

LE GUIDE CYBER WANUP

Tout savoir sur la cyber entre réel et marketing

Ce qui menace vraiment votre entreprise, ce qui la protège vraiment, et ce que l'on vous vend parfois un peu vite. Pour décider en connaissance de cause.

01 Les attaques

02 Les conséquences

03 La défense en couches

04 Le rôle de chaque outil

05 Focus : les menaces dans HTTPS

06 Ce que WANUP couvre

07 La souveraineté, barrière cyber

08 Compléments & bons réflexes

■ Par où entrent les attaquants ?

Une attaque a toujours besoin d'une porte d'entrée. Il y en a cinq principales : connaître les portes, c'est savoir où placer les barrières.



Les 9 attaques à connaître



Phishing

Un faux mail ou SMS qui imite une banque, un fournisseur ou un collègue pour faire cliquer, ouvrir une pièce jointe ou saisir un mot de passe.

Outils : anti-spam, filtrage web

Porte : messagerie



Virus & malwares

Un programme malveillant (virus, cheval de Troie, logiciel espion) caché dans un fichier téléchargé, une pièce jointe ou un site piégé.

Outils : filtrage web, CTI, EDR

Portes : web, messagerie



Clé USB infectée

Le malware entre physiquement, branché sur un poste. Il ne passe pas par le réseau, donc aucune barrière réseau ne le voit arriver.

Outil : antivirus / EDR

Porte : poste de travail



Rançongiciel

Chiffre les fichiers de l'entreprise et exige une rançon pour les rendre. Les données sont souvent volées avant, avec menace de publication.

Outils : EDR, CTI, sauvegardes

Portes : messagerie, accès distant



Déni de service (DDoS)

Des milliers de machines envoient en même temps un flot de requêtes vers une adresse IP pour saturer le lien ou le serveur et le rendre indisponible.

Outil : anti-DDoS opérateur

Porte : services exposés



Intrusion par une faille

Des robots scannent Internet à la recherche d'un service mal protégé ou non mis à jour, puis exploitent la faille pour entrer.

Outils : firewall, IPS / IDS

Porte : services exposés



Vol d'identifiants

Un mot de passe volé, deviné ou réutilisé suffit pour se connecter comme un salarié, souvent via l'accès à distance.

Outils : ZTNA, MFA

Porte : accès à distance



Spam & botnets

Des réseaux de machines piratées (« zombies ») envoient des mails en masse et servent de relais aux autres attaques.

Outils : anti-spam, IP toxiques

Portes : messagerie, Internet



Menaces dans HTTPS

Le cadenas chiffre la connexion... y compris le malware qu'elle transporte. Sans précaution, il passe inaperçu (voir page 6).

Outils : inspection SNI, CTI

Porte : navigation web

■ Quand l'attaque réussit

Une attaque touche d'abord les données. Mais c'est toute l'entreprise qui en paie le prix : activité, finances, clients, image et conformité.



Scénario type : un simple clic, trois semaines d'arrêt

Exemple illustratif, construit à partir du déroulé classique d'une attaque par rançongiciel.



À RETENIR

Chaque étape est une chance

Bloquer le mail, le lien, le téléchargement ou la communication avec l'attaquant suffit à casser la chaîne.

Le temps joue contre vous

Plus l'intrusion reste invisible, plus elle se propage. Détecter vite compte autant que bloquer.

Déclarer est obligatoire

Une fuite de données personnelles se notifie à la CNIL sous 72 h (RGPD). NIS 2 ajoute ses propres obligations.

■ Comme un château fort

Douves, remparts, gardes, portes à badge, coffre-fort : aucune barrière n'est parfaite seule, c'est leur empilement qui protège. Une menace qui passe une couche doit être arrêtée par la suivante.

WANUP brique intégrée **Hors périmètre** solution tierce ou opérateur

 **Internet** là d'où viennent les menaces : mails piégés, sites infectés, robots, attaquants

Couche 1 Opérateur

Anti-DDoS

absorbe le flot avant qu'il ne sature votre lien

Hors périmètre

Arrête :

déni de service (DDoS)

Couche 2 Périmètre réseau

IPS / IDS

repère les signatures suspectes

WANUP

Firewall

le garde à la porte, applique les règles

WANUP

CTI & IP toxiques

listes de menaces connues

WANUP

Arrête :

intrusions, scans, IP et serveurs malveillants, botnets

Couche 3 Web & mails

Filtrage web

bloque les sites et domaines dangereux

WANUP

Anti-spam

trie le courrier avant la boîte mail

Hors périmètre

Arrête :

phishing, spam, sites piégés

Couche 4 Accès

ZTNA & postures

la bonne personne, sur un poste sain, vers les seules applis autorisées

WANUP

Arrête :

vol d'identifiants, accès non autorisés

Couche 5 Poste de travail

Antivirus / EDR

surveille ce qui s'exécute sur le poste, isole s'il le faut

Hors périmètre

Arrête :

clé USB, fichiers piégés, rançongiciel

Couche 6 Dernier recours

Journaux · SIEM

garder la trace pour détecter et comprendre

WANUP

Sauvegardes

une copie hors ligne pour tout restaurer

Hors périmètre

Permet :

redémarrer après une attaque



Le réseau protège les couches 1 à 4, le poste la couche 5. Une clé USB ou un fichier déjà sur le poste ne traverse aucune barrière réseau : c'est pourquoi WANUP se combine avec un antivirus / EDR.

■ Les outils, expliqués simplement

Chaque outil a un rôle précis. En une phrase, avec une image du quotidien.



Firewall

Disponible

Décide quels flux ont le droit d'entrer et de sortir, selon des règles (provenance, destination, port, application).

Le vigile à l'entrée, avec sa liste d'invités.



IPS / IDS

Disponible

Analyse les paquets qui passent et reconnaît les signatures d'attaques connues. L'IDS alerte, l'IPS bloque le flux.

Le portique détecteur de métaux.



CTI (renseignement)

Disponible

Listes de menaces mises à jour en continu (IP, domaines, URL, empreintes de fichiers), transmises au firewall pour bloquer.

Le fichier des personnes recherchées, partagé par la police.



Filtrage web

Disponible

Bloque l'accès aux sites malveillants ou indésirables, par domaine et par catégorie, au bureau comme en mobilité.

Le GPS qui refuse les rues mal famées.



ZTNA & postures

Disponible

Seul un agent reconnu, sur un poste conforme, ouvre l'accès, et uniquement aux applications autorisées, selon la posture du poste.

Le badge nominatif qui n'ouvre que vos portes.



Journaux · SIEM

Disponible

Centralise les événements de sécurité pour repérer une attaque en cours et comprendre après coup. WANUP exporte en Syslog.

La salle de contrôle des caméras.



Antivirus / EDR

Hors périmètre

Sur chaque poste. L'antivirus reconnaît les virus connus ; l'EDR surveille les comportements suspects et peut isoler la machine.

Le médecin installé dans chaque bureau.



Anti-spam

Hors périmètre

Filtre les mails avant la boîte de réception grâce à des bases d'expéditeurs et de robots spammeurs connus.

Le tri du courrier au secrétariat.



Anti-DDoS

Hors périmètre

Absorbe et nettoie le trafic d'attaque en amont, chez l'opérateur ou dans le cloud, avant qu'il ne sature votre lien Internet.

La digue avant le village, pas la porte de la maison.



Sauvegardes

Hors périmètre

Des copies régulières, dont une hors ligne que l'attaquant ne peut pas atteindre. Le seul vrai remède au rançongiciel.

Le double des clés, rangé chez le notaire.

■ Les menaces cachées dans le cadenas

Presque tout le trafic web est aujourd'hui chiffré (HTTPS). C'est une bonne nouvelle pour la confidentialité, mais un malware peut voyager dans ce tunnel sans être vu.

Une connexion HTTPS, c'est une lettre scellée



L'enveloppe : visible

L'adresse IP de destination et le nom du site (lu dans le SNI, ex. **exemple.com**).



Le contenu : scellé

L'URL complète (/page/fichier.exe), le texte des pages et les fichiers téléchargés.

Deux façons de se protéger

OPTION A

Ouvrir chaque lettre

déchiffrement SSL / TLS

Poste > ouvre · inspecte · referme > Internet

- + Voit tout le contenu, fichiers compris.
- Matériel très puissant : le débit utile chute fortement.
- Un certificat à installer sur chaque poste ; certaines applis cessent de fonctionner.
- Lire les échanges des salariés est très encadré : information, CSE, exclusion des sites bancaires et de santé.

OPTION B · L'APPROCHE WANUP

Vérifier l'adresse, pas la lettre

SNI + IP toxiques + CTI

Poste > lit l'enveloppe · compare aux listes > Internet

- + Les destinations dangereuses sont bloquées avant même la connexion.
- + Pas de déchiffrement : débit préservé, pas de matériel surdimensionné.
- + Pas de certificat à déployer, vie privée des salariés respectée.
- + Listes de domaines et d'IP malveillants mises à jour en continu par la CTI.

Inspection
SNI



CTI
Sekoia

Le cadenas n'est plus un angle mort

WANUP sait où va chaque connexion chiffrée et le compare en temps réel aux listes de menaces : la destination dangereuse est bloquée avant le moindre échange, sans déchiffrer ni ralentir le réseau.

■ Attaque par attaque : la couverture WANUP

Pour chaque menace, les protections qui l'arrêtent, et celles que WANUP apporte déjà.

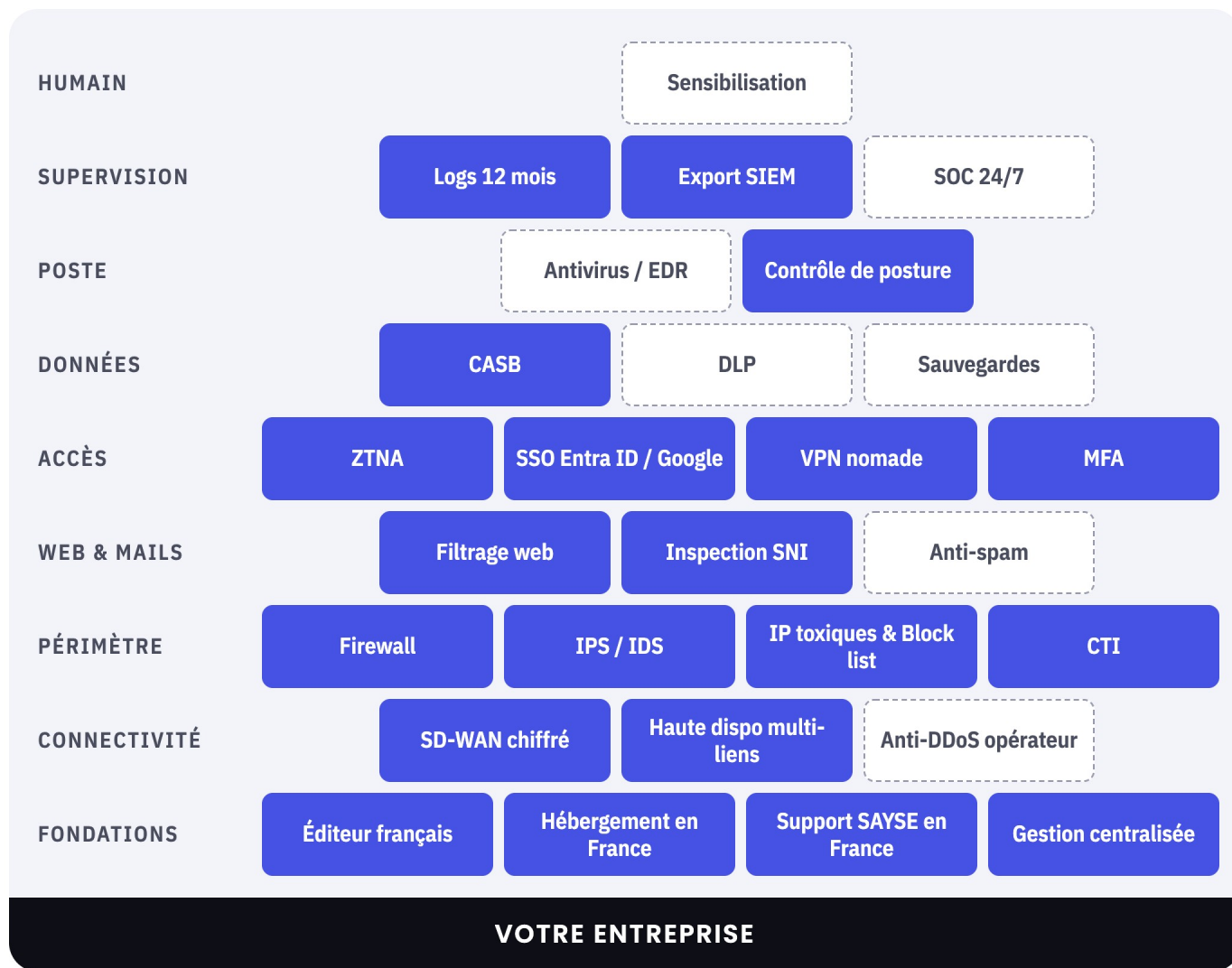
26 / 34 protections assurées par WANUP

ATTAQUE	TYPE DE PROTECTION	BRIQUE WANUP
Intrusion par une faille	Firewall	✓ Couvert
	IPS / IDS	✓ Couvert
	Block list	✓ Couvert
Vol d'identifiants, accès distant	ZTNA	✓ Couvert
	Double authentification (MFA)	✓ Couvert
	SSO Entra ID / Google	✓ Couvert
	Contrôle de posture du poste	✓ Couvert
Botnets, serveurs malveillants	IP toxiques	✓ Couvert
	Block list Data-Shield	✓ Couvert
	Renseignement sur les menaces (CTI)	✓ Couvert
Menaces dans HTTPS	Inspection SNI	✓ Couvert
	CTI (domaines et IP malveillants)	✓ Couvert
	Filtrage web par catégories	✓ Couvert
Phishing	Filtrage web	✓ Couvert
	CTI (liens de phishing)	✓ Couvert
	Anti-spam messagerie	Non couvert
Virus & malwares	Filtrage web	✓ Couvert
	CTI	✓ Couvert
	IPS / IDS (signatures)	✓ Couvert
	Antivirus / EDR	Non couvert
Rançongiciel	Coupure du contact avec l'attaquant (CTI, IP toxiques)	✓ Couvert
	Segmentation du réseau (firewall)	✓ Couvert
	Antivirus / EDR	Non couvert
	Sauvegardes hors ligne	Non couvert
Fuite de données	Règles de firewall sortantes	✓ Couvert
	CASB (contrôle des applis cloud)	✓ Couvert
	DLP (analyse du contenu)	Non couvert
Attaque passée inaperçue	Journaux conservés 12 mois	✓ Couvert
	Export vers un SIEM (Syslog)	✓ Couvert
	Surveillance SOC 24/7	Non couvert
Clé USB infectée	Posture : antivirus actif exigé	✓ Couvert
	Antivirus / EDR	Non couvert
Déni de service (DDoS)	Haute dispo multi-liens	✓ Couvert
	Anti-DDoS opérateur	Non couvert

Le mur de sécurité, brique par brique

Une sécurité solide s'empile, des fondations jusqu'aux utilisateurs. En bleu, les briques apportées par WANUP ; en pointillés, celles à confier à un partenaire.

 Brique WANUP
 Hors périmètre



20

briques apportées par WANUP, de la connectivité à la supervision, pilotées depuis une seule console.

7

briques hors périmètre réseau, à confier à un partenaire : poste, messagerie, données, opérateur, SOC et formation.

■ La souveraineté, une barrière cyber à part entière

Protéger ses données des pirates ne suffit pas : encore faut-il qu'aucun État étranger ne puisse les exiger légalement. Une donnée lue par un tiers est déjà sortie du coffre.

FOURNISSEUR SOUMIS AU DROIT AMÉRICAIN

Autorité américaine

✓ demande via Cloud Act ou FISA

Le fournisseur doit obéir

✓ même si les serveurs sont en Europe

Vos données remises

Sans juge français, et le client n'est pas forcément prévenu.

WANUP · ÉDITEUR FRANÇAIS

Autorité étrangère

✗ aucune prise directe sur SAYSE

Passage obligé par la justice française

✓ entraide judiciaire, droit français et RGPD

Vos données restent en France

Société française, hébergement et exploitation en France.

Les textes à connaître

Cloud Act · 2018

Oblige les fournisseurs américains à remettre les données qu'ils contrôlent, où qu'elles soient stockées, sur réquisition d'une autorité américaine.

FISA, section 702

Permet au renseignement américain de collecter les communications de non-Américains auprès des fournisseurs US, sans mandat individuel.

Data Privacy Framework

Accord UE-USA de 2023, contesté devant la Cour de justice de l'UE. Ses deux prédécesseurs ont été annulés (2015, 2020).

Ce que l'entreprise risque concrètement

Espionnage économique

Appels d'offres, prix, R&D, fichiers clients : des informations qui valent cher pour un concurrent étranger.

Carte de votre activité

Un réseau ou un SASE voit tout passer : sites, applis, partenaires, horaires. Même sans le contenu, c'est très parlant.

Procédures extraterritoriales

Enquêtes anticorruption ou sur les sanctions : Alstom et BNP Paribas ont payé cher l'application du droit américain.

Coupure de service

Des sanctions américaines peuvent priver un client de ses outils du jour au lendemain, comme l'a vécu la Cour pénale internationale en 2025.

Non-conformité RGPD

Un accès étranger aux données personnelles est un transfert hors UE que l'entreprise doit pouvoir justifier.

Secret professionnel

Avocats, santé, défense, secteur public : l'exigence de souveraineté est souvent écrite dans les marchés.

AVEC WANUP

Éditeur français

SAYSE, non soumis au Cloud Act.

Hébergé en France

Concentrateurs redondés dans des datacenters français.

Exploité en France

Support et exploitation par les équipes SAYSE.

Métadonnées seulement

Pas de contenu collecté ; logs gardés 12 mois en France.

■ Compléter WANUP

WANUP protège le réseau et les accès. Quatre briques complètent la défense, hors du réseau.

Antivirus / EDR

Clés USB, fichiers piégés, rançongiciel sur le poste.

Sécurité messagerie

Anti-spam et anti-phishing avant la boîte mail.

Anti-DDoS

Option à demander à l'opérateur Internet.

Sauvegardes

Dont une copie hors ligne, testée régulièrement.

Les 6 bons réflexes, outils ou pas

1

Former les équipes

La plupart des attaques commencent par un clic. Un salarié qui doute et signale vaut un outil.

2

Activer la double authentification

Un mot de passe volé ne suffit plus pour entrer, surtout à distance.

3

Mettre à jour

Systèmes, logiciels et équipements : chaque mise à jour ferme des failles connues.

4

Sauvegarder en 3-2-1

3 copies, sur 2 supports, dont 1 hors ligne. Et tester la restauration.

5

Donner le strict nécessaire

Chacun n'accède qu'à ce dont il a besoin : un compte piraté fait moins de dégâts.

6

Préparer le jour J

Savoir qui appeler et quoi faire avant que l'attaque n'arrive.

En cas d'attaque

Isoler

Débrancher le poste du réseau, sans l'éteindre.

>

Alerter

Le référent informatique et votre prestataire.

>

Se faire aider

cybermalveillance.gouv.fr

>

Déclarer

Plainte, CNIL sous 72 h si données personnelles.

Ne pas payer de rançon : rien ne garantit le retour des données.

PARLONS DE VOTRE RÉSEAU

Faites le point sur votre couverture cyber

contact@sayse.fr

sayse.fr