RAPID7

RAPID7.COM

ARGUMENTS EN FAVEUR D'UNE CONSOLIDATION DES FOURNISSEURS DE SÉCURITÉ

Guide pour réduire les coûts et augmenter le retour sur investissement

TABLE DES MATIÈRES

Pourquoi consolider ? 3

Avantages de la consolidation 4

Problèmes supposés en matière de consolidation 7

Consolidation - Par où commencer 9

Conclusion : solution de sécurité Jenga® 12

POURQUOI CONSOLIDER ?

En matière d'efficacité, rien ne vaut la consolidation. Nous consolidons constamment nos vies personnelles et professionnelles (nos biens, nos données, nos abonnements à des services de streaming et même nos assurances) dans le but de nous simplifier la vie. Pourquoi devrait-il en être autrement pour les fournisseurs de services de sécurité d'une organisation ?

Dans une enquête récente, Gartner a constaté que 75 % des organisations envisageaient une consolidation des fournisseurs de sécurité en 2022, soit une augmentation de près de 50 % par rapport à 2020. De nombreuses sociétés sont confrontées à une surabondance de fournisseurs de sécurité. Dans la même enquête de Gartner, 43 % des organisations ont notamment révélé qu'elles travaillaient avec plus de dix fournisseurs.

Cette deuxième enquête est préoccupante pour plusieurs raisons : la multiplicité des fournisseurs coûte cher, entraîne des inefficacités opérationnelles et crée une image fragmentée des risques dans l'ensemble de votre environnement. Les équipes confrontées à un surplus d'outils peuvent également avoir du mal à définir de manière cohérente les risques, ce qui peut empêcher leur classement et entrainer une incapacité à y répondre de manière appropriée.

Au cours des dernières années, le climat économique mondial s'est transformé : l'inflation est élevée, les dépenses sont en baisse et les licenciements se sont multipliés, ce qui a conduit la plupart des organisations à réévaluer leurs habitudes de dépenses. La récente vague de licenciements dans tous les secteurs d'activité a également mis en évidence et exacerbé le manque de compétences auquel la plupart des entreprises sont confrontées. Il n'y a tout simplement pas assez de ressources pour que les entreprises disposent d'experts pour chacune de leurs solutions de sécurité ou pour qu'elles puissent entretenir des relations avec un si grand nombre de fournisseurs.

LES SOCIÉTÉS ONT BESOIN DE L'EFFICACITÉ, DES PERFORMANCES ET DE LA PRODUCTIVITÉ D'UNE APPROCHE CONSOLIDÉE.

Dans cet eBook, nous examinerons les avantages de la consolidation, ses obstacles les plus courants et les premières étapes pour la mettre en œuvre.

75 %

des organisations envisageaient de consolider leurs fournisseurs de sécurité en 2022 et

43 %

d'entre elles travaillent avec plus de dix fournisseurs de sécurité.

Gartner

AVANTAGES DE LA CONSOLIDATION

Une organisation qui envisage de consolider sa sécurité s'intéresse souvent à ce qu'elle essaie d'éviter (solutions redondantes, manque de compétences et augmentation des coûts), mais ne tient pas compte de ce qu'elle y gagnera. La plupart des entreprises se contentaient de sélectionner des solutions auprès de différents fournisseurs et de se constituer une boîte à outils de sécurité remplie à ras bord des « meilleurs produits de la catégorie ». Aujourd'hui, les sociétés constatent que cette approche crée plus de problèmes qu'elle n'en résout. Examinons quelques-uns des principaux avantages de la consolidation.

La consolidation des fournisseurs de sécurité aide les équipes à créer une vision plus holistique, de bout en bout, des risques et des menaces. Grâce à elle, les équipes ne sont plus frustrées par la multiplicité des ensembles de données et des plateformes.

Amélioration de la posture de sécurité

En 2021, IBM a publié les résultats de sa sixième étude annuelle Cyber Resilient Organization Study. L'étude révèle que 45 % des équipes de sécurité utilisent plus de 20 outils pour enquêter et répondre à un incident de cybersécurité. On pourrait penser qu'une prolifération d'outils ne peut qu'être bénéfique pour répondre à un incident de cybersécurité, mais ce n'est pas le cas. Au contraire, un trop grand nombre d'outils provenant de fournisseurs de sécurité différents peut être source de confusion. En effet, chacun d'entre eux fournit une interprétation légèrement différente mais cruciale des événements ou de la chronologie du système, ainsi que des définitions différentes du risque et de la sévérité, ce qui accapare une attention précieuse et exacerbe le syndrome de la chaise tournante. Ainsi, les équipes passent souvent beaucoup de temps à comparer des bribes de données entre les produits, au lieu de se concentrer sur l'objectif principal, qui est d'atténuer les risques.

La consolidation des fournisseurs de sécurité aide les équipes à créer une vision plus holistique, de bout en bout, des risques et des menaces. Grâce à elle, les équipes ne sont plus frustrées par la multiplicité des ensembles de données et des plateformes. Cela leur permet non seulement de répondre plus rapidement aux risques et aux vulnérabilités au sein de leur infrastructure, mais cela encourage également une plus grande collaboration entre les équipes. Une source de

vérité unique et unifiée peut aider les équipes à développer une approche proactive de la sécurité, à gérer les menaces de manière plus efficace et à prioriser les risques. Ainsi, la posture de sécurité globale de l'organisation est renforcée et l'infrastructure informatique est plus résiliente.

Réduction des coûts et amélioration du retour sur investissement

Moins, c'est plus lorsqu'il s'agit de consolider la posture de sécurité de votre organisation. Il en va de même avec l'argent économisé et les gains de retour sur investissement. L'évaluation et l'élimination des redondances dans les solutions de sécurité de votre organisation sont quelques-uns des moyens les plus simples pour économiser votre budget. En outre, une organisation typique constate qu'en réduisant le nombre de solutions, elle peut bénéficier de remises de consolidation de la part de ses fournisseurs favoris.

Grâce au budget économisé en consolidant vos solutions de sécurité, votre organisation pourra mieux se développer et se protéger contre l'évolution des cybermenaces. Les fonds économisés grâce à la rationalisation des services et à la réduction du nombre de fournisseurs peuvent être redirigés vers d'autres départements, utilisés pour former votre personnel ou investis dans les dernières technologies des fournisseurs de sécurité avec lesquels vous avez choisi de continuer à travailler. Par exemple, IBM a constaté que 77 % des organisations utilisent ou envisagent d'utiliser l'intelligence artificielle (IA). Celle-ci présente une multitude d'applications, mais la même étude a révélé que près de 30 % des organisations utilisent spécifiquement l'IA pour détecter les menaces et s'en protéger. L'argent économisé grâce à la consolidation peut donner à vos équipes informatiques la marge de manœuvre nécessaire pour apprendre à maîtriser l'IA, le machine learning et d'autres technologies émergentes sans exposer votre organisation à des risques inutiles.

La consolidation peut également permettre à votre organisation de gagner du temps dans la recherche et la réponse aux menaces. Les organisations qui utilisent plusieurs outils provenant de différents fournisseurs doivent souvent passer de l'un à l'autre pour résoudre un problème de sécurité. Un temps précieux est perdu à se connecter à différents systèmes, à transférer des données entre ces outils et à rechercher les faux positifs et les alertes redondantes. La consolidation des outils permet de rationaliser le transfert des données, de faciliter l'accès à des plateformes uniques et de réduire les « fausses » alertes. Le temps gagné grâce à la consolidation peut accroître la productivité et la satisfaction des employés, et améliorer le retour sur investissement de votre programme de sécurité.

Amélioration de l'efficacité opérationnelle

En ce qui concerne la satisfaction des employés, jongler entre plusieurs fournisseurs est une tâche complexe qui prend du temps. En réduisant votre quantité de fournisseurs, vous permettez à votre équipe de consacrer moins de temps aux contrats, aux démarches auprès du service client, aux signalements de problèmes et aux demandes d'assistance pour les nouvelles fonctionnalités.

+77 %

des organisations utilisent ou envisagent l'utilisation de l'IA et

30 %

des organisations utilisent spécifiquement l'IA pour détecter les menaces et s'en protéger.

Gartner

Elle aura également l'occasion d'établir de meilleures relations avec vos fournisseurs favoris. Selon Forbes, « pour qu'un fournisseur propose plus qu'un simple produit ou service, il doit comprendre votre activité, vos priorités et être à vos côtés en tant que client. » Lorsque vous ne jonglez pas avec une douzaine d'autres fournisseurs, il est beaucoup plus facile d'établir ce type de collaboration étroite, qui peut également déboucher sur des remises, un accès plus rapide aux nouveaux produits et un support plus complet.

En limitant votre quantité de fournisseurs, votre équipe comprendra mieux comment utiliser vos solutions de sécurité et les adapter aux besoins spécifiques de votre organisation. Par exemple, réduire votre nombre de fournisseurs simplifie et allège le temps nécessaire à la configuration et à l'installation de nouveaux produits. Par conséquent, votre équipe peut s'investir davantage dans chaque produit, apprendre à les maîtriser complètement et ainsi les optimiser pour votre infrastructure.

Au-delà de la configuration et de l'installation, lorsqu'un problème survient dans votre pile technologique, il est plus facile d'en trouver la cause et d'y remédier lorsque vous avez consolidé vos solutions de sécurité. Les organisations qui travaillent avec un grand nombre de fournisseurs et de produits rencontrent souvent des difficultés à suivre les performances de chaque application. Cela signifie qu'un produit peut ne pas fonctionner de manière optimale et que l'équipe informatique n'en est pas consciente jusqu'à ce que le problème prenne de l'ampleur, souvent avec des répercussions plus importantes sur la sécurité, comme une violation de données ou une vulnérabilité non contrôlée.

Grâce à une pile technologique moins complexe et à une meilleure visibilité, il est plus facile de s'assurer que vos applications sont conformes aux frameworks industriels et réglementaires, ce qui est crucial pour les organisations dans des secteurs très réglementés comme les services financiers et les soins de santé.

LA CONSOLIDATION VOUS PERMET DE MIEUX GÉRER LES MISES À JOUR DE VOTRE PILE TECHNOLOGIQUE ET LES AUDITS DE DONNÉES POUR ASSURER ET MAINTENIR VOTRE CONFORMITÉ.

> **Pour qu'un fournisseur propose plus qu'un simple produit ou service, il doit comprendre votre activité, vos priorités et être à vos côtés en tant que client.**
>
> Forbes

PROBLÈMES SUPPOSÉS EN MATIÈRE DE CONSOLIDATION

Si les avantages de la consolidation sont évidents, certaines organisations peuvent encore considérer que les inconvénients supposés sont une raison suffisante pour s'en tenir à l'écart. Cependant, de nombreuses objections à la consolidation sont fondées sur une mauvaise compréhension ou un manque de contexte, et deux préoccupations majeures sont souvent exprimées.

La peur de passer à côté de la « meilleure solution de la catégorie »

La première est la peur de passer à côté de la « meilleure solution de la catégorie » en matière de sécurité. Les organisations effectuent des recherches pour trouver les bons produits pour chaque domaine d'application et constatent souvent qu'un fournisseur excelle dans un domaine mais échoue dans un autre. Par conséquent, cela peut laisser à penser que la consolidation n'est pas compatible avec la qualité.

Cette préoccupation est compréhensible. Toutefois, un nombre croissant de professionnels estiment que les avantages de la consolidation sont bien plus importants que ceux d'une approche « meilleur de la catégorie ». Dans une récente enquête de Gartner, 41 % des personnes interrogées ont déclaré que l'amélioration de la posture de risque de leur organisation était le principal avantage de la consolidation de leurs solutions de sécurité. Comme mentionné plus haut, la consolidation offre des améliorations majeures en matière de sécurité, d'efficacité opérationnelle et de visibilité de bout en bout. C'est pourquoi les experts estiment aujourd'hui que la somme de ces éléments garantit une sécurité bien plus efficace que l'assemblage d'un groupe d'excellentes solutions individuelles, mais décousues.

La crainte d'un blocage avec un fournisseur

Le deuxième problème soulevé par la consolidation est la crainte d'être bloqué avec un certain fournisseur. En d'autres termes, les organisations craignent de consolider leur pile technologique et de découvrir que le fournisseur n'est pas à la hauteur ou qu'il n'est pas en mesure de tenir les promesses de sa feuille de route. Cela les contraindrait à attendre la fin de leur contrat ou de leur abonnement avant de se remettre en quête d'une solution satisfaisante.

La meilleure façon de dissiper la crainte d'une consolidation avec des fournisseurs de qualité médiocre est d'évaluer soigneusement les prestataires. Analyser les différents fournisseurs permet de s'assurer que chaque partenaire potentiel répondra à vos besoins en matière de produits, qu'il ne risque pas de faire l'objet de vulnérabilités et qu'il ne sera pas dépassé par ses concurrents en termes d'innovation.

41 %

des organisations interrogées par Gartner déclarent que la consolidation des solutions de sécurité a amélioré leur posture en matière de risques.

VOICI QUELQUES QUESTIONS À VOUS POSER LORSQUE VOUS EXAMINEZ DES FOURNISSEURS POTENTIELS.

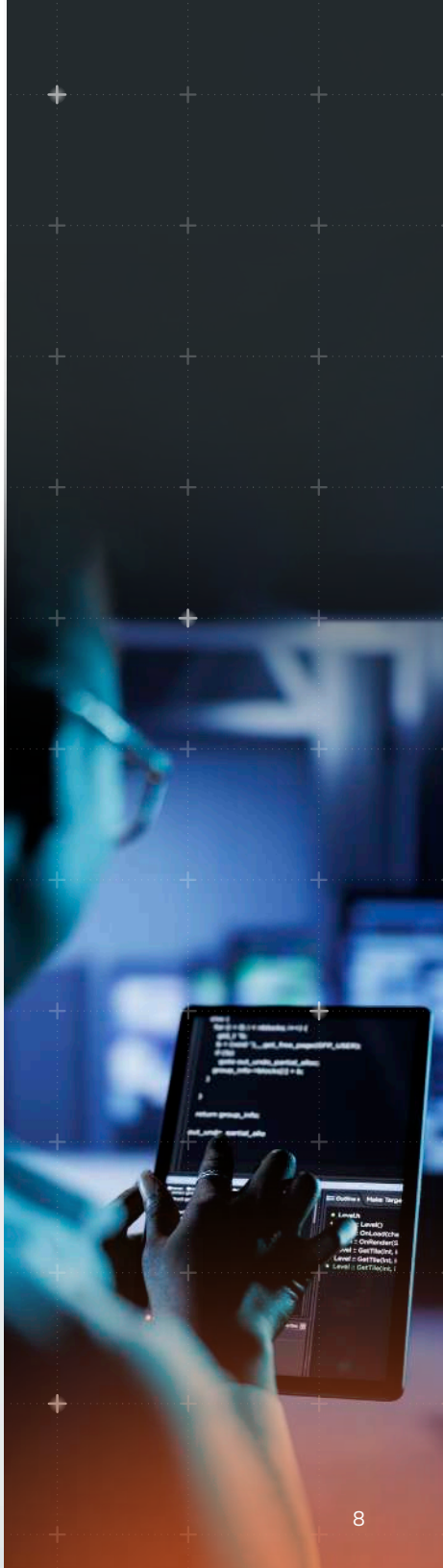
1. **Comment le fournisseur aborde-t-il la question de la sécurité ?** Vous pouvez notamment lui demander s'il fait appel à des fournisseurs tiers pour gérer la sécurité et si certaines de vos données seront stockées sur leurs systèmes, et vous renseigner sur la manière dont il a répondu aux menaces de sécurité par le passé.

2. **Quels sont les coûts à prendre en compte ?** Souvent, les fournisseurs proposent un prix qui n'inclut pas la maintenance, les frais d'abonnement supplémentaires, les ajouts de licences ou d'autres modules nécessaires à votre service. Déterminer tous les coûts potentiels peut non seulement vous aider à respecter votre budget, mais aussi éviter que votre équipe ne se sente déconcertée par des frais cachés.

3. **Dans quelle mesure leurs outils s'intègrent-ils aux systèmes de votre organisation ?** Bien que vous puissiez être impressionné par leurs offres, il est préférable d'éviter une consolidation avec un fournisseur dont les outils ne s'intègrent pas bien à vos systèmes existants. Adapter un outil à vos besoins peut demander beaucoup de temps et d'efforts, contrairement à l'achat d'une solution conçue pour prendre en charge et compléter les différents éléments de votre infrastructure informatique.

4. **Sera-t-il difficile de les intégrer ou de changer de fournisseur plus tard ?** Rien n'est éternel, et il se peut que votre organisation doive changer de fournisseur un jour ou l'autre. Dans ce cas, il est important que le processus soit fluide et sans complication. Poser les bonnes questions concernant la mise en service et l'arrêt des activités lorsque vous recherchez un fournisseur est le meilleur moyen de s'assurer que les deux phases de transition se déroulent en douceur.

Confronter votre organisation aux idées fausses sur la consolidation peut contribuer à éliminer les obstacles à l'adoption d'une approche plus efficace et plus sûre de la sécurité. Cela peut également vous aider à entamer la conversation avec les cadres et les autres services intéressés par la consolidation, mais qui se méfient de ses inconvénients supposés. Une fois ce cap franchi, il est temps de vous lancer !



CONSOLIDATION - PAR OÙ COMMENCER

Démêler le sac de nœuds de vos solutions de sécurité actuelles et de vos fournisseurs peut sembler insurmontable. Rassurez-vous ! Nous pouvons vous montrer comment mener à bien votre parcours de consolidation. Lorsque vous entreprenez cette démarche, il est important de connaître tous les outils et toutes les solutions dont vous disposez et de rassembler des informations sur les fournisseurs concernés.

De la même manière que vous avez besoin d'une visibilité de bout en bout sur votre système pour prendre des décisions solides en matière de sécurité, vous devez avoir une connaissance approfondie de votre pile technologique existante pour identifier les domaines qui bénéficieront le plus d'une consolidation.

Éviter la consolidation sur plusieurs couches

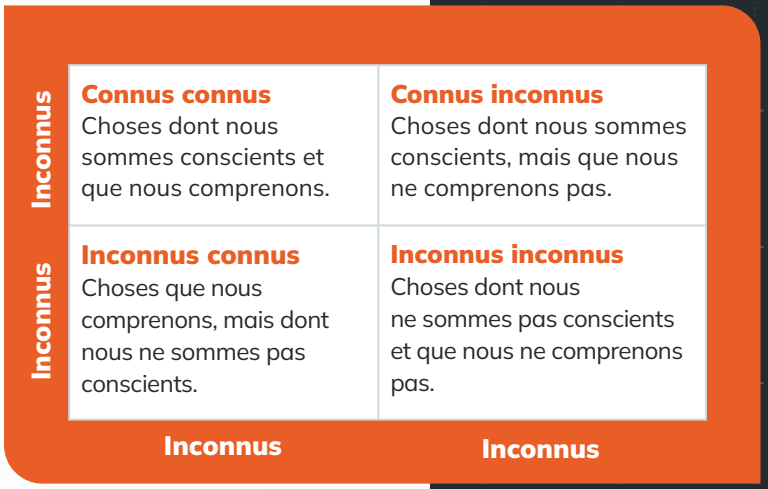
Après avoir répertorié vos ressources actuelles, vous devrez réfléchir à la bonne manière de les consolider. Nous vous suggérons de consolider les fonctions et non les couches. En d'autres termes, votre infrastructure comporte des couches de sécurité, ou des redondances pour détecter les vulnérabilités, dans le cadre d'une stratégie que beaucoup appellent « défense en profondeur ». Par exemple, cela peut prendre la forme d'une solution de sécurité qui surveille les terminaux et d'une solution distincte qui gère les menaces dans l'ensemble de l'écosystème.

Alors pourquoi ne pas consolider les différentes couches ? Une telle approche peut en réalité affaiblir votre posture de sécurité, en éliminant les redondances utiles au sein de votre système. Les principes de conception sécurisée permettent de gérer le risque d'un contrôle « défaillant » grâce à la redondance. Compte tenu de la complexité de l'infrastructure hybride moderne, la défense en profondeur n'est pas seulement une bonne pratique, c'est aussi une nécessité. Par exemple, confier la sécurité de vos systèmes d'exploitation (ainsi que les solutions de maintenance et de mise à jour associées) au même fournisseur que votre solution de détection et de réponse aux terminaux non seulement brouille les lignes de partage des tâches, mais peut également entraîner un risque systémique incontrôlé. Non seulement les terminaux de l'organisation sont vulnérables, mais vous dépendez également du même fournisseur pour corriger « leur propre » faiblesse.

Consolidation des fonctions

La consolidation des fonctions est l'approche privilégiée. Au moment de choisir les fonctions à consolider, il est judicieux d'examiner vos besoins en matière de sécurité dans un domaine particulier. Par exemple, une organisation confrontée à la surface d'attaque croissante générée par sa volonté d'innover dans le domaine du cloud pourrait envisager de consolider les fonctions suivantes : sécurité cloud, gestion des vulnérabilités et sécurité des applications. Regrouper ces fonctions chez un même fournisseur permet d'offrir une meilleure visibilité et une surveillance accrue pour une gestion plus complète des risques liés au cloud.

Il peut également être utile de consolider les fonctions au sein d'une couche. Dans ce cas, il convient d'examiner les objectifs de l'organisation au sein d'une couche particulière et d'identifier les fonctions à consolider. Cela pourrait prendre la forme d'une organisation qui rendrait opérationnel son programme de détection et de réponse ou le ferait évoluer en consolidant les fonctions suivantes : détection et réponse, threat intelligence et gestion des vulnérabilités. Il en résulte une approche plus globale de la gestion des risques.



Trouver les bons outils

Une fois que vous avez identifié les meilleures fonctions à consolider, ou la façon dont vous souhaitez aborder la consolidation des fonctions au sein des différentes couches, vous devez déterminer les offres et les outils les mieux adaptés à votre organisation.

Si vous souhaitez sécuriser votre migration vers le cloud, voici quelques-unes des fonctionnalités les plus importantes à rechercher dans les offres et les solutions de consolidation :

- **Workflows automatisés :** si l'objectif de la consolidation est de simplifier les efforts de sécurité de votre organisation, l'automatisation est essentielle. En veillant à ce que votre package de consolidation comprenne des workflows et des contrôles automatisés, s'assurant par exemple qu'aucun bucket S3 n'est défini comme public, vous aiderez votre équipe à répondre plus rapidement aux menaces et à réduire le risque global dans votre infrastructure.
- **Hiérarchisation des risques :** la consolidation peut éviter la confusion causée par des flux de données multiples provenant de différentes solutions, mais vous devez également trouver un outil qui apporte le contexte nécessaire pour classer les signaux de risque dans l'ensemble de votre écosystème. Il s'agit notamment des solutions qui permettent à votre équipe de déterminer quels ports indésirables sont ouverts sur vos actifs publics.
- **Automatisation de la conformité :** votre solution consolidée doit vous aider à respecter les réglementations internes et externes en matière de conformité en détectant les lacunes et en y remédiant. Les outils qui surveillent et appliquent les réglementations spécifiques à votre secteur tout en travaillant de concert avec vos workflows pour garantir une conformité continue sont à privilégier.

- **Scanning de sécurité :** le paysage des menaces évolue constamment, c'est pourquoi le scanning et le test continus des applications de votre infrastructure sont essentiels à votre stratégie de sécurité. Une offre de consolidation idéale devrait fournir à votre organisation des évaluations de sécurité en temps réel, des rapports détaillés pour une meilleure collaboration entre les équipes, et des informations utiles sur l'évolution des risques. Les meilleurs outils veilleront également à ce que votre équipe soit consciente des quatre principaux types de risques dans votre système : les risques connus, les risques connus inconnus, les risques inconnus connus et les risques inconnus inconnus..

En revanche, si votre priorité est de développer votre programme de détection et de réponse en recourant à la sous-traitance, voici quelques fonctionnalités critiques à rechercher :

- **Couverture complète :** lorsque vous consolidez votre programme de détection et de réponse, vous devez pouvoir être sûr que l'ensemble de votre surface d'attaque est sous contrôle. Cela signifie que vous devez disposer d'outils offrant une couverture complète de vos terminaux, de votre réseau, de vos utilisateurs et du cloud, afin de pouvoir éliminer les menaces dans l'ensemble de votre environnement.
- **Partenariat transparent :** une bonne offre de consolidation gérée doit être un véritable partenariat. Vous devez pouvoir compter sur une collaboration fluide avec des experts, afin d'obtenir des réponses à tout moment et de pouvoir savoir exactement ce que l'équipe SOC externe voit.
- **Détection et réponse de bout en bout :** une offre consolidée de détection et de réponse doit aller au-delà de ces fonctions élémentaires. Vous devez choisir une solution qui vous assiste tout au long du processus, avec une investigation numérique de bout en bout et une intervention complète en cas d'incident.

Une fois que vous avez identifié les bons outils et packages de consolidation, vous pouvez les affecter aux domaines de votre organisation qui, selon vous, ont le plus besoin d'être consolidés. Il est judicieux de discuter de vos objectifs avec vos fournisseurs potentiels, afin qu'ils puissent vous aider à identifier les meilleures offres, voire à créer une solution personnalisée.

CONCLUSION : SOLUTION DE SÉCURITÉ JENGA®

En matière de consolidation, certaines organisations ont tendance à rester sur leurs positions. Si les avantages de la consolidation sont évidents, les équipes s'inquiètent des perturbations potentielles liées à l'introduction de nouveaux produits dans leur environnement ou à l'abandon de solutions existantes. C'est comme une partie de Jenga®. Au lieu de blocs de bois, les organisations construisent une solution de sécurité instable, et bien qu'elle soit bancale et encombrée de dysfonctionnements, de redondances et de coûts croissants, il est toujours difficile de s'en séparer.

Cependant, le paysage des menaces évolue rapidement et la consolidation offre les améliorations de sécurité dont une organisation a besoin pour faire pencher la balance en sa faveur. Il est temps de simplifier et de rationaliser votre solution de sécurité, et cela commence par une meilleure visibilité sur votre pile technologique et par l'identification des domaines dans lesquels la consolidation peut renforcer la productivité et l'efficacité de votre équipe en matière de détection et d'atténuation des risques.

VOUS SOUHAITEZ CONSOLIDER VOTRE PILE TECHNOLOGIQUE ? RAPID7 EST LÀ POUR VOUS AIDER.

Rapid7 Command Platform unifie les capacités de gestion de l'exposition et de détection et réponse en une solution SecOps centralisée et complète, permettant aux organisations de sécuriser leurs environnements hybrides et de maîtriser leur surface d'attaque. En unifiant la gestion de l'exposition et les workflows de détection et de réponse aux menaces, les équipes accélèrent les décisions grâce à une compréhension approfondie du comportement de l'attaquant pour atténuer les expositions et faciliter la réponse. Command Platform renforce la résilience en matière de sécurité des organisations de toutes tailles grâce à deux solutions sur mesure : **Exposure Command** et **Managed Threat Complete**.

Exposure Command offre une visibilité complète sur l'ensemble de votre environnement numérique, de l'intérieur comme de l'extérieur, en rassemblant la télémétrie et le contexte de tout votre écosystème d'outils pour identifier les lacunes de contrôle et établir une source unique de vérité. En enrichissant la visibilité de la surface d'attaque sur les

actifs locaux, le cloud et les applications avec un contexte de haute fidélité sur le risque et l'exposition, les équipes peuvent prioriser efficacement les efforts de remédiation en fonction des actions qui auront le plus grand impact sur la réduction de leur posture de risque globale. Les workflows d'automatisation natifs sans code permettent aux équipes d'agir rapidement lorsque des expositions validées sont détectées et de fournir des conseils de remédiation exploitables aux parties prenantes de leur organisation.

Managed Threat Complete est l'un des premiers programmes MDR à offrir une gestion complète et avancée de l'exposition, intégrée directement dans votre pile d'outils MDR, permettant aux équipes de réduire de manière proactive leur surface d'attaque et de répondre aux menaces dans leur environnement hybride. Managed Threat Complete aide les organisations à consolider leur programme de sécurité et à reconnaître les gains d'efficacité dans les principales initiatives de sécurité, notamment MDR, SOAR, VRM, DFIR, SIEM, DRP, et plus encore, le tout avec un abonnement unique. Managed Threat Complete permet aux équipes de sécurité de protéger leurs organisations contre les menaces accélérées dès leur apparition, 24h/24, sans aucune limite en matière d'ingestion de données, d'analyse des vulnérabilités ou de réponse aux incidents.

À propos de Rapid7

Rapid7 contribue à créer un avenir numérique plus sûr pour tous en aidant les organisations à renforcer leurs programmes de sécurité face à l'accélération de la transformation numérique. Notre portefeuille de solutions de pointe permet aux professionnels de la sécurité de gérer les risques et d'éliminer les menaces dans l'ensemble du spectre des activités, des applications au cloud en passant par l'infrastructure classique et le dark web. Nous soutenons les mouvements open source et la recherche d'avant-garde en utilisant ces informations pour optimiser nos produits et doter la communauté mondiale de la sécurité des dernières méthodes utilisées par les attaquants. Plébiscités par plus de 11 000 clients à travers le monde, nos solutions et services novateurs aident les entreprises à garder une longueur d'avance sur les attaquants, à devancer la concurrence et à se préparer pour l'avenir.

RAPID7

PRODUITS

Sécurité Cloud
XDR et SIEM
Threat intelligence
Gestion des risques liés aux vulnérabilités
Sécurité des applications
Orchestration et automatisation
Services managés

SERVICE CLIENT

Appelez-nous au
+1 866 380 8113

Pour en savoir plus ou commencer un essai gratuit, rendez-vous sur https://www.rapid7.com/try/insight/

© RAPID7 2025 V2.0