paloalto NETWORKS

PRISMA BY PALO ALTO NETWORKS

Prisma Access Cloud SWG

Renforcez vos défenses face aux nouvelles menaces web

SOMMAIRE

Ces dernières années, le monde du travail a radicalement changé. La majorité des entreprises se sont tournées vers le travail hybride, qui permet à leurs collaborateurs d'alterner présentiel et distanciel, tandis que d'autres ont complètement déserté leurs bureaux pour adopter un modèle de télétravail à 100 %. En parallèle, ces entreprises ont généralisé l'usage du SaaS (Software-as-a-Service) pour maintenir et même accroître la productivité de leurs télétravailleurs.

Dans l'ensemble, cette nouvelle approche du travail est bénéfique aux entreprises et à leurs collaborateurs. Pourtant, les vrais grands gagnants de ce changement sont les cybercriminels.

L'adoption massive du travail hybride et des applications SaaS impose aux entreprises de garantir un accès sécurisé au web pour leurs salariés, et ce quel que soit le lieu de connexion. Car il est aujourd'hui possible d'accéder à Internet quasiment n'importe où et sur n'importe quel type d'appareil. Cette situation a fondamentalement élargi le champ des menaces, ouvrant une multitude de brèches dans lesquelles les cybercriminels ne tardent pas à s'engouffrer à l'aide de techniques extrêmement élaborées qui prennent à défaut les solutions de sécurité classiques.

Face à un tel éventail de menaces venues du web, une nouvelle approche de la sécurité s'impose. Plus question de s'appuyer sur des méthodes dépassées pour bloquer des menaces nouvelles et inconnues. L'heure est venue d'évoluer vers une solution aux fonctionnalités conçues pour tenir tête à des adversaires qui ne cessent de se renouveler.

Les trois facteurs d'expansion
de la surface d'attaque du web

1 Nous sommes de plus en plus dépendants du web

Incontestablement, le web et les applications qu'il héberge forment le socle de notre productivité au quotidien. Pour des motifs professionnels ou personnels, nous visitons tous les jours des sites sur toute une panoplie d'appareils. Certes, le recours au web nous a fait gagner en efficacité, mais il a aussi étendu la surface d'attaque exploitable.

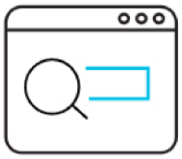
2 Le modèle de travail hybride accroît la vulnérabilité des collaborateurs

Aujourd'hui, le travail n'est plus un lieu où l'on se rend, mais une activité que l'on pratique.
Les collaborateurs sont libres de travailler depuis chez eux, dans des lieux publics ou tout autre environnement doté d'une connexion Wi-Fi. Cependant, les nombreux avantages du Work-From-Anywhere ne doivent pas occulter l'introduction de risques majeurs en parallèle. Les salariés passent désormais par leur réseau domestique ou des Wi-Fi publics pour exécuter des tâches professionnelles sensibles. Jusqu'à présent, les entreprises s'en sont remises à des technologies comme les réseaux privés virtuels (VPN) et la sécurité Zero Trust Network Access 1.0 (ZTNA) pour protéger leurs télétravailleurs. Mais outre leur manque de souplesse, ces méthodes souffrent de trop nombreuses limitations intrinsèques. Par conséquent, les télétravailleurs sont aujourd'hui exposés à des menaces que le système de sécurité de leur entreprise bloquerait s'ils étaient au bureau.

3 Des attaques toujours plus sophistiquées

Les acteurs malveillants connaissent parfaitement le mode de fonctionnement des solutions de sécurité classiques. C'est ainsi qu'ils ont su imaginer de nouvelles techniques plus avancées pour les prendre à défaut. Cloaking, attaques multi-étape, liens à usage unique… ils redoublent d'inventivité pour lancer de nouvelles attaques capables de contourner facilement les dispositifs de sécurité.

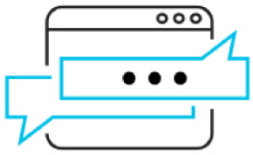
1 minute sur Internet
en 2022



5,7 millions
de recherches Google

856
minutes de webinaires sur Zoom

6 millions
d'acheteurs en ligne



148 000
envois de messages Slack

Les menaces web que vous devez connaître

Dans ce nouveau monde du travail, Internet est devenu le théâtre d'un volume très conséquent de tâches et d'interactions sensibles.

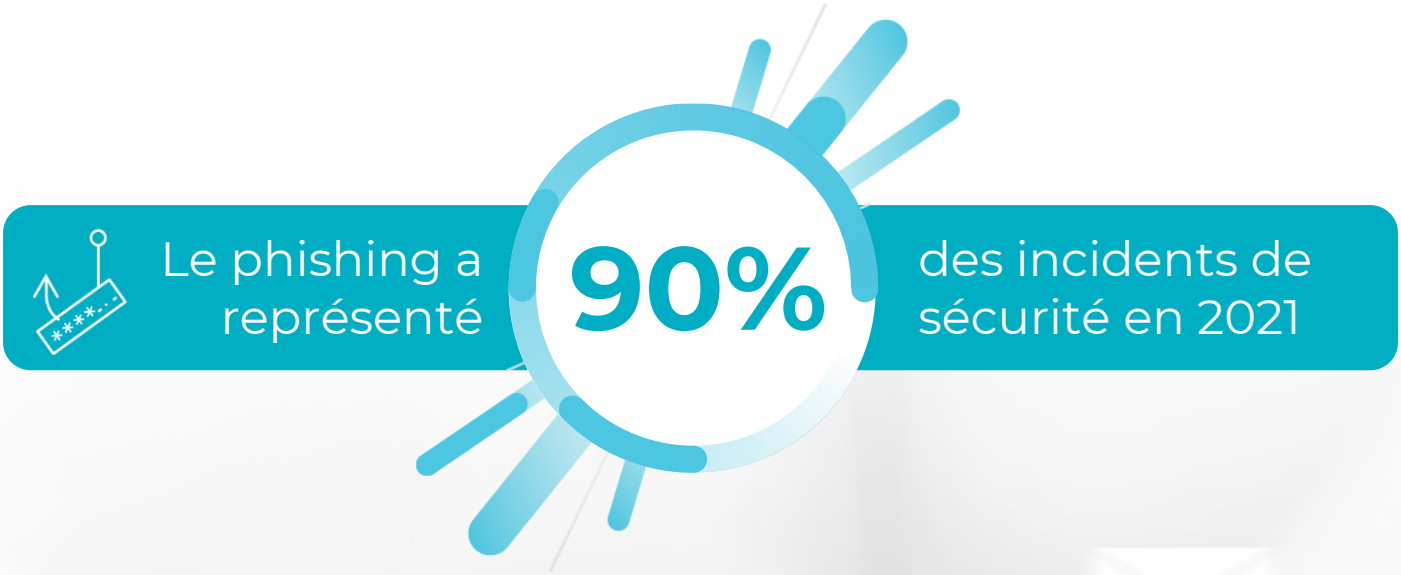
En entreprise, la communication passe principalement par l'e-mail, Zoom et Slack. Pour collaborer et partager des informations confidentielles au sein de l'entreprise, nous comptons sur les applications SaaS comme Google Workspace ou Microsoft 365. En parallèle, les collaborateurs en quête de productivité peuvent être tentés par des applications non validées par leur DSI, notamment Trello, Asana, Dropbox ou Evernote. Cette forte dépendance au web et aux applications SaaS facilite considérablement l'accès des cybercriminels à des informations sensibles, avec des conséquences parfois très graves et très coûteuses pour les entreprises victimes.

Parmi les nombreux types d'attaques véhiculées par le web, le phishing, le ransomware et les malwares semblent particulièrement prisés des cybercriminels. Le phishing a le double avantage d'être relativement simple à exécuter tout en obtenant des taux de réussite élevés. Quant aux attaques par ransomware, elles peuvent s'avérer très lucratives pour leurs auteurs. Enfin, les malwares ouvrent toute une diversité d'opportunités qui vont du gain financier au vol de données.

Phishing

Une menace croissante pour l’entreprise

Le phishing est une méthode d'ingénierie sociale dans laquelle des acteurs malveillants passent par des moyens de communication courants (e-mail, SMS, réseaux sociaux, téléphone, etc.) pour inciter leurs destinataires à télécharger un malware ou à divulguer des informations sensibles, par exemple des identifiants de connexion, des données personnelles ou des informations d'ordre financier. Bien que le phishing sévisse depuis des décennies, il n'a pas pris une ride et reste parmi les méthodes cybercriminelles les plus courantes et les plus nocives.



Étant donné le volume colossal de communications effectuées en ligne, l'e-mail est une méthode de propagation très prisée des phishers. Des études montrent ainsi qu'**en 2021, 96 % des attaques de phishing sont passées par l'e-mail.** Les attaquants choisissent souvent de ratisser très large en envoyant une quantité massive d'e-mails contenant des liens malveillants, dans l'espoir d'attraper au moins une victime dans leurs filets.

5 types courants
d’attaques de phishing

Spear-phishing

Message personnalisé et ciblé qui inclut souvent un lien ou une pièce jointe contenant un malware. Une fois que le destinataire clique sur l’un ou l’autre, l’attaquant peut se saisir de ses informations privées.

Whaling

Comme son nom l’indique, le whaling cible les gros poissons, à savoir des dirigeants d’entreprise, dans le but de leur soustraire des informations sensibles (identifiants de connexion, informations financières, etc.) ou de télécharger un malware sur l’appareil ciblé.

Smishing

Cette forme de phishing par SMS contient souvent un lien ou une pièce jointe frauduleux que l’utilisateur est invité à ouvrir sur son smartphone.

Vishing

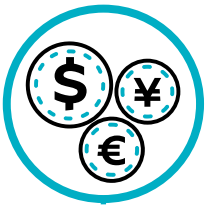
Également appelé « phishing vocal », le vishing est une forme de phishing par téléphone dans laquelle l’appelant se fait souvent passer pour l’employé d’une banque ou d’une administration, le but étant là encore d’obtenir des données sensibles.

Angler Phishing

Apparue sur les réseaux sociaux, cette forme de phishing consiste à repérer les clients mécontents d’une marque légitime, puis à endosser l’identité d’un représentant du service client pour leur soutirer des informations personnelles ou leurs identifiants de connexion.

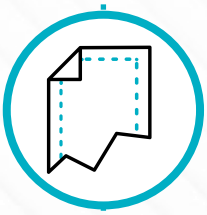
Risques des attaques de phishing

Une attaque de phishing peut avoir des répercussions désastreuses sur une entreprise. Si les conséquences financières viennent tout naturellement à l'esprit, elles sont loin d'être les seules. Tour d'horizon.



Perte financière

Constante incontournable des compromissions par phishing, les pertes financières peuvent prendre différentes formes. Par exemple, le collaborateur d'une entreprise peut, à force de persuasion, être amené à transférer des fonds à un attaquant. De même, une entreprise peut s'exposer à de lourdes amendes en cas d'infraction à des politiques de type RGPD, PCI ou PIPEDA, sans oublier les coûts d'investigation d'une intrusion et d'indemnisation des éventuels tiers concernés.



Perte de données

Une fois que la victime a mordu à l'hameçon, les phishers peuvent accéder à une variété de données sensibles : identifiants de connexion, informations à caractère personnel (adresses, numéros de téléphone, etc.), données d'entreprise, dossiers médicaux ou informations bancaires.

Atteinte à la réputation

Lorsqu'elles sont victimes d'une attaque de phishing, les entreprises tentent souvent de passer l'incident sous silence pour préserver la confiance de leurs clients et investisseurs. L'enjeu est d'autant plus considérable s'il s'agit d'une structure connue pour gérer les informations confidentielles de ses clients.

Perturbation de l'activité

Les compromissions par phishing peuvent se traduire par une paralysie des systèmes ou des perturbations majeures dans la prestation de services qui, dans un cas comme dans l'autre, plombent la productivité de l'entreprise.

Infection par malware

Les victimes de phishing peuvent involontairement télécharger des malwares sur leur poste de travail, avec des conséquences multiples (vol de données, panne de réseau, perturbations opérationnelles, etc.).

Ransomware

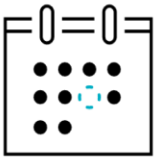
Le ransomware est un type de malware particulièrement dévastateur en termes financiers et de pertes de données. Le principe consiste à chiffrer des données sensibles, puis à exiger le versement d'une rançon en échange de la clé de déchiffrement.

14,8 M$

Coût moyen d'une attaque de phishing en 2021

4,24 M$

Coût moyen d'une compromission de données en 2021



50 jours

Perte de productivité moyenne pour une entreprise victime d'un malware

L’inquiétante ascension du ransomware

Le ransomware est un type de malware conçu pour empêcher un utilisateur ou une entreprise d'accéder à des fichiers, données ou informations de première importance. Le principe est simple : l'attaquant chiffre cette précieuse data, puis exige une forte rançon en échange de la clé de déchiffrement.

Les attaques par ransomware font régulièrement les gros titres et rien ne laisse présager une accalmie. **En 2021, on a dénombré plus de 623 millions d'attaques par ransomware, soit 105 % de plus que l'année précédente.** Cette explosion est en grande partie due à l'essor du Ransomware-as-a-Service (RaaS), qui démocratise l'accès à des kits d'attaques clé en main que même des acteurs peu versés techniquement peuvent exécuter sans peine.

En quoi consiste le Ransomware-as-a-Service (RaaS) ?

Le RaaS (Ransomware-as-a-Service) est un modèle conçu par et pour les cybercriminels. Ce nouveau business model a eu pour effet d'abaisser les barrières à l'entrée pour des attaquants sans compétences techniques particulières. Pour se rémunérer, les fournisseurs engrangent une redevance mensuelle et un pourcentage des rançons payées.

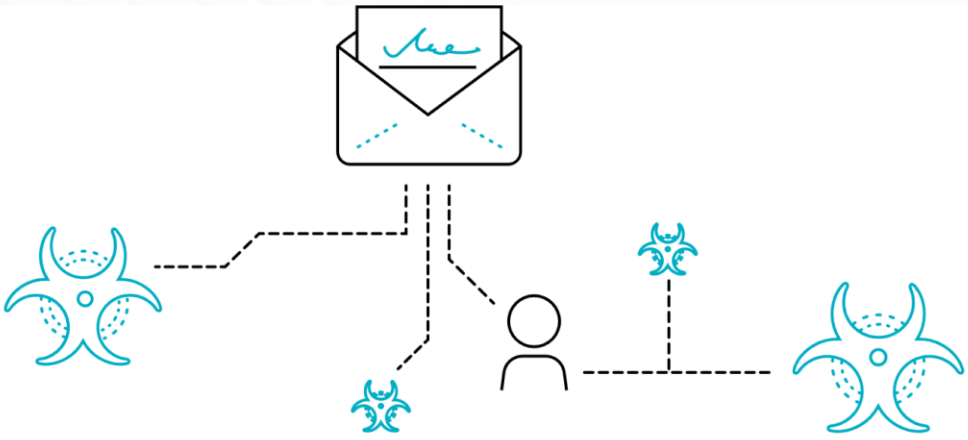
Quelle est la méthode de propagation de ransomware la plus courante ?

E-mails de phishing

Les e-mails de phishing représentent l'un des principaux véhicules du ransomware, notamment en raison du volume colossal de messages envoyés par jour.

Aujourd'hui, on compte environ **333,2 milliards d'e-mails envoyés quotidiennement, soit 3,5 millions chaque seconde.** Cette prééminence du courrier électronique augmente du même coup la probabilité qu'un utilisateur clique sur un lien malveillant et télécharge un ransomware sur son appareil.

Sur ces 333,2 milliards d'e-mails envoyés quotidiennement, **3,4 milliards sont des e-mails de phishing,** soit un e-mail sur 100. Ainsi, en fonction du nombre d'adresses électroniques que vous utilisez, vous pouvez être exposé chaque jour à plusieurs e-mails de phishing.



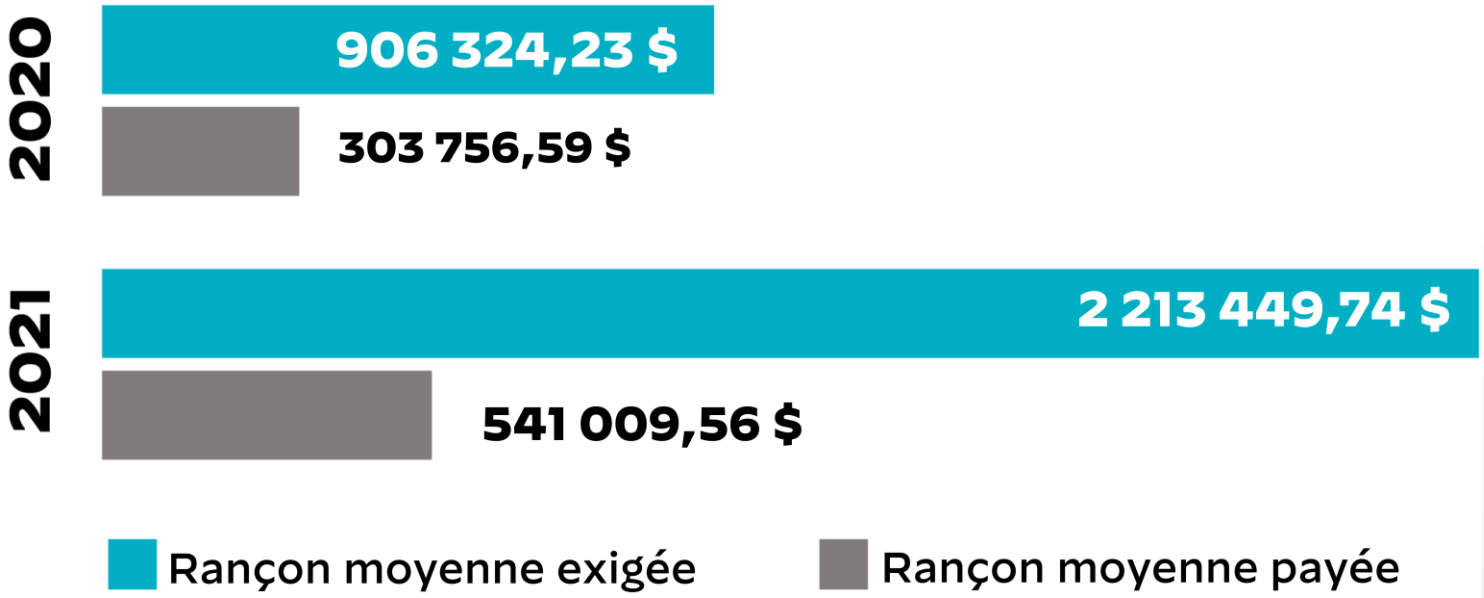
78 % des entreprises

ont reçu en 2021 un e-mail de phishing contenant un ransomware ou un lien pour en télécharger un.

Impact des attaques par ransomware

Non seulement le volume d'attaques par ransomware continue d'enfler, mais leur coût affiche également une forte hausse.

En 2021, le montant moyen de la rançon exigée s'élevait à **2,2 millions de dollars, soit 144 % de plus qu'en 2020. Quant au paiement moyen, il a atteint 541 000 dollars, soit une hausse de 78 % par rapport à l'année précédente.**
Le volume de ces attaques, conjugué à leurs ramifications potentielles, fait du ransomware une menace extrêmement dévastatrice et préjudiciable pour ses victimes.



Montant moyen des rançons exigées par rapport aux sommes effectives versées en 2020 et 2021, d'après les données de l'équipe de réponse aux incidents d'Unit 42

Malware

Personne n’est à l’abri

Le malware, ou logiciel malveillant en bon français, est l'outil n° 1 des attaquants pour infecter des systèmes et des réseaux.

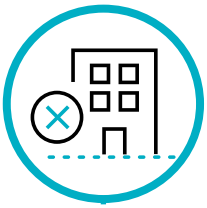
Dès lors qu'il parvient à installer un malware sur l'appareil d'un utilisateur, un attaquant peut établir une **communication CnC (Command and Control). De là, il peut accéder à distance à l'ordinateur infecté**, propager le malware à d'autres utilisateurs, récupérer des identifiants, analyser le réseau local puis progresser vers ses objectifs finaux : vol de données sensibles, déploiement d'un botnet, voire détournement du réseau pour lancer une attaque contre une autre entreprise. Les attaquants emploient une variété de moyens pour diffuser leurs malwares. Néanmoins, le phishing est devenu une méthode extrêmement prisée depuis l'essor des modèles de travail hybride.

En quoi consistent les activités de commande et contrôle ?

La technique CnC (Command and Control) permet aux acteurs malveillants de communiquer avec des appareils compromis sur un réseau pour leur fournir des instructions supplémentaires, comme le téléchargement d'autres malwares, la création de botnets ou l'exfiltration de données.

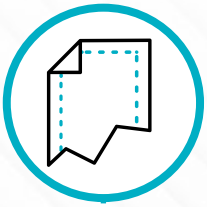
Impact des malwares

Une attaque par malware peut gravement endommager l'infrastructure réseau d'une entreprise, sans parler des autres problèmes de sécurité ni du temps et des ressources à mobiliser pour y remédier. Parmi les préjudices les plus courants :



Perturbation de l'activité

Un malware peut perturber ou bloquer un réseau pour freiner les opérations de l'entreprise, voire paralyser la prestation de ses services dans certains cas. Ces perturbations peuvent rogner la productivité de l'entreprise et se solder par des pertes désastreuses.



Perte de données

Une entreprise victime d'un malware peut s'exposer à de graves conséquences en cas de perte de données : poursuites judiciaires, érosion de la confiance des clients, atteinte à la réputation.

Préjudice réputationnel

Une attaque par malware ne se limite pas à des pertes financières directes dues à l'interruption des opérations. Exode des clients, efforts de récupération des données, coûts d'investigation, sanctions juridiques ou administratives, indemnisations de tiers… la facture totale est beaucoup plus conséquente.

Lacunes des solutions de sécurité traditionnelles

Phishing, malware, ransomware… les entreprises vivent sous la menace constante d'une compromission. Mais face aux nouvelles techniques sophistiquées des cybercriminels, les solutions de sécurité traditionnelles ne font pas le poids.

Des adversaires toujours plus inventifs

Les menaces web actuelles doivent en grande partie leur succès à la **sophistication des méthodes employées par les acteurs malveillants.** Au fil du temps, ces derniers ont fait évoluer leurs techniques pour échapper aux solutions de sécurité traditionnelles et contourner les défenses.

1. Entre le cloaking, les proxys inverses MitM et l'utilisation de plateformes SaaS légitimes, les attaquants ne manquent pas d'imagination pour éviter la détection.

2. Les kits de phishing clé en main et la puissance des infrastructures cloud permettent de générer des milliers d'URL de phishing en quelques minutes.

3. Les attaquants utilisent des menaces nouvelles et inconnues, indétectables par les solutions de sécurité classiques, qui leur permettent de contourner facilement les lignes de défense.

5 types courants
de techniques de contournement

Utilisation d'URL nouvelles et inconnues

Les web crawlers conventionnels étant trop lents pour détecter les URL malveillantes nouvelles et inconnues, les attaquants peuvent facilement contourner les systèmes de sécurité en place.

Masquage du contenu malveillant (cloaking)

Comme les robots d'indexation, ou web crawlers, n'analysent pas le trafic web en direct, les attaquants peuvent dissimuler leurs viles intentions en renvoyant les scanners de sécurité vers un site inoffensif ou une page vide, avant de le transformer en site malveillant.

Attaques multi-étapes et images CAPTCHA

Les adversaires camouflent le contenu malveillant derrière plusieurs rideaux inoffensifs, comme des images CAPTCHA, pour éviter que les web crawlers détectent le véritable contenu malveillant qu'ils dissimulent.

Liens dynamiques et kits de phishing

Grâce aux kits de phishing et aux outils d'automatisation, la création en quantités massives d'URL nouvelles et inconnues n'a jamais été aussi simple et économique. Cette véritable industrialisation permet aux attaquants d'utiliser une URL malveillante pendant quelques secondes ou minutes avant de la remplacer par une nouvelle URL, ce qui complique leur dépistage par les solutions de sécurité.

Compromission de sites web et de plateformes SaaS

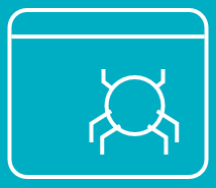
Les attaquants peuvent compromettre des sites web inoffensifs ou exploiter les plateformes SaaS légitimes pour lancer des attaques de phishing, trompant ainsi la vigilance des systèmes de détection traditionnels.

Pourquoi la sécurité d'hier

est impuissante face aux attaques d'aujourd'hui

Beaucoup d'entreprises comptent encore sur d'anciennes méthodes, à l'image des web crawlers, pour neutraliser les menaces hautement furtives et sophistiquées d'aujourd'hui. Résultat : un nombre croissant d'entreprises sont victimes d'attaques web de type phishing.

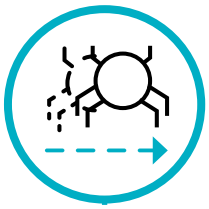
C'est un fait bien établi : les méthodes traditionnelles peinent à détecter les menaces nouvelles et inconnues. En 2021, le web s'est enrichi de **56 millions de nouvelles pages web malveillantes**. Il n'est donc pas surprenant que **93 % des entreprises aient été victimes d'opérations de phishing en 2021.** Si les solutions classiques de sécurité web ont du mal à neutraliser les nouvelles menaces, c'est en raison d'une conjonction de plusieurs facteurs.



Qu'est-ce qu'un web crawler ?

Un web crawler, ou robot d'indexation, a pour mission de parcourir Internet pour rechercher des sites, indexer leur contenu et créer une liste de pages, telles que vous les voyez ensuite dans les résultats de vos recherches sur Internet.

La page suivante répertorie trois raisons pour lesquelles les solutions de sécurité web traditionnelles sont à la peine face aux nouvelles menaces.



Les web crawlers sont trop lents

La recherche et l'analyse effectuées par les web crawlers sont trop lentes face à la vitesse et à la furtivité des nouvelles menaces. Grâce à des outils d'automatisation et à de nouvelles techniques de contournement, les attaquants génèrent des quantités massives de pages web malveillantes qui finissent par submerger les défenses traditionnelles. Si ces menaces ne sont pas bloquées avant de s'introduire sur votre réseau, les pertes potentielles peuvent être considérables.

Les bases de données de filtrage des URL manquent d'évolutivité

Pour identifier et bloquer l'accès aux sites de phishing et autres contenus malveillants, les systèmes de sécurité web traditionnels se sont longtemps reposés sur les bases de données de filtrage d'URL, sorte d'immenses référentiels des données recueillies par les web crawlers. Comme ces robots ne peuvent pas se déployer suffisamment vite, les bases de données de filtrage des URL contiennent des données obsolètes qui empêchent de bloquer à temps les menaces nouvelles et hautement furtives.

L'essentiel du trafic web est chiffré

Comme l'essentiel du trafic web actuel est chiffré, un attaquant peut très facilement masquer ses activités malveillantes. Bien que 99 % du temps de navigation sur Chrome se déroule sous le protocole HTTPS, la plupart des solutions de sécurité web actuelles ne déchiffrent pas le trafic SSL/TLS. En cause : la puissance de traitement élevée nécessaire pour déchiffrer, inspecter et rechiffrer le trafic. En l'absence des technologies adéquates, un tel déchiffrement peut de surcroît ralentir notablement la performance du réseau. De fait, comme les organisations ne déchiffrent pas le trafic, elles sont toujours plus nombreuses à être victimes d'attaques de type phishing. **En pratique, 83 % des sites de phishing utilisés actuellement recourent au chiffrement SSL pour masquer leur activité malveillante aux yeux des scanners de sécurité.**

Détection des menaces inconnues et furtives : la bonne méthode

Au moment de choisir votre prochaine solution de sécurité web, assurez-vous que les outils et la méthodologie employés soient capables d'évoluer au même rythme que les modes opératoires des acteurs malveillants.

Qu'est-ce qu'un patient zéro ?

Le patient zéro est la première personne ou le premier système victime d'une cyberattaque jusqu'alors inconnue. Si une entreprise est avertie d'une compromission, le protocole consiste à isoler le patient zéro (mise en quarantaine) pour stopper la propagation de l'attaque.

5 fonctionnalités
indispensables aux besoins de sécurité web actuels

Données et détection des menaces

Une solution de sécurité web moderne doit être équipée de fonctionnalités de détection renseignées par des volumes gigantesques d'informations sur les menaces. Ces données permettent aux modèles de machine learning d'apprendre à analyser et à détecter avec précision les menaces potentielles, sans intervention humaine ni ingénierie fonctionnelle.

Analyse du trafic en direct

L'analyse inline du trafic permet de détecter instantanément le trafic malveillant dès qu'il accède au réseau. Cette méthode est essentielle pour bloquer les menaces nouvelles et inconnues, car leurs techniques de contournement ne résistent pas à une analyse en temps réel.

Application des protections en temps réel

Non seulement les menaces doivent être détectées dès qu'elles pénètrent sur un réseau, mais également bloquées immédiatement pour éviter le scénario du patient zéro. En ce sens, votre solution doit pouvoir rediriger le trafic vers le cloud pour inspection, puis recevoir un verdict en temps réel.

Analyse dans le cloud et puissance de traitement

Les modèles de machine learning exigent une puissance de traitement colossale pour produire des résultats en quelques millisecondes et un verdict en temps réel, deux conditions essentielles à la prévention du scénario du patient zéro.

Base de données d'URL avec mises à jour instantanées

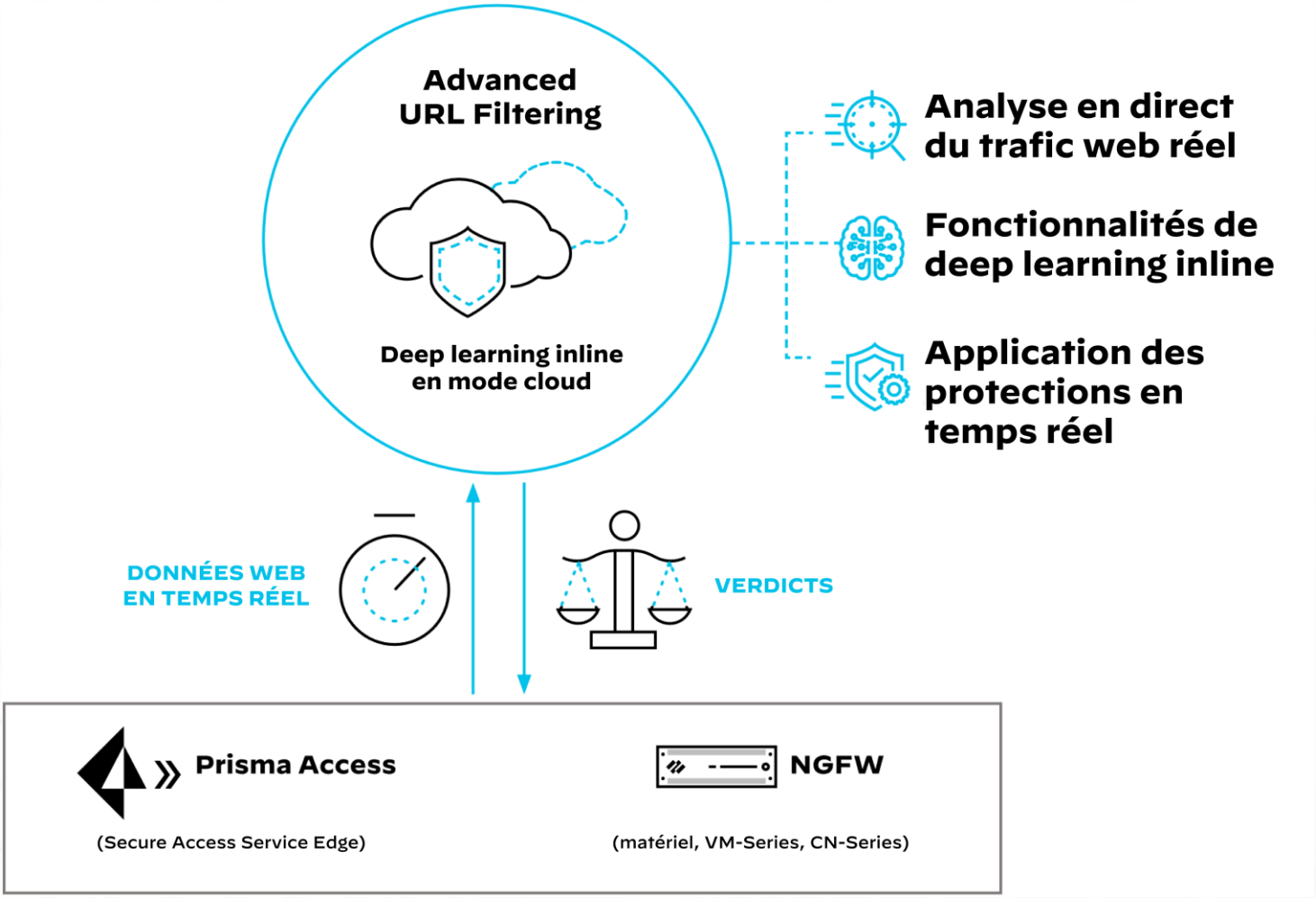
Pour que la sécurité web se hisse à la hauteur du défi, un changement de méthode s'impose. Les bases de données statiques ne forment qu'une composante de la solution. Pour faire échec aux nouvelles techniques des attaquants, il vous faut un service cloud capable d'exploiter les modèles de machine learning pour fournir des verdicts instantanés sur des données temps réel.

Prisma Access Cloud SWG

Advanced URL Filtering

Prisma Access Cloud SWG fait appel à Palo Alto Networks Advanced URL Filtering pour neutraliser en temps réel les menaces web inconnues et avancées.

Basé sur notre technologie de deep learning inline, Advanced URL Filtering est la seule solution de sécurité web du marché capable de neutraliser les nouvelles menaces en temps réel, **bloquant ainsi 40 % plus de menaces** que les bases de données de filtrage web classiques. Vous mettez alors toutes les chances de votre côté pour éviter le scénario du patient zéro.



En quoi consiste le deep learning ?

Le deep learning est une déclinaison du machine learning. Grâce à ses réseaux neuronaux multicouches, il apprend des événements de sécurité qu'il observe avec un minimum d'intervention des data scientists.

Analyse du trafic web réel

Fini les analyses différées : le trafic web réel est passé au crible dès qu'il pénètre sur le réseau et les menaces sont instantanément bloquées.

Détection des menaces furtives

L'inspection du trafic web réel, et non plus seulement des données des web crawlers, permet de détecter les attaques ciblées et furtives avec davantage de précision.

Protection

Contrez les attaques web furtives et inconnues en temps réel pour éviter le scénario du patient zéro.

40 %

de protection en plus par rapport aux bases de données de filtrage web traditionnelles

88 %

des URL malveillantes bloquées au moins 48 h avant les autres fournisseurs

11,5 M

d'URL malveillantes détectées par jour

Renforcez votre protection web avec paloalto NETWORKS

Prisma Access Cloud SWG avec Advanced URL Filtering déjoue les cyberattaques les plus furtives et sophistiquées, mais pas seulement : il simplifie également les opérations tout en améliorant l'expérience utilisateur. Sur site distant, en déplacement ou en télétravail, vos utilisateurs peuvent se connecter en toute sécurité à Internet et à toutes les applications critiques d'entreprise, avec le même niveau d'accès et de sécurité qu'au QG de l'entreprise.

Prisma Access Cloud SWG

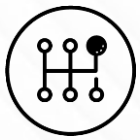
Sécurité des accès Internet et SaaS pilotée par IA/ML

Visitez notre site

Cloud SWG vs appliances proxy web

Comparatif des solutions

Télécharger l'infographie



Démo interactive SE

Jugez par vous-même

S'inscrire

Modernisez votre SWG avec le SASE

Livre blanc ESG

Télécharger

SOURCES :

- 90 % des incidents de sécurité en 2021 comportaient une part de phishing
- Chaque minute, nous envoyons 197,6 millions d'e-mails, dépensons 1,6 million de dollars en ligne et téléchargeons presque 415 000 applications à l'échelle mondiale
- L'employé lambda passe en moyenne plus de 75 % de son temps de travail sur un navigateur web
- Le coût moyen d'une attaque de phishing s'élève à 14,8 millions de dollars
- 93 % des entreprises ont été victimes d'opérations de phishing en 2021
- 83 % des sites de phishing appliquent le déchiffrement SSL
- 90 % des kits de phishing incluent des techniques de contournement
- 3,4 milliards d'e-mails de phishing sont envoyés quotidiennement

paloalto® NETWORKS

www.paloaltonetworks.fr

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas

Téléphone : +31 20 888 1883