# Bitdefender GravityZone Ultra

## DÉTECTE ET BLOQUE LES MENACES ÉVASIVES AVEC AGILITÉ ET PRÉCISION

**GravityZone Ultra** est une solution de sécurité pour endpoints conçue spécialement pour être un EPP intégré next-gen et un EDR facile à utiliser. Elle regroupe des fonctionnalités de détection des menaces, de réponse automatique, de visibilité pré et post compromission, de tri des alertes, d'investigation, de recherche avancée et de résolution en un clic.

En s'appuyant sur des technologies hautement efficaces de prévention, de détection automatisée des menaces et de réponse, GravityZone Ultra limite grandement les incidents nécessitant une analyse manuelle, réduisant ainsi les efforts opérationnels nécessaires à l'utilisation d'une solution EDR. Disponible dans le cloud et conçue comme une solution unifiée à un seul agent et gérée depuis une seule console, elle est également facile à déployer et à intégrer dans l'architecture de sécurité existante.

GravityZone Ultra permet aux entreprises de protéger leurs actifs numériques contre les cybermenaces les plus furtives, et de réagir de manière efficace lors de toutes les phases d'une attaque :

- Réduire la surface d'attaque (grâce au pare-feu, au contrôle des applications, au contrôle de contenu et au patch management)
- La protection des données (via le module complémentaire de chiffrement complet de disque)
- Détecter les menaces dès la phase de pré-exécution et éradiquer les malwares (grâce au Machine Learning paramétrable, à la surveillance des processus en temps réel et à l'analyse en sandbox)
- Détection des menaces en temps réel et réparation automatique
- Visibilité sur les attaques avant et après la compromission (analyse de cause racine)
- Tri, investigation et réponse rapide en cas d'incident
- Recherche des données actuelles et passées
- Une sécurité encore plus complète grâce au module de Patch Management

Le résultat : une prévention transparente des menaces, une grande visibilité, une détection précise des incidents et une réponse intelligente pour minimiser l'exposition aux infections et stopper les violations de données.

En tant que suite intégrée pour la protection des endpoints, **GravityZone Ultra** garantit un niveau de sécurité constant à l'ensemble de l'environnement informatique ; ainsi, les attaquants ne peuvent avoir accès à des endpoints mal protégés qu'ils pourraient utiliser comme points de départ pour diffuser des actions malveillantes contre l'entreprise. **GravityZone Ultra** s'appuie sur une architecture simple et intégrée avec gestion centralisée des endpoints et des datacenters. La solution permet aux entreprises de déployer rapidement la protection sur tous les endpoints et nécessite moins d'efforts d'administration après sa mise en œuvre.

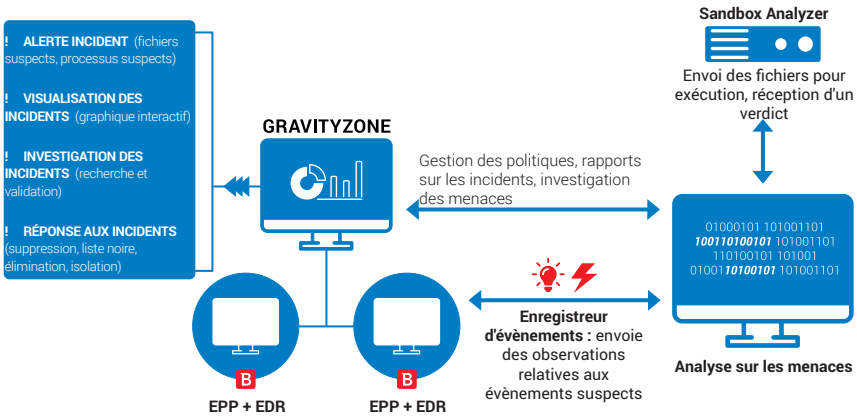



Figure 1. Bitdefender Ultra : prévention, détection et remédiation au sein d'un seul et unique agent, géré par la console GravityZone

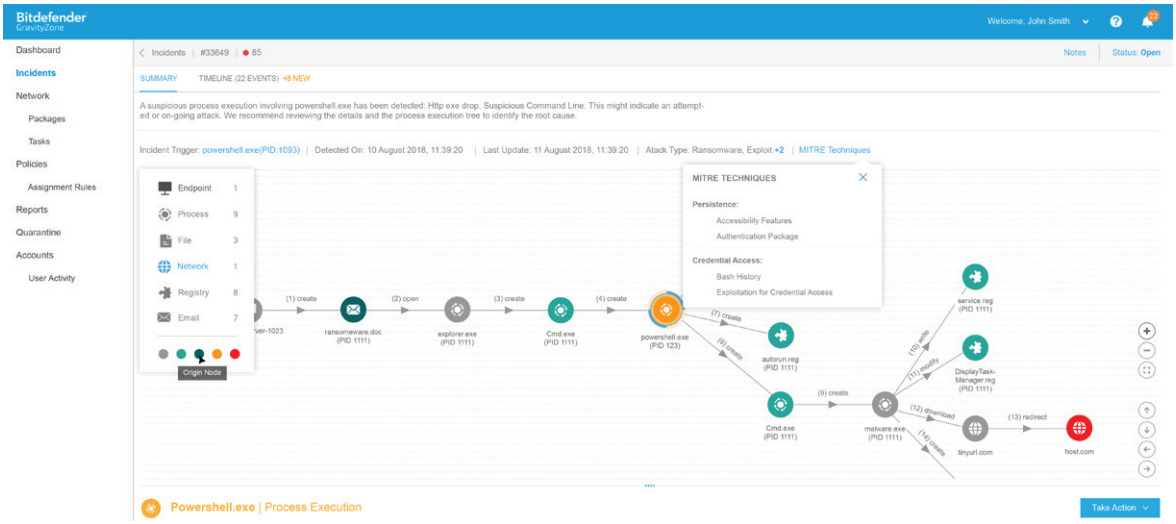
# L'EDR facilitée

Avec une visibilité claire sur les indicateurs de compromission (IOC), l'investigation des menaces en un clic et les processus de réponses aux incidents, GravityZone Ultra réduit les besoins en ressources et en connaissances pour les équipes de sécurité. Le nouvel enregistreur de données des endpoints s'intègre à la solution existante de protection contre les menaces et réalise une capture étendue des activités des systèmes (fichiers et processus, installation de programmes, chargement de modules, modification du registre, connexions au réseau, etc.) afin de contribuer à la visualisation, à l'échelle de l'entreprise, de la chaîne des évènements impliqués lors d'une attaque.

# Avantages clés

Allant au-delà des fonctionnalités EPP traditionnelles, GravityZone Ultra fournit aux analystes en sécurité et aux équipes chargées de traiter les incidents, les outils dont ils ont besoin pour analyser les activités suspectes, pour investiguer et répondre de manière appropriée aux menaces avancées :

- Détection en temps réel et réparation automatique
- Tri, investigation et réponse rapide en cas d'incident : détection et validation des activités suspectes, tri des alertes, réponse en un clic
- Analyse pré et post compromission (analyse de cause racine)
- Recherche des données actuelles et passées basée sur : IOC Tags Mitre Processus, fichiers, entrées de registre et autres paramètres



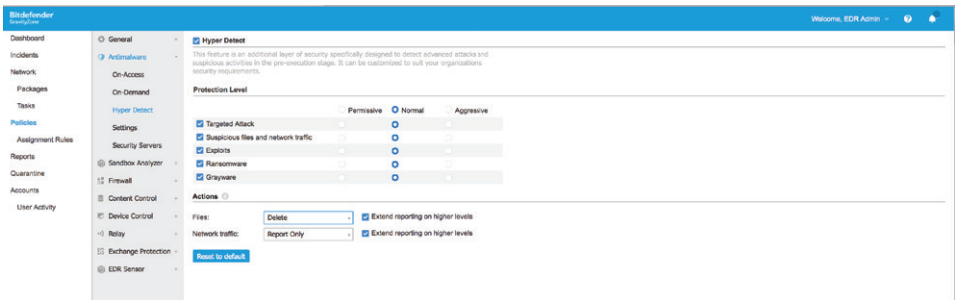

Graphique 2. La fenêtre d'informations relative aux incidents fournit un aperçu clair et détaillé de l'ampleur des incidents de sécurité. L'administrateur peut ainsi facilement obtenir les éléments dont il a besoin et répondre efficacement aux attaques.

# Une détection précise pour une meilleure visibilité de la sécurité et moins d'alertes inutiles

Seuls les évènements pertinents, corrélés et jugés sérieux sont présentés en vue d'une analyse et d'une résolution manuelles. Les informations inutiles et redondantes sont réduites à leur minimum, dans la mesure où la grande majorité des malwares et des attaques avancées sont bloqués lors de la phase de pré-exécution ou à l'exécution. Les menaces évasives, y compris les malwares sans fichier, les exploits, les ransomwares et les malwares obfusqués sont neutralisés par nos technologies multi-couches Next-Gen et par Process Inspector, technologie de détection basée sur le comportement des processus. La réponse et la remédiation automatiques éliminent la nécessité d'une intervention humaine dans le cas d'attaques bloquées.

La précision de la détection permet au personnel en charge de la sécurité de se concentrer uniquement sur les incidents et les menaces réels :

- Minimisation des efforts inutiles liés aux faux positifs
- Réduction du nombre d'incidents grâce à une prévention efficace des menaces
- Élimination de la remédiation manuelle des attaques bloquées grâce à la remédiation et à la désinfection automatiques



## Investigation simple des incidents et réponse intelligente

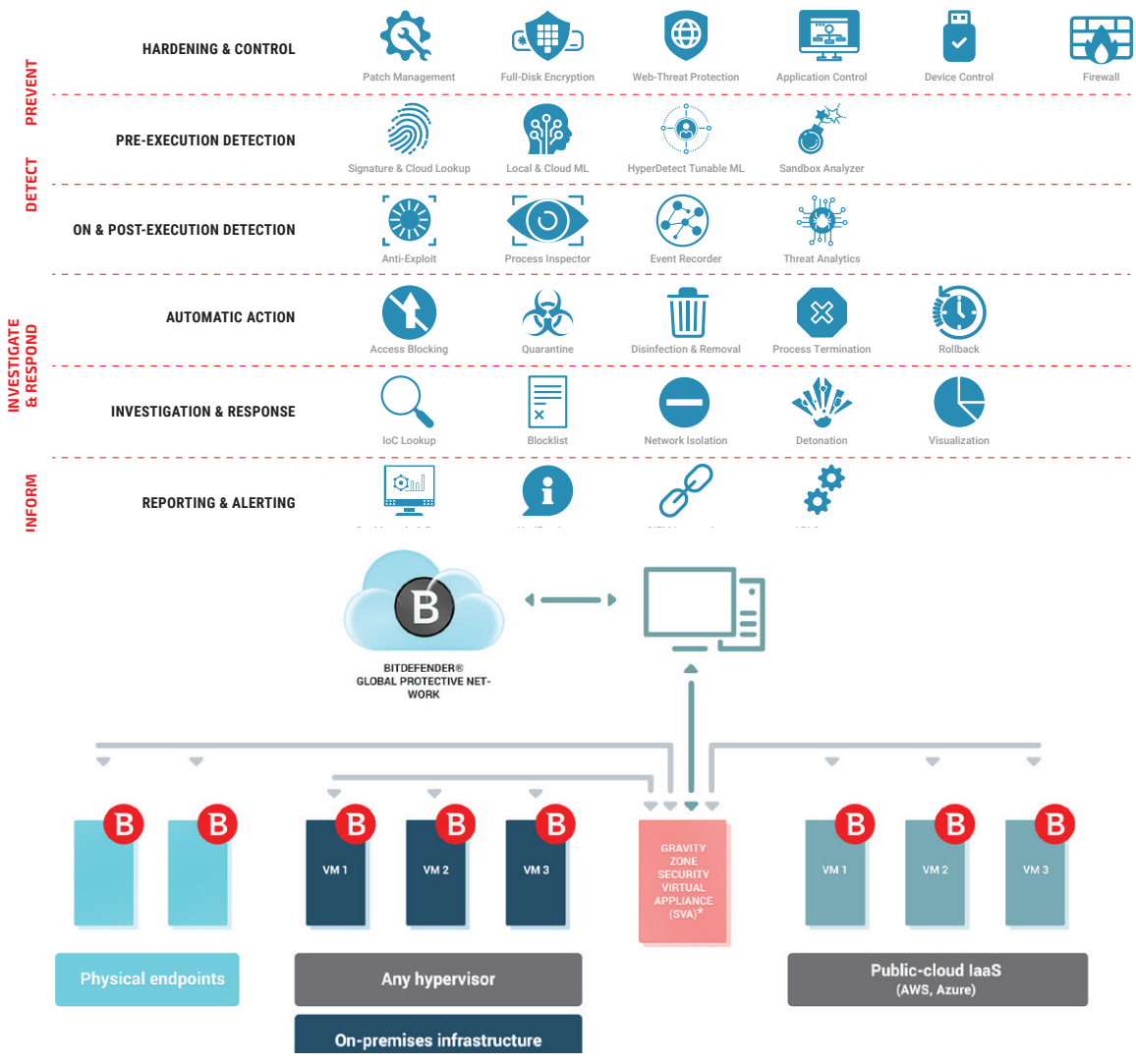
Avec son approche intégrée (prévention-détection-réponse-évolution), GravityZone Ultra permet de rapidement répondre aux menaces et de restaurer les endpoints avec une sécurité « encore meilleure ». Les outils d'investigation sur les incidents, tels que l'analyse de cause racine et les rapports de la sandbox, aident les équipes de sécurité à valider les activités suspectes et à répondre de manière adéquate aux cybermenaces. La recherche avancée des données actuelles comme passées selon leurs IOC, leurs tags MITRE ou tout autre artefact permet d'identifier rapidement les menaces qui pourraient se cacher dans l'infrastructure du endpoint.

En vous appuyant sur les informations collectées sur les endpoints pendant l'investigation, vous pouvez, via une seule et unique interface, régler immédiatement les politiques et corriger les vulnérabilités identifiées, et ainsi améliorer la sécurité de votre environnement.

## Une plateforme de sécurité complète pour endpoints via un seul agent et une seule console

GravityZone Ultra propose le même renforcement et les mêmes contrôles préventifs Next-Gen que la solution GravityZone Elite :

- Minimisation de l'exposition aux attaques grâce à une meilleure prévention
- Détection à base de Machine Learning et d'analyse comportementale, permettant de bloquer les menaces inconnues à l'exécution et à la pré-exécution
- Détection et blocage des attaques par script, sans fichier, offusquées et des malwares personnalisés, avec remédiation automatique
- Protection de la mémoire pour empêcher les exploits
- Réduction de la surface d'attaque en simplifiant les contrôles de sécurité
- Pare-feu client intégré, contrôle des appareils, filtre de contenu Web, contrôle des applications et bien plus encore
- Modules complémentaires : Chiffrement de disque et Patch Management




*** Les déploiements sans agent sont également pris en charge sous VMware vShield ou NSX**

Graphique 3. Bitdefender GravityZone Ultra : la plateforme de sécurité complète pour endpoints, EPP + EDR

# Protection des datacenters et des infrastructures cloud

GravityZone Security for Virtualized Environments est intégré à GravityZone Ultra pour assurer la protection des charges de travail. Il a été conçu pour assurer agilité, efficacité opérationnelle et maîtrise des coûts de l'infrastructure dans les environnements définis par logiciel, hyperconvergés et de cloud hybride.

## Avantages clés

**Amélioration de l'efficacité opérationnelle et de l'agilité**
Compatible avec de nombreuses plateformes cloud et tous les hyperviseurs (dont VMware ESXi, Citrix XenServer, Microsoft Hyper-V, Nutanix AHV, KVM, RedHat Enterprise Virtualization), GravityZone permet de simplifier les opérations IT et de sécurité tout en améliorant la mise en conformité. La console d'administration unifiée de GravityZone simplifie le déploiement et l'administration de la sécurité, tout en permettant le provisionnement automatisé, l'application centralisée des politiques et une visibilité depuis un seul et unique tableau de bord à travers tous les environnements hétérogènes et distribués. L'intégration à des outils de gestion de la virtualisation (vCenter Server, XenServer et Nutanix Prism) donne à GravityZone des informations en temps réel sur le contexte opérationnel sous-jacent de l'infrastructure, et notamment accès à l'inventaire complet des machines virtuelles (VM). GravityZone peut donc appliquer automatiquement les politiques de sécurité appropriées à chaque VM en fonction des charges de travail, quel que soit leur emplacement dans le cloud hybride, permettant ainsi aux équipes informatiques d'assurer la sécurité de milliers de VM en quelques heures.

**Performance et utilisation de pointe de l'infrastructure**
Les algorithmes de sécurité brevetés de GravityZone - qui évite d'avoir à utiliser des agents gourmands en ressources sur chaque VM - permettent d'améliorer de jusqu'à 35% la densité de virtualisation et de 17% le temps de réponse des applications, améliorant ainsi l'utilisation de l'infrastructure, tout comme l'expérience des utilisateurs.

**Évolutivité linéaire illimitée**
L'architecture modulaire et résiliente de GravityZone fournit l'adaptabilité nécessaire à la sécurisation des déploiements de type carrier-grade. La plateforme peut s'étendre à la demande de façon linéaire et efficace par l'ajout d'appliances virtuelles de sécurité ou par la multiplication des rôles des serveurs du Control Center, si besoin.

**Compatibilité universelle**
La solution est compatible avec les principaux hyperviseurs du marché (VMware ESXi, Microsoft Hyper-V, Citrix Xen, Red Hat KVM, Nutanix AVH, etc.) et les OS invités Windows et Linux.

## Le Control Center GravityZone

Le Control Center GravityZone Ultra est une console d'administration intégrée et centralisée qui fait office de tableau de bord unique pour toutes les composantes de gestion de la sécurité, notamment la sécurité des endpoints, des datacenters, du cloud, et des boîtes de messagerie Exchange. Avec GravityZone Ultra, seule une console hébergée dans le cloud est disponible. Le Control Center regroupe de nombreux rôles et intègre un serveur de base de données, un serveur de communication, un serveur de mise à jour et une console Web.

**GravityZone Ultra** est fourni sous la forme d'une console cloud. La solution protège les postes de travail, les serveurs et les boîtes de messagerie Exchange. Au maximum 35 % des endpoints protégés peuvent être des serveurs.

Pour consulter la configuration système détaillée, rendez-vous sur www.bitdefender.com/business/enterprise-products/ultra-security

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