CROWDSTRIKE

eBook

5 FONCTIONNALITÉS CRITIQUES DE LA SÉCURITÉ MODERNE DES ENDPOINTS

Pourquoi une visibilité totale contribue à une meilleure protection

Tout ce que vous ne voyez pas sur les endpoints *est* une menace

Chaque jour, les entreprises migrent de nouvelles applications, infrastructures et données vers le cloud. Et le nombre d'endpoints qui y accèdent explose. Un endpoint est un terminal qui peut être connecté à un réseau constitué d'ordinateurs de bureau, d'ordinateurs portables, de téléphones mobiles, de tablettes et de serveurs, ainsi que d'autres terminaux susceptibles d'être connectés à Internet, appelés « terminaux IoT » (Internet des objets). Les endpoints sont dès lors logiquement considérés comme l'une des principales sources de risque pour toute entreprise.

Un manque de visibilité et d'évolutivité dans cet environnement en pleine expansion représente un défi de taille pour les équipes informatiques et de sécurité chargées de la protection des endpoints — et les systèmes de sécurité d'ancienne génération ne sont pas d'une grande aide. Ces solutions, développées à l'origine pour identifier les fichiers malveillants connus, n'ont jamais eu pour vocation d'être évolutives et d'offrir le niveau de visibilité nécessaire pour vous protéger dans l'environnement en perpétuelle expansion que nous connaissons aujourd'hui, et que les cyberattaquants ciblent au moyen de **logiciels malveillants sans fichier**, de l'exploitation des vulnérabilités des plateformes et applications, du vol et de l'usurpation d'identités et de l'injection de **menaces persistantes avancées**.

Les cyberattaquants jouent la carte de la complexité. Bénéficier d'une visibilité et d'un contrôle sur ce qui se passe sur les endpoints devient de plus en plus difficile, voire impossible, et cela pour de nombreuses raisons, notamment le nombre croissant d'endpoints qui changent fréquemment d'emplacement. Les cybercriminels exploitent les failles de sécurité résultant de ce manque de visibilité et de contrôle pour faire pencher la balance en leur faveur.

Que peuvent donc faire les équipes informatiques et de sécurité pour rester agiles, efficaces et performantes à l'heure de protéger les endpoints ?

Visibilité totale : un impératif de la protection moderne des endpoints

Pour être réellement efficace, une solution de protection des endpoints doit offrir un niveau de sécurité optimal, tout en étant simple à utiliser. La complexité met les équipes et les processus à rude épreuve, en créant des failles de sécurité qui augmentent le risque de baisse de la productivité et d'atteinte à la réputation des entreprises.

Pour parvenir à un tel niveau de sécurité et de simplicité, la protection des endpoints doit inclure cinq fonctionnalités essentielles :

1. **Prévention** — pour bloquer autant d'éléments malveillants que possible
2. **Détection** — pour identifier et neutraliser les cyberattaquants
3. **Threat Hunting managé** — pour dépasser le stade de l'automatisation en matière de détection
4. **Cyberveille** — pour comprendre les cyberattaquants et garder une longueur d'avance
5. **Gestion des vulnérabilités et hygiène informatique** — pour préparer et renforcer l'environnement contre les cybermenaces et les attaques

Ces cinq fonctionnalités ne peuvent être pleinement activées, intégrées et exploitées qu'au travers d'une plateforme native au cloud qui simplifie les opérations de sécurité et offre la rapidité, la flexibilité et l'évolutivité nécessaires pour contrer les menaces actuelles les plus sophistiquées.

Prévention : bloquer l'accès aux cybercriminels

À l'instar des solutions antivirus, la protection classique des endpoints axée sur les logiciels malveillants s'avère efficace uniquement contre les logiciels malveillants connus, ce qui est insuffisant dans le paysage actuel des menaces, compte tenu de la prolifération des tactiques sans fichiers et sans logiciels malveillants de plus en plus sophistiquées.

Les équipes informatiques et de sécurité ont besoin de l'intelligence d'une solution **antivirus de nouvelle génération** capable de reconnaître et de bloquer à la fois les logiciels malveillants connus et zero day, les ransomwares et les attaques sans fichiers ni logiciels malveillants. Les solutions antivirus de nouvelle génération avancées peuvent tirer parti de l'analyse comportementale pour rechercher automatiquement les signes d'attaques et bloquer ces dernières au moment même où elles se produisent.

Contrairement aux solutions de sécurité d'ancienne génération qui doivent sans cesse être mises à jour, laissant par intermittence les endpoints sans protection, les solutions antivirus de nouvelle génération peuvent exploiter le Machine Learning (ML) pour maintenir la sécurité à jour, sans surcharger les équipes informatiques et de sécurité. Les solutions antivirus de nouvelle génération les plus performantes combinent ces technologies et d'autres techniques de pointe pour offrir la visibilité et le contexte nécessaires pour contrer les tactiques, techniques et procédures modernes d'attaque.

Toutefois, même la stratégie de prévention la plus efficace qui soit ne suffit pas pour contrer les cyberattaquants ingénieux et aux moyens financiers conséquents, et les experts en sécurité en sont bien conscients. L'approche la plus sûre pour les entreprises consiste à intégrer la prévention dans une stratégie robuste de détection afin d'identifier et de bloquer toute attaque furtive.

AU-DELÀ DES LOGICIELS MALVEILLANTS

Une étude récente a révélé que 68 % des menaces détectées entre avril et juin 2021 n'impliquaient pas de logiciel malveillant. De plus en plus, les cyberattaquants tentent de parvenir à leurs fins sans injecter de logiciel malveillant sur l'endpoint et recourent à des identifiants légitimes et à des outils intégrés (exploitant les ressources locales) pour échapper à la détection des antivirus traditionnels. SOURCE : RAPPORT 2021 SUR LE THREAT HUNTING DE CROWDSTRIKE

Détection : identifier et neutraliser les cybercriminels qui passent au travers des mailles du filet

Dès lors qu'un cybercriminel parvient à s'immiscer incognito dans une entreprise, il peut s'implanter discrètement dans l'environnement et y sévir pendant des jours, des semaines, voire des mois, sans se faire repérer.

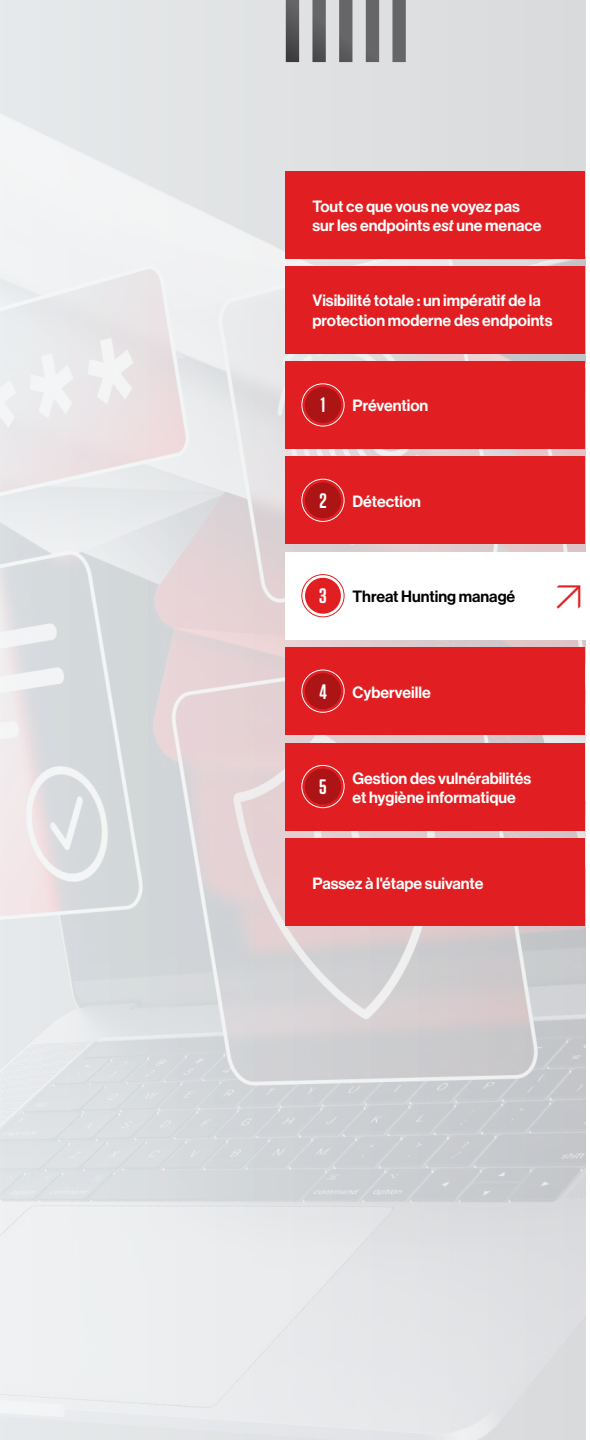
Les solutions de détection et d'intervention sur les endpoints (EDR) qui intègrent des fonctionnalités de prévention offrent aux équipes de sécurité la visibilité dont elles ont besoin pour détecter les cyberattaquants aussi rapidement que possible. Pour ce faire, la solution EDR doit enregistrer toutes les activités dignes d'intérêt sur un endpoint afin de les soumettre à une inspection plus approfondie, à la fois en temps réel et a posteriori, et enrichir ces données d'une cyberveille pour fournir le contexte nécessaire à un Threat Hunting et à une investigation efficaces.

Les équipes de sécurité ne devraient pas perdre leur temps à écrire et à optimiser les règles de détection. Une solution EDR efficace doit être à même de détecter automatiquement les activités malveillantes et de présenter aux équipes les attaques réelles, sans les distraire avec des faux positifs ou des activités inoffensives. L'application de mesures efficaces permet aux équipes de confiner et d'analyser les systèmes compromis, avec notamment un accès à distance à la volée pour une intervention immédiate, ainsi que de bloquer la progression de la compromission.

Les solutions EDR avancées permettent aux entreprises de détecter les attaques furtives et les menaces qui ont contourné les mesures de prévention. Toutefois, les entreprises peuvent protéger leurs endpoints de manière plus proactive encore en intégrant des threat hunters en chair et en os.

DES SOLUTIONS ANTIVIRUS D'ANCIENNE GÉNÉRATION TOTALEMENT DÉPASSÉES

Fin 2021, une attaque de la supply chain a entraîné la compromission d'un progiciel populaire (plus de 7 millions de téléchargements hebdomadaires à partir de la bibliothèque NPM) et ce dernier a été utilisé pour distribuer des mineurs de cryptomonnaie et des voleurs de mots de passe. La meilleure défense contre ce type d'attaque consiste à détecter les indicateurs d'attaque sur la base des comportements afin d'identifier et de bloquer les logiciels malveillants distribués au moyen de la bibliothèque corrompue. Cette détection s'appuie sur la cyberveille recueillie grâce à la surveillance continue des tactiques, techniques et procédures utilisées par les cybercriminels et les groupes non identifiés. SOURCE : « COMPROMISED NPM PACKAGE USED IN SUPPLY CHAIN ATTACK », BLOG CROWDSTRIKE, 26 OCTOBRE 2021



Threat Hunting managé : une détection au-delà de l'automatisation

Le **Threat Hunting** offre la possibilité aux entreprises d'adopter une approche proactive, pilotée par l'homme, et de rechercher activement les activités suspectes plutôt que de se reposer uniquement sur les technologies pour détecter automatiquement des activités malveillantes potentielles et déclencher l'alerte.

Le Threat Hunting managé vient au secours des entreprises qui ne disposent pas des ressources et d'une expertise en sécurité suffisantes pour repérer les cybercriminels et empêcher les menaces avancées de s'immiscer discrètement dans leur environnement. Une équipe de Threat Hunting hautement expérimentée peut surveiller votre environnement 24 heures sur 24, 7 jours sur 7, et y détecter les activités furtives malveillantes.

Les équipes responsables du Threat Hunting managé analysent les menaces et travaillent en étroite collaboration avec les équipes internes des entreprises afin de les guider tout au long du processus, de la détection à l'intervention. Cette interaction avec les experts augmente le niveau de maturité des équipes informatiques et de sécurité internes pas seulement de manière ponctuelle, mais aussi dans la durée.

Les threat hunters adoptent une approche proactive de la protection des endpoints basée sur leurs années d'expérience. Grâce à une visibilité sur l'ensemble des endpoints et à un accès à la cyberveille pertinente, ils peuvent non seulement comprendre ce qu'ils observent, mais aussi anticiper les cybermenaces qui planent sur l'entreprise.

Cyberveille : comprendre et anticiper les attaques

Les cyberattaquants sont tellement rapides et furtifs qu'il est très compliqué pour les technologies de protection et les responsables de la sécurité de rester au courant des dernières cybermenaces et de s'en protéger de façon proactive. Pour répondre tout aussi rapidement, les solutions de sécurité des endpoints doivent intégrer la cyberveille et/ou avoir la capacité d'intégrer les renseignements fournis par des sources tierces.

La **cyberveille** doit :

- Fournir des informations exploitables permettant aux équipes de sécurité et aux solutions de sécurité utilisées de comprendre les incidents, d'y réagir et d'y remédier plus rapidement, de façon à accélérer les investigations et la résolution.
- Générer et prioriser les alertes afin d'aider les équipes de sécurité à mieux comprendre les tactiques et campagnes associées aux différents cybercriminels.
- Être étroitement intégrée à une solution de protection des endpoints pour être accessible instantanément par les équipes informatiques et de sécurité. De cette façon, les équipes ne devront plus basculer manuellement d'une solution de sécurité à l'autre, et pourront voir le contexte d'une alerte et accéder à un écran plus détaillé d'un simple clic.

La capacité à comprendre et à prédire les attaques informées par la cyberveille constitue un aspect essentiel de la préparation d'une entreprise aux attaques avancées, tandis que la gestion des vulnérabilités et l'hygiène informatique renforcent les défenses de l'entreprise.

Gestion des vulnérabilités et hygiène informatique : renforcer les défenses de votre environnement contre les attaques

La **gestion des vulnérabilités** et l'hygiène informatique procurent la visibilité et les informations exploitables dont ont besoin les équipes informatiques et de sécurité pour comprendre quels systèmes et applications sont vulnérables, mais aussi les acteurs et les tactiques actifs dans l'environnement.

Une gestion efficace des vulnérabilités requiert une surveillance régulière et continue de tous les endpoints afin d'identifier les failles de sécurité où qu'elles se situent, sur site ou hors site. Pour garantir la sécurité des systèmes de production et l'application des derniers correctifs, les entreprises doivent savoir quelles vulnérabilités présentent le risque le plus élevé et cibler les mesures de correction à prendre.

En dépit de tous les efforts consentis, les entreprises passeront inévitablement à côté de certains correctifs ou de certaines mesures d'atténuation, compte tenu du nombre en constante augmentation de vulnérabilités réputées critiques. Accorder à chaque vulnérabilité le temps nécessaire pour atténuer les risques et intervenir en cas d'incident afin de protéger l'environnement est une tâche colossale, voire impossible. Les solutions d'hygiène informatique surveillent en continu les modifications apportées aux ressources, aux applications et aux utilisateurs, et identifient les systèmes non managés ou ceux qui peuvent présenter un risque pour le réseau, par exemple les appareils personnels non protégés des employés ou les systèmes de tiers.

La visibilité sur les tendances de connexion (activités et durée, par exemple) dans tout l'environnement, tant en ce qui concerne les identifiants d'utilisateur que ceux des administrateurs, permet de détecter et d'atténuer les abus d'identifiants et les attaques qui emploient des identifiants volés.

La gestion des vulnérabilités et l'hygiène informatique procurent aux équipes de sécurité les informations nécessaires pour adopter une approche proactive et efficace, renforcer le niveau de protection de l'entreprise et se préparer à anticiper et contrer les attaques.

Passez à l'étape suivante

Cet eBook fait la lumière sur les fonctionnalités que toute approche complète de la protection des endpoints doit proposer : prévention, détection, Threat Hunting managé, cyberveille ainsi que gestion des vulnérabilités et hygiène informatique.

Ensemble, ces cinq fonctionnalités fournissent une protection complète à l'échelle de l'entreprise, tout en réduisant les frais généraux de gestion et en améliorant considérablement les performances, l'agilité et l'évolutivité.

Ces cinq fonctionnalités critiques de la sécurité moderne des endpoints ne peuvent être pleinement activées, intégrées et exploitées qu'au travers d'une plateforme native au cloud qui simplifie les opérations de sécurité et offre la rapidité, la flexibilité et les capacités nécessaires pour contrer les cyberattaquants actuels.

Êtes-vous prêt à trouver une solution dotée de ces cinq fonctionnalités critiques, qui garantisse une protection robuste des endpoints ?

- **Consultez cette infographie** pour comprendre en un clin d'œil les différences entre les solutions de protection des endpoints d'hier et d'aujourd'hui.
- **Découvrez comment** la protection des endpoints native au cloud de CrowdStrike vous procure la visibilité propre à activer les cinq fonctionnalités critiques dont les entreprises ont besoin pour renforcer leur sécurité.

À PROPOS DE CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq : CRWD), leader mondial de la cybersécurité, redéfinit la sécurité moderne en proposant l'une des plateformes natives au cloud les plus avancées au monde, conçue spécifiquement pour protéger les ressources critiques de l'entreprise, à savoir les endpoints, les workloads cloud, les identités et les données.

Optimisée par l'architecture de sécurité cloud de CrowdStrike, la plateforme CrowdStrike Falcon® s'appuie sur des indicateurs d'attaque en temps réel, la cyberveille, l'évolution des techniques des cybercriminels et des données télémétriques enrichies récoltées à l'échelle de l'entreprise pour assurer une détection ultraprécise, une protection et une correction automatisées, un Threat Hunting de pointe et une observation priorisée des vulnérabilités.

Spécialement conçue dans le cloud au moyen d'une architecture à agent léger unique, la plateforme Falcon permet aux clients de bénéficier d'un déploiement rapide et évolutif, d'une protection et de performances de haut niveau, d'une complexité réduite et d'une rentabilité immédiate.

CrowdStrike : **We stop breaches.**

En savoir plus : **https://www.crowdstrike.com/**

Suivez-nous : **Blog | Twitter | LinkedIn | Facebook | Instagram**

Profitez sans plus tarder d'une évaluation gratuite : **https://www.crowdstrike.com/free-trial-guide/**