FICHE SOLUTION

FortiXDR : détection, investigation et réponse automatisées aux menaces

Synthèse

Pendant des années, les entreprises ont déployé des produits de cybersécurité, les uns après les autres, pour répondre aux menaces web. Bien qu'efficaces dans de nombreux cas, ces produits sont devenus, compte tenu de leur multiplicité, difficiles à gérer par des équipes de sécurité déjà fortement mobilisées. Pour les entreprises, le risque est de passer à côté de cyberattaques furtives et à fort potentiel de dommages, d'autant qu'elles peinent à gérer efficacement des alertes de sécurité toujours plus nombreuses. La majorité des entreprises actuelles ont pour ambition de consolider leur parc d'outils de sécurité, dans l'optique d'améliorer la sécurité et la productivité opérationnelle. Cependant, pour tenir cet objectif, la consolidation doit aboutir à une solution de sécurité intégrée et efficace, et non à une collection de produits indépendants proposés par un seul fournisseur. C'est précisément cette approche qu'offre FortiXDR qui capitalise sur la Security Fabric large, intégrée et automatisée de Fortinet et sur ses fonctions de détection, d'investigation et de réponse intégrées face aux menaces. C'est à ce titre que les entreprises pourront renforcer leur posture de sécurité et leur productivité opérationnelle, et ainsi relâcher la pression sur les équipes de sécurité.

Une consolidation qui tire parti de XDR (eXtended Detection and Response)

Selon Gartner, 80 % des entreprises ont déjà initié la consolidation de leur parc d'outils de sécurité, ou envisagent de le faire dans les 2 à 3 années à venir.[1] Plutôt que de consolider en simplifiant leurs achats (en investissant dans une suite ou des licences d'entreprise), les entreprises préfèrent consolider autour d'une architecture de sécurité de type XDR. FortiXDR convertit votre Fortinet Security Fabric en une solution XDR. Les nombreuses fonctions de sécurité de Fortinet qui se déploient sur l'ensemble de votre organisation intègrent leurs informations au sein d'un référentiel centralisé. Un traitement analytique est ensuite appliqué pour détecter tout incident à haut risque et initier les opérations d'investigation/classification. Enfin, des actions de prise en charge de ces incidents peuvent être prédéfinies à des fins de remédiation et de réponse. Ce processus peut être totalement automatisé pour détecter et maîtriser des attaques qui ont su passer entre les mailles du filet, compte tenu d'alertes trop nombreuses, et pour relâcher la pression sur les équipes de sécurité.

Des fonctions de sécurité élargies

La Security Fabric de Fortinet protège la totalité de l'entreprise numérique, et notamment :

- Les endpoints et utilisateurs, grâce à une plateforme de protection des endpoints (EPP) et à la gestion des identités et des accès (IAM)
- Le réseau et sa couche d'accès via à des commutateurs filaires, des points d'accès sans fil et des pare-feux d'entreprise
- Le cloud, l'aide d'une solution CASB (cloud access security broker), d'un pare-feu d'application web (WAF) et d'une passerelle de sécurité email.

Tous ces produits sont intégrés entre eux et envoient leurs indicateurs vers une plateforme de traitement analytique centralisée.

Analyses de détection

Nos fonctions avancées de traitement analytique, conçues par les experts des FortiGuard Labs, identifient les indicateurs précoces de cyberattaques potentielles. Elles sont appliquées aux indicateurs centralisés, pour les normaliser et les corréler.

Des investigations basées sur l'Intelligence Artificielle (IA)

Selon le type de menace potentielle détectée, un processus automatisé d'investigation est mis en œuvre par un moteur de décision basé sur l'IA, répliquant les actions expertes d'un vrai analyste en sécurité. Ce moteur décisionnel fait appel à différents micro-services qui enrichissent et affinent les analyses. Parmi ces services, la veille sur les menaces de FortiGuard Labs ou provenant de tiers, des analyses de fichiers sur la base de règles statiques Yara, des analyses en sandbox, des services de réputation ou l'étude des comportements utilisateur. De telles fonctions permettent d'établir la classification finale de la menace potentielle.

Une prise en charge prédéfinie

Les entreprises ont le choix de définir leurs règles en amont pour exécuter des tâches sur la base de la classification de la menace, de groupes d'utilisateur, d'exposition aux risques et d'autres critères. Ceci accélère les tâches de remédiation et de réponse aux menaces.

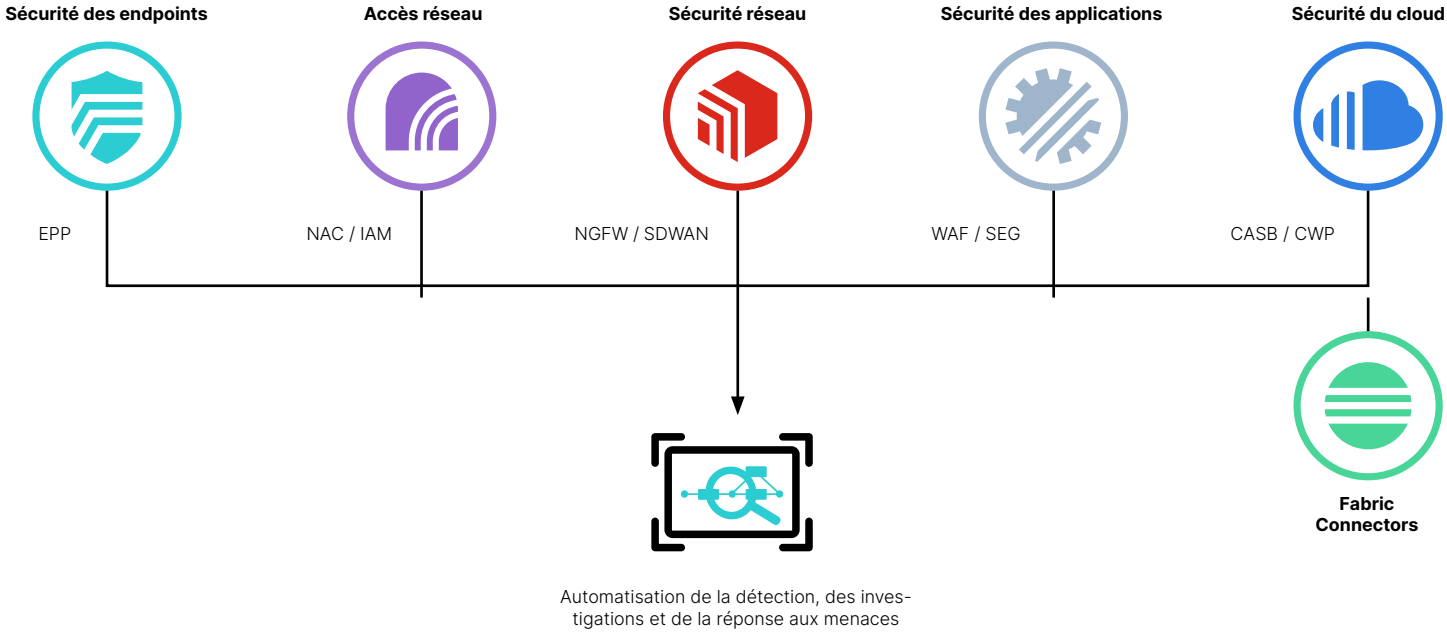

Schéma 1 : FortiXDR et Fortinet Security Fabric

La différence FortiXDR

La technologie XDR, un sujet particulièrement d'actualité, s'inscrit parfaitement dans la vision de notre Security Fabric, et lui confère nombre d'avantages naturels : large périmètre de couverture, efficacité des composants individuels, davantage d'automatisation, etc. Les entreprises sont ainsi mieux positionnées pour concrétiser les avantages de la consolidation de leur parc d'outils de sécurité.

Un périmètre de couverture élargi

Une solution XDR qui s'étend permet de recueillir davantage d'informations à des fins d'analyse, d'enrichissement et de classification. Les fonctions de sécurité qui s'appliquent au réseau et aux endpoints doivent ainsi prendre en charge l'accès au réseau, l'email, les applications web et le cloud. C'est précisément ce que propose FortiXDR. Si cette solution analyse les étapes intermédiaires d'une chaîne d'attaque (fourniture du malware, exploit, installation et communication), elle porte également sur les étapes en amont et en aval, couvrant ainsi l'ensemble de la chaîne d'attaque. Notons également que la visibilité que proposent les technologies de leurre facilite la détection des phases de reconnaissance des attaques, et qu'elle est complétée par un monitoring en aval des données, basée sur une analyse comportementale UEBA (user and entity behavior analytics).

En moyenne, FortiXDR traite 100 alertes de valeur pour en faire 10 alertes fiables de détection d'incident à des fins d'investigation et de réponse.

Efficacité des composants

Le déploiement de fonctions de sécurité et XDR par Fortinet dans une optique de consolidation ne résulte pas en un environnement de produits d'entrée de gamme. Tous les produits de sécurité Fortinet qui alimentent FortiXDR affichent des scores de premier rang lors de tests indépendants menés par AV-Comparatives, ICSA Labs, NSS Labs, Virus Bulletin et autres. Sur le terrain, les solutions de sécurité Fortinet sont celles qui ont reçu le plus de certifications dans le secteur.

Degré d'automatisation

Il est certes essentiel de détecter des menaces furtives et capables de lourdement peser sur les entreprises qui en sont victimes. Cependant, des alertes trop nombreuses ne font que surcharger les équipes de sécurité. Certains éditeurs ont opté pour une approche qui corrèle les informations de sécurité pour les restituer de manière pertinente et graphique. Chez Fortinet, cette approche est actée et nous allons au-delà : FortiXDR permet, certes, une automatisation complète de la normalisation/corrélation des données et facilite les investigations post-incident et le processus de remédiation. Ceci allège la tâche pour les équipes de sécurité tout en renforçant la posture de cybersécurité.

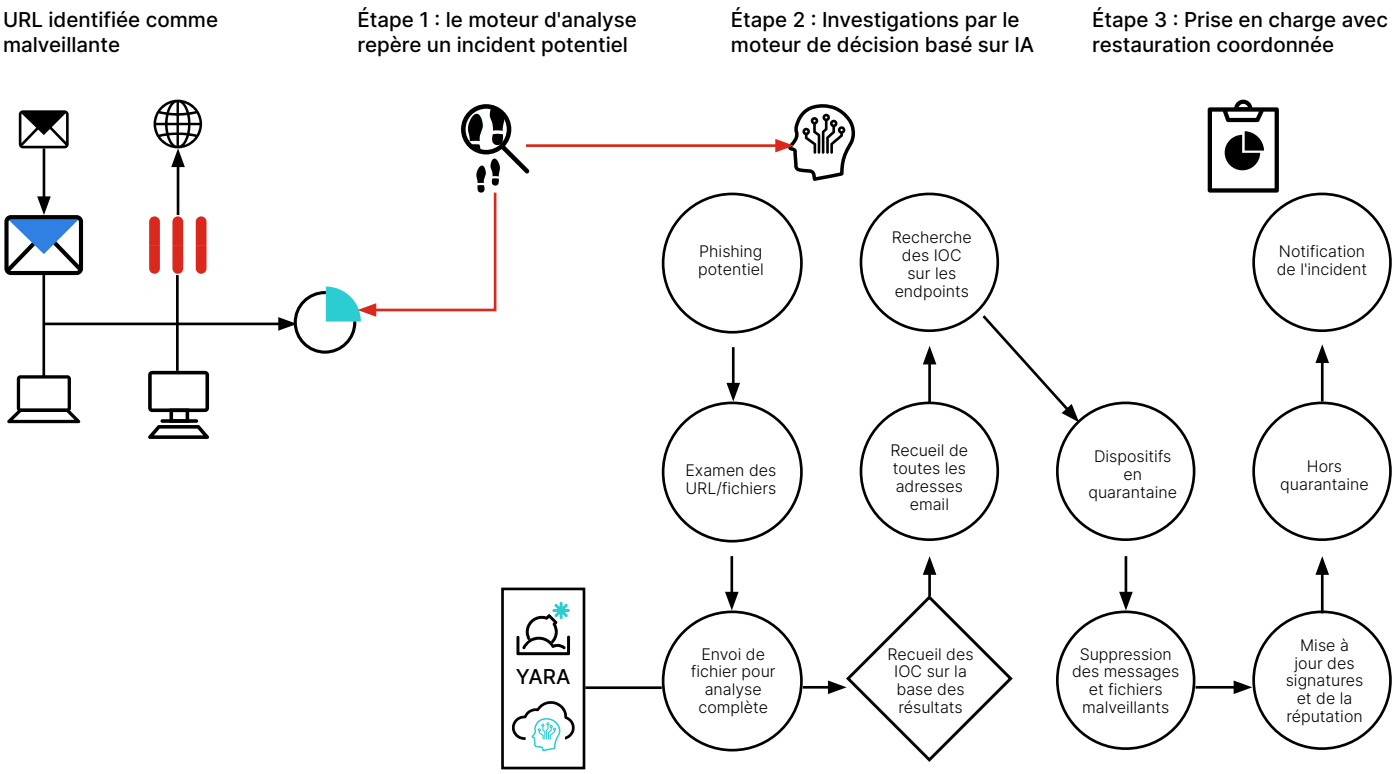

Schéma 2 : détection du phishing, investigations et réponse.

Améliorer la posture de sécurité et la productivité opérationnelle avec FortiXDR

Face au volume, à la sophistication et au dynamisme de l'univers actuel des menaces, les équipes de sécurité sont plus impactées que jamais, à l'heure de la pénurie de compétences en cybersécurité. Face à une multiplicité de produits de sécurité à gérer, à un volume important d'informations à analyser et aux incidents à traiter, une nouvelle approche à la sécurité d'entreprise s'impose. C'est la raison pour laquelle nombre d'entreprises souhaitent consolider leur parc d'outils de sécurité et lorgnent sur de nouvelles solutions prometteuses comme XDR. FortiXDR adopte une approche unique pour automatiser entièrement le processus de détection, d'investigation et de réponse. Ceci améliore la probabilité d'identifier les cyberattaques en cours, avant tout piratage de données ou infection par ransomware. D'autre part, la solution facilite la tâche des équipes de sécurité et leur permet de se repositionner sur des initiatives plus stratégiques.

[1] John Watts et Peter Firstbrook, "Security Vendor Consolidation Trends: Should You Pursue a Consolidation Strategy ?" Gartner, 30 juillet 2020.

FORTINET

www.fortinet.com/fr

juillet 1, 2021 1:53 PM
sb-FA-fully-automate-threat-detection-investigation-and-response-w-FortiXDR-A4_FR_imp
859551-A-1-FR