6 FONCTIONNALITÉS ESSENTIELLES

D'UN FIREWALL MODERNE

1. INSPECTION SSL/TLS HAUTE PERFORMANCE

Si vous n'utilisez pas de déchiffrement HTTPS ni d'inspection de contenu, vous n'avez probablement pas connaissance des **2/3 des malwares** qui atteignent votre entreprise.

Plus de 80 % du trafic d'entreprise s'effectue via des canaux chiffrés et 50 % des sites de phishing utilisent le protocole HTTPS pour dissimuler leurs attaques. L'inspection HTTPS permet de déchiffrer le trafic HTTPS, d'examiner le contenu à la recherche de signes d'attaque, puis de chiffrer à nouveau le trafic à l'aide d'un nouveau certificat pour un delivery sûr.

SANS DÉCHIFFREMENT :
Aucune visibilité sur le type de données, l'application, le respect des stratégies, le type de fichier ou les tentatives d'exfiltration de données via HTTPS.

CONSEILS

Recherchez un firewall offrant une inspection du trafic HTTPS haute performance lorsque TOUS les services de sécurité sont actifs.

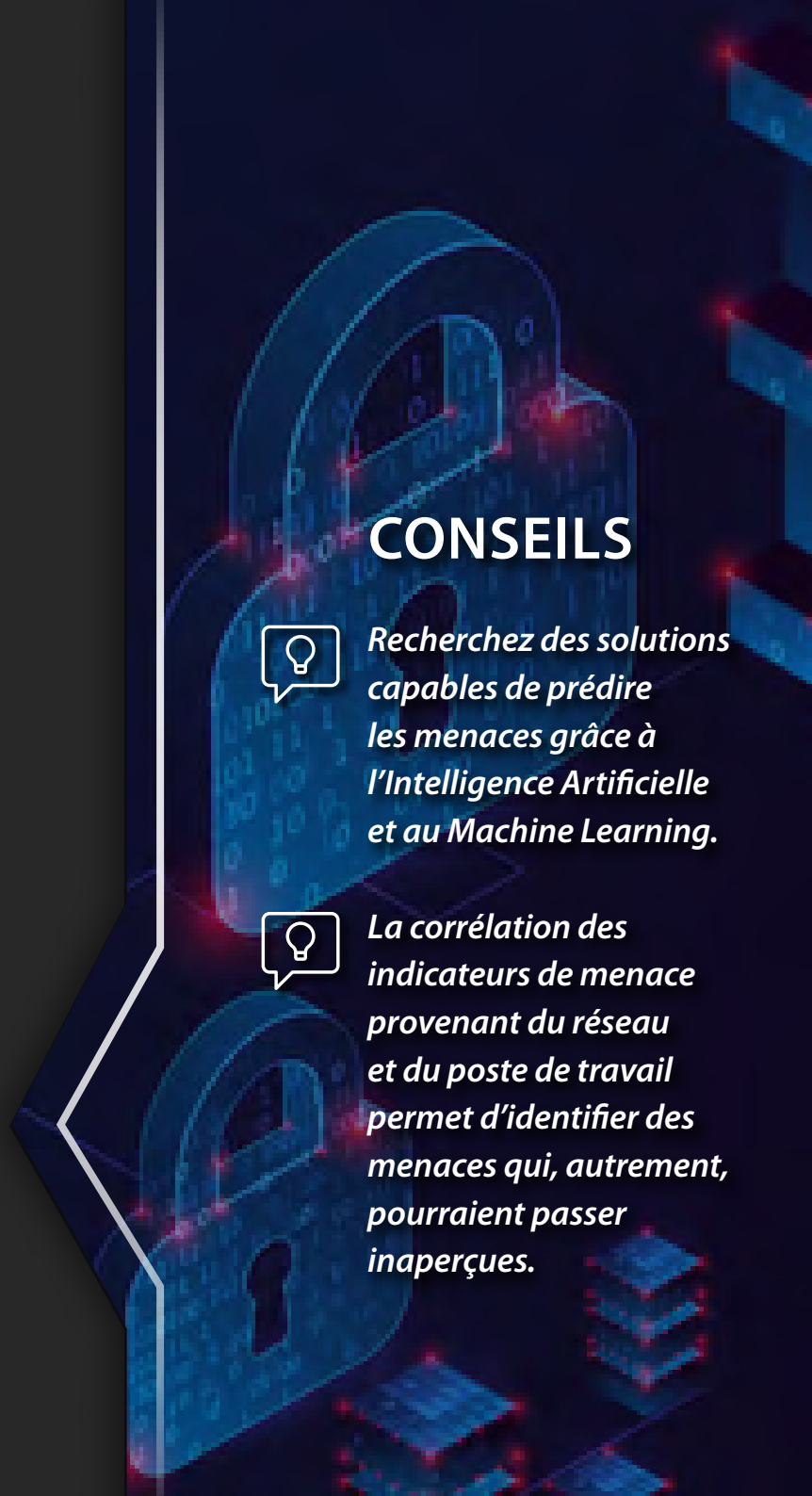
Recherchez une solution qui prend en charge l'inspection COMPLÈTE de TLS 1.3.

2. COUCHES DE DÉFENSE CONTRE LES MALWARES DE TYPE « ZERO DAY »

Les malwares de type « Zero Day » représentent **64 % des malwares** rencontrées sur les réseaux d'entreprise classiques.

Une attaque de type « Zero Day » est une tentative d'exploitation d'une vulnérabilité dans un logiciel ou un équipement informatique, avant que celle-ci ne soit identifiée et qu'une mesure préventive spécifique ne soit mise en place. Une protection de type « Zero Day » doit donc être capable de bloquer ce type de menace, même si les mécanismes exacts de l'attaque sont inconnus.

UNE APPROCHE PAR COUCHE POUR UNE COUVERTURE MAXIMALE :
Détection au moyen de l'IA, sandbox dans le Cloud, détection et réponse intégrées au niveau des postes de travail.



CONSEILS

Recherchez des solutions capables de prédire les menaces grâce à l'Intelligence Artificielle et au Machine Learning.

La corrélation des indicateurs de menace provenant du réseau et du poste de travail permet d'identifier des menaces qui, autrement, pourraient passer inaperçues.

3. PROTECTION CONTRE LE PHISHING ET LES COMPORTEMENTS IMPRUDENTS

83 % des entreprises ont déjà été victimes de phishing.

Les pirates informatiques s'appuient sur le DNS pour hameçonner leurs victimes. Un examen attentif des demandes DNS constitue donc un excellent moyen d'identifier et d'intercepter les attaques. Les tentatives involontaires de connexion par vos utilisateurs à des adresses DNS malveillantes connues peuvent être automatiquement bloquées, les utilisateurs étant ensuite redirigés de manière transparente vers une page de renvoi sûre.

LA PREMIÈRE LIGNE DE DÉFENSE :
Bloquer les domaines de détournement de clics et de phishing malveillants, quels que soient le type de connexion, le protocole ou le port.

CONSEILS

Recherchez des solutions qui bloquent aussi bien les tentatives de phishing que les canaux de commande et de contrôle.

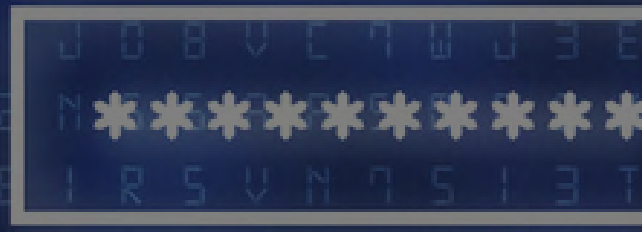
Recherchez des solutions qui informent immédiatement l'utilisateur lorsqu'il est victime d'une campagne de phishing.

4. PORTAIL WEB D'ACCÈS SÉCURISÉ

L'utilisateur moyen passe **36 minutes par mois** à saisir manuellement ses identifiants et mots de passe, perdant ainsi près d'une journée de travail complète par an.

Grâce au SSO (pour Single Sign-On), les employés peuvent se connecter une seule fois, grâce à un identifiant et un mot de passe, et accéder à toutes les applications, sites Web et données nécessaires. Le SSO améliore la sécurité en réduisant au maximum le nombre de mots de passe que les utilisateurs doivent retenir et allège la charge de travail des équipes informatiques submergées de demandes de réinitialisation de mots de passe.

BONNE PRATIQUE :
Combinez le SSO et l'authentification multifacteur pour sécuriser les connexions RDP (bureau à distance), SSH et d'accès au Web.



CONSEILS

- ***Veillez à ce que le portail prenne en charge les fournisseurs d'identité populaires, tels que AuthPoint, Shibboleth, OneLogin, ADFS et Okta.***
- ***Recherchez une solution prenant en charge les tokens logiciels les plus courants, notamment AuthPoint, Okta Mobile, Google Authenticator, OneLogin Protect, Duo Mobile, ou encore RSA SecureID.***

5. PRISE EN CHARGE DE LA DERNIÈRE TECHNOLOGIE VPN

68 % des entreprises ont étendu leur utilisation des réseaux privés virtuels (VPN) en conséquence directe de la pandémie de COVID-19.

Les VPN permettent de fournir un tunnel sécurisé entre des sites distants et un bureau central. Il existe plusieurs types de technologies VPN pour utilisateurs mobiles ou distants. Certains fournisseurs vendent des licences VPN supplémentaires avec leur firewall, tandis que d'autres les incluent dans chaque modèle.

TECHNOLOGIES VPN POUR UTILISATEURS DISTANTS :

IKEv2 (le plus récent, le plus rapide), IPSec (mais n'utilisez pas de clés pré-partagées), SSL (le plus largement utilisé), L2TP (système hérité, à éviter !)

CONSEILS

L'authentification multifacteur doit être utilisée pour les connexions aux applications hébergées dans le Cloud (SaaS) et pour l'accès VPN aux réseaux d'entreprise.

Recherchez les plateformes prenant en charge un tunnel de routage par défaut qui redirige le trafic vers le firewall central pour une inspection de sécurité complète.

6. AUTOMATISATION NATIVE

Il a été démontré que l'automatisation **réduit de 80 % les heures de travail** que les équipes consacrent à la gestion de la sécurité.

Un haut niveau d'automatisation est nécessaire pour suivre l'évolution des menaces, réduire le gaspillage de temps et d'argent et augmenter la visibilité dans un environnement de réseau moderne. Les plateformes de sécurité intégrées sont conçues avec une automatisation de A à Z, ce qui leur permet d'étendre la valeur de sécurité de votre réseau au-delà du périmètre classique.

4 NIVEAUX D'AUTOMATISATION : opérationnelle, réactive, prédictive et gestionnelle.

CONSEILS

L'intégration aux outils RMM et PSA peut permettre une réponse plus rapide aux besoins d'assistance.

La protection prédictive basée sur l'IA peut aider à bloquer les menaces sophistiquées qui, autrement, nécessiteraient une équipe d'experts en interne pour être détectées.

Firebox®

1. Meilleur déchiffrement SSL/TLS de sa catégorie
2. 3 couches de protection de type « Zero Day »
3. Filtrage DNS dans le Cloud
4. Portail d'accès inclus
5. 4 types de VPN mobiles, dont IKEv2
6. 4 niveaux d'automatisation de la sécurité inclus

Pour en savoir plus, rendez-vous sur
www.watchguard.com/fr/wgrd-products/firewall-appliances

250
attaques réseau

1 300
fichiers malveillants

~ nombre moyen de menaces bloquées par appliance Firebox en 2019

WatchGuard offre une sécurité hautement efficace et un faible coût total de possession. C'est **l'un des deux seuls produits à bloquer 100 % des évasions.**

— NSS Labs

LE PORTEFEUILLE DES SOLUTIONS DE SÉCURITÉ WATCHGUARD

Sécurité réseau

Les solutions de sécurité réseau WatchGuard sont spécifiquement conçues pour être faciles à déployer, à utiliser et à gérer, en plus d'offrir la meilleure sécurité qui soit. Notre approche novatrice de la sécurité réseau s'efforce de fournir une protection de pointe à toutes les entreprises, indépendamment de leur taille et de leur niveau d'expertise technique.

Wi-Fi sécurisé

Conçue pour offrir un environnement Wi-Fi de confiance et sécurisé, éliminant les tâches d'administration fastidieuses et réduisant considérablement les coûts, les solutions de Wi-Fi sécurisé WatchGuard changent littéralement la donne sur le marché actuel. Avec des outils d'engagement exhaustifs et une parfaite visibilité sur vos données d'entreprise, cette solution confère à votre entreprise un avantage concurrentiel indéniable.

Authentification multifacteur

WatchGuard AuthPoint® permet de combler la faille de sécurité qu'induit le recours à des mots de passe au moyen d'une authentification multifacteur, via une plateforme Cloud facile à utiliser. L'approche unique de WatchGuard se démarque grâce au facteur « ADN de téléphone portable » qui permet de vérifier que seules les personnes autorisées ont accès aux réseaux et aux applications Cloud sensibles.

Sécurité des postes de travail

WatchGuard Endpoint Security est une gamme Cloud native de pointe qui assure la sécurité des postes de travail et protège les entreprises contre tout type de cyberattaques, actuelles et futures. Sa solution phare reposant sur l'Intelligence Artificielle, Panda Adaptive Defense 360, améliore instantanément la posture des entreprises en matière de sécurité. Elle associe des capacités de protection des postes de travail (EPP) et de détection et de réponse au niveau des postes de travail (EDR) aux solutions Zero-Trust Application Service et Threat Hunting Service.

À PROPOS DE WATCHGUARD

WatchGuard® Technologies, Inc. est un leader mondial de la sécurité réseau, des connexions Wi-Fi sécurisées, de l'authentification multifacteur et de l'intelligence réseau. Les produits et les services primés de WatchGuard sont recommandés par plus de 10 000 revendeurs et prestataires de services spécialisés dans la sécurité et protègent plus de 80 000 clients dans le monde. WatchGuard a pour mission d'offrir une sécurité de pointe aux entreprises de tous types et de toutes tailles, ce qui en fait la solution idéale pour les entreprises multisites et pour les PME et les entreprises multisites. L'entreprise a établi son siège social à Seattle, dans l'État de Washington, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie-Pacifique et en Amérique latine.

Pour en savoir plus, rendez-vous sur le site **WatchGuard.fr**.

SERVICE COMMERCIAL FRANCE +33 (0)1 40 90 30 35 SERVICE COMMERCIAL INTERNATIONAL +1 206 613 0895 SITE WEB : www.watchguard.fr