Fiche technique

Zscaler Sandbox

Une solution optimisée par IA pour détecter, prévenir et confiner les malwares

Zscaler Sandbox prévient toute infection du patient zéro et l'accès des menaces persistantes avancées (APT) à votre réseau.

Dans le monde actuel qui fait la part belle à la mobilité et au cloud, vos utilisateurs accèdent à leurs fichiers d'où ils le souhaitent, directement à partir d'Internet et d'applications SaaS. L'époque des clients de messagerie déployés au niveau du siège social de l'entreprise et protégés par de multiples couches de sécurité est révolue. Une ligne de défense traditionnelle, centrée sur le réseau corporate, ne permet pas de répondre aux exigences d'utilisateurs qui recherchent une expérience conviviale. Les entreprises doivent composer avec une surface d'attaque élargie, ciblée par des attaques de plus en plus sournoises et des acteurs malveillants qui exploitent les failles de sécurité existantes.

Afin de protéger les données d'entreprise et personnelles sensibles, la quasi-totalité du trafic Internet est désormais chiffrée. Ce chiffrement, s'il dissuade certains assaillants, nourrit néanmoins un faux sentiment de sécurité. Les sandbox traditionnelles, dotées d'une architecture passthrough manquent de visibilité et permettent involontairement à des fichiers malveillants de passer entre les mailles du filet, en se dissimulant dans le trafic chiffré. Elles évitent ainsi une inspection approfondie ou d'une mise en quarantaine. Des dispositifs de déchiffrement SSL peuvent être déployés pour aider. Cependant, à l'instar de la plupart des outils matériels, ils ne sont pas évolutifs, induisent de nouvelles tâches d'administration et contribuent à une prolifération coûteuse des dispositifs.

Avantages de Zscaler Cloud Sandbox :

- **Moteur de prévention des malwares, optimisé par IA** Identifiez, confinez et neutralisez de manière intelligente les menaces inconnues ou suspectes à l'aide d'une IA/AA avancée et sans devoir de nouveau analyser les fichiers sains.
- **Inspection complète inline pour détecter les attaques furtives** Identifiez et neutralisez les menaces furtives et les malwares qui se dissimulent dans un trafic chiffré sur les protocoles Web et FTP, sans latence ni limites en capacité.
- **Prévention cohérente et partagée à l'échelle mondiale** Bénéficiez d'une protection automatisée contre les menaces jusque-là inconnues, grâce au partage en temps réel d'informations de veille sur les menaces avec tous les utilisateurs.
- **Amélioration des workflows SOC grâce à une veille sur les menaces** Accélérez les investigations et la réponse aux menaces : des API permettent de partager des informations sur le comportement des malwares et permettent de bénéficier d'un reporting détaillé.
- **Une alternative aux appliances physiques et aux logiciels coûteux** Déployez votre sécurité en quelques secondes, sans investissement matériel ou logiciel : il vous suffit de configurer et de mettre en œuvre une politique dédiée à la sandbox pour la rendre immédiatement opérationnelle.
- **Protection fournie depuis le cloud et présence mondiale** Bénéficiez d'une sécurité et d'une expérience utilisateur intégrées avec Zscaler Internet Access™, une composante de Zscaler Zero Trust Exchange™.

En conséquence, les infections du patient zéro par des malwares inconnus continuent à peser sur les réseaux et obligent les équipes informatiques et de sécurité à se mobiliser pour neutraliser le déplacement latéral des menaces et l'exfiltration de données, des exactions menées par des malwares qui auraient dû être déjoués dès le départ.

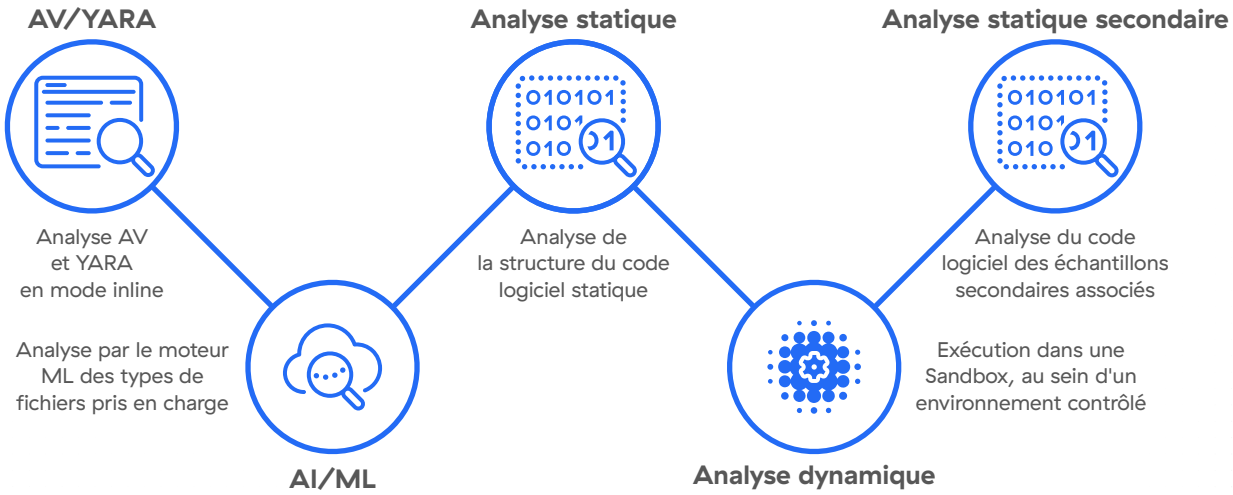
Zscaler Sandbox

En tant que pièce maîtresse d'un arsenal de sécurité, une sandbox doit fournir des mesures préventives contre les fichiers et les logiciels malveillants. Contrairement aux sandbox déployées en mode hors bande dont la protection s'active en aval de la compromission initiale, Zscaler Sandbox est élaboré pour détecter et déjouer les menaces modernes et discrètes qui utilisent des techniques de contournement et exploitent les faiblesses des sandbox traditionnelles.

Adossée à une architecture cloud native basée sur un proxy, Zscaler Sandbox est le tout premier moteur de prévention des malwares optimisé par IA au monde. La solution détecte, neutralise et met en quarantaine les menaces inconnues et les fichiers suspects, cette prestation étant réalisée en mode inline et de manière automatique. L'inspection illimitée et sans latence du trafic Web et FTP (protocole de transfert de fichiers), y compris sous SSL/TLS, permet à la sandbox cloud d'effectuer une analyse approfondie et en temps réel, pour garantir qu'aucun fichier inconnu n'infecte un utilisateur suite au téléchargement d'un fichier malveillant.

Tout fichier inconnu ou suspect est d'abord envoyé à un préfiltre qui compare le contenu du fichier à plus de 40 flux de données sur les menaces, des signatures antivirus, des règles YARA et des modèles AI/AA pour rendre un verdict rapide sur la nocuité du fichier, et neutraliser toute menace similaire connue. En aval de ce tri initial, le fichier est soumis à une analyse statique, dynamique et secondaire robuste, avec exécution du fichier dans un environnement contrôlé et cloisonné pour obtenir un verdict décisionnel. Vient ensuite l'étape du post-traitement, qui met à jour la base de données des menaces de Zscaler et applique la politique du client.

Grâce aux verdicts optimisés par IA, les fichiers sains sont instantanément transmis tandis que les fichiers malveillants sont neutralisés pour tous les utilisateurs mondiaux de Zscaler, grâce à la protection mutualisée.



Cette approche met fin aux infections de patient zéro et aux menaces émergentes pour tous les utilisateurs, quel que soit le dispositif qu'ils utilisent ou leur emplacement.

Avantages d'une sandbox cloud

Au-delà de la mise en quarantaine inline des fichiers suspects, de l'analyse en temps réel optimisée par IA et des verdicts instantanés, les rapports détaillés de Zscaler Sandbox font de la sandbox la première étape d'un processus de sécurisation optimisé par IA. Les informations comportementales provenant de malwares ciblant votre entreprise peuvent enrichir les workflows SecOps, ainsi que votre arsenal de défense.

Déjouer intelligemment les menaces émergentes et les infections du patient zéro Les assaillants misent sur le chiffrement et des applications cloud fiables pour exécuter leurs attaques furtives.

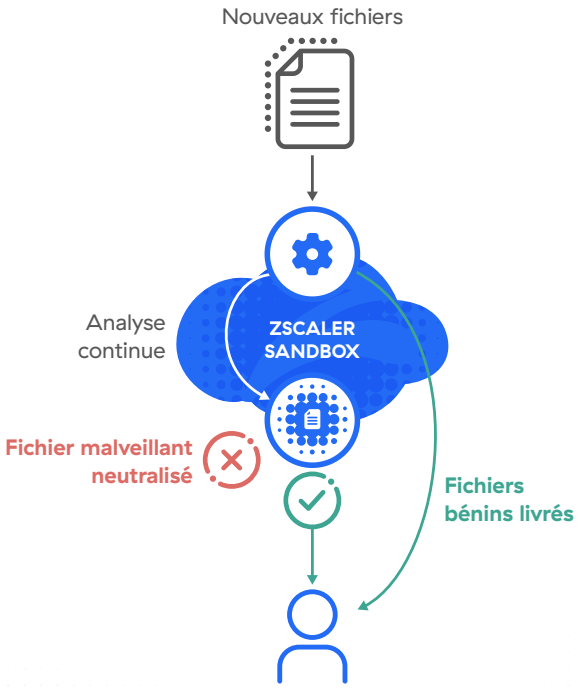
Un récent rapport ThreatLabZ a observé des malwares diffusés depuis Google Drive, AWS et OneDrive. La possibilité d'analyser les fichiers sur le Web et le FTP, notamment lorsque le trafic est chiffré, favorise la visibilité et empêche les assaillants d'accéder à votre réseau.

Avant qu'un collaborateur ne télécharge et n'ouvre accidentellement un nouveau document Office malveillant (Maldocs) dissimulant une macro, la fonction inline de quarantaine pilotée par l'IA de Zscaler Sandbox entre en action. Si l'analyse approfondie de fichiers résulte en un indice de menace élevé, l'accès au fichier est neutralisé pour tous les utilisateurs protégés par Zscaler. Les verdicts en temps réel, sans analyse supplémentaire des fichiers, évitent tout impact sur la productivité des collaborateurs. La mise en quarantaine automatique des fichiers inconnus ou malveillants évite le recours intempestif des utilisateurs à leur support technique.

Après un déploiement express en vingt minutes de Zscaler Sandbox, l'équipe informatique et de sécurité d'un client a pu fournir instantanément et en toute sécurité 91 % des fichiers inoffensifs aux utilisateurs, ceci suite à un verdict basé sur l'IA. Les fichiers inconnus résiduels ont été transmis pour une analyse approfondie révélant que 5 % des fichiers contenaient des malwares ou avaient une intention malveillante. Les fichiers malveillants sont neutralisés pour les utilisateurs destinataires, mais également pour tous les utilisateurs et dispositifs mondiaux protégés par Zscaler, quels que soient leur emplacement. La protection est ainsi mutualisée et identique pour tous.

La quarantaine optimisée par IA stoppe les malwares inconnus

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



Améliorer les workflows du SOC grâce aux informations sur les malwares et à MITRE ATT&CK L'analyse approfondie des fichiers et l'exécution des malwares inconnus dans un environnement cloisonné donne lieu à un rapport d'analyse. L'environnement contrôlé et cloisonné de la sandbox réalise des captures d'écran et informe les analystes des techniques de contournement, des communications de type callback et de toute autre action menée par un malware. Ce rapport détaille le cycle de vie d'une attaque détectée, la chaîne de frappe d'un événement, le comportement d'un malware, ainsi que l'intention d'un payload malveillant. Un mapping avec le framework MITRE ATT&CK est assuré.

Avec cette mise en correspondance des résultats contextuels de la sandbox avec MITRE ATT&CK, les équipes de sécurité et IT peuvent encourager le partage d'informations entre les différents outils de l'arsenal de sécurité. La sandbox cloud devient ainsi une nouvelle ligne de défense contre les malwares qui contribue à une détection en amont des malwares, ce qui accélère les tâches d'investigation et de réponse et facilite la traque des menaces.

Gestion simplifiée de la politique et contrôles granulaires La sandbox, en tant que solution fournie depuis le cloud, n'implique aucun investissement ou configuration de matériel, ni gestion de logiciel, ce qui est un vecteur de simplicité. Vous pouvez utiliser Zscaler Sandbox sans devoir être sur site pour configurer et connecter chaque dispositif, grâce à une configuration simple en deux étapes : **critères** et **action**. En prime, les politiques sont faciles à gérer, à configurer et à déployer. En quelques clics, les administrateurs peuvent mettre en œuvre des politiques, notamment une séquence des règles pour une application précise et des politiques qui s'appliquent aux utilisateurs ou groupes d'utilisateurs, quel que soit leur emplacement.

Pour des contrôles plus granulaires, le sandbox cloud peut améliorer l'analyse statique et dynamique des fichiers grâce à une détection automatisée des empreintes JA3. Il est possible de configurer des listes noires sur la base des hashs, ainsi que des règles YARA. De plus, les politiques basées sur un score de risque peuvent prendre des mesures contre les fichiers grayware et adware gênants ou suspects, généralement considérés comme présentant un niveau moindre de risque qu'une menace.

Active sur une plate-forme Zero Trust cloud-native, Zscaler Sandbox est une fonctionnalité entièrement intégrée à Zscaler Internet Access et fait partie de la solution Zscaler Zero Trust Exchange. L'architecture basée sur un proxy protège les utilisateurs en mode inline, et non en aval d'une infection : le trafic est orienté vers un vaste panel de fonctionnalités de sécurité cloud pour assurer une protection en profondeur et intelligente à chaque utilisateur, quel que soit son emplacement ou son réseau. Bénéficiez d'une protection mondiale mutualisée, grâce à des mises à jour en temps réel basées sur 300 000 milliards de signaux de menace quotidiens, une sécurité fournie depuis le cloud et au principe du moindre privilège de Zero Trust.

Sandbox standard vs avancée

	Sandbox standard	Sandbox avancée	
Versions de ZIA	Professional Edition Business Edition	Transformation Edition ELA Edition	**La sandbox avancée peut être un module complémentaire à ZIA Professional Edition et Business Edition**
Fichiers compatibles	.exe, .dll,	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, fichiers script dans des zips	
Mise en quarantaine optimisée par IA	—	OUI	
Politiques granulaires	—	OUI	
Reporting	—	OUI	
API	—	OUI	

Fonctionnalités fournies depuis le cloud

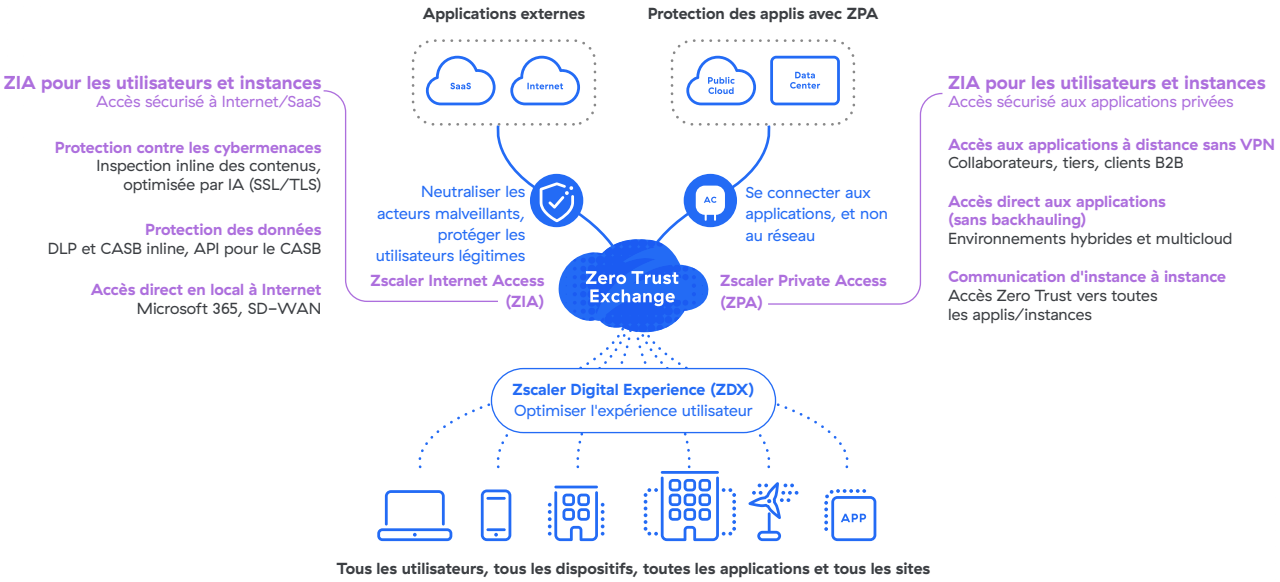
Préfiltrage	AV, listes noires de hask, règles YARA, détections automatisées d'empreintes JA3 et modèles IA/AA
Analyse statique, dynamique et secondaire	Analyse statique et analyse dynamique, y compris l'analyse du code et l'analyse des payloads secondaires
Fichiers compatibles	.exe, .dll, .scr, .ocx, .sys, .class, .jar, .pdf, .swf, .doc(x), .xls(x), .ppt(x), .apk, .zip, .rar, .7z, .bz, .bz2, .tar, .tgz, .gtar, .rtf, .ps1, .hta, .vbs, fichiers script dans des zips
Inspection SSL	Capacité illimitée d'inspection SSL/TLS
Conservation des fichiers	Zscaler Cloud Sandbox opère uniquement en mémoire. Les fichiers sont débarrassés de toute information identifiable pendant l'analyse. Une fois l'analyse terminée, les fichiers inoffensifs sont purgés de la mémoire tandis que les fichiers malveillants sont chiffrés et stockés indéfiniment, ce qui permet de partager les informations entre tous les utilisateurs de Zscaler et d'assurer protection continue.
Compatibilité aux OS	Windows XP, Windows 10, Android
Protocoles pris en charge	HTTP, HTTPS, FTP, FTP sur HTTP
Fichiers par jour	Illimité
Taille maximale du fichier	20 Mo pour Windows et 50 Mo pour Android
Méthode de déploiement	Dans le cloud
Intégration de la veille sur les menaces	Plus de 40 flux d'informations sur les menaces provenant de partenaires de sécurité
Gestion et reporting	Rapports complets incluant le comportement et l'intention des malwares, les indicateurs de compromission (IOC), les fichiers déposés, les PCAP
Expertise post-incident	Échantillon initial, payloads secondaires, PCAP
API	Prise en charge des API, récupération de rapports via API au format JSON
Politiques granulaires	Politiques faciles à utiliser et à configurer pour les utilisateurs, les lieux, les groupes de lieux, les types de fichiers, les groupes d'utilisateurs, les services, les catégories d'URL et les protocoles
Certifications de confidentialité et de conformité	Conformité aux normes internationales les plus strictes en matière de risques et de confidentialité, applicables aux entreprises et aux organisations publiques
Conformité aux réglementations sectorielles et de confidentialité des données	Conformité aux réglementations sectorielles et nationales en matière de confidentialité des données

Zscaler Sandbox est entièrement intégré à Zscaler Internet Access™ et fait partie de la plateforme globale Zero Trust Exchange

Zscaler Zero Trust Exchange assure des connexions rapides et sécurisées et permet à vos collaborateurs de télétravailler en utilisant Internet en tant que réseau corporate. En capitalisant sur le principe du moindre privilège, clé de voûte du Zero Trust, la solution déploie une sécurité complète qui prend en compte le contexte des identités et applique les politiques.

Zscaler : fournir une politique Zero Trust aux utilisateurs, aux instances et à l'IIoT/OT

Un déploiement en quelques semaines pour améliorer la cyberprotection et l'expérience utilisateur



zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique de ses clients pour qu'ils gagnent en agilité, efficacité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications, indépendamment de leur emplacement. Adossée à plus de 150 data centers dans le monde, la solution SASE Zero Trust Exchange constitue la plus vaste plateforme intégrée de sécurité cloud. Pour en savoir plus, rendez-vous sur **zscaler.fr** ou suivez-nous sur Twitter **@zscaler**.

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