E-BOOK

Guide d'achat des solutions de prévention des menaces

Trouvez la meilleure solution de protection contre les menaces pilotée par l'IA pour neutraliser les attaques basées sur les fichiers.

Sommaire

Repenser la sécurité en fonction des menaces actuelles

La sécurité basée uniquement sur le périmètre est trop risquée pour le monde numérique moderne

Le passage au travail hybride et les applications hébergées dans le cloud ont changé la façon d'accéder aux ressources de l'entreprise. Les employés utilisent des appareils non gérés sur des réseaux non sécurisés tels que le Wi-Fi public pour rester productifs à distance ou en déplacement, faisant d'Internet le nouveau réseau d'entreprise. Cette expansion des points d'accès rend l'ancienne approche cloisonnée de la sécurité totalement inappropriée pour protéger vos utilisateurs, vos applications et vos données. S'appuyer uniquement sur des défenses basées sur le périmètre présente des risques car les contrôles centrés sur le réseau sont contournés au profit d'un accès direct à Internet, la facilité d'utilisation étant souvent privilégiée par rapport à la sécurité.

La nouvelle génération de cyberattaques se joue facilement des contrôles de sécurité traditionnels. Il est temps de rapprocher la sécurité des utilisateurs et de passer de la protection du périmètre à la sécurisation des utilisateurs, des workloads et des systèmes OT/IOT.

Les adversaires profitent de la vague de migration vers le cloud

Prises entre le marteau et l'enclume, les équipes de sécurité ont fait de leur mieux pour adapter les contrôles de sécurité traditionnels au monde moderne, axé sur le mobile et le cloud. Cette inadéquation a été une victoire pour les adversaires. Alors que les entreprises s'efforcent de protéger les différentes périphéries du réseau, les portes sont involontairement laissées ouvertes aux malwares, comme en témoignent les conclusions de Zscaler ThreatLabz :

- **86 %** des menaces sont transmises par des canaux chiffrés, les malwares représentant 78 % des attaques chiffrées.[1]
- Les attaques de ransomware ont augmenté de **40 %** d'une année sur l'autre.
- Les payloads observés dans le Zscaler Sandbox ont augmenté de **58 %**.[2]

Cette évolution rapide des menaces numériques, aggravée par l'expansion de la surface d'attaque du cloud, souligne à quel point les équipes de sécurité doivent réévaluer leurs stratégies et renforcer les défenses contre les cyber-risques modernes.

1. Rapport Zscaler ThreatLabz 2023 sur l'état des attaques chiffrées
2. Rapport Zscaler ThreatLabz 2023 sur les ransomwares

Une évolution vers une protection contre les malwares de type « zero day » est nécessaire

Les adversaires disposent de deux atouts majeurs : la **rapidité** et la **prolifération**. Les développeurs de malwares conçoivent des menaces plus rapidement que les défenseurs ne peuvent les définir, en tirant parti de l'intelligence artificielle (IA) pour créer des variantes capables d'échapper aux mesures de sécurité et aux méthodes de détection conventionnelles.

Le phishing mené au moyen de pièces jointes ou de liens malveillants demeure actuellement un des mécanismes de diffusion les plus courants. L'omniprésence du trafic chiffré complique encore davantage les stratégies de défense. Les menaces modernes se dissimulent souvent dans le trafic chiffré, ce qui souligne l'importance d'inspecter l'ensemble du trafic Web et non Web, sous peine de laisser involontairement des malwares s'introduire dans votre réseau.

En tant que fonction critique dans la pile de sécurité, les sandbox constituent une mesure préventive contre les fichiers malveillants et les exécutions de code. Ils sont censés être une défense efficace contre les attaques basées sur des fichiers inconnus qui visent à échapper à l'EDR et à d'autres analyses de détection de malwares connus. De nombreux sandbox sont hélas déployés hors bande, s'appuyant sur des échantillons de malwares qui leur sont transmis par des NGFW, des produits de sécurité cloud ou des agents de terminaux.

Cela signifie souvent que la détection a lieu après le téléchargement d'un malware sur un appareil utilisateur, ce qui permet des infections par des malwares ou des ransomwares de type patient zéro, et ne respecte certainement pas les concepts de Zero Trust. En outre, de nombreux sandbox n'exploitent pas l'analyse AI/AA à grande échelle pour détecter automatiquement et mettre en quarantaine les menaces inconnues et les fichiers suspects, ce qui est un facteur clé pour une défense inline contre les menaces de type patient zéro sans perturber la productivité.

Les antivirus et les systèmes de prévention des intrusions (IPS) basés sur les signatures ne peuvent à eux seuls prévenir les menaces de type « zero day » et polymorphes.

Exigences du sandbox cloud

Jusqu'à présent, les adversaires ont eu le dessus en exploitant l'architecture changeante de l'environnement cloud.

Le choix du bon cloud sandbox est essentiel pour prévenir les infections de type « zero day » et bloquer l'accès des menaces persistantes avancées à votre réseau.

La section suivante est destinée à vous aider à comprendre les exigences spécifiques à prendre en compte lors de la sélection d'un cloud sandbox.

Déchiffrement et inspection à grande échelle

Le chiffrement est devenu une tendance prometteuse en matière de sécurité, permettant de protéger et de sécuriser les communications privées et les informations sensibles. Malheureusement, les cybercriminels profitent du trafic chiffré pour cacher des payloads malveillants.

Le déchiffrement et l'inspection du trafic, des processus gourmands en ressources informatiques, peuvent transformer des appliances sandbox très performantes en processus extrêmement lents, interrompant les activités avec une latence inacceptable.

Lorsque vous évaluez une solution moderne de sandboxing, il est important de sélectionner des fournisseurs capables de fournir un déchiffrement et une inspection en mode inline, sans limites ni latence.

Les menaces sur HTTPS ont augmenté de 24,3 % d'une année sur l'autre, ce qui représente 30 milliards d'attaques chiffrées en 2023.[3]

Liste de contrôle d'achat :

- ☐ Aucun matériel supplémentaire ni installation de machine virtuelle (VM) requis pour déchiffrer le trafic SSL
- ☐ Inspecte et analyse les types de fichiers suivants, sans latence ni limite de capacité :

EXE	DOC(X)	TAR
DLL	XLS(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	Fichiers de script et fichiers ZIP
SWF	BZ2	

3 Rapport Zscaler ThreatLabz 2023 sur l'état des attaques chiffrées

Liste de contrôle d'achat :

- ☐ Application immédiate des politiques à tous les utilisateurs avec une protection identique, aussi bien sur le réseau de l'entreprise qu'en dehors
- ☐ Règles et capacités de mise en quarantaine avancées pour tous les fichiers provenant de destinations suspectes
- ☐ Gestion centralisée des politiques permettant un contrôle granulaire des opérations de sandboxing, y compris les autorisations de type de fichier et les mises en attente automatisées des destinations suspectes

Gestion centralisée des politiques et des règles

Évitez la gestion incorrecte des règles et la configuration manuelle des sandbox à chaque passerelle grâce à une gestion centralisée des politiques et des règles fournies dans le cloud. Envisagez des solutions assorties de politiques adaptatives et dynamiques qui respectent les principes de Zero Trust décrits par la **norme NIST 800-207**. En établissant des politiques d'accès et de sécurité basées sur le contexte, notamment le rôle et l'emplacement de l'utilisateur, la posture de l'appareil et les données demandées, le Zero Trust minimise les surfaces d'attaque. Les solutions fournies dans le cloud présentent des avantages supplémentaires qui peuvent vous permettre de bloquer les menaces pour tous les utilisateurs de l'entreprise. Cela signifie que le traitement rétroactif de fichiers est supprimé (par exemple, les inspections hors bande et les protections appliquées après coup) pour fournir une sécurité davantage synchronisée. Un aspect essentiel de la politique de sandboxing est qu'elle offre la flexibilité nécessaire pour soutenir l'entreprise, en proposant des règles granulaires pour différents ensembles d'utilisateurs, d'emplacements, de catégories d'URL ou d'actions. Les contrôles granulaires vous permettent d'aligner les politiques sur la tolérance au risque et les attentes de performance de votre entreprise.

Alignement des politiques sur la tolérance au risque et les attentes en matière de performances

Une solution de cloud sandbox doit contrôler les risques et appliquer des politiques en répondant aux besoins uniques de votre entreprise. Commencez par déterminer si vous êtes affecté par les éléments suivants :

- **Faible tolérance aux fichiers malveillants :** les entreprises qui souhaitent éviter les risques peuvent choisir « Quarantine for First-Time Action » (mise en quarantaine en tant que première action) pour les fichiers inconnus ou suspects. Cela permet d'éliminer le risque d'infection de type patient zéro, étant donné que le sandbox analysera le fichier avant qu'il ne puisse être téléchargé.
- **Faible tolérance à la mise en quarantaine des fichiers :** les entreprises tolérantes au risque qui souhaitent éviter les retards et les interruptions peuvent choisir « Quarantine and Isolate for First-Time Action » (mise en quarantaine et isolation en tant que première action). Cette action intègre le sandbox aux fonctionnalités d'isolation du navigateur cloud, fournissant aux utilisateurs un accès immédiat à un PDF en lecture seule sans contenu actif pendant que le sandbox analyse les fichiers potentiellement dangereux en arrière-plan.

Peu importe vos besoins spécifiques, les politiques doivent être faciles à appliquer à tous les utilisateurs, groupes, départements, emplacements et groupes d'emplacements à partir d'une plateforme unique.

Analyse intelligente et renseignements sur les menaces

Les adversaires sont connus pour réitérer les attaques qui réussissent. Il est donc essentiel de partager les protections avec la communauté de sécurité pour arrêter rapidement les menaces dans leur lancée. Les cloud sandbox jouent un rôle important à cet égard en capturant les données de télémétrie et en partageant les informations sur les menaces nouvellement identifiées avec la communauté de la sécurité et les flux de menaces.

Moteur de prévention des malwares optimisé par l'IA

Les sandbox fournis dans le cloud sont en mesure de gérer des modèles AI/AA à forte charge de calcul pour assurer une protection supérieure.

Recherchez un sandbox qui identifie, met en quarantaine et prévient intelligemment les menaces inconnues ou suspectes inline à l'aide d'une IA/AA avancée, sans devoir procéder à une analyse plus poussée :

- **Verdicts instantanés concernant les fichiers :** en comprenant instantanément quels fichiers risquent d'être malveillants, les utilisateurs ne doivent pas attendre un verdict.
- **Prévention des vulnérabilités de type « zero day » :** même si cela semble difficile à croire, tous les sandbox ne préviennent pas les infections du patient zéro en mettant en quarantaine les menaces inconnues avant d'autoriser leur téléchargement.

Flux de travail SOC avec informations sur les menaces

Les analystes peuvent passer plusieurs heures par jour à analyser une seule menace. Recherchez un sandbox cloud qui réduit cette charge et accélère les enquêtes et les réponses en partageant des informations comportementales et des renseignements sur les menaces concernant les payloads malveillants. Les équipes de sécurité doivent être en mesure de soutenir les enquêtes avec une analyse directe des fichiers dans le sandbox grâce à des envois via l'API hors bande. Assurez-vous que les flux de menaces s'intègrent à vos outils de sécurité existants. Ils doivent inclure un contexte actualisé sur les URL signalées, des indicateurs de compromission (IoC) extraits, et des tactiques, techniques et procédures (TTP) qui s'alignent sur les cadres de cybersécurité tels que MITRE ATT&CK®.

Liste de contrôle d'achat :

- ☐ Capacités de mise en quarantaine basées sur l'IA qui peuvent exploiter l'IA/AA pour rendre un verdict instantané sur les fichiers afin de stopper les menaces sans nécessiter d'analyse de fichiers
- ☐ Contribution autonome aux protections quotidiennes contre les menaces, partagée entre les utilisateurs et les réseaux, quel que soit leur emplacement
- ☐ Intégration des flux de menaces avec les outils de sécurité existants
- ☐ Envois de fichiers sandbox « hors bande » programmatiques et basés sur l''API avec file distincte pour les fichiers envoyés via l''API

Veillez à choisir un sandbox qui peut fournir plus qu'un score de menace. Envisagez un sandbox qui peut identifier les techniques de contournement utilisées, telles que :

- Retarder l'exécution du code pour éviter la détection par le sandbox
- Capturer et visualiser le trafic qui transite sur le réseau
- Ouvrir des ports pour permettre une connexion à distance
- Tenter de se déplacer en interne pour identifier des cibles de valeur
- Tenter de prendre le contrôle à distance

Rapports

Les solutions de sécurité proposant des rapports ne sont utiles que dans la mesure où ils sont exploitables. Les rapports sur les cloud sandbox devraient comporter les caractéristiques suivantes :

- Porter sur l'ensemble du cycle de vie des attaques malveillantes
- Être simple à utiliser et à exploiter
- Être compréhensible
- Être disponibles via une interface de programmation d'applications (API) afin de pouvoir être corrélés avec les journaux existants
- Faire partie d'une plateforme plus large qui prend également en charge les rapports de conformité

Améliorer votre SOC avec le cadre MITRE ATT&CK

Lorsque vous évaluez les capacités de reporting, pensez aux informations du sandbox qui peuvent être mises en correspondance avec le **cadre ATT&CK de MITRE**. Grâce à cette capacité, les équipes SOC peuvent exploiter les informations fournies pour élaborer des défenses tactiques dans d'autres fonctions de la pile de sécurité. Ainsi, le sandbox fait partie intégrante des flux de travail des opérations de sécurité.

En fonction de votre degré de maîtrise du cadre, vous pouvez utiliser la création de rapports de plusieurs manières :

- Faciliter les tâches de classification en utilisant la taxonomie fournie
- Visualiser les techniques furtives qui peuvent être utilisées pour contourner votre solution EDR (détection et réponse aux menaces)
- Comparer et évaluer l'efficacité d'autres fonctions
- Vous concentrer sur les TTP les plus courantes ciblant votre entreprise plutôt que de tenter de déjouer toutes les tactiques et techniques
- Réaliser un rapport de rétro-ingénierie

Questions à se poser avant d'acheter

Pour vous orienter dans votre processus de décision, voici un récapitulatif des principales questions que vous devez poser et pourquoi vous devez les poser :

Le sandbox permet-il une infection initiale du patient zéro, même une seule ?

Les sandbox qui permettent une infection initiale du patient zéro pendant qu'un fichier est en cours d'analyse ne parviennent pas à assurer la sécurité de l'entreprise.

La solution couvre-t-elle tous les utilisateurs et leurs appareils, quel que soit leur emplacement ?

Vos utilisateurs peuvent accéder aux ressources de l'entreprise en déplacement, sur leurs propres appareils ou via des réseaux non sécurisés. Il est indispensable de sécuriser tous les appareils qui sont essentiels à leur travail.[4]

La solution détecte-t-elle les envois de fichiers inline ou nécessite-t-elle des envois hors bande ?

Les solutions qui fonctionnent inline peuvent identifier les menaces et les bloquer directement sans avoir à s'appuyer sur les flux réseau NGFW ni à impliquer un logiciel EDR.

Le sandbox examine-t-il le trafic de tous les protocoles HTTP, HTTPS, FTP et FTP sur HTTP ? Y a-t-il des limitations ?

Il est important d'examiner le trafic pour déceler les malwares furtifs. Un sandbox fourni dans le cloud peut mieux convenir pour inspecter tout le trafic sans créer de latence.

Est-il conforme aux lois et réglementations en vigueur, y compris aux exigences de Zero Trust ?

Les règlements de conformité peuvent avoir des exigences strictes sur la façon dont le sandboxing est géré et sur les questions de conservation des fichiers et de confidentialité. Une solution qui fonctionne uniquement en mémoire et qui supprime les informations identifiables pendant l'analyse vous aide à répondre à ces exigences. En outre, vérifiez si les solutions adhèrent aux principes de Zero Trust tels que définis par les normes mondiales NIST 800-207 et utilisez-les comme guide pour réduire les surfaces d'attaque et protéger les données.

Avec quels autres modules de sécurité le sandbox collabore-t-il ?

Aucun produit ne peut à lui seul assurer une protection totale contre les menaces avancées persistantes (APT). Au contraire, une approche multicouche de prévention, d'atténuation, de détection et de réponse aux menaces est indispensable. Le sandboxing est une couche intégrale et, en tant que tel, il doit parfaitement collaborer avec d'autres solutions et modules.

4. us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox et protection avancée contre les menaces

Il est temps de disposer d'une véritable solution de sandbox inline cloud native

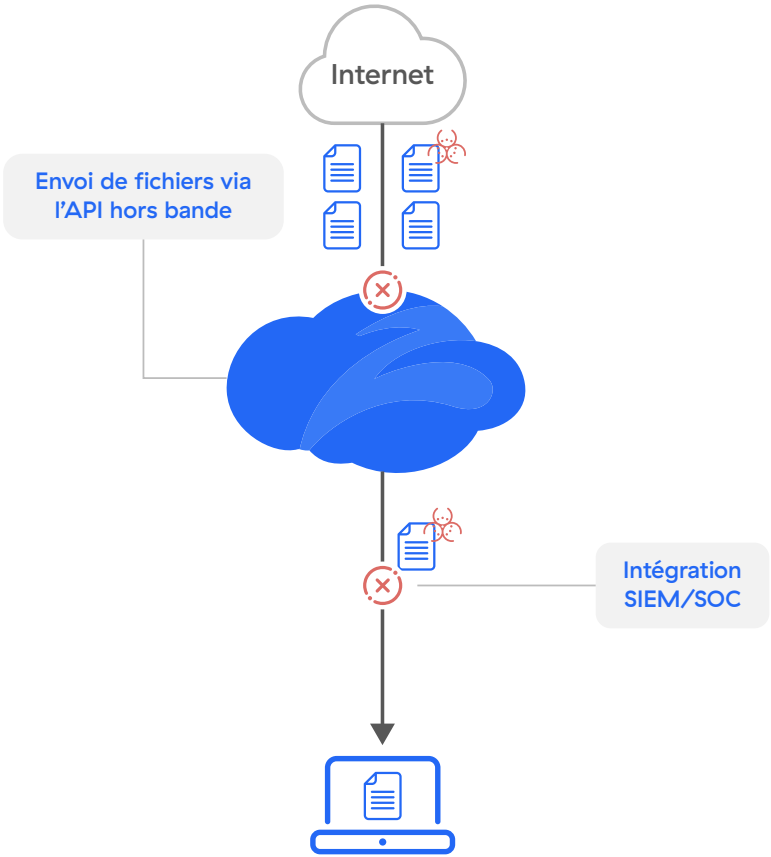
Alors que les entreprises sont confrontées à un élargissement de leurs surfaces d'attaque et que les adversaires profitent des lacunes de la pile de sécurité existante, le moment n'a jamais été aussi propice pour choisir une véritable solution de sandbox inline cloud native. Zscaler Cloud Sandbox est spécialement conçu pour intercepter et stopper les menaces modernes tout en assurant une protection contre les malwares de type « zero day » pour tous les utilisateurs, sur tous les emplacements.

Construit sur une architecture cloud native basée sur un proxy, Zscaler Cloud Sandbox est le premier moteur de prévention des malwares piloté par l'IA au monde qui détecte, empêche et met en quarantaine les menaces inconnues et les fichiers suspects inline, le tout de manière automatique et intelligente. L'inspection illimitée et sans latence sur le Web, assortie des protocoles de transfert de fichiers (FTP), y compris SSL/TLS, permet au cloud sandbox d'effectuer une analyse dynamique approfondie en temps réel, garantissant qu'aucun fichier inconnu ne parvient à l'utilisateur du fait du téléchargement d'un fichier malveillant.

Avantage de l'IA de Zscaler Sandbox : entraîné avec plus de 500 millions d'échantillons, avec des mises à jour de sécurité en temps réel provenant de 300 000 milliards de signaux quotidiens.

La quarantaine optimisée par l'IA stoppe les malwares inconnus

Protection inline avec livraison instantanée des fichiers inoffensifs, défense contre les infections de type patient zéro et règles granulaires des politiques



Réduction de la complexité et des coûts

- Facile à déployer, aucun matériel ni logiciel à gérer
- Suppression des produits ponctuels redondants et dissociés
- Élimination du backhauling du trafic Internet sur MPLS ou VPN

Protection immédiate et adaptative pour tous les utilisateurs et tous les emplacements

- Définition de politiques globales à partir d'une console unique et centralisée
- Application immédiate des changements de politique
- Identification des menaces une seule fois pour les bloquer immédiatement et définitivement pour tous les clients

Détection des menaces dissimulées

- Prévention des infections de type patient zéro provenant de menaces connues et émergentes grâce à la mise en quarantaine pilotée par l'IA
- Chargement des fichiers pour analyse (portail de vérification des fichiers)

Service de plateforme intégré

- Pré-filtrage de toutes les menaces connues à l'aide d'antivirus, de listes de blocage de hachage, de règles de classification YARA des malwares, de détections automatisées d'empreintes JA3 et de modèles d'AA/AI
- Les flux CIF (Collective Intelligence Framework) permettent à Zscaler d'intégrer plus de 60 flux de menaces, en plus du flux de menaces propre à Zscaler, alimenté par des milliards de transactions de sa base de clients.
- Superposition d'un cloud sandbox avec une solution EDR pour augmenter l'efficacité de la sécurité et limiter l'accès initial, l'exécution et les tactiques persistantes

Une étude de validation économique d'ESG a révélé que Zscaler Zero Trust Exchange a créé une réduction de 90 % des appliances de sécurité.[5]

- Analyse statique, dynamique et secondaire, y compris l'analyse du code et des payloads secondaires
- Inspection SSL illimitée et sans latence
- Protection du trafic entrant et sortant
- Amélioration des enquêtes et des réponses en matière de sécurité grâce à des données analytiques détaillées sur les envois de fichiers via l''API, notamment sur l'utilisateur, l'origine géographique, les tactiques de contournement, etc.

Zscaler Cloud Sandbox™ est une fonctionnalité entièrement intégrée de Zscaler Internet Access™, qui fait partie de Zscaler Zero Trust Exchange™.

Pour plus d'informations, rendez-vous sur **zscaler.com/fr/technology/cloud-sandbox**

5. info.zscaler.com/resources-industry-report-esg-economic-validation

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **www.zscaler.com/fr**.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.com/fr