Bitdefender®

GravityZone

GUIDE DES SOLUTIONS

Simplifiez vos opérations de sécurité tout en réduisant les risques

Et si tout ce qu'on nous avait raconté sur la cybersécurité était faux ? Si le fait d'ajouter des niveaux de sécurité ne sécurisait pas plus, mais qu'à l'inverse, cela générait des vulnérabilités ? En réalité, nombre de systèmes sont devenus si complexes qu'ils constituent la plus grande faiblesse.

Chaque outil de sécurité apporte davantage de protection, mais crée également de la confusion et des zones d'ombres. Les cybercriminels se glissent à travers les fissures que nous avons créées. Le Forum économique mondial le confirme : « le cyberespace est plus complexe et difficile que jamais en raison des progrès technologiques rapides, de la sophistication croissante des cybercriminels et de l'interconnexion sans précédent des chaînes d'approvisionnement. »

Le futur de la cybersécurité ne consiste pas à rajouter. Il consiste à simplifier la sécurité, à éliminer les alertes et à se concentrer sur ce qui compte vraiment.

Pourquoi les menaces sont plus difficiles à détecter et à stopper ?

C'est une histoire connue : chaque jour, les cybermenaces évoluent, devenant plus sophistiquées et plus difficiles à contrer. Les entreprises opèrent dans des environnements tentaculaires et interconnectés comprenant des milliers d'actifs. Chaque nouvelle initiative commerciale ajoute des endpoints, des flux de données et des dépendances. Et bien qu'elles apportent de la valeur, elles présentent également des risques.

Au fur et à mesure que votre environnement se développe, la visibilité du service IT se fragmente. Il devient alors presque impossible de corréler des données provenant de plusieurs sources disparates. Votre équipe de sécurité s'efforce d'assembler les pièces, risquant pourtant de passer à côté de failles que les adversaires ne manqueront pas d'exploiter.

En même temps, les hackers ont fait évoluer leurs méthodes. Ils ne s'appuient plus uniquement sur des attaques par force brute ou des approches de type « Zero-day ». Ils maîtrisent désormais des techniques de survie, combinant leurs actions malveillantes avec des outils et des procédures légitimes déjà présents dans les systèmes.

Les intrusions sont donc beaucoup plus faciles à exécuter et beaucoup plus difficiles à détecter. Même les attaques rudimentaires, lorsqu'elles sont menées avec précision et rapidité, peuvent avoir des conséquences dévastatrices si elles contournent suffisamment longtemps les défenses. Pendant ce temps, les hackers intègrent l'automatisation et l'IA, ce qui amplifie leur portée et accélère la vitesse à laquelle ils peuvent identifier les vulnérabilités, exploiter les lacunes et étendre leurs opérations.

Cette tâche est rendue plus difficile par le fait que les menaces se limitent rarement à un seul point d'attaque. De par leur conception, elles sont multifacettes et touchent simultanément plusieurs niveaux de l'entreprise. Par exemple, les hackers peuvent commencer par un email de phishing, élevér des privilèges, tirer parti d'actifs cloud mal configurés et, enfin, exécuter un mouvement latéral sur les endpoints. Chaque étape renforce la suivante, créant une réaction en chaîne qu'il est beaucoup plus difficile d'interrompre une fois qu'elle est en marche.

Cette approche signifie que l'impact d'une attaque ne se limite plus à un seul système ou service. Par exemple :

- Les ransomwares ont souvent tendance à désactiver les sauvegardes tout en exfiltrant simultanément les données sensibles afin de procéder à une double extorsion.
- Les campagnes de Business Email Compromise (BEC) peuvent avoir des conséquences bien plus graves que le simple piratage d'une boîte de réception, impliquant souvent une fraude financière ou une infiltration de la chaîne d'approvisionnement.

Comme les hackers peuvent exploiter plusieurs vecteurs simultanément, cela augmente leur probabilité de réussite. Cette situation entraîne des conséquences désastreuses : des environnements de plus en plus complexes qui se heurtent à des adversaires de plus en plus redoutables. Et en l'absence de visibilité, de compréhension et de capacités de réponse adéquates, les entreprises éprouvent des difficultés à établir la meilleure façon de prioriser les efforts de protection.

Plus d'outils = plus d'alertes

Les environnements des entreprises d'aujourd'hui, extrêmement complexes, exercent une pression sans précédent sur les équipes chargées de la sécurité. Chaque nouvel appareil, chaque nouvelle application ou encore chaque nouveau cloud apporte son lot d'alertes, de journaux et de vulnérabilités. Pour rester dans la course, la plupart des entreprises ont adopté une panoplie d'outils de sécurité, notamment :

- l'EDR (Endpoint detection and response),
- les pare-feux,
- la protection de l'identité,
- le cloud et la sécurité SaaS,
- la gestion des vulnérabilités,
- et bien plus encore...

Chaque outil a sa propre fonction. Mais le simple fait d'essayer de les rassembler pour qu'ils forment une défense cohérente crée souvent plus de problèmes qu'il n'en résout. Comment expliquer cela ?

- **Des données hétérogènes :** chaque plateforme génère ses propres formats de données, sa propre logique d'alerte et ses propres tableaux de bord. Votre équipe de sécurité est contrainte de passer beaucoup de temps à réconcilier les schémas incohérents et les évènements en doublon plutôt que de se concentrer sur les menaces prioritaires.
- **Les doublons et les alertes :** le chevauchement des fonctionnalités des différents outils signifie qu'un même évènement peut déclencher plusieurs alertes, ce qui surcharge les équipes et leur fait perdre du temps, tout en portant atteinte à la confiance accordée au processus global de détection.
- **Les défis en matière d'intégration :** l'intégration entre les outils est rarement fluide. Les API changent, les connecteurs se cassent et l'ajustement des règles de corrélation nécessite un effort d'ingénierie continu que de nombreuses équipes ne peuvent tout simplement pas assumer.

Au fur et à mesure que la pile de sécurité s'étoffe, la visibilité globale diminue. L'enquête Hybrid Cloud Security Survey de Gigamon publiée en 2024, a révélé que 41 % des RSSI s'inquiétaient de la prolifération des outils et des lacunes que cela entraîne en matière de visibilité et de sécurité, en raison de la complexité de l'intégration et des difficultés de gestion de chaque outil. Au lieu d'avoir une vue d'ensemble, les analystes doivent naviguer entre plusieurs consoles, chacune offrant une vue partielle de l'environnement. Cette visibilité cloisonnée ralentit les investigations. Les équipes doivent passer d'une plateforme à l'autre pour reconstituer le scénario de l'attaque, ce qui augmente le temps moyen de détection (MTTD) et le temps moyen de réponse (MTTR).

Pour pallier cela, de nombreuses entreprises s'appuient sur les plateformes SIEM (Security Information and Event Management) et SOAR (Security Orchestration, Automation and Response) afin de centraliser les données et automatiser les flux de travail. Cependant, les SIEM et les SOAR présentent leur propre complexité, notamment des coûts élevés liés à l'ingestion des journaux, des règles de détection fragiles et la nécessité de faire appel à des ingénieurs spécialisés pour les régler et les entretenir.

Dans le rapport « State of SIEM Detection Risk » de CardinalOps publié en 2025, il a été constaté que, malgré l'ingestion de centaines de journaux, les SIEM ne couvrent généralement qu'une fraction des techniques adverses connues, laissant ainsi de dangereuses lacunes. Les entreprises ne constatent « pas toujours d'augmentation proportionnelle de la couverture » lorsqu'elles investissent dans des SIEM pour consolider leurs outils.

Alors, quelle est la solution ? Il est clair que la solution ne consiste pas à ajouter de nouveaux outils, mais plutôt à adopter une approche intégrée qui réduit la complexité tout en améliorant la couverture et les résultats.

Bitdefender

Simplifier vos opérations de sécurité tout en réduisant les risques

Intégration = simplification

Face à l'escalade des menaces, à la fragmentation des outils et à la pression exercée sur les équipes, la cybersécurité nécessite une approche prudente et bien structurée. L'ajout d'endpoints ne fait que multiplier le fardeau de l'intégration et augmenter le bruit des données. Votre équipe a besoin d'une plateforme intégrée qui simplifie les opérations, améliore la visibilité, automatise la détection et la réponse, et fournit l'expertise adéquate.

Parler le même langage

Une plateforme de sécurité intégrée réunit l'ensemble des outils et des fonctionnalités en matière de sécurité, garantissant qu'ils parlent tous le même langage. Plutôt que des consoles disparates et des données cloisonnées, vous pouvez gérer la sécurité des endpoints, des identités, des clouds et des applications SaaS depuis un environnement unique.

Ce regroupement :

- → évite les répétitions,
- → réduit la charge opérationnelle,
- → veille à ce que les alertes, les journaux et les données télémétriques soient transmis à un niveau d'intelligence central pour corrélation et analyse en temps réel.

Le résultat ? Des opérations de sécurité simplifiées avec des capacités de détection et de réponse plus fiables sur l'ensemble de votre surface d'attaque.

Prévention, protection, détection et réponse intégrées

Une plateforme de sécurité intégrée renforce la protection en regroupant dans un seul système connecté, la prévention, la protection, la détection et la réponse. Au lieu de traiter ces domaines séparément, elle met en corrélation les données télémétriques avec les endpoints, les identités, les charges de travail en cloud, les réseaux et les applications SaaS. Cela permet d'identifier rapidement les vulnérabilités, les mauvaises configurations ou les activités anormales, réduisant ainsi la probabilité que les attaques s'étendent davantage dans l'environnement de l'entreprise.

L'application de politiques intégrées et la gestion des vulnérabilités permettent d'optimiser encore davantage la prévention et la protection. Les contrôles de sécurité, les politiques d'accès et les paramètres de configuration peuvent être appliqués de manière cohérente dans l'ensemble de l'environnement à partir d'une console unique. Lorsque des mises à jour de la logique de détection ou des flux de renseignements sont introduites, elles sont distribuées simultanément. Cela garantit la mise à jour et la synchronisation des protections, l'amélioration de la couverture et la réduction de la complexité.

Ce regroupement d'outils améliore également la visibilité et rend la compréhension de la surface d'attaque plus facile. Les analystes peuvent rapidement identifier les actifs les plus susceptibles d'être ciblés, prioriser les mesures correctives en fonction du risque commercial réel et utiliser le contexte associé pour accélérer les actions de réponse. Cette connexion de bout en bout, de la prévention à la réponse, permet de stopper plus rapidement les menaces, de simplifier les enquêtes et de remédier aux problèmes avec plus de rapidité et de confiance.

Une automatisation simplifiée et plus efficace

Grâce à des outils interconnectés, la détection et la réponse peuvent être automatisées et rationalisées, transformant des processus manuels en flux de travail fluides et fiables. La plateforme corrèle automatiquement les données, les évènements et les alertes, générant ainsi des détections de haute précision et déclenchant automatiquement des actions de réponse.

Au lieu de perdre du temps à passer d'une console à une autre, trier les alertes ou tenter des intégrations personnalisées, les analystes reçoivent des alertes hiérarchisées et riches en contexte. L'automatisation génère un ROI considérable : le rapport Cost of a Data Breach d'IBM de 2024 a révélé que les entreprises ayant déployé une automatisation complète de la sécurité parviennent à contenir les violations avec 74 jours d'avance et économisent environ 31 % des coûts liés aux violations.

Grâce à l'automatisation, vous pouvez détecter les violations plus rapidement, enregistrer les incidents avec une plus grande confiance et réagir plus efficacement sur l'ensemble de la chaîne d'attaque. Cela permet d'enrichir les alertes avec des informations sur les menaces, de cartographier les activités selon les techniques MITRE ATT&CK, de contenir les actifs compromis et de générer automatiquement des rapports pour d'éventuels audits. La différence est considérable pour les équipes réduites et aux ressources limitées : les analystes sont libérés d'un travail répétitif de tri et peuvent se concentrer sur la chasse proactive aux menaces, la planification de la résilience et l'amélioration stratégique de la sécurité.

L'automatisation accélère la détection et la réponse, simplifie les opérations de sécurité, réduit la complexité et permet aux équipes de travailler plus efficacement.

Renforcez votre équipe avec des ressources expertes

La technologie ne suffit pas à assurer la sécurité ; vous avez besoin de services qui renforcent vos expertises et capacités. Travailler avec un fournisseur de services MDR (Managed Detection and Response) renforce votre sécurité grâce à une surveillance 24/7, une détection des menaces avancées et une réponse aux incidents par des experts.

Avec le MDR, vous bénéficiez d'un accès à des analystes, des chasseurs de menaces et des experts judiciaires qui peuvent enregistrer les alertes, enquêter sur les incidents et coordonner la réponse, réduisant ainsi le temps entre la détection et la mise en place de mesures correctives. Grâce à une veille sur les menaces, une surveillance du dark web et une protection des marques, le MDR vous permet de bénéficier d'une visibilité et d'une protection de niveau professionnel.

Mais les plateformes intégrées doivent aller plus loin que la détection et réponse en proposant des services de prévention et de conseils. Il peut être intéressant de recourir à des services de sécurité offensive, telles que le Pen Testing, le Red Teaming ou les exercices de simulation. Ces mesures identifient de manière proactive les faiblesses avant que les adversaires ne les exploitent.

Les services de conseil peuvent vous guider dans l'élaboration et le développement de programmes de cybersécurité. Ils veillent à ce que les politiques, les procédures et les contrôles correspondent avec les besoins de l'entreprise et répondent aux exigences de conformité.

Favorisez une communication claire et démontrez votre valeur ajoutée

Une plateforme intégrée ne simplifie pas seulement les tâches de sécurité, elle transforme aussi la manière dont les informations circulent en interne. Comme toutes les données télémétriques, les alertes et les résultats sont centralisés, la plateforme a la possibilité de présenter les informations dans des formats différents. Les analystes bénéficient d'alertes contextuelles et de données légales, tandis que la direction, les membres du CA et les responsables de la conformité disposent de tableaux de bord clairs qui mettent en évidence les tendances, les indicateurs clés de la performance et la position globale en matière de risques.

Cette clarté permet aux non-spécialistes de la sécurité d'exercer leurs fonctions avec plus d'efficacité. En effet, la direction peut facilement comprendre la position de l'entreprise, les membres du CA peuvent évaluer les investissements en matière de sécurité en toute confiance et les équipes chargées de la conformité peuvent produire des preuves pour un éventuel audit. La capacité à présenter les résultats en termes simples et accessibles garantit que la valeur de la fonction de sécurité est non seulement reconnue en interne, mais également démontrée en externe aux parties prenantes et aux régulateurs.

Il en résulte un programme de sécurité qui est à la fois plus solide, plus fluide, plus responsable et qui s'aligne parfaitement avec les objectifs de l'entreprise. En simplifiant la manière dont les informations sont exploitées, les plateformes intégrées permettent à la sécurité de passer d'une discipline purement technique à un outil commercial intégré.

Spécialement conçu pour les équipes de sécurité réduites

Contrairement aux ensembles d'outils issus de produits de sécurité disparates, les plateformes intégrées mettent l'accent sur la simplicité, l'intégration et les résultats mesurables. Cette philosophie de conception se traduit par moins d'interfaces à apprivoiser, un déploiement plus rapide et un niveau d'automatisation qui amplifie les capacités des petites équipes. Les équipes de sécurité ont accès à des fonctionnalités de niveau entreprise sans avoir à en gérer la complexité. Elle offre les fonctions de visibilité, de prévention, de protection, de détection et de réponse indispensables pour se défendre contre les menaces modernes, mais dans un format accessible et durable.

Cela permet de maîtriser plus rapidement les menaces, de réduire les vulnérabilités de manière proactive et de garantir que les efforts en matière de sécurité sont en adéquation avec les risques commerciaux. En réduisant le temps consacré au tri manuel et à la maintenance des outils, vous pouvez consacrer plus d'énergie à des initiatives stratégiques, telles que la planification de la résilience, la conformité réglementaire et l'établissement de rapports destinés à la direction.

Concentrez-vous sur ce qui compte le plus

Prêt à en faire plus avec moins ? Créez une plateforme de sécurité intégrée grâce à la fusion d'outils technologiques et la collaboration avec des fournisseurs experts. Au lieu de vous noyer sous une masse de données et d'alertes fragmentées, vous pourrez vous concentrer sur ce qui compte le plus : assurer la sécurité des données et des systèmes de votre entreprise.

Vous recherchez une sécurité de niveau professionnel sans la complexité ? Les solutions de sécurité professionnelles de Bitdefender peuvent vous aider à réduire les risques de manière proactive et à vous défendre contre les cybermenaces.

LEARN MORE

Siège social en Roumanie
Orhideea Towers
Şoseaua Orhideelor 15A
Sector 6,
București 060071

Tél. : +40 21 4412452

Bureaux en France
49 rue de la Vanne,
92120 Montrouge,
France,

Tél. : +33 1 47 35 72 73

Disponible à partir d'octobre 2025

Pour plus d'informations, rendez-vous à l'adresse suivante : https://www.bitdefender.com/fr-fr/.