Pourquoi une plateforme de cybersécurité complète surpasse les solutions ponctuelles

Barracuda

Alors que les technologies émergentes continuent d'atteindre de nouveaux niveaux de sophistication et de prouesse, les cyberattaquants ont accès à un ensemble d'outils de plus en plus puissants. Le rapport Global Cybersecurity Outlook 2025 du Forum économique mondial affirme que les entreprises évoluent « dans un cyberespace complexe, caractérisé par des incertitudes géopolitiques, des inégalités croissantes en matière de cybersécurité et des cybermenaces de plus en plus sophistiquées ». Cet environnement aggrave les défis auxquels les entreprises de toutes tailles sont déjà confrontées pour sécuriser leur cyberinfrastructure.

De nombreuses entreprises actuelles s'appuient sur un patchwork complexe de solutions ponctuelles pour protéger leurs actifs de ces menaces. Les recherches de Barracuda révèlent que 65 % des organisations estiment qu'elles ont trop d'outils de sécurité à gérer. Cela s'accompagne de nombreux défis, que nous explorerons dans cet eBook. Cependant, il existe également des entreprises qui adoptent une approche plus consolidée, en utilisant une plateforme unique et globale. Poursuivez votre lecture pour découvrir pourquoi cela pourrait être la solution à toute une série de défis en matière de cybersécurité auxquels des organisations comme la vôtre sont confrontées.

Qu’est-ce qu’une solution ponctuelle ?

Une solution ponctuelle est un outil spécialisé qui exécute une fonction précise, répondant à un besoin unique d’une organisation. Le magazine PC Mag définit une solution ponctuelle comme une solution qui « résout un problème particulier sans tenir compte des problèmes connexes. Les solutions ponctuelles sont largement utilisées pour résoudre un problème ou mettre en œuvre rapidement un nouveau service. »

Voici quelques exemples de solutions ponctuelles :

- Pare-feux
- Outils de sécurité des emails
- Logiciel antivirus
- Outils de gestion des identités et des accès (IAM)
- Scanners de vulnérabilités

Les solutions ponctuelles peuvent jouer un rôle positif dans le renforcement de la cybersécurité d’une organisation. Beaucoup proposent des fonctionnalités de pointe qui contribuent à assurer la sécurité. Un problème se pose toutefois lorsque ces solutions ponctuelles deviennent difficiles, voire impossibles, à intégrer.

Les inconvénients des solutions ponctuelles

Selon le rapport 2024 de CDW Cybersecurity Report: Challenges, Staffing, Tools & More, « la grande majorité des organisations (68 %) utilisent entre 10 et 49 outils ou plateformes de sécurité ». Un rapport d'IBM, intitulé Capturing the cybersecurity dividend, cite un chiffre encore plus élevé : en moyenne 89 solutions de sécurité provenant de 29 fournisseurs différents. Les organisations qui utilisent autant d'outils pour se défendre contre les cyberattaques se retrouvent à gérer un environnement complexe et tentaculaire.

Cela pose une série de problèmes. Tout d'abord, il faut consacrer du temps et des efforts à la surveillance de chaque outil, ainsi qu'à la vérification de son bon fonctionnement et de l'efficacité des protections et mesures correctives mises en place. Cela nécessite une supervision et des compétences importantes, qui font défaut sur le marché actuel des talents : le rapport Global Cybersecurity Outlook 2025 du Forum économique mondial souligne que « seulement 14 % des organisations estiment actuellement disposer des effectifs et des compétences nécessaires ».

Ensuite, il y a la difficulté d'intégrer les outils, même si cette intégration est vitale pour obtenir une source fiable unique pour l'analyse des données. Comme Forbes le précise, « chaque solution ponctuelle doit être intégrée à d'autres systèmes ponctuels. À mesure que le nombre de systèmes ponctuels augmente, le besoin d'intégrations de systèmes et de données augmente ». Mais tous les outils ne s'intègrent pas aux autres. Nos recherches montrent que plus de la moitié (53 %) des organisations affirment que leurs outils ne peuvent pas être intégrés.

Le manque d'intégration et d'interopérabilité n'est pas seulement inefficace : il engendre également des coûts. Charles Henderson, ancien responsable de l'unité X-Force d'IBM Sécurité, a déclaré à Cybersecurity Dive : « Nous en sommes à un stade en cybersécurité où les solutions ponctuelles qui ne fonctionnent pas ensemble représentent une perte de plus en plus importante pour nos clients... Lorsqu'elles opèrent de manière isolée, le temps et l'argent investis dans ces solutions ne sont tout simplement pas rentables. »

Ce ne sont pas les seuls défis auxquels sont confrontées les organisations qui utilisent un large éventail de solutions ponctuelles. Mais l'impossibilité de les gérer, le manque d'intégration et l'augmentation des coûts suffisent à pousser de nombreuses entreprises à chercher une alternative. Une plateforme de cybersécurité constitue une meilleure option.

Qu’est-ce qu’une plateforme de cybersécurité ?

Une plateforme de cybersécurité est un système centralisé qui intègre la sécurité et la gestion de l’infrastructure numérique d’une entreprise. Elle offre une solution unique, intégrée et globale qui assure toutes les fonctions de cybersécurité nécessaires à une organisation.

Les plateformes de cybersécurité offrent également une vue d’ensemble des menaces, des alertes, des réponses et de l’analyse post-événement, en consolidant les données dans un endroit facile d’accès. Elles sont évolutives et flexibles, et incluent généralement des fonctionnalités d’automatisation ainsi que de détection et de réponse alimentées par l’IA.

Les avantages d'une plateforme de cybersécurité

Les plateformes de cybersécurité offrent de nombreux avantages, en particulier pour les utilisateurs qui migrent depuis une solution multipoint complexe et difficile à gérer. L'un des principaux avantages de l'utilisation des plateformes est la rapidité avec laquelle elles peuvent détecter les menaces et y remédier. Il est essentiel de détecter rapidement les menaces, car plus une menace reste tapie longtemps dans votre environnement, plus le cyberattaquant peut causer de dégâts en se déplaçant dans le réseau.

Outre une détection et une réponse plus rapides, les plateformes de cybersécurité offrent un meilleur retour sur investissement que les solutions ponctuelles. Le même rapport d'IBM a révélé que les plateformes « génèrent également un retour sur investissement moyen de 101 %, contre 28 % pour les organisations qui ne les ont pas encore adoptées ». L'approche simplifiée et centralisée d'une plateforme diminue également la dépendance à un personnel spécialisé, dont les exigences salariales sont élevées et dont le recrutement peut s'avérer difficile dans un marché très concurrentiel. C'est un autre exemple de la façon dont le choix de la bonne plateforme peut réduire les coûts liés à la cybersécurité.

La facilité d'utilisation est un avantage significatif des plateformes de cybersécurité. Grâce à la consolidation des solutions et des fournisseurs, les organisations bénéficient d'une réduction des efforts manuels et de l'administration. En revanche, les exigences sont beaucoup plus élevées pour ceux qui utilisent plusieurs solutions de différents fournisseurs. L'analyse des données avec les plateformes est également plus facile, grâce à l'environnement simplifié et rationalisé. En outre, le service client est plus fluide, puisqu'il n'y a qu'un seul interlocuteur pour toutes les questions ou préoccupations.

Barracuda

Cinq étapes pour réussir la transition vers une plateforme de cybersécurité

Si votre organisation est prête à passer à une plateforme de cybersécurité, prenez le temps de préparer sa mise en œuvre en suivant cette approche en cinq étapes.

Évaluez votre portefeuille actuel d'outils de cybersécurité

Avant de vous lancer dans la consolidation et l'optimisation de votre pile de sécurité avec une plateforme de cybersécurité, il est essentiel de commencer par évaluer l'état actuel de votre portefeuille d'outils. Entreprenez un audit complet en cataloguant vos outils. Faites l'inventaire de leurs fonctions et de la manière dont votre entreprise les utilise. Identifiez les chevauchements et les outils inutilisés.

Examinez les accords de niveau de service et les contrats des fournisseurs

Examinez attentivement les contrats et les accords de niveau de service (SLA) de vos outils actuels. Cela vous aidera à identifier la durée du contrat, les clauses de résiliation, les pénalités financières et les outils qui approchent de la fin du cycle de renouvellement, afin de ne pas renouveler inutilement des outils que vous n'utiliserez plus. À ce stade, vous pouvez commencer à consolider vos fournisseurs en vue de la transition vers une plateforme.

Élaborez un argumentaire solide

Pour obtenir l'adhésion des parties prenantes à l'adoption d'une plateforme, il est important de communiquer clairement la raison de la transition. Cela signifie non seulement décrire les avantages, mais aussi le retour sur investissement potentiel. Vous pouvez générer ces informations à l'aide d'outils tels que le calculateur de retour sur investissement du Gartner. Les domaines à prendre en compte lors du calcul du retour sur investissement sont la réduction des dépenses en outils dupliqués, la réduction des coûts de gestion des fournisseurs, le gain de temps et les gains d'efficacité grâce à la simplification de la surveillance, de l'analyse des données et de la prise de décision. Présentez la transition vers une plateforme comme une démarche stratégique visant à renforcer la sécurité tout en réduisant les coûts, les charges administratives et les goulots d'étranglement liés à l'analyse des données.

Identifiez le bon moment pour une transition

Il est important de choisir le bon moment pour recentrer vos efforts de cybersécurité autour d'une approche basée sur une plateforme. Planifiez la transition vers votre plateforme en la synchronisant avec des étapes clés, comme l'expiration de contrats importants pour vos autres outils, les cycles de planification fiscale ou tout autre calendrier de transformation technologique prévu. Un bon timing peut vous aider à minimiser les perturbations et à éviter de payer trop cher pour des solutions redondantes, ce qui peut être un problème si vous avez de nombreux contrats qui se chevauchent.

Évaluez la nécessité d'un modèle de service géré

Si votre organisation manque de compétences internes ou les perd, les fournisseurs de services gérés peuvent prendre en charge le déploiement et la gestion de votre plateforme de cybersécurité. Ils peuvent offrir une surveillance 24/7, une réponse aux incidents experte et des conseils avisés pour vous aider à soutenir votre stratégie et vos efforts de cybersécurité. Cela peut répondre aux défis liés à la pénurie de compétences à un moment où les talents en cybersécurité sont rares, coûteux et difficiles à retenir.

Découvrez comment Barracuda peut vous aider

Barracuda propose une plateforme de cybersécurité alimentée par l'IA qui maximise votre protection et renforce votre cyberrésilience. BarracudaONE protège votre entreprise des menaces qui pèsent sur vos emails, vos données, vos applications et vos réseaux. Il unifie vos solutions dans un tableau de bord centralisé, offrant une détection et une réponse approfondies et intelligentes aux menaces. Découvrez comment BarracudaONE peut améliorer votre cybersécurité ou planifiez une démo dès aujourd'hui.

Barracuda en quelques mots

Barracuda est une entreprise de cybersécurité leader sur son marché, offrant aux entreprises de toutes tailles une protection complète face aux menaces complexes. Notre plateforme BarracudaONE, propulsée par l'IA, sécurise les emails, les données, les applications et les réseaux grâce à des solutions innovantes, un XDR managé et un tableau de bord centralisé afin de maximiser la protection et renforcer la résilience cyber. Des centaines de milliers d'organisations et de fournisseurs de services managés (MSP) du monde entier nous font confiance pour les protéger et les accompagner, avec des solutions faciles à acquérir, déployer et utiliser. Pour plus d'informations, visitez fr.barracuda.com.

Barracuda