Préparé pour

riverbed

La convergence des opérations réseau et de sécurité

Livre blanc EMA d'avril 2021
par Shamus McGillicuddy

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Synthèse

La collaboration des équipes des opérations réseau et de sécurité est toujours positive pour l'entreprise. L'étude d'EMA a révélé que de nombreuses entreprises encouragent cette collaboration, au point de fusionner les deux groupes. Une telle collaboration permet de réduire les risques et les coûts, de stimuler la productivité et de rendre l'entreprise IT plus réactive aux besoins de l'organisation. Ce livre blanc donne des indications sur la manière d'encourager cette collaboration et identifie certains pièges à éviter.

Les équipes des opérations réseau de l'entreprise s'associent à la sécurité IT

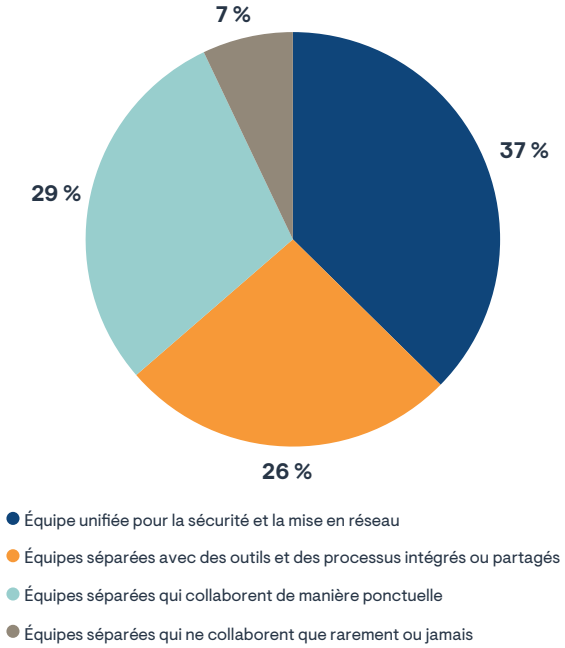
De nos jours, nul responsable réseau ne peut ignorer la sécurité. Par exemple, la sécurité est souvent responsable, tout en en partie, des problèmes et pannes de services IT complexes qui nécessitent un diagnostic interdomaine. Selon une étude d'Enterprise Management Associates (EMA), parmi les causes les plus fréquentes de ces problèmes complexes, les systèmes de sécurité (défaillance d'un équipement ou règle inadéquate) occupent la troisième place, et les incidents de sécurité (attaques ou brèches) la quatrième (l'infrastructure réseau étant la première cause et les erreurs système ou utilisateur côté client final, la deuxième).[1] Ne serait-ce que pour cette raison, l'équipe réseau doit être sensibilisée à la sécurité pour pouvoir désengager sa responsabilité, car le réseau est souvent le premier à être pointé du doigt en cas de problème de service.

La sécurité est un moteur stratégique majeur de la gestion réseau. Par exemple, depuis plus de dix ans, la sécurité réseau occupe la première place dans les initiatives technologiques qui influencent les priorités de gestion réseau. Et 2020 ne déroge pas à cette règle. Lorsque EMA a demandé aux responsables réseau d'identifier les marqueurs de plus en plus importants pour mesurer la réussite des opérations réseau, la réduction des risques de sécurité a été citée plus souvent que la qualité de service, l'amélioration de la visibilité réseau et les performances applicatives.

Il n'est donc pas surprenant que les équipes de gestion réseau se rapprochent des groupes de sécurité afin de renforcer la collaboration et d'améliorer la visibilité et la réactivité globales. En fait, 89 % des responsables réseau déclarent avoir augmenté leur niveau de collaboration avec les équipes de sécurité de leur organisation au cours des deux dernières années, contre 42 % en 2018. Cet effort de collaboration se traduit par des changements organisationnels. Trente-sept pour cent des entreprises déclarent avoir fusionné leurs équipes de gestion du réseau et de la sécurité, en les dotant d'outils et de processus partagés. Vingt-six pour cent d'entre elles continuent à fonctionner avec des équipes de gestion du réseau et de la sécurité distinctes, mais ont intégré des outils ou des processus qui facilitent leur collaboration.

[1] Toutes les données citées dans ce livre blanc proviennent de l'étude d'EMA intitulée « Network Management Megatrends 2020: Enterprises Embrace NetSecOps, the Internet of Things, and Streaming Telemetry », publiée en avril 2020.

Figure 1. Liens de collaboration entre les équipes de gestion du réseau et de la sécurité des informations d'aujourd'hui



Cette collaboration a de vastes répercussions. Les entreprises y voient une occasion d'intégrer la sécurité dans l'ADN de leurs réseaux. Les responsables réseau affirment que, stratégiquement, le point de collaboration le plus important avec l'équipe de sécurité concerne l'amélioration de la performance réseau, suivie de la réduction des risques et de l'accélération de la détection des incidents de sécurité et de leur réponse.

Stratégies en matière d'outils de collaboration avec la sécurité IT

L'équipe de gestion réseau doit développer une stratégie en matière d'outils afin de s'acquitter de son mandat de collaboration avec le groupe de sécurité. EMA recommande une approche intégrée. L'équipe réseau doit chercher des moyens d'enrichir ses outils existants plutôt que d'en ajouter de nouveaux, autonomes qu'il faudra installer, maintenir et apprendre à utiliser, avec une intégration limitée aux workflows et ensembles de données réseau. Les responsables réseau tireront plus d'avantages d'un outil de gestion ou de surveillance de la sécurité qui partage des jeux de données avec les outils existants des opérations réseau et offre une vue intégrée sur la performance réseau et la surveillance de la sécurité.

Une des raisons pour laquelle EMA recommande cette approche est que les boîtes à outils de gestion réseau sont déjà saturées et fragmentées. Plus le nombre d'outils de gestion est important, plus l'infrastructure est complexe et son administration onéreuse, ce qui peut avoir un impact négatif sur l'efficacité globale. Chaque année, les entreprises affirment souhaiter réduire le nombre d'outils qu'elles utilisent, mais EMA n'avait constaté aucun progrès sur ce front avant 2020. Bien que ce nombre ait diminué par rapport aux résultats de 2018, l'enquête de 2020 a révélé que 64 % des équipes des opérations réseau utilisent encore 4 à 10 outils pour surveiller et diagnostiquer leurs réseaux. Et 17 % des équipes en utilisent 11 ou plus.

Un ensemble d'outils important ne va pas nécessairement rendre inefficace l'équipe des opérations réseau. Ils sont souvent nécessaires. De nombreuses organisations acquièrent de grandes boîtes à outils pour gérer des réseaux lourds et complexes qui sont intrinsèquement plus difficiles à exploiter. En fait, plus de la moitié des entreprises (54 %) qui utilisent 11 outils de gestion réseau ou plus déclarent que leurs opérations réseau produisent des résultats positifs, contre 28 % des entreprises utilisant 1 à 3 outils et 29 % des entreprises utilisant 4 à 5 outils. Toutefois, EMA recommande une consolidation et une intégration chaque fois que cela est possible.

Outils de gestion réseau qui favorisent la collaboration dans le domaine de la sécurité

L'étude d'EMA a identifié trois types d'outils de gestion réseau essentiels pour permettre la collaboration avec les groupes de sécurité. Le premier est un outil de surveillance de l'infrastructure réseau, qui collecte les metrics des équipements via SNMP, les API des équipements, etc., et détecte une activité inhabituelle sur un équipement réseau, comme la saturation d'une interface par une attaque. Selon EMA, la surveillance de l'infrastructure réseau est l'outil de collaboration qui a la préférence des équipes réseau intégralement unifiées avec les équipes de sécurité, mais que les équipes qui collaborent de manière ponctuelle adoptent moins volontiers.

Le deuxième outil de collaboration le plus important dans le domaine de la sécurité est l'automatisation/orchestration du réseau. Les outils d'automatisation réseau permettent aux entreprises de modifier rapidement le réseau pour répondre à un événement lié à la sécurité. Ils facilitent également l'application des règles de contrôle des changements, qui réduisent le risque d'introduction de vulnérabilités en cas de modification du réseau erronée.

Le troisième outil de collaboration le plus important dans le domaine de la sécurité est la surveillance des flux réseau (NetFlow, sFlow, IPFIX, etc.). La surveillance des flux offre une vue de haut niveau sur les modèles d'activité et de trafic réseau. L'analyse sophistiquée des flux peut révéler des modèles de comportements suspects, et même les comportements types des menaces connues.

Les fonctionnalités de sécurité des outils de gestion réseau facilitent la collaboration des équipes des opérations de sécurité réseau

L'étude d'EMA a révélé que la majorité des équipes réseau (97 %) souhaitent utiliser les fonctionnalités de sécurité de leurs fournisseurs de gestion de réseau afin de favoriser la collaboration. Pour 30 % d'entre elles, cela occupe même une place stratégique dans leurs efforts de collaboration avec le groupe de sécurité. Ces capacités comprennent la collecte de renseignements, des fonctionnalités ou des produits dédiés à la sécurité.

Ces capacités de sécurité des outils de gestion réseau sont potentiellement essentielles pour la collaboration des équipes des opérations de sécurité réseau. Cependant, les entreprises doivent s'assurer qu'elles peuvent être intégrées avec les données et les workflows de leurs outils de gestion réseau, même si elles adoptent des produits de sécurité distincts de ce fournisseur de gestion réseau.

EMA a demandé aux personnes qui souhaitent avoir des capacités de sécurité intégrées à leurs solutions de gestion réseau où elles aimeraient les voir s'appliquer. Le data center a pris la première place avec 47 %, suivi des charges de travail cloud avec 43 % et de l'équipement IoT avec 39 %. Parmi les autres priorités, on comptait les applications SaaS (31 %), les sites distants/succursales et l'équipement des utilisateurs finaux/BYOD (28 %).

Bénéfices et défis liés à une gestion convergée du réseau et de la sécurité

Les entreprises ont beaucoup à gagner à la fusion et à la collaboration de leurs équipes de gestion de réseau et de la sécurité, mais y parvenir ne sera pas chose facile. L'étude d'EMA a identifié les quatre principaux défis de cette collaboration. Avant toute chose, les groupes responsables de la mise en réseau et de la sécurité ne partagent pas les mêmes objectifs, selon 31 % des responsables réseau. En effet, ces équipes ne sont pas nécessairement des partenaires naturels et vont souvent dans des directions opposées. L'équipe réseau se concentre sur la connectivité en fournissant aux employés, aux partenaires et aux clients un accès aux applications, aux données et aux services. L'équipe de sécurité, quant à elle, s'emploie à verrouiller les données et à limiter la connectivité aux applications. Il est donc important de reconnaître les défis auxquels les organisations IT sont confrontées lorsque ces équipes tentent de collaborer. Un solide leadership sera donc nécessaire pour assurer la réussite de la collaboration. Si ce leadership est inexistant au sein de ces deux groupes, ils doivent se tourner vers les dirigeants IT pour obtenir un soutien et une orientation.

Principaux obstacles à une collaboration fructueuse entre les équipes réseau et de sécurité

1. Objectifs conflictuels
2. Écarts de compétences entre les équipes
3. Différends au sujet du partage et de la propriété des données
4. Qualité et pertinence des données

Les écarts de compétences entre les équipes (29 %) constituent également un problème important. Il est fréquent que les membres d'une équipe ne possèdent pas les compétences et l'expérience requises pour utiliser la technologie, les outils et les processus sur lesquels s'appuient leurs homologues de l'autre équipe. Ce défi est d'autant plus présent au sein des équipes IT spécifiques. Les équipes des opérations réseau efficaces sont moins susceptibles d'être confrontées à ces écarts de compétences (21 %). Un autre obstacle tout aussi problématique est que les outils ne sont pas suffisamment adaptés pour la collaboration, selon 29 % des personnes interrogées. Pour résoudre ce problème, les outils de gestion réseau auront besoin de workflows et de fonctionnalités qui facilitent la collaboration et fournissent des renseignements sur la sécurité.

Vingt-sept pour cent d'entre elles sont aux prises avec d'importants conflits concernant le partage et la propriété des données. Chacune des équipes peut se montrer ultra-protectrice des données qu'elle extrait du réseau, tant du côté sécurité que du côté réseau de l'entreprise. EMA suggère que, pour résoudre ce problème, les dirigeants IT doivent établir un programme de coopération. Par ailleurs, 27 % des équipes de mise en réseau et de sécurité signalent des problèmes majeurs concernant la qualité des données qu'elles partagent. Pour remédier au dilemme des données obsolètes ou incohérentes, les équipes responsables du réseau et de la sécurité doivent trouver des moyens d'unifier leur collecte de données et les outils qu'elles utilisent pour les analyser, dans la mesure du possible.

Bénéfices de la collaboration entre les équipes réseau et de sécurité

Lorsque les équipes de gestion du réseau et de la sécurité partagent des outils, combinent des données et collaborent, les bénéfices pour l'entreprise sont nombreux. L'étude d'EMA a identifié les cinq principaux moteurs de cette collaboration. Premièrement, 39 % des entreprises IT sont convaincues que la fusion des équipes réseau et de sécurité se traduira par une amélioration de la performance réseau. En fait, les entreprises qui ont unifié leurs équipes réseau et de sécurité ont plutôt tendance à améliorer la performance réseau (48 %).

Le deuxième moteur de cette collaboration est la réduction des risques (34 %). Avec des processus adéquats et une intégration efficace des outils, les entreprises IT obtiendront une meilleure visibilité sur le réseau et pourront améliorer son intégrité globale. Les responsables réseau qui collaborent avec les responsables de la sécurité auront tendance à commettre moins d'erreurs de conception, de configuration et de modification du réseau qui pourraient introduire des vulnérabilités. En outre, l'équipe de sécurité imposera peut-être moins de contrôles de sécurité pouvant dégrader la santé et la performance du réseau.

Troisièmement, 32 % des entreprises IT espèrent détecter les incidents de sécurité et y répondre plus rapidement. Leur fusion peut accélérer leur capacité à identifier les incidents et à y remédier. La simplification des workfows réduit également le temps consacré par les ingénieurs hautement qualifiés à la réponse aux incidents pour leur permettre de se concentrer sur des projets stratégiques. Ainsi, de nombreuses entreprises IT visent l'efficacité des coûts opérationnels (27 %).

Principaux moteurs de la collaboration entre les équipes de gestion réseau et de la sécurité

1. Performance réseau améliorée
2. Réduction des risques de sécurité
3. Détection des incidents de sécurité et réponse plus rapides
4. Efficacité des coûts opérationnels

Le point de vue d'EMA

Collaborer avec l'équipe de sécurité ne sera pas toujours une chose facile pour les responsables réseau. Il y a des obstacles techniques et culturels à surmonter, mais les bénéfices potentiels sont difficiles à ignorer. L'étude d'EMA montre clairement que les entreprises reconnaissent non seulement l'importance de cette collaboration, mais que les équipes responsables des opérations réseau travaillent aujourd'hui plus étroitement que par le passé avec les équipes responsables de la sécurité des informations. Les partenariats commencent par de simples conversations, et s'étendent progressivement à des analyses techniques des processus et des technologies que chaque groupe utilise pour assumer ses responsabilités envers l'entreprise. Chaque équipe doit faire des concessions et peut-être même céder le contrôle à l'autre groupe.

Les outils auront un rôle majeur à jouer. Les équipes réseau et de sécurité doivent identifier les possibilités de partager et d'intégrer leurs systèmes de gestion et de surveillance, leurs ensembles de données et leurs workflows. Les outils prenant en charge ces exigences de manière native seront extrêmement précieux. Les fonctionnalités de sécurité des outils de gestion réseau constituent potentiellement une bonne pratique pour la collaboration des équipes des opérations de sécurité réseau.

À propos de Riverbed

Riverbed donne aux organisations les moyens d'optimiser les performances et la visibilité des réseaux et des applications, afin de surmonter la complexité et de valoriser pleinement leurs investissements dans le digital et le cloud. La plateforme de performances applicatives et réseau de Riverbed leur permet de visualiser, de sécuriser, d'optimiser, de corriger et d'accélérer les performances de n'importe quel réseau, quelle que soit l'application. Les performances et la visibilité sont abordées par la plateforme de manière globale avec une optimisation WAN de pointe, la gestion des performances réseau (NPM), l'accélération des applications (Microsoft 365, SaaS, client et cloud, entre autres) et le SD-WAN haute performance. Plus de 30 000 clients, dont 99 % des entreprises du Fortune 100, font confiance à Riverbed. Pour en savoir plus, visitez le site riverbed.com/fr.

À propos d'Enterprise Management Associates, Inc.

Fondé en 1996, Enterprise Management Associates (EMA) est un cabinet d'analyse de premier plan qui fournit des informations approfondies sur l'ensemble du spectre des technologies IT et de gestion des données. Les analystes d'EMA utilisent une combinaison unique d'expérience pratique, d'informations sur les bonnes pratiques du secteur et d'une connaissance approfondie des solutions actuelles et prévues des fournisseurs pour aider les clients d'EMA à atteindre leurs objectifs. Pour en savoir plus sur les services de recherche, d'analyse et de conseils d'EMA pour les utilisateurs en entreprise, les professionnels IT et les fournisseurs IT, consultez **www.enterprisemanagement.com**. Suivez également EMA sur **Twitter** ou **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 - États-Unis +1 303.543.9500 **www.enterprisemanagement.com**

4080.033121