

Process Inspector

- Brief technique



Techniques de détection multi-niveaux :

1. Machine Learning

2. HyperDetect

3. Sandbox Analyzer

4. Protection de la mémoire

5. **Process Inspector**

Présentation

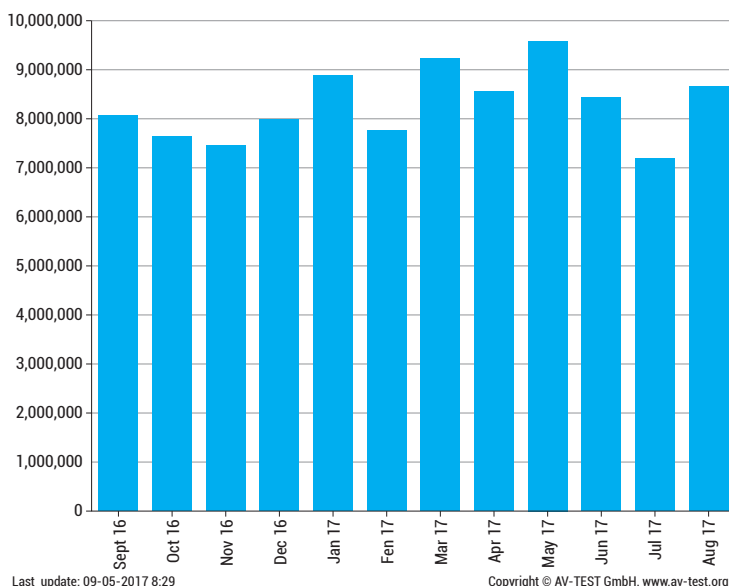
Dans le paysage actuel de la cybersécurité, les cybercriminels réalisent régulièrement des tests et modifient fréquemment leurs techniques d'attaques, rendant les entreprises plus vulnérables aux incidents et épidémies de malwares, aux interruptions d'activité et aux violations de données. La plateforme Bitdefender GravityZone Endpoint Security protège vos endpoints contre l'ensemble des cyberattaques sophistiquées avec une grande efficacité, un faible impact pour l'utilisateur final et en limitant la charge de travail des administrateurs. Elle est composée de multiples couches de protection pour entraver les activités de toute personne mal intentionnée. Chaque couche de sécurité est conçue pour stopper certains types précis de menaces, outils ou techniques, assurant ainsi une protection à plusieurs niveaux contre les cyberattaques.

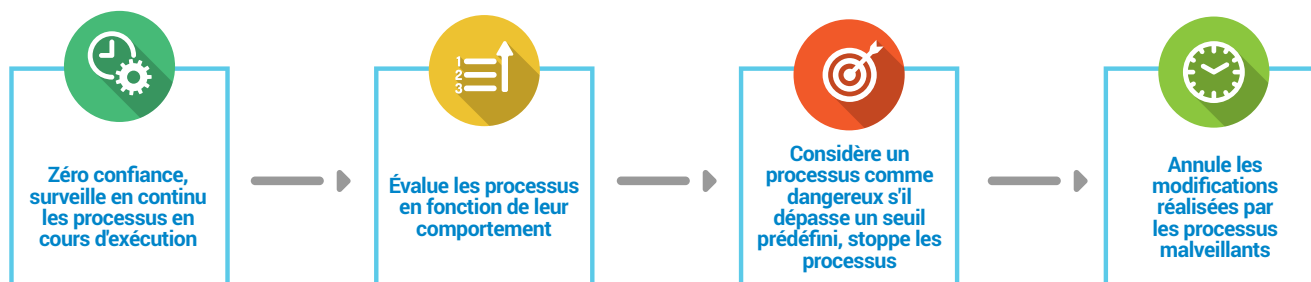
Bitdefender Process Inspector est intégré à la plateforme GravityZone Endpoint Security. Il s'agit d'une technologie de détection des anomalies comportementales qui assure la protection contre les menaces inconnues, et ce dès la phase d'exécution.

| Phase de détection | Type de technologie | Types de menaces détectées |
|--------------------|--|--|
| À l'exécution | Détection des anomalies comportementales | Malwares obfusqués, attaques ciblées, malwares sur mesure, attaques par scripts, exploits, malwares à retardement, attaques au niveau de la mémoire, injection de code, élévation des privilèges, attaques sans fichier (tel que me détournement de PowerShell), ransomwares |

Intérêt de la technologie Bitdefender Process Inspector

Avec plus de 390 000 nouveaux malwares détectés chaque jour, il est absolument fondamental pour les équipes de sécurité de protéger leur environnement des menaces émergentes et de type Zero-day. Process Inspector est une couche de protection qui agit lors de la phase d'exécution, complétant ainsi toutes les technologies de détection impliquées lors de la phase de pré-exécution. Elle réduit drastiquement le risque de compromission d'un système par une menace nouvelle ou émergente. Elle fonctionne selon une approche « zéro confiance » et surveille les processus en cours d'exécution sur le système d'exploitation à l'aide de filtres en modes utilisateur et noyau. Elle recherche des comportements spécifiques aux malwares et assigne une note à chaque processus en fonction des actions qu'il prend et du contexte. Cette technique d'approche est primordiale, car des processus analysés de manière isolée ne vont pas forcément donner d'indices sur une intention malveillante, alors qu'une analyse « collective » donne une meilleure visibilité sur la situation réelle. Lorsque le score général d'un processus atteint un certain seuil, celui-ci est considéré comme dangereux et des mesures de remédiation appropriées sont prises, avec notamment la possibilité d'annuler les modifications réalisées par le processus malveillant.





Caractéristiques

- Suivi des anomalies comportementales : les applications et les processus en cours d'exécution sont surveillés en continu, notamment : la copie ou le déplacement de fichiers dans les dossiers System ou Windows ou les emplacements à accès limité, l'exécution ou l'injection de code dans l'espace d'un autre processus pour qu'il bénéficie de privilèges plus élevés, l'exécution de fichiers créés avec des informations stockées dans un fichier binaire, l'autoréplication, la création d'une entrée à démarrage automatique dans le registre, l'accès à des emplacements du registre nécessitant des privilèges élevés ou l'exécution d'opérations interdites, la suppression ou l'installation de pilotes, le détournement de PowerShell (par exemple si powershell.exe est exécuté avec plusieurs arguments bien précis), une détection spécifique pour les ransomwares (par exemple la suppression de fichiers de sauvegarde / Shadow Copy, la génération de clés de chiffrement, etc.).
- Action automatique : attribue automatiquement une note aux processus en cours d'exécution et prend automatiquement des mesures quand une menace est détectée.
- Annulation des modifications/nettoyage : réalise des audits sur les modifications réalisées par les processus sur les endpoints. Lorsqu'une menace est détectée, stoppe automatiquement les processus et annule les modifications malveillantes réalisées par ceux-ci.
- Exclusion de processus : exclut certains processus de l'analyse.
- Boucle de rétroaction avec Bitdefender Global Protective Network (GPN) : les menaces détectées par le module Process Inspector sont instantanément transmises au cloud de sécurité de Bitdefender, appelé Bitdefender Global Protective Network (GPN), pour en garantir la détection par tous les autres endpoints dans le monde entier.

Avantages

- Détecte les attaques avancées en amont et empêche les violations de données, réduit les coûts et les efforts en réponse aux incidents.
- Réduit les efforts de recherche des menaces.
- Améliore le taux de détection des malwares furtifs ou récents, y compris les attaques sans fichier, en assurant la surveillance d'un processus tout au long de sa durée de vie, et en s'appuyant sur son comportement réel plutôt que sur des signatures, des binaires ou des empreintes de code.
- Protège contre les malwares obfusqués, les attaques ciblées, les malwares sur mesure, les attaques par scripts, les exploits, les malwares à retardement, les attaques au niveau de la mémoire, l'injection de code, l'élévation des privilèges, les attaques sans fichier, (tel que le détournement de PowerShell) et les ransomwares.
- Annule automatiquement les modifications malveillantes réalisées sur les systèmes.
- Fonctionne dès l'installation, avec peu ou pas de configuration, et ne nécessite pas l'activation ou la mise en place de règles complexes.
- Optimise de façon intelligente les performances de la surveillance des applications et des processus, garantissant ainsi le plus faible impact sur les systèmes.
- Utilise les informations collectées sur les fichiers détectés afin d'améliorer les modèles de Machine Learning en charge de la détection en phase de pré-exécution.
- Est intégré à l'agent de sécurité unifié pour endpoint GravityZone et à la plateforme centralisée d'administration, réduisant ainsi la charge de travail des administrateurs. Ces derniers n'ont ainsi pas à déployer plusieurs solutions de sécurité pour endpoints.



Bitdefender est une entreprise mondiale de sécurité qui développe des solutions de cybersécurité de pointe et qui protège plus de 500 millions d'utilisateurs dans plus de 150 pays. Depuis 2001, Bitdefender développe des technologies régulièrement récompensées, pour les marchés des entreprises et des particuliers, et est un fournisseur recommandé pour sécuriser les infrastructures hybrides et protéger les endpoints. Grâce à ses équipes R&D, ses alliances et partenariats, Bitdefender est reconnu pour être un éditeur innovant, proposant des solutions de sécurité fiables et efficaces, sur lesquelles vous pouvez compter. Plus d'informations sur www.bitdefender.fr

Tous droits réservés. © 2018 Bitdefender. Toutes les marques, noms commerciaux et produits cités dans ce document sont la propriété exclusive de leurs détenteurs respectifs. Pour plus d'informations, veuillez consulter www.bitdefender.fr/business

