La maîtrise des risques liés à la surface d'attaque

Synthèse

La pandémie mondiale a imposé aux entreprises de nombreux défis en matière de santé, de sécurité et de logistique. Ce sont également des perturbations d'ordre géopolitique qui ont lourdement impacté l'opérationnel des entreprises. La transformation digitale s'est accélérée à un rythme soutenu, donnant lieu à un écosystème IT plus complexe à gérer et une progression des cyber-risques.

À mesure que les entreprises évoluent et s'adaptent à la réalité du travail hybride, à la fourniture d'applications depuis le cloud et à une infrastructure IT en constante évolution, la surface d'attaque devient une préoccupation majeure pour gérer les risques en entreprise. Trend Micro One, plateforme unifiée de cybersécurité, capitalise sur 30 ans d'expérience et d'innovation en cybersécurité. Elle permet aux entreprises de mieux comprendre, notifier et maîtriser les cyber-risques.

Un processus permanent de transformation digitale

Le monde évolue à un rythme stupéfiant, sans précédent. La transformation digitale, accélérée par la pandémie, a favorisé les changements dans tous les secteurs de l'entreprise.

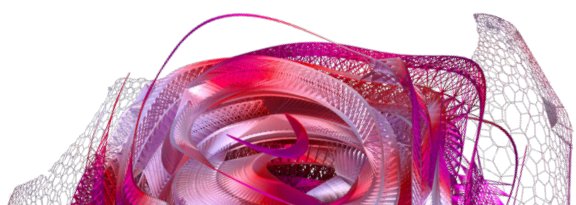
Le travail à distance, imposé pour des raisons sanitaires et qui s'inscrit désormais dans la durée, a transformé un risque élevé à court terme en un risque permanent.[1] La prise en charge de nouveaux objectifs business et les besoins du distanciel ont modifié les modalités d'utilisation du cloud. Mobilisées initialement par une migration des applications existantes vers le cloud, les entreprises (50 % en 2022[2]), adoptent une approche "cloud native" et modifient leurs stratégies pour accompagner tant leurs collaborateurs que leurs clients.

Les dispositifs connectés, toujours plus nombreux, devraient se chiffrer à plus de 55,7 milliards dans le monde d'ici 2025[3], ce qui induit de la complexité. Il s'agit d'équipements IT traditionnels, mais aussi de systèmes industriels (OT) essentiels à l'outil de production et à la chaîne logistique.

Ces changements n'impactent pas que les équipes IT. Les technologies comme le cloud et l'intelligence artificielle (IA) ont le potentiel de modifier la culture d'entreprise, les opérations business et la relation client.

La transition digitale est tributaire d'un contexte international. L'instabilité géopolitique et les réglementations de plus en plus strictes sur la confidentialité des données, comme le RGPD, ne simplifient en rien la gestion des risques.

1 - Gartner, 2022 Planning Guide for Security and Risk Management, octobre 2021
2 - Forrester, Predictions 2022 : Cloud Computing", 27 octobre 2021
3 - IDC, IoT Growth Demands Rethink of Long-Term Storage Strategies, juillet 2020

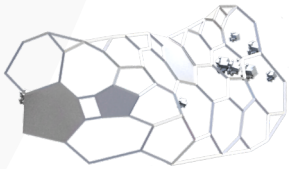


Une surface d'attaque de plus en plus complexe

La transformation digitale a incontestablement accéléré les cycles de production. Toutefois, elle induit un niveau de complexité qui met les équipes IT face à une surface d'attaque de plus en plus étendue, tandis que les outils de sécurité à disposition sont souvent hétérogènes et autonomes.

Qu'il s'agisse des vulnérabilités des logiciels libres, de services cloud mal configurés, d'une l'utilisation non-contrôlée d'applications SaaS, de systèmes d'exploitation sans patch ou de vulnérabilités endpoints ou réseau, la surface d'attaque digitale est un vecteur majeur de cyber-risques pour une entreprise.

Schéma : La surface d'attaque d'une entreprise d'aujourd'hui



À l'aide de différentes tactiques, les acteurs malveillants concentreront leurs efforts sur cette surface d'attaque. Cette approche impacte les entreprises, notamment en matière de cyber-assurances dans le cadre d'une stratégie de gestion des risques.

Le succès des rançongiciels au cours des récentes années a transformé le secteur de la cyber-assurance. Les polices d'assurance imposent de nouvelles exigences, et notamment d'utiliser des technologies de détection et de réponse aux menaces présentes sur les endpoints. Pour pallier l'impact délétère de ces menaces, notamment en termes de perte de revenus, les professionnels de la sécurité ont beaucoup à faire.

TOP 5 des conséquences d'une attaque :

1. Perte de revenus
2. Équipements endommagés ou volés
3. Perte de clients
4. Coûts liés aux consultants/experts externes
5. Perturbations ou dégradations des infrastructures critiques

Source : The Cyber Risk Index S2-2021, Trend Micro Research et Ponemon Institute, mars 2022

Le rapport de prédictions de Trend Micro pour 2022 souligne que les entreprises doivent rester vigilantes en matière de gestion des cyber-risques. Nous pensons que les attaques interviendront plus en amont par rapport à aujourd'hui, en ciblant les outils et le pipeline DevOps, les informations d'identification des développeurs et les systèmes de versioning, pour en faire des passerelles pour les malware. Ceux-ci cibleront les chaînes collaboratives et logistiques pour s'en prendre à de multiples entreprises.

Nos chercheurs pensent que les failles seront exploitées en des temps records. Les exploits zero-day et les attaques polymorphes seront plus nombreuses et cibleront en cascade de multiples produits logiciels.

Nous prévoyons également une intensification des rançongiciels. Une perspective déconcertante dans la mesure où la plupart des entreprises ont déjà été ciblées, d'une manière ou d'une autre, par des rançongiciels en 2021. Avec des fournisseurs de Ransomware-as-a-Service (RaaS) tels que REvil et Conti, à l'origine de millions d'attaques dans le monde, nous pensons que les rançongiciels deviendront plus ciblés, leurs auteurs forçant les victimes solvables, via différentes techniques d'extorsion, à régler de fortes rançons.

La gestion et la notification des risques sont complexes

Si gérer la surface d'attaque est essentiel, disposer des compétences adéquates relève du défi. Le nombre de professionnels de la cybersécurité progresse. Pour autant, la pénurie mondiale se chiffre à plus de 2,7 millions de professionnels de cette discipline[5].

Près d'

1/3

des décideurs IT cite la

cybersécurité comme risque majeur pour l'entreprise.

Source : Trend Micro Global Risk Survey of IT Decision Makers and C-Level Executives, octobre 2021

Cette pénurie de ressources et de compétences pèse sur la gestion de la surface d'attaque, d'autant que les outils de sécurité sont cloisonnés et que les alertes sont bien trop nombreuses. Cette situation est aggravée par une dissémination des utilisateurs, applications et données sur l'ensemble du périmètre réseau et par une réglementation contraignante en matière de confidentialité des données.

La notification des cyber-risques est une démarche aussi bien cruciale que contraignante. Selon notre étude internationale, les cyber-risques sont devenus une priorité pour les dirigeants d'entreprise. Près d'un dirigeant sur trois fait de la cybersécurité son principal défi[6]. Pourtant, moins de 50 % des cadres dirigeants non spécialistes de l'IT en comprennent tous les enjeux.

La réalité du quotidien vient souvent perturber/compliquer cette communication des risques: trop d'alertes, visibilité limitée, données cloisonnées et pléthore d'outils de sécurité. 62 % des professionnels de l'IT déclarent qu'il est essentiel d'améliorer le reporting et la visibilité sur les risques métiers. Dans la mesure où 82 % d'entre eux disent avoir ressenti une pression pour minimiser la gravité des risques auprès de leurs dirigeants, les besoins en outils de communication n'ont jamais été aussi grands.

4 - Vers un nouvel élan : Prédictions de sécurité de Trend Micro Security pour 2022
5 - ISC2 Cybersecurity Workforce Study 2021
6 - Trend Micro Global Risk Survey of IT Decision Makers and C-Level Executives, Octobre 2021

Piloter le cycle de vie de la surface d'attaque

Votre surface d'attaque est à la fois complexe et dynamique, ce qui en fait une cible de choix pour les assaillants. Pour mieux gérer vos risques, il est important de traiter dans une optique de cycle de vie devant être géré en permanence.

Vous devez être en mesure de déterminer, en continu et dans tous les environnements, les modalités d'évolution de cette surface, en recueillant les données clés qui évaluent vos risques potentiels. Le risque peut être issu d'un ou de plusieurs éléments de votre surface, ce qui ne facilite pas l'évaluation du niveau réel de vulnérabilité.

Qui plus est, les actions pour atténuer les risques peuvent être multiples (changements de configuration, ajustements des règles ou application de contrôles de sécurité spécifiques) pour prévenir une attaque ou déjouer rapidement une attaque déjà en cours.

Alors que la surface d'attaque peut évoluer à tout moment, par exemple au milieu de la session d'un utilisateur compromis et dont le comportement devient suspect, le niveau de risque de votre écosystème doit être surveillé et évalué en permanence.

Trend Micro One : une plateforme unifiée de cybersécurité

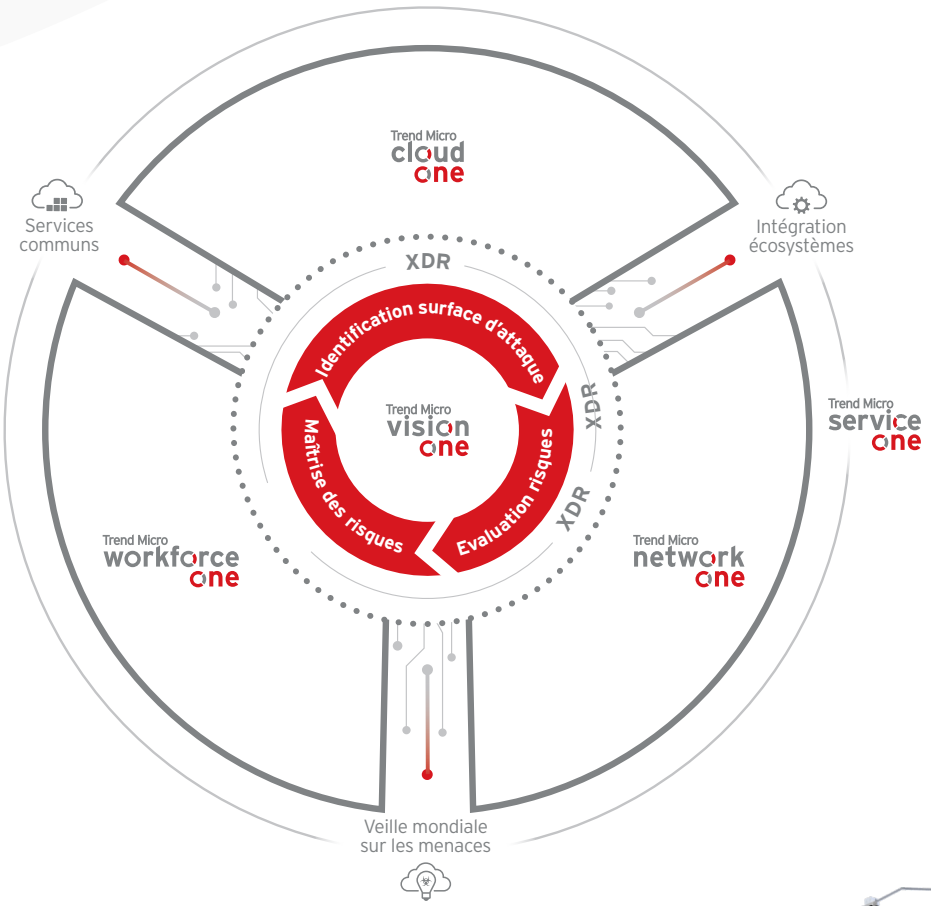
Trend Micro One est une plateforme unifiée de cybersécurité qui tire parti de plus de 30 années d'expérience et d'innovation. Elle permet aux entreprises de comprendre, communiquer et maîtriser les cyber-risques sur l'ensemble de leur périmètre.

Les professionnels de la sécurité gardent ainsi la main sur une surface d'attaque qui évolue, identifient et hiérarchisent les vulnérabilités, détectent et traitent rapidement les menaces et appliquent la fonction de sécurité la plus pertinente, au moment le plus opportun. Nos fonctionnalités de sécurité intégrées comme la technologie XDR, les perspectives sur les risques, l'évaluation des menaces et une intégration étroite à votre infrastructure IT, aident les équipes à gérer plus efficacement le cycle de vie des risques sur la surface d'attaque.

Avec son périmètre fonctionnel qui couvre l'ensemble de l'entreprise, Trend Micro One permet aux entreprises de gagner en agilité et de s'adapter rapidement aux nouveaux besoins métiers et de conformité, notamment en prenant en charge des stratégies de sécurité telles que le Zero Trust, et en répondant aux exigences de cyber-assurance et de conformité. Grâce à une veille pointue sur les menaces et les vulnérabilités, fournie par notre équipe de recherche dans le monde, et aux services d'experts (XDR et réponse aux incidents), Trend Micro One vous aide à mieux gérer le cycle de vie de votre surface d'attaque.

Trend Micro one

Une plateforme unifiée de cybersécurité



Détecter et répondre plus rapidement aux attaques

Avec ses fonctionnalités XDR[7] de pointe, Trend Micro One vous offre une vision complète sur votre sécurité grâce à des capteurs natifs, présents sur les différentes composantes de votre environnement : endpoints, email, cloud, IoT/OT et réseau. Ces capteurs permettent à la plateforme de collecter des données pour assurer une détection corrélée, des investigations précises et traquer efficacement les menaces.

De plus, l'intégration avec des partenaires et leurs technologiques (pare-feu, gestion des vulnérabilités, Microsoft Active Directory, SIEM et SOAR) nous fournit davantage de données pour enrichir les analyses et optimiser les processus et les workflows.

Il en résulte une identification et une corrélation rapides des activités suspectes, des détections fiables de menaces, ainsi que des fonctions de recherche, d'investigation, d'analyse et de réponse aux incidents, fournis par une console unique. Grâce à une visibilité intégrale, vos équipes de sécurité améliorent leurs temps de réponse de 70 % et notifient précisément les cyber-risques aux décisionnaires, cadres dirigeants et autres parties prenantes.

Simplifier et renforcer la sécurité du cloud

Conçu à l'intention des utilisateurs et architectes du cloud, Trend Micro One offre une automatisation de la sécurité, des API personnalisables et des intégrations clés en main pour répondre à vos besoins en matière de sécurité sur AWS, Microsoft Azure, Google Cloud, etc.

Retenu par nombre d'entreprises dans le monde pour protéger leurs projets de transformation digitale dans le cloud, Trend Micro One gère votre posture de sécurité, évalue les risques liés à l'open-source et protège vos instances, conteneurs, infrastructures serverless, espaces de stockage et réseaux cloud. Cette plateforme cloud-native renforce la sécurité du cloud, maîtrise les risques et améliore de jusqu'à 188 % le retour sur investissement en matière de sécurité.

Sécuriser vos collaborateurs en toutes circonstances

Que votre entreprise opère en mode télétravail, présentiel ou hybride, vous devez être en mesure de protéger vos utilisateurs, où qu'ils soient, contre des menaces qui évoluent : logiciels malveillants sans fichier, attaques ciblées, rançongiciels, cryptomining… Leader de la protection des utilisateurs en entreprise selon Gartner et Forrester, Trend Micro One offre plusieurs couches de sécurité capables de s'adapter, d'anticiper et de garder une longueur d'avance sur les menaces présentes sur les edges réseau, l'email, le web et les applications SaaS telles que Microsoft 365.

Protégez votre réseau contre les attaques sophistiquées et zero-day

Le réseau s'est étendu bien au-delà des bureaux traditionnels. Il couvre désormais les sites distants, le cloud et des environnements opérationnels critiques comme les usines.

Trend Micro One va au-delà de la protection traditionnelle des réseaux grâce à des fonctionnalités qui détectent les menaces inconnues et protègent les ressources IT et OT non-managés.

Adossé à Trend Micro™ Zero Day Initiative™ (ZDI), le plus important programme de récompense à l'identification de bugs, vous êtes protégés contre les menaces non divulguées, en moyenne 102 jours avant la mise à disposition d'un patch par son éditeur. Cette protection en amont protège votre surface d'attaque, tout en laissant votre entreprise innover et avancer dans sa transition digitale.

Des experts en sécurité compétents et disponibles en 24/7

Des équipes sécurité insuffisantes et surchargées impactent votre capacité à gérer le cycle de vie de la surface d'attaque et communiquer efficacement les risques au sein de l'entreprise. Avec Trend Micro One, une pénurie de ressources ne vous ralentit plus. Nos experts vous aident à gagner en résilience grâce à un support premium qui vous rend rapidement opérationnel et optimise la configuration de vos solutions. Managed XDR vous aide à identifier et analyser les menaces tandis que nos services de gestion des incidents se tiennent prêts à intervenir en cas d'attaques critiques.

Grâce à nos compétences acquises auprès de plus de 500 000 clients et à nos 250 millions de capteurs dans le monde, notre service de détection des attaques analyse les indicateurs de compromission (IoC) et fournit des alertes proactives, sur des menaces potentielles, ainsi qu'une assistance pour vous aider à réagir rapidement.

Simplifier la sécurité au sein un univers digital complexe

Le monde est chaque jour plus complexe. Votre surface d'attaque évolue constamment pour accompagner votre transformation digitale et l'évolution de vos objectifs. Vous devez être en mesure de gérer les risques sur l'ensemble de votre surface d'attaque en découvrant, évaluant et minimisant les risques en permanence. Nous pouvons vous y aider.

Trend Micro One est une plateforme unifiée de cybersécurité qui vous permet de comprendre, notifier et maîtriser les cyber-risques sur votre périmètre organisationnel. Elle intègre des fonctions clés comme le XDR, des informations sur les risques et une protection de référence sur l'ensemble de votre infrastructure IT. Vous pouvez ainsi déployer des stratégies de type zero trust, mieux gérer les risques de votre entreprise et répondre aux termes et conditions des cyber-assurances. Trend Micro One bénéficie de la veille sur les menaces et les vulnérabilités proposée par nos chercheurs, offrant ainsi aux entreprises les moyens d'aller plus loin et d'en fare plus.

7 - Forrester New Wave : Extended Detection and Response (XDR) Providers, T4 2021
8 - ESG : Analyzing the Economic Benefits of Trend Micro Vision One, mai 2021
9 - Worldwide Cloud Workload Security Market Shares, 2020 IDC #US47837121, juin 2021
10 - Forrester TEI Study : Trend Micro Cloud One, Juin 2021
11 - Gartner "Magic Quadrant for Endpoint Protection Platforms," par Rob Smith, Paul Webber, Mark Harris, Peter Firstbrook et Prateek Bhajanka
12 - The Forrester Wave™ : la sécurité des endpoints dans un format SaaS, T2 2021

TREND MICRO™
Securing Your Connected World