Hacking :
Evolution des menaces

Juin 2022

Les dernières cyberattaques médiatisées en France

Mai 2022 — 14

Avril 2022 — 16

Mars 2022 — 24

Février 2022 — 13

Janvier 2022 — 18

Les dernières cyberattaques médiatisées en France

Décembre 2021 — 22

Novembre 2021 — 20

Octobre 2021 — 22

Septembre 2021 — 15

Août 2021 — 8

Juillet 2021 — 12

WatchGuard

Les dernières cyberattaques médiatisées en France

Juin 2021 — 26

Mai 2021 — 28

Avril 2021 — 39

Mars 2021 — 22

Les dernières cyberattaques médiatisées en France

Février 2021 — 23

Janvier 2021 — 10

Décembre 2020 — 21

Novembre 2020 — 28

Octobre 2020 — 15

Septembre 2020 — 23

Evolution du hacking

1,5 x revenu de la contrefaçon
2,8 x trafic de drogue

Brutalité

Exfiltration des données

Mafias

https://www.ouest-france.fr/societe/cyberattaque/entretien-toutes-les-mafias-du-monde-sont-en-train-de-converger-vers-la-cybercriminalite-7139877

Dr Mike McGuire
Chercheur en criminologie
Université de Surrey

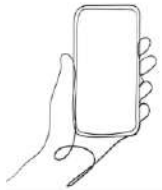
https://www.thalesgroup.com/fr/monde/groupe/press-release/thales-alerte-risques-lies-cybercriminalite-mondiale-travers-sa-nouvelle

1%

du PIB mondial en 2020

https://www.latribune.fr/entreprises-finance/banques-finance/industrie-financiere/cyberattaques-un-groupe-de-travail-du-g20-planche-sur-des-criteres-communs-pour-proteger-les-entreprises-894658.html

Protection des données



Données informatiques

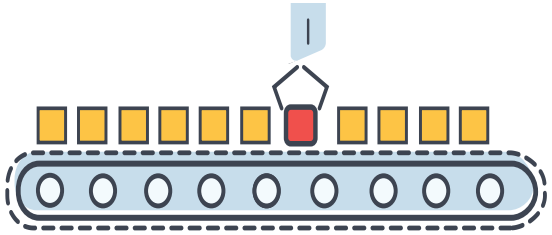
Problèmatique :
La protection des endpoints

Antivirus traditionnel

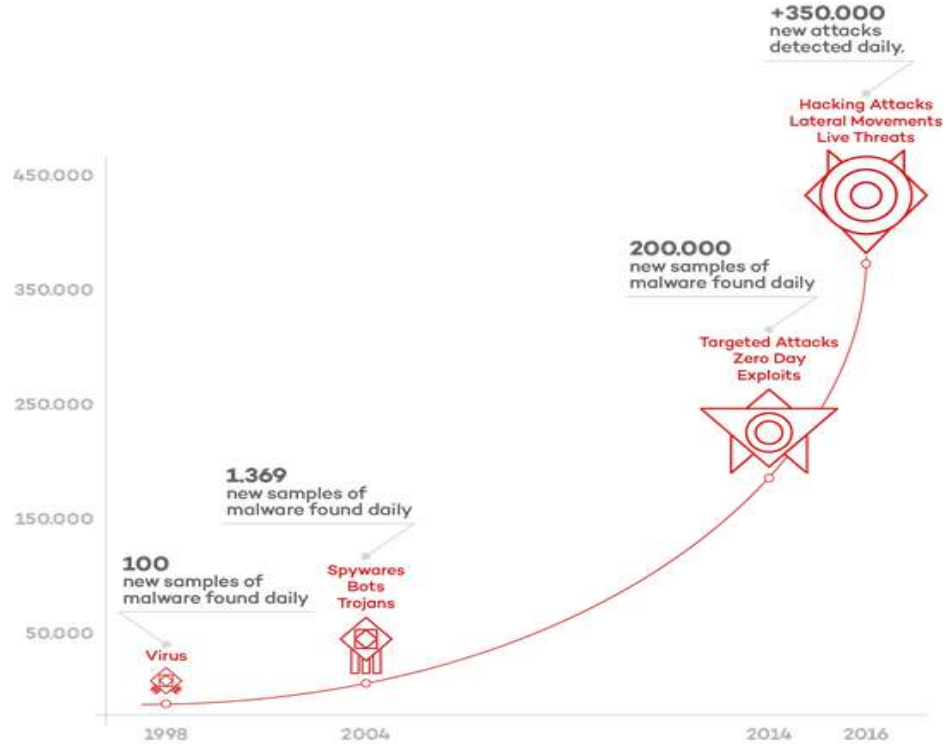
Antivirus traditionnels

- Signatures virales
- Analyse Heuristique
- Réputation web
- Listes de blocages

Pas de contexte
Pas de corrélation



Pré-Execution



https://www.watchguard.com/wgrd-resource-center/infographic/internet-security-insights-q1-2021

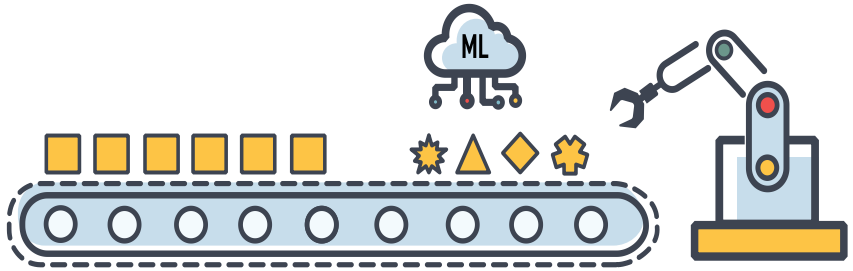
+ Fileless Malwares

Antivirus Next-Generation

Antivirus Next-Generation

- Execution Live ou par Sandbox
- Basé sur du comportemental
  (Machine Learning, Intelligence Artificielle, ou autres technologies)
- Good vs. Bad

Pas de corrélation



Comportement anormal détecté

EDR : EndPoint Detection & Response

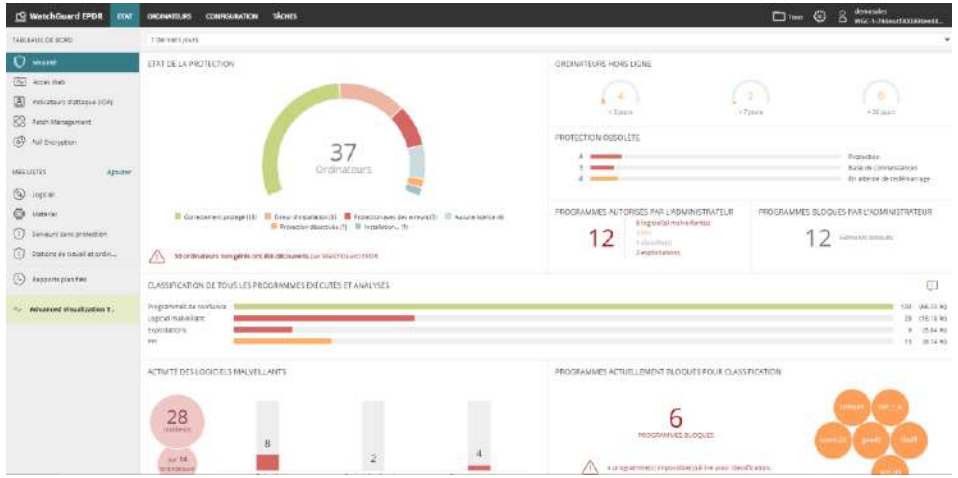
Détection

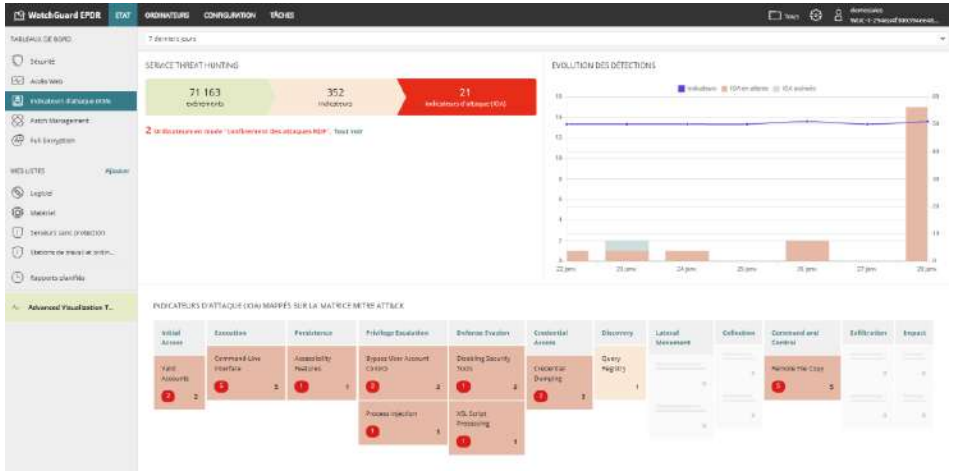
IA + Auto-apprenant
Corrélation d'évènements

Investigation

Visibilité
Chronologie
Compréhension origine d'une attaque

Remédiation





WatchGuard EPDR

Par : Amine SAÏM

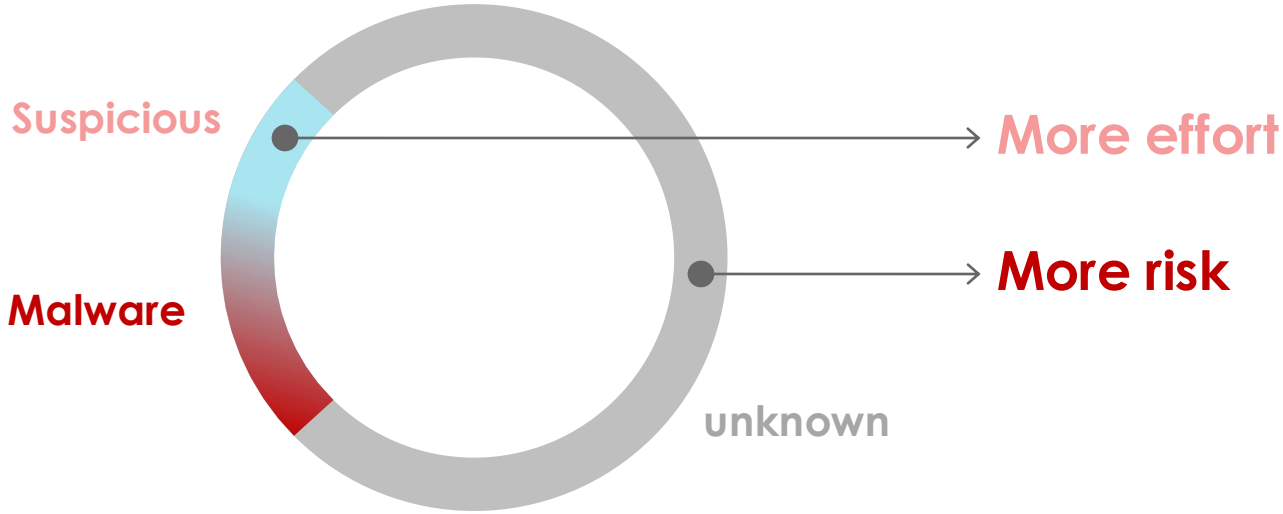
EDR + AV
Managed services-as-features
Single lightweight agent

WINDOWS LINUX MAC OS X ANDROID IOS

The current model…

…is based on the **isolated detection of known malicious processes** which means:

- All suspicious activity must be investigated on a case-by-case basis.
- **Unknown processes are allowed.**
  That's why hackers can work around these systems so easily and their success rate is so high.



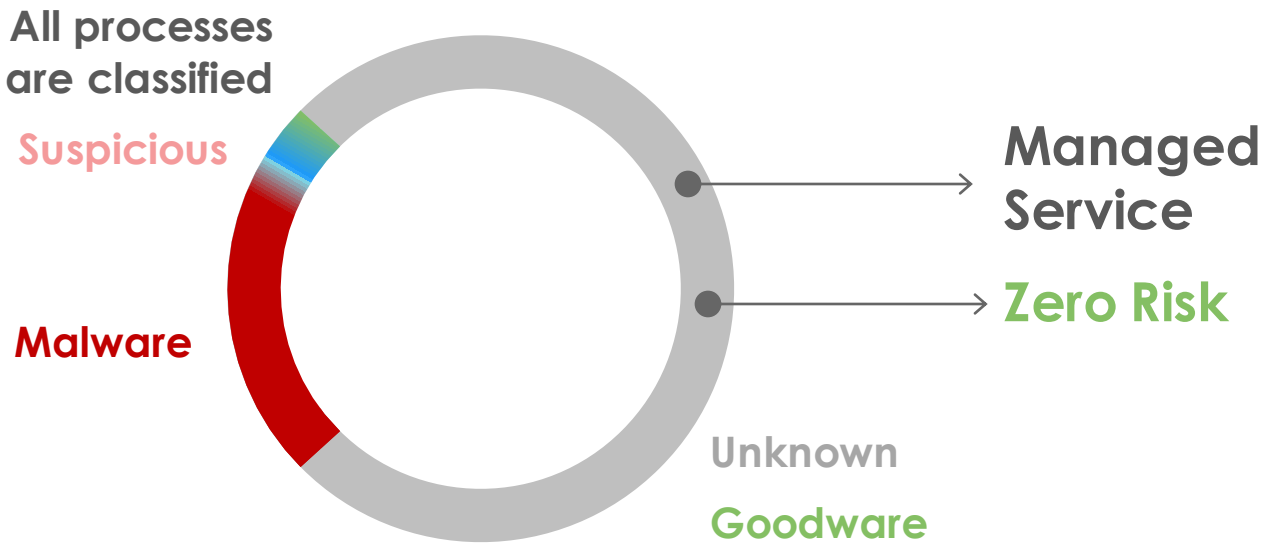
Suspicious items need to be investigated by customers.
Unknowns are allowed to run.

The WatchGuard EPDR approach

Service managed by Real-time visibility and forensic analysis

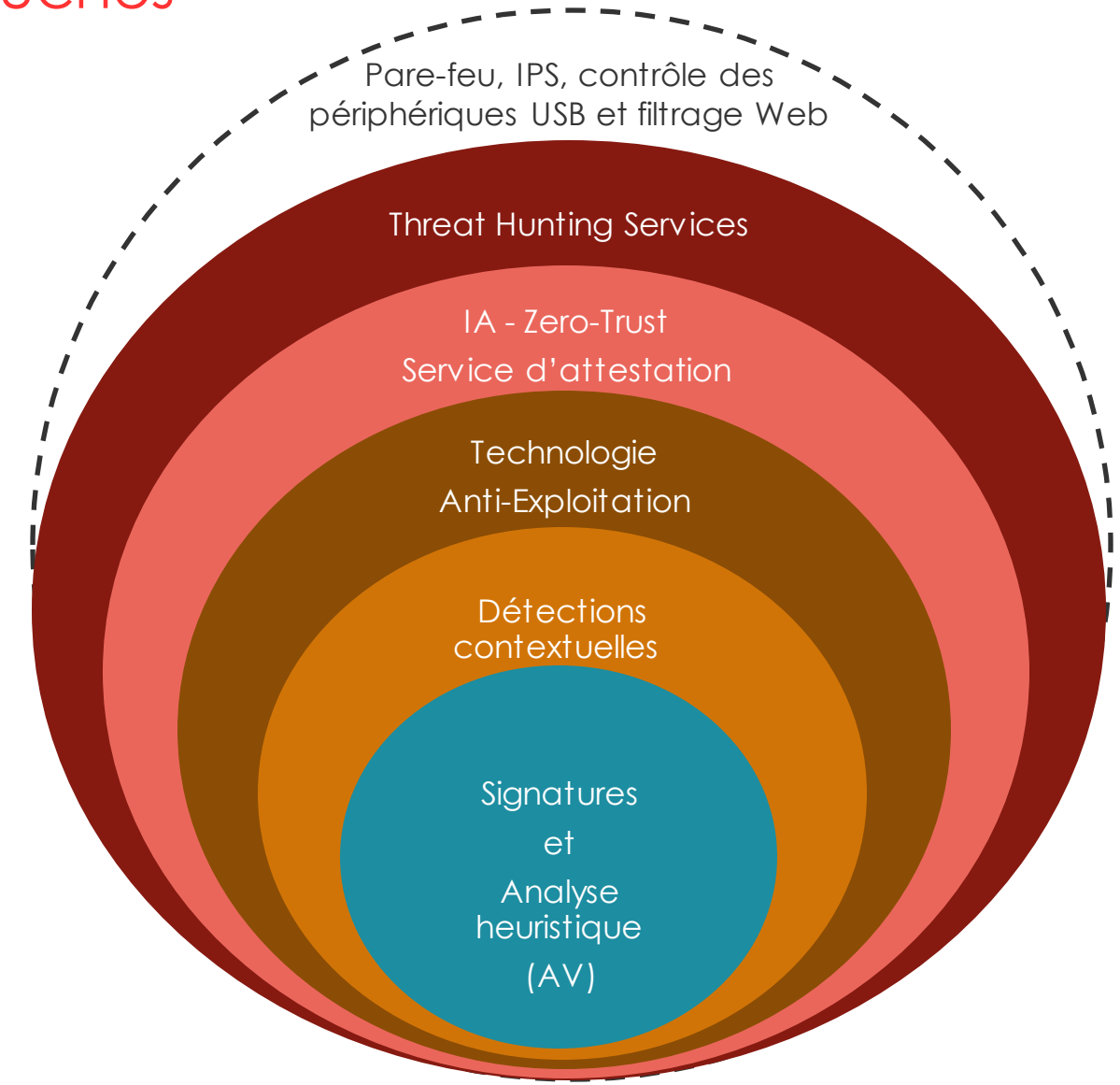
Based on the **classification of all running processes** on your network.

- **Every program's activity is monitored and analyzed in real time.**
- All **behavior is verified by the managed service.**
- The administrator does not have to investigate anything.
- **Maximum level of protection, less effort, and no risk.**



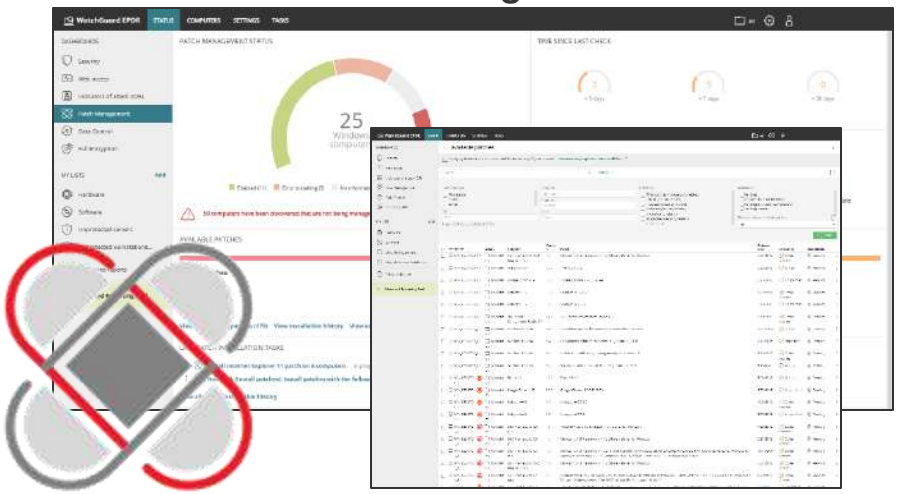
100% Attestation Service

Protection en couches

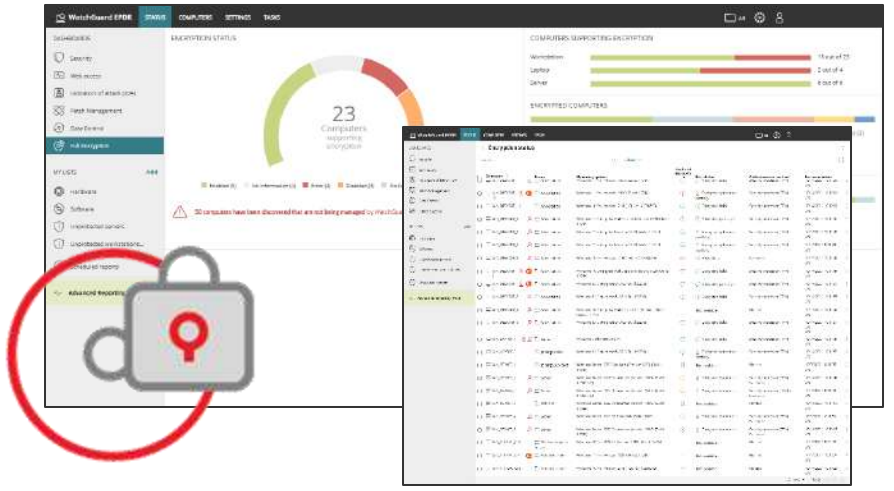


Modules Endpoint

WatchGuard Patch Management

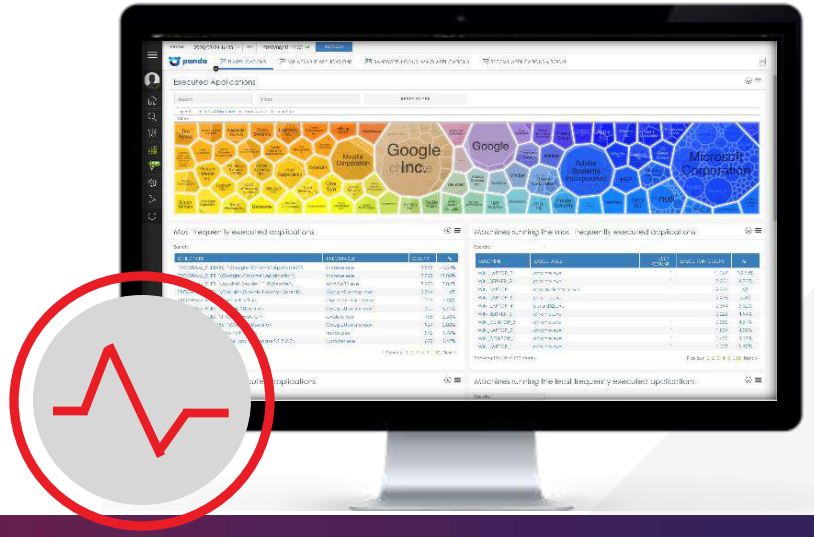


WatchGuard Full Encryption



WatchGuard Data Control

WatchGuard Advanced Reporting Tool



Merci

Notre EDR en synthèse

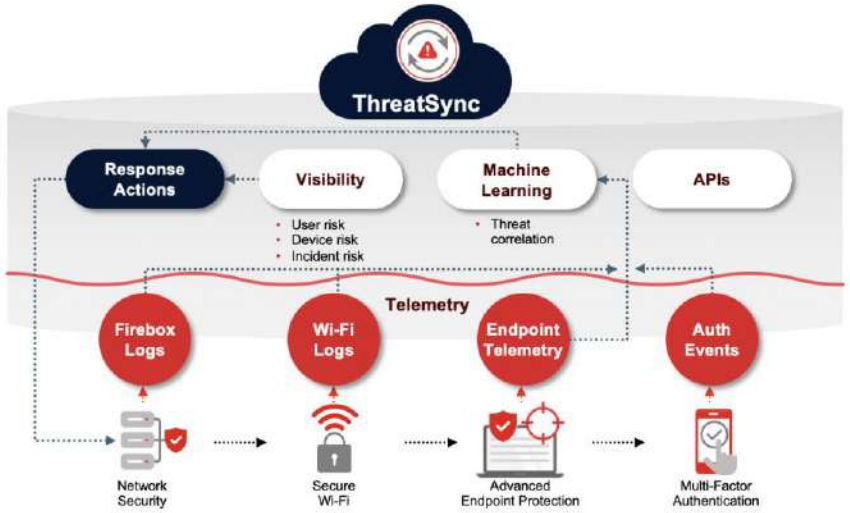
- EDR Zero-Trust
- Threat Hunting inclus de base
- Indicateurs d’Attaques inclus de base
- Reclassification permanente
- Non chronophage

Dans la roadmap :

XDR
WatchGuard

XDR - Corrélation avec ThreatSync™ 2.0

ThreatSync permettra aux équipes de sécurité d'économiser des cycles, d'accélérer la détection et d'augmenter leur précision en corrélant automatiquement les données pertinentes sur les menaces provenant de l'ensemble de la Unified Security Platform de WatchGuard.



ThreatSync :

- Plateforme intégrée proposant une solution de détection et de réponse étendues (XDR) pour tous les environnements, les utilisateurs et les appareils
- Collecte, met en corrélation, analyse et répond aux menaces sur l'ensemble des couches de sécurité
- Établit un score de menace facile à comprendre pour les indicateurs et les incidents
- Fournit une image détaillée, contextualisée et exploitable de votre surface de menace

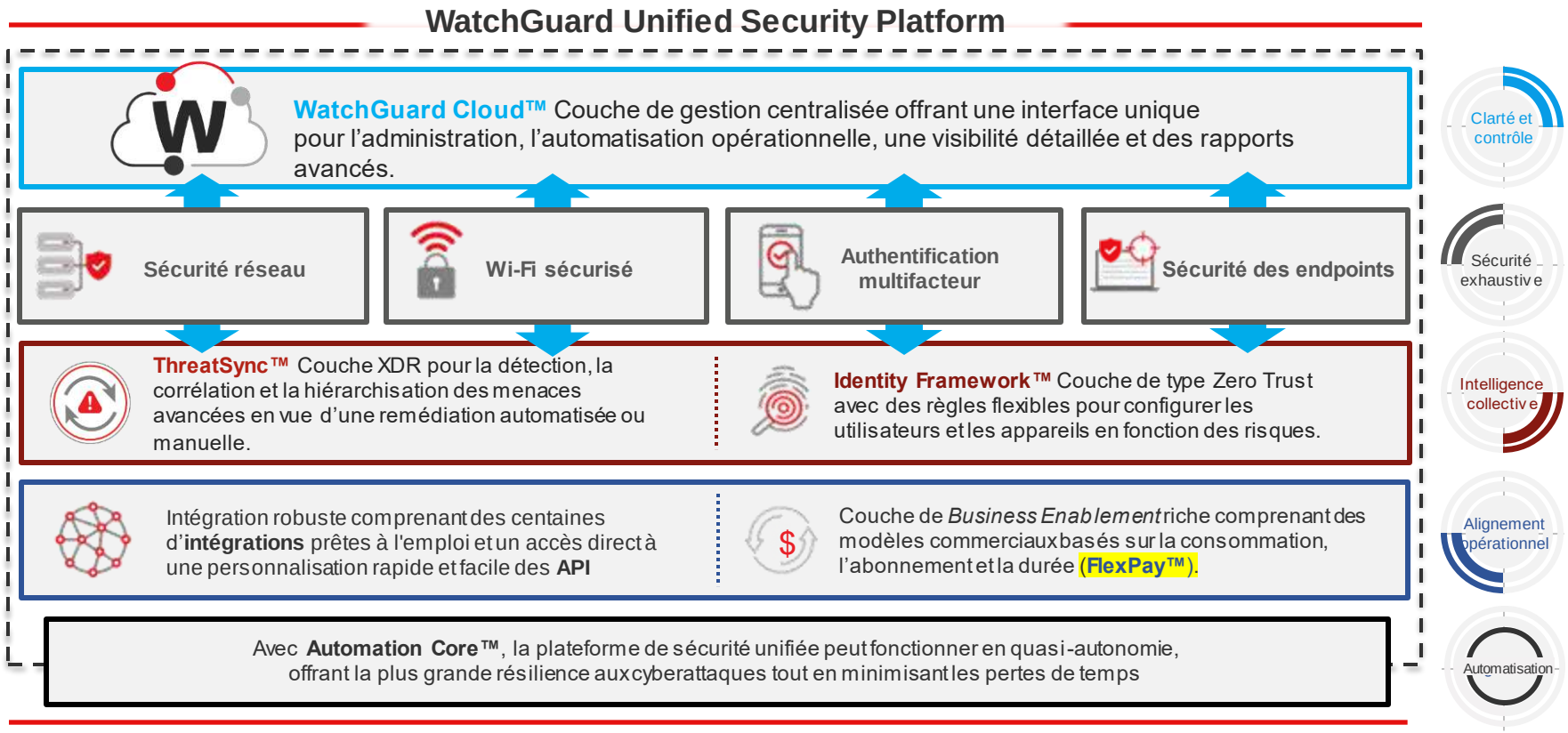
Des centaines de milliards d'évènements analysés

2,1 milliards de binaires classés

Des millions de mouvements adverses suivis

Des milliers de malwares de type Zero Day bloqués

Une sécurité avancée et centrée sur l'utilisateur



WatchGuard Unified Security Platform

Une plateforme évolutive pour des prestations de services de sécurité encore plus efficaces

APPROCHE GLOBALE DE LA SÉCURITÉ

Portefeuille complet de produits et de services en matière de sécurité réseau, d'authentification multifacteur et de sécurité des endpoints pour la protection des environnements, des utilisateurs et des appareils.

CLARTÉ ET CONTRÔLE

Administration centralisée de la sécurité, visibilité et rapports avancés via WatchGuard Cloud™.

ALIGNEMENT OPÉRATIONNEL

Opérations simplifiées grâce à un accès direct aux API, vaste écosystème d'intégrations prêtes à l'emploi et prise en charge de tous les modèles de paiement et de consommation via FlexPay™.

INTELLIGENCE COLLECTIVE

Plateforme entièrement intégrée permettant d'adopter une posture de sécurité de type Zero Trust via WatchGuard Identity Framework™ et de déployer une véritable approche XDR pour détecter et remédier aux menaces via ThreatSync®.

AUTOMATISATION

WatchGuard Automation Core™ pour une automatisation de l'activité et de la sécurité intégrée à chaque couche de la plateforme, simplifiant ce faisant tous les aspects de la gestion de la sécurité.

Questions?