sans coopération active.

3. **Durcissement des Politiques de Télémétrie :**
   - Utiliser les politiques d'entreprise (GPO, MDM) pour désactiver la télémétrie au niveau le plus strict ("Security" ou "Off") sur Windows, Office, et VS Code.[40]
   - Mettre en œuvre le blocage DNS des domaines de télémétrie non essentiels.
4. **Alternatives Souveraines et Open Source :**
   - Évaluer la migration vers des solutions auto-hébergées pour la messagerie (ex: Mattermost, Matrix) et le code (GitLab On-Prem) pour les périmètres les plus sensibles, afin de s'extraire de la juridiction du CLOUD Act.
5. **Audit Juridique et Contractuel :**
   - Refuser les clauses contractuelles floues concernant l'utilisation des données pour "l'amélioration du service" ou "l'entraînement de l'IA". Exiger des garanties écrites de non-entraînement sur les données confidentielles.

L'avenir de la sécurité industrielle ne réside plus dans la hauteur des murs périmétriques, mais dans la maîtrise souveraine des flux de données qui traversent les frontières numériques, juridiques et financières de l'entreprise.

Rapport compilé par : Analyste Bryan Ouellette du Lichen-Collectives, Cyber-Espionage & Audit d'Infrastructure Critique.

Ouvrages cités

1. Microsoft 365 Productivity Score vs. Worklytics Workplace Insights: A ..., dernier accès : février 10, 2026, https://www.worklytics.co/resources/microsoft-365-productivity-score-vs-worklytics-workplace-insights-2025-comparison
2. Breaking down the infinite workday - Microsoft, dernier accès : février 10, 2026, https://www.microsoft.com/en-us/worklab/work-trend-index/breaking-down-infinite-workday
3. Slack Linkedin Anthropic AI Training Data | Terms.Law, dernier accès : février 10, 2026, https://terms.law/2025/12/05/slack-linkedin-anthropic-ai-training-data/
4. Following Pushback, Zoom Says It Won't Use Customer Data to ..., dernier accès : février 10, 2026, https://www.darkreading.com/cybersecurity-analytics/following-pushback-zoom-says-it-won-t-use-customer-data-to-train-ai-models
5. Are US Cloud Services an emerging risk for European companies? - Gislen Software, dernier accès : février 10, 2026, https://www.gislen.com/us-cloud-services-emerging-risk/
6. Why do we choose not to use American cloud providers? - Hailey HR, dernier accès : février 10, 2026, https://haileyhr.com/blog/why-do-we-choose-not-to-use-american-cloud-provide/

7. FISA Section 702: Civil Rights Abuses | Brennan Center for Justice, dernier accès : février 10, 2026, https://www.brennancenter.org/our-work/research-reports/fisa-section-702-civil-rights-abuses
8. Reforming Section 702 of the Foreign Intelligence Surveillance Act for a Digital Landscape, dernier accès : février 10, 2026, https://www.csis.org/analysis/reforming-section-702-foreign-intelligence-surveillance-act-digital-landscape
9. Tracking Vanguard/Blackrock Corporate Ownership, dernier accès : février 10, 2026, https://blackrockvanguardwatch.com/
10. Do Vanguard, Blackrock, and State Street Run the World? | Flagship Financial Advisors, dernier accès : février 10, 2026, https://www.flagshipfinancialtn.com/blog/do-vanguard-blackrock-and-state-street-run-the-world
11. Who Owns LiveRamp Company? – PortersFiveForce.com, dernier accès : février 10, 2026, https://portersfiveforce.com/blogs/owners/liveramp
12. Margins: Estimating the Influence of the Big Three on Shareholder Proposals - SMU Scholar, dernier accès : février 10, 2026, https://scholar.smu.edu/cgi/viewcontent.cgi?article=4856&context=smulr
13. Full article: The New Permanent Universal Owners: Index funds, patient capital, and the distinction between feeble and forceful stewardship - Taylor & Francis, dernier accès : février 10, 2026, https://www.tandfonline.com/doi/full/10.1080/03085147.2020.1781417
14. Slack vs. Microsoft Teams: Which Is Best? (2025 Comparison) - CX Today, dernier accès : février 10, 2026, https://www.cxtoday.com/crm/slack-vs-microsoft-teams/
15. Microsoft Teams Revenue and Usage Statistics (2026) - Business of Apps, dernier accès : février 10, 2026, https://www.businessofapps.com/data/microsoft-teams-statistics/
16. Employee Wellbeing, Work Behaviours and Work Outcomes in a Hybrid Work Context: A Study of the Relationship Between Work, Health - RAND, dernier accès : février 10, 2026, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2000/RRA2083-1/RAND_RRA2083-1.pdf
17. How AI Helps Reduce Burnout and Improve Employee Wellbeing - TechClass, dernier accès : février 10, 2026, https://www.techclass.com/resources/learning-and-development-articles/how-ai-helps-reduce-burnout-improve-employee-wellbeing
18. Monitor call and meeting quality in Microsoft Teams, dernier accès : février 10, 2026, https://support.microsoft.com/en-us/office/monitor-call-and-meeting-quality-in-microsoft-teams-7bb1747c-d91a-4fbb-84f6-ad3f48e73511
19. Use real-time telemetry to troubleshoot poor meeting quality - Microsoft Teams, dernier accès : février 10, 2026, https://learn.microsoft.com/en-us/microsoftteams/use-real-time-telemetry-to-troubleshoot-poor-meeting-quality

20. Introducing Microsoft Teams Real-time Call Quality Analytics, dernier accès : février 10, 2026, https://techcommunity.microsoft.com/blog/microsoftteamsblog/introducing-microsoft-teams-real-time-call-quality-analytics/2912146
21. Microsoft Teams call flows, dernier accès : février 10, 2026, https://learn.microsoft.com/en-us/microsoftteams/microsoft-teams-online-call-flows
22. (PDF) DNS over HTTPS Detection Using Standard Flow Telemetry - ResearchGate, dernier accès : février 10, 2026, https://www.researchgate.net/publication/370740786_DNS_over_HTTPS_Detection_Using_Standard_Flow_Telemetry
23. TOWARD ZERO-WASTE TERABIT NETWORKED SYSTEMS Liangcheng Yu A DISSERTATION in Computer and Information Science Presented to the Fa, dernier accès : février 10, 2026, https://liangchengyu.com/doc/liangchengyu_phd_dissertation.pdf
24. Malware of the Day - C2 over ICMP (ICMP-GOSH) - Active Countermeasures, dernier accès : février 10, 2026, https://www.activecountermeasures.com/malware-of-the-day-c2-over-icmp-icmp-gosh/
25. Zoom sets AI Companion roadmap across platform - Constellation Research, dernier accès : février 10, 2026, https://www.constellationr.com/insights/news/zoom-sets-ai-companion-roadmap-across-platform
26. Optimize Zoom cloud recording workflows -- guidance and tips for developers for extracting data-rich AI-powered insights, dernier accès : février 10, 2026, https://developers.zoom.us/blog/openapi-guide-cloud-recording/
27. Evolving Zoom IQ, our smart companion, with new features and a collaboration with OpenAI, dernier accès : février 10, 2026, https://news.zoom.com/evolving-zoom-iq-our-smart-companion-with-new-features-and-a-collaboration-with-openai/
28. private zoom meetings recorded and/or used in AI training?, dernier accès : février 10, 2026, https://community.zoom.com/t5/Zoom-AI-Companion/private-zoom-meetings-recorded-and-or-used-in-AI-training/m-p/132580
29. Article - Zoom: AI Companion at U-M - TeamDynamix - University of Michigan, dernier accès : février 10, 2026, https://teamdynamix.umich.edu/TDClient/30/Portal/KB/ArticleDet?ID=10902
30. Monitoring Teams & Zoom on macOS Devices - Exoprise, dernier accès : février 10, 2026, https://www.exoprise.com/2024/01/15/monitoring-teams-zoom-macos/
31. Zoom Security Bulletins, dernier accès : février 10, 2026, https://www.zoom.com/en/trust/security-bulletin/
32. GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools | Google Cloud Blog, dernier accès : février 10, 2026, https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools

33. Exploring Information Security: Insights, Trends, and Strategies Blog, dernier accès : février 10, 2026, https://www.exploresec.com/blog
34. Microsoft Teams vs Slack (2025): Pros, cons, and what's best - Merlin computer, dernier accès : février 10, 2026, https://www.merlin.computer/blog/microsoft-teams-vs-slack-2025-pros-cons-and-what-s-best
35. What's Brewing at Slack? Controversy Over AI Training Policy | Salesforce Ben, dernier accès : février 10, 2026, https://www.salesforceben.com/whats-brewing-at-slack-controversy-over-ai-training-policy/
36. Cyber Alert: Salesloft Drift Breach and Associated Supply Chain Attack, dernier accès : février 10, 2026, https://www.hiroc.com/news/cyber-alert-salesloft-drift-breach-and-associated-supply-chain-attack
37. Slack Updates AI Principles After Customer Data Training Uproar - UC Today, dernier accès : février 10, 2026, https://www.uctoday.com/unified-communications/slack-updates-ai-principles-after-customer-data-training-uproar/
38. CIOs Lessons from Disney's Post-Breach Decision to Leave Slack - InformationWeek, dernier accès : février 10, 2026, https://www.informationweek.com/cyber-resilience/cios-lessons-from-disney-s-post-breach-decision-to-leave-slack
39. Telemetry - Visual Studio Code, dernier accès : février 10, 2026, https://code.visualstudio.com/docs/configure/telemetry
40. Manage telemetry in enterprise environments - Visual Studio Code, dernier accès : février 10, 2026, https://code.visualstudio.com/docs/enterprise/telemetry
41. Google Antigravity - Hacker News, dernier accès : février 10, 2026, https://news.ycombinator.com/item?id=45967814
42. Visual Studio Code Server, dernier accès : février 10, 2026, https://code.visualstudio.com/docs/remote/vscode-server
43. GitHub Copilot Chat: From Prompt Injection to Data Exfiltration - Embrace The Red, dernier accès : février 10, 2026, https://embracethered.com/blog/posts/2024/github-copilot-chat-prompt-injection-data-exfiltration/
44. ChatGPT vs. Copilot: An Enterprise Feature Comparison (2025) - IntuitionLabs, dernier accès : février 10, 2026, https://intuitionlabs.ai/articles/chatgpt-vs-copilot-enterprise-comparison
45. AI Code Security Risks: Why Enterprise Vibe Coding Created a Security Nightmare | ZioSec, dernier accès : février 10, 2026, https://ziosec.com/article?slug=ai-code-security-risks-why-enterprise-vibe-coding-created-a-security-nightmare
46. Understanding SSL Inspection | Zscaler, dernier accès : février 10, 2026, https://help.zscaler.com/zia/about-ssl-inspection
47. Defending Against Encrypted Threats: A Guide to SSL Traffic Inspection with Zscaler, dernier accès : février 10, 2026,

https://www.zscaler.com/blogs/product-insights/best-practices-encrypted-ssl-tls-traffic-inspection-guide
48. Zscaler Logs and AI Training Privacy Debate: Data Containment ..., dernier accès : février 10, 2026, https://windowsforum.com/threads/zscaler-logs-and-ai-training-privacy-debate-data-containment-explained.378421/
49. When Zero Trust Meets AI Training: The Zscaler GDPR Data Processing Controversy, dernier accès : février 10, 2026, https://www.compliancehub.wiki/when-zero-trust-meets-ai-training-the-zscaler-gdpr-data-processing-controversy/
50. Deploy SSL Decryption Using Best Practices - Palo Alto Networks, dernier accès : février 10, 2026, https://docs.paloaltonetworks.com/best-practices/10-1/decryption-best-practices/decryption-best-practices/deploy-ssl-decryption-using-best-practices
51. SSL Decryption : r/networking - Reddit, dernier accès : février 10, 2026, https://www.reddit.com/r/networking/comments/s4la6l/ssl_decryption/
52. Data Collaboration Patterns for Advertising on AWS, dernier accès : février 10, 2026, https://builder.aws.com/content/2yHblVVzRSTbRUPmLnJil21vaB8/data-collaboration-patterns-for-advertising-on-aws
53. How Data Cloud Clean Rooms Enable Ad Sales and Media Planning - Mphasis Silverline, dernier accès : février 10, 2026, https://silverlinecrm.com/blog/media-entertainment/how-data-cloud-clean-rooms-enable-ad-sales-and-media-planning/
54. SNOW - 2025 Proxy Statement, dernier accès : février 10, 2026, https://s26.q4cdn.com/463892824/files/doc_financials/2025/ar/Snowflake-2025-Annual-Report-and-Proxy-Web-Version.pdf
55. What Should Your Customer Data Strategy Be in 2025? - Cyntexa, dernier accès : février 10, 2026, https://cyntexa.com/blog/customer-data-strategy/
56. Mitigating the risk of US surveillance for public sector services in the cloud, dernier accès : février 10, 2026, https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud
57. Cloud Act, FISA, ... why the Privacy Shield is now invalid? - Seald, dernier accès : février 10, 2026, https://www.seald.io/blog/privacy-shield-invalid
58. Clarifying Lawful Overseas Use of Data (CLOUD) Act - Amazon Web Services, dernier accès : février 10, 2026, https://aws.amazon.com/compliance/cloud-act/
59. Data sovereignty in light of the CLOUD Act: back to the future?, dernier accès : février 10, 2026, https://www.osler.com/en/insights/updates/data-sovereignty-in-light-of-the-cloud-act-back-to-the-future/
60. Who Owns BlackRock? List of Top 10 Shareholders - Admiral Markets, dernier accès : février 10, 2026, https://admiralmarkets.com/education/articles/shares/largest-blackrock-shareholders

61. All Blackrock Companies by Weight - Slickcharts, dernier accès : février 10, 2026, https://www.slickcharts.com/blackrock
62. Proxy-Voting Insights: How Differently Do The Big Three Vote on ESG Resolutions, dernier accès : février 10, 2026, https://corpgov.law.harvard.edu/2023/07/03/proxy-voting-insights-how-differently-do-the-big-three-vote-on-esg-resolutions/