Chapitre 18
EDR (EndPoint Security)

1. Introduction

Pourquoi ?

Ce chapitre traite de la gamme EndPoint Security, qui englobe les solutions pour les endpoints. Entre 2017 et 2020, les cyberattaques ont connu une évolution rapide, incitant WatchGuard à acquérir Panda Security et son produit exceptionnel **Panda Adaptive Defense 360 (AD360)**. L'objectif était de proposer une solution **EDR** (*Endpoint Detection and Response*) de dernière génération pour contrer tout type de menaces, y compris les plus avancées telles que les LoTL, LOLBins ou LOLBAS (*Living Off The Land Binaries and Scripts and Also Libraries*), les failles zero day ou encore les APT (*Advanced Persistent Threat*).

AD360 a été intégré au catalogue commercial de WatchGuard, sous plusieurs formes :

- **WatchGuard EPP (*Endpoint Protection Platform*)** comme simple antivirus (EPP).
- **WatchGuard EDR Core (*Endpoint Detection and Response Core*)** comme complément à un EPP proposant une version légère de l'approche par EDR.
- **WatchGuard EDR (*Endpoint Detection and Response*)** comme complément à un EPP proposant une version complète de l'approche par EDR.
- **WatchGuard EPDR (*Endpoint Protection, Detection and Response*)** comme solution EPP + EDR complète.
- **WatchGuard EPDR Advanced** comme solution EPP + EDR complète avec des outils pour l'intégration à un SOC.

L'EDR et l'EPDR peuvent se voir ajouter cinq modules supplémentaires :

– Le module **Patch Management (PM)** pour la mise à jour automatique des OS et applications.
– Le module **Data Control (DC)** pour la cartographie des données sensibles PII et autres.
– Le module **Full Encryption (FE)** pour le chiffrement des disques durs (HDD/SSD).
– Le module **Siemfeeder** pour envoyer les données collectées avec les agents vers le SIEM de l'entreprise.
– Le module **Advanced Reporting Tool (ART)**, qui est un SIEM orienté endpoints.

Remarque

***EPP** peut se voir ajouter seulement les modules **Patch Management (PM)** et **Full Encryption (FE)**.*

***EDR Core** ne peut pas se voir ajouter les modules.*

***EDR Core** est disponible lorsque l'on achète un UTM Firebox avec un abonnement **TSS**.*

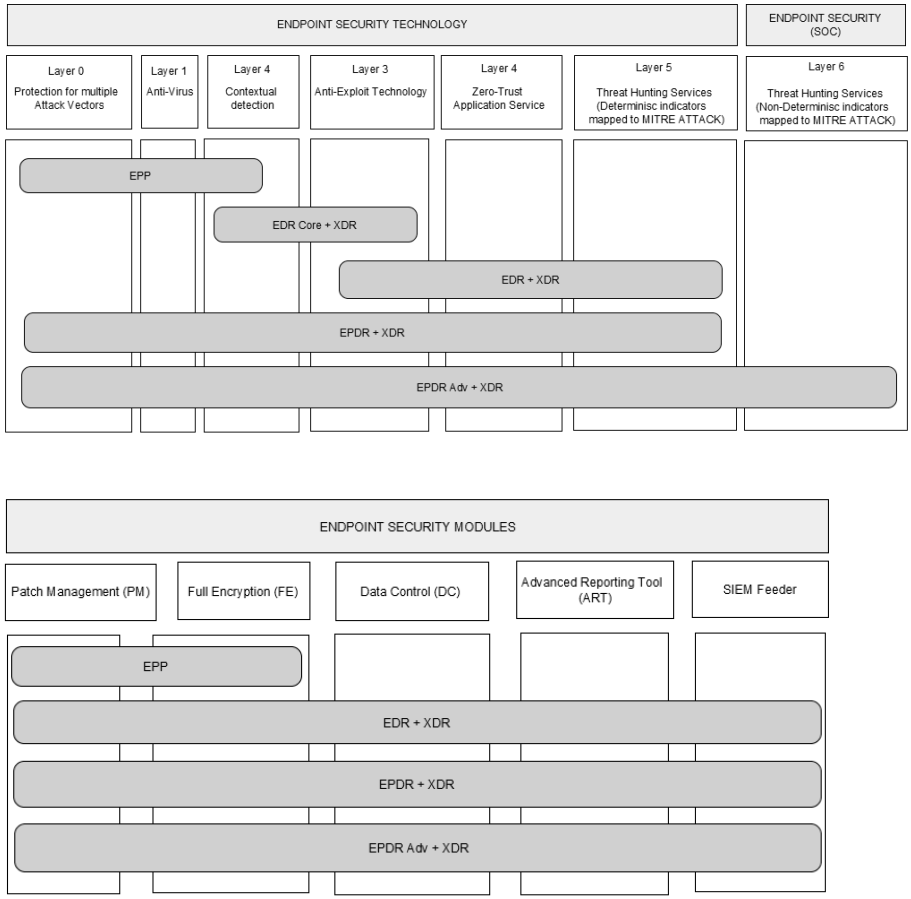
*Toutes les solutions **excepté EPP** peuvent être utilisées pour faire du **XDR**.*

***EPP**, **EPDR** et **EPDR Advanced** disposent nativement de l'option **Protection for Multiple Attack Vectors** qui contient **Personal Firewall + IDS/HIPS + Network Attack protection + Device Control + URL Filtering**.*

Informations

Nous vous recommandons d'utiliser au minimum **WatchGuard EPDR**, car c'est la seule solution qui propose une protection intégrale. **WatchGuard EPP**, **WatchGuard EDR Core** et **WatchGuard EDR** sont bien trop limités et donnent un faux sentiment de protection.

Panda Adaptive Defense 360 (AD360) ou **WatchGuard EPDR** sont globalement très simples d'utilisation pour une très bonne efficacité. En revanche, l'utilisation de plusieurs noms pour parler d'un même produit avec des options limitées provoque un sentiment de confusion pour les clients. WatchGuard, normalement, n'a pas besoin de ces artifices commerciaux grossiers pour se démarquer, et il est important que cette pratique ne devienne pas une mauvaise habitude.



Logigramme endpoints

2. Technologie EPP vs EDR

Les outils de protection pour les endpoints sont divisés en deux familles. Actuellement, l'une s'appelle EPP, l'autre EDR. L'EPP est conçu pour la prévention et le blocage des menaces connues en temps réel, tandis que l'EDR est orienté sur la détection et la réponse aux menaces avancées. On parle de menaces inconnues qui échappent à la détection des solutions de sécurité traditionnelles.

WatchGuard utilise plusieurs niveaux de protection ainsi qu'un ensemble de modules dans ses produits :

- **Layer 0 Protection for Multiple Attack Vectors** (Firewall + IDS/HIPS + NET Protection + Web & USB control).
- **Layer 1 Signature Files and Heuristic Scanners (AV)** (détection des attaques connues).
- **Layer 2 Contextual Detections + Collective Intelligence** (détection des attaques LOLBAS sans fichiers).
- **Layer 3 Anti-Exploit Technology** (détection des attaques LOLBAS orientées exploitation de vulnérabilités).
- **Layer 4 Zero-Trust Application Services** (classement de 100 % des processus identifiables + blocage automatique des processus non identifiables).
- **Layer 5 Threat Hunting Services** (détection déterministe de l'IOA mappé sur la matrice MITRE).
- **Layer 6 Threat Hunting Services++** (détection non déterministe de l'IOA avec télémétrie contextuelle, recherche de règles STIX IOC et YARA en temps réel, shell à distance et stratégie avancée).

2.1 WatchGuard EPP

EPP (*Endpoint Protection Platform*) est le nouveau nom donné par les observateurs de marché (Gartner, Forrester, etc.) pour désigner les antivirus classiques. Bien qu'avec un fonctionnement traditionnel, WatchGuard EPP, expliqué ci-dessous, est boosté par l'approche multicouche suivante :

- **Layer 0 Protection for Multiple Attack Vectors** propose de base un firewall personnel intégrant IDS (*Intrusion Detection System*) + HIPS (*Host-based Intrusion Prevention System*), le contrôle des équipements USB et un filtrage web. Cette couche est importante pour bloquer les menaces internes. Une des menaces internes les plus préoccupantes sont les HOTPLUG ATTACKS (clé USB avec Payload malveillante). Par exemple, le site Hak5 propose pour 100 € des clés USB appelées BASH BUNNY qui peuvent être utilisées pour des attaques sur port USB très faciles à réaliser. Souvent (mais pas toujours), les hackeurs déposent des clés USB infectées sur les parkings devant l'entreprise afin que les employés les ramassent puis les branchent sur leurs PC. Une fois la clé USB connectée, celle-ci peut tenter une exfiltration des mots de passe, l'installation de malwares ou même la configuration de tunnel avec un serveur Internet propriété du hackeur. Cela afin qu'il puisse à son tour l'emprunter pour pénétrer le système depuis l'extérieur, etc.

– **Layer 1 Signature Files and Heuristic Scanners (AV)**. Les antivirus traditionnels détectent les menaces en les comparant à leurs bases de signatures virales ou heuristiques (comportementales). Concrètement, ils protègent des malwares, ransomwares et exploits à hauteur de leurs connaissances et ne sont pas performants contre les nouvelles menaces qu'ils ne connaissent pas. WatchGuard EPP peut donc détecter et neutraliser la plupart des menaces présentes dans sa base de signature et partiellement les nouvelles menaces par analyse heuristiques. Lorsqu'il détecte une infection, l'EPP est en mesure de répondre par des actions de remédiation comme le retour arrière avant l'attaque (rollback), la mise en quarantaine (*centralized quarantine*) ou encore l'analyse et la désinfection automatique.
– **Layer 2 Contextual Detections + Collective Intelligence** permet de détecter et bloquer les attaques de type LOLBAS. LOLBAS fait référence à la pratique des attaquants qui utilisent des binaires, des scripts et des bibliothèques légitimes déjà présents sur un système cible pour mener des activités malveillantes. Ces outils sont des logiciels de confiance et couramment utilisés, qui ne sont pas malveillants en eux-mêmes, mais qui peuvent être détournés par des attaquants pour éviter la détection par les solutions de sécurité traditionnelles. En utilisant LOLBAS, les attaquants peuvent exploiter des outils et des fonctionnalités existants pour exécuter du code malveillant, effectuer un déplacement latéral, obtenir une persistance et atteindre leurs objectifs sans introduire de fichiers suspects qui pourraient éveiller les soupçons.

Remarque

EPP ne dispose pas des fonctions EDR, ne permet pas de faire du XDR, contrairement à tous les autres produits de la gamme EndPoint Security, ne protège pas contre les ATP et dispose seulement des modules Patch Management (PM) et Full Encryption (FE).

2.2 WatchGuard EDR Core

WatchGuard EDR Core est le produit qui remplace TDR et qui correspond à la couche d'un EPP déjà en place sur le endpoint. L'approche pour protéger les endpoints est totalement différente des EPP. Tandis que les EPP se concentrent sur leurs connaissances pour trouver les menaces, les EDR se concentrent sur ce qu'ils ne connaissent pas.

EDR Core est proposé avec les licences TSS (*Total Security Suite*) nécessaires au bon fonctionnement des UTM Firebox. Donc si vous avez déjà un EPP et que vous avez acheté un UTM Firebox avec TSS, il est dommage de ne pas l'utiliser pour renforcer la protection du SI. Par contre, il est recommandé de mettre en place une stratégie de remplacement de votre EPP par WatchGuard EPDR, qui protège intégralement le endpoint.

Concrètement, EDR Core est une version limitée d'EDR. Celle-ci est limitée aux couches 2 et 3 :

– **Layer 2 Contextual Detections + Collective Intelligence** (voir WatchGuard EPP).
– **Layer 3 Anti-Exploit Technology** permet de détecter et bloquer les exploits. « Exploit » est un terme couramment utilisé en cybersécurité pour désigner un code, un script ou une technique qui profite d'une vulnérabilité spécifique dans un logiciel, un système d'exploitation ou une application pour exécuter une action malveillante ou obtenir un accès non autorisé à un système ou à des données. Lorsqu'une vulnérabilité est découverte, les développeurs travaillent généralement rapidement pour publier des correctifs (mises à jour) afin de combler cette vulnérabilité et empêcher son exploitation. Pour se protéger contre les exploits, il est essentiel de maintenir à jour les logiciels et les systèmes avec les derniers correctifs. Il faut aussi fermer ou protéger les ports correctement avec des pare-feu.

La technologie anti-exploit de WatchGuard tente le blocage d'exploits (comme la tentative d'injection de code...) à deux moments distincts :

– pendant le déroulement de l'exploit (sans terminer les processus) ;
– après le déroulement de l'exploit (avec terminaison de processus et reboot).

Comme EDR Core est un EDR, il profite de la technologie XDR (ThreatSync 2.0), ce qui lui permet de participer à la corrélation d'informations entre les différents équipements (endpoint, UTM, etc.) pour une meilleure couverture de la détection et des réponses aux menaces. Il a presque les mêmes actions de réponses que TDR (logique avec XDR ThreatSync en version 2.0) :

– quarantine
– kill
– isolate

Remarque

EDR Core ne permet pas la désinfection du endpoint et dispose du VPN Enforcement pour les accès VPN sur les endpoints renforcé par agent EDR. EDR Core ne dispose pas de Layer 0 Protection for Multiple Attack Vectors et ne dispose pas non plus de Layer 4 Services Zero-Trust Application Services (excepté le mode Audit). EDR Core ne dispose pas de Layer 5 Threat Hunting Services ni de Layer 6 Threat Hunting Services++.

2.3 WatchGuard EDR

Comme WatchGuard EDR Core, WatchGuard EDR fonctionne comme complément d'un EPP. Il ne dispose pas des couches 0 et 1 mais dispose des couches 2 et3 vues précédemment plus les couches de protection 4 et 5.

La bonne pratique consiste à réaliser une phase d'apprentissage de l'environnement sur quelques semaines (**mode HARDENING**), suivie d'une phase de verrouillage (**mode LOCK**). En mode LOCK, aucune menace, même avancée, ne peut être lancée, car rien ne peut se lancer en dehors des services et applications apprises par l'EDR pendant la phase d'apprentissage. Le principe de base de l'EDR est donc de faire du monitoring temps réel pour déterminer les exécutables de confiance (*goodware*) et ceux qui ne sont pas de confiance (*malware*). On parle alors de **processus de classification automatique**. Voici les principaux éléments monitorés :

– les processus ;
– les connexions ;
– le registre ;
– l'OS ;
– les accès aux données (fichiers/dossiers).

La première étape pour l'identification d'un exécutable consiste à utiliser les **technologies locales préventives** :

– les signatures ;
– l'analyse heuristique comportementale (*behavioural heuristics*) ;
– les indicateurs d'attaques connues ou IOA (*Known Indicator of Attacks*) ;
– le cache local.

Si ces méthodes ne parviennent pas à identifier l'exécutable, entre en scène le service **Layer 4 Zero-Trust Application Services** (aussi appelé **100 % Attestation Service**).

Celui-ci commence par rechercher des informations dans la base de données mondiale de Panda/WatchGuard, appelée **Cloud-Based Collective Intelligence**. Cette base de données est alimentée par des millions de clients de toutes tailles et contient tous les goodwares et malwares connus à ce jour. Après analyse par le service, seules trois réponses sont possibles :

– **Goodware** : l'exécutable est autorisé.
– **Malware** : l'exécutable est bloqué.
– **Unknown** : l'exécutable est bloqué puis celui-ci est téléchargé dans les serveurs WatchGuard en Cloud avec ses métadonnées pour inspection.

Dans le cloud, les fichiers exécutables « Unknown » sont soumis à une inspection approfondie par sandbox physique et traitement par algorithme automatique de type machine learning. La plateforme traite 2,5 milliards d'événements quotidiennement et utilise l'IA de type machine learning pour classer plus de 5 millions d'applications. Cette méthode permet de classer automatiquement généralement 99,98 % des fichiers.

Si nécessaire, une analyse manuelle pour classification par des Security Analysts est réalisée pour déterminer la véritable nature du fichier. Même classés comme goodwares, les exécutables sont toujours surveillés et réévalués à chaque exécution.

Un autre point important est le service qui, en parallèle, permet d'identifier les patterns d'attaques sur les postes clients et les serveurs. C'est le service que l'on appelle **Layer 5 Threat Hunting Services** (aussi appelé **Threat Hunting & Investigation Services**).

Ce service repose sur **Zero-Trust Application Services**, les équipes de Panda et WatchGuard utilisent des outils spécifiques pour détecter les attaques très sophistiquées en cours de réalisation et ainsi développer de nouveaux patterns de détection.

Pour cela, le flux d'événements des postes de travail est vérifié en temps réel par les agents EDR. Chaque anomalie est comparée à des baselines de profils comportementaux du réseau et des ordinateurs. Les IOA sont mappés sur la matrice MITRE pour une meilleure visibilité du comportement des hackeurs ainsi que des conseils de protection.

Threat Hunting Services peut aussi faire des nouvelles hypothèses d'IOA, si le pattern découvert est une anomalie intéressante. Dans ce cas, une vérification a lieu sur le pattern considérant une hypothétique attaque qui n'est pas encore identifiée comme une véritable attaque. Si l'hypothèse est confirmée, alors un nouvel indicateur d'attaque est référencé dans les IOA. Puis le client est informé de l'attaque par l'envoi d'un rapport qui inclut des recommandations pour limiter la surface d'attaque.

Bien sûr, d'autres équipes de chercheurs continuent de produire des hypothèses sur le pattern et valident des IOA. Pour les tester, ils utilisent la chronologie des événements et comparent leurs résultats. Puis les analyses filtrent les faux positifs des vraies attaques. Pour terminer, le service cherche à améliorer l'agent sur le endpoint, pour qu'il puisse dorénavant détecter et bloquer l'attaque localement.

Les acronymes **IOA** et **IOC** étant couramment utilisés pour désigner les concepts liés à la détection et à l'analyse d'attaques en cybersécurité, nous allons brièvement expliquer ces termes :

– **IOA (*Indicators of Attack*)** permet un travail **proactif**.
– **IOC (*Indicators of Compromise*)** permet un travail **réactif**.