Enterprise Strategy Group | Getting to the bigger truth.™

LIVRE BLANC d'ESG

La NPM unifiée de Riverbed prend en charge et améliore la sécurité et les opérations réseau

par Jon Oltsik, Analyste principal et chargé de recherche, Enterprise Strategy Group

Juin 2021

Ce livre blanc d'ESG a été commandé par Riverbed
et est distribué sous licence d'ESG.

Sommaire

Synthèse

Une étude d'ESG indique que 43 % des entreprises utilisent des outils d'analyse du trafic réseau (NTA) comme première ligne de défense pour la détection et la résolution des menaces.[1] Cette stratégie fait écho au vieil adage de sécurité selon lequel « le réseau ne ment pas ». Les cyberattaques se déplacent latéralement sur les réseaux et se connectent à des ressources externes (serveurs C2, serveurs de programmes malveillants, etc.) dans le cadre de campagnes d'attaques. L'identification des connexions ou charges utiles malveillantes sur le réseau peut accélérer la détection des menaces et minimiser les temps d'arrêt.

De nos jours, les organisations utilisent des technologies NTA et de détection et résolution réseau (NDR), mais les données recueillies par ESG indiquent que quelque chose ne va toujours pas. De nombreuses entreprises ont du mal à faire évoluer, optimiser et rendre opérationnelle la sécurité réseau en fonction des besoins. Pourquoi la sécurité réseau est-elle si difficile et comment les organisations peuvent-elles remédier à cette complexité ? Ce livre blanc conclut ainsi :

- **Chaque année, la sécurité réseau se complexifie encore un peu plus.** Les organisations utilisent des réseaux basés sur le cloud et internes (c'est-à-dire des réseaux hybrides) pour mener à bien des initiatives telles que la transformation digitale et la prise en charge des équipes de travailleurs distants. Les réseaux revêtent donc un aspect stratégique pour les entreprises. Il est par conséquent d'autant plus alarmant de savoir que 85 % des professionnels de la sécurité estiment que, au cours des deux dernières années, la sécurité réseau s'est complexifiée en raison de la dangerosité croissante des menaces, de l'expansion de la surface d'attaque et de la prolifération des outils de sécurité réseau.[2] Ces difficultés entraînent une augmentation des cyberrisques, rendant les organisations vulnérables à des cyberattaques coûteuses.

- **Les équipes chargées de la sécurité et des opérations réseau ne sont pas toujours sur la même longueur d'ondes.** La sécurité réseau doit être menée conjointement par les équipes de sécurité et des opérations réseau. Pourtant, près de la moitié des organisations pensent que ces deux groupes ont du mal à travailler de concert et à surmonter les problèmes de communication et de collaboration.

- **La solution ? Des sources de données partagées et une visibilité du réseau de bout en bout.** Trop souvent, les équipes chargées de la mise en réseau et de la sécurité utilisent des outils différents pour surveiller le comportement du réseau, ce qui entraîne confusion, redondance et surcoûts. Or, les deux groupes examinent foncièrement les mêmes données. ESG estime que les organisations ont tout intérêt à la mise en place de solutions qui collectent, traitent et analysent les données du réseau utiles à la fois pour la sécurité et pour les opérations. La NPM unifiée de Riverbed répond à ces exigences : la combinaison de NetProfiler et d'AppResponse fournit une visibilité réseau complète, des données réseau haute fidélité et la possibilité d'examiner le comportement du réseau sous de nombreux angles (par exemple, les réseaux internes, les réseaux basés sur le cloud, le réseau étendu, etc.) Au cours des dernières années, Riverbed a adapté ses outils NPM aux besoins de sécurité et dispose d'une feuille de route ambitieuse pour accélérer la prise en charge de la sécurité à l'avenir. De cette façon, la NPM unifiée de Riverbed peut agir comme une source d'information unique, améliorant l'efficacité et la productivité des équipes de sécurité et des opérations réseau.

L'état de la sécurité réseau

Les technologies de sécurité réseau existent depuis les années 1980, lorsque Digital Equipment Corporation (DEC) a lancé le premier pare-feu commercial. Forte de 30 ans d'expérience, la sécurité réseau devrait être mature et sous

[1] Source : Résultats principaux de l'étude d'ESG, *The Threat Detection and Response Landscape* (Panorama sur la détection et la résolution des menaces), avril 2019.
[2] Source : Rapport de recherche d'ESG, *The State of Network Security: A Market Poised for Transition* (L'état de la sécurité réseau : un marché prêt pour la transition), mars 2020.

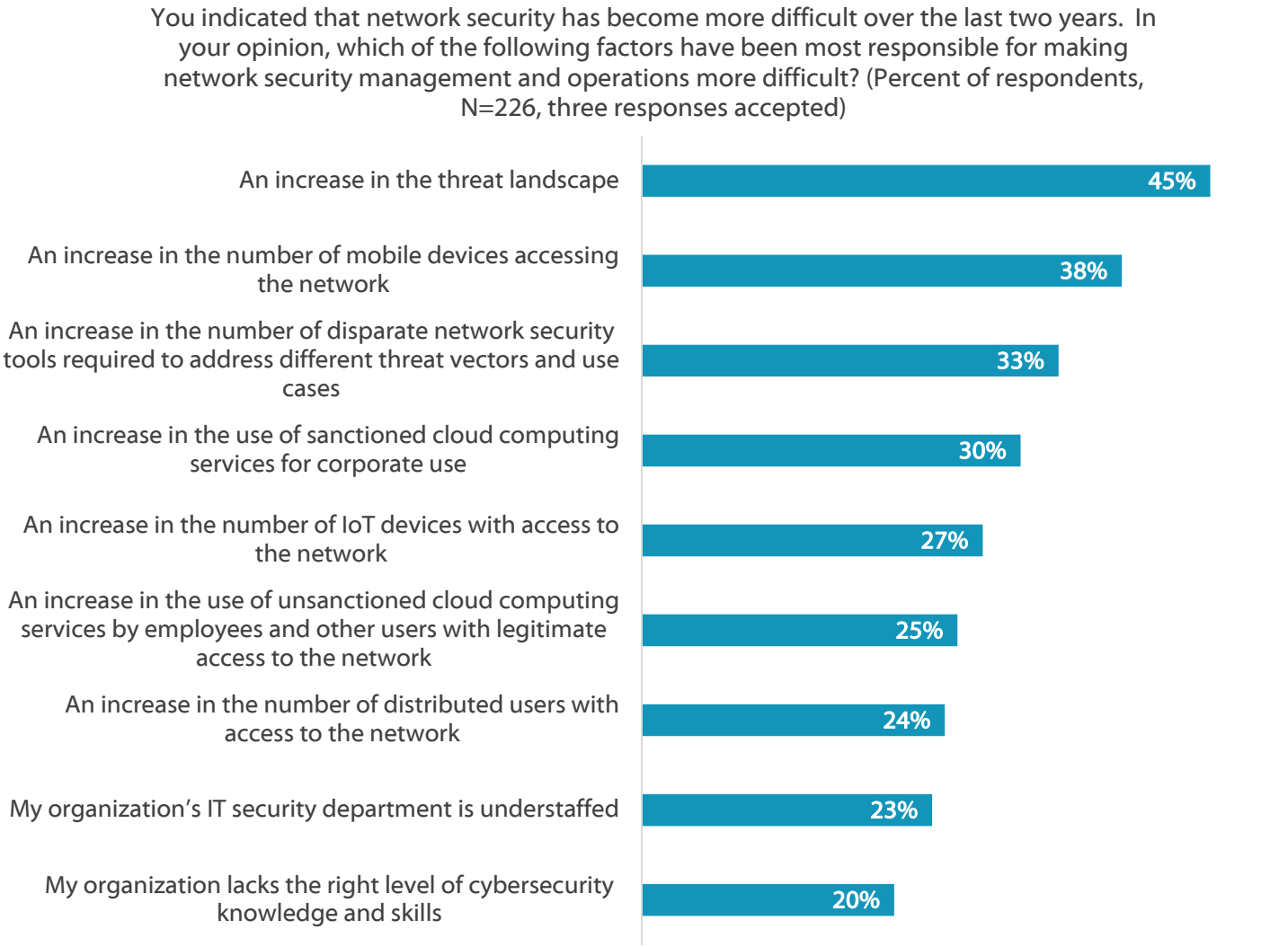
contrôle, mais les informations d'ESG révèlent que cela est loin d'être le cas. L'étude d'ESG indique que 85 % des organisations estiment que la sécurité réseau est plus difficile aujourd'hui qu'il y a deux ans à peine. Pourquoi ? Il y a plusieurs raisons à cela, notamment (voir la figure 1) :[3]

- **Une augmentation des cybermenaces :** le premier semestre 2021 a été marqué par des cyberattaques très médiatisées comme celle de SUNBURST et celles ciblant des organisations précises telles que l'agence de recherche nucléaire sud-coréenne, la société de croisière Carnival Cruise Lines, les usines de bœuf JBS, l'entreprise de gazoduc Colonial Pipelines et la chaîne de supermarchés Wegmans. Cette liste non exhaustive démontre qu'aucune région, aucun secteur ou aucune organisation n'est à l'abri d'une attaque. Pour faire face à cette situation, les spécialistes de la sécurité réseau ont besoin d'avoir une visibilité complète des réseaux, de règles de détection précises et de données scientifiques approfondies pour mener des enquêtes rapides et exactes.
- **Une expansion de la surface d'attaque :** l'étude d'ESG pointe du doigt une augmentation du nombre d'appareils mobiles, d'applications, d'appareils IoT et de services cloud non approuvés. Mises bout à bout, ces tendances se traduisent par une expansion de la surface d'attaque. Du point de vue de la sécurité réseau, les équipes SOC doivent avoir une visibilité détaillée et à grande l'échelle des applications, des appareils, des connexions et des protocoles. De nombreuses organisations ne disposant pas de ce niveau de visibilité, les équipes SOC sont réduites à faire des suppositions en se basant sur une visibilité limitée et les données historiques disponibles, c'est-à-dire à accepter le meilleur compromis.
- **La prolifération des outils de sécurité réseau :** l'association menaces sophistiquées/expansion de la surface d'attaque a poussé de nombreuses organisations à déployer de nouveaux types de capteurs et d'outils de détection. Malheureusement, cela a entraîné une flambée du nombre d'alertes de sécurité. D'une manière ou d'une autre, les analystes SOC sont censés trier, examiner et hiérarchiser ce volume croissant d'alertes de sécurité, une tâche impossible pour de nombreuses organisations.

Il convient également de souligner que 23 % des personnes interrogées déclarent que leur service de sécurité IT manque de personnel, tandis que 20 % affirment que leur organisation ne dispose pas du niveau adéquat de connaissances et de compétences en matière de cybersécurité. Compte tenu de la pénurie mondiale de compétences en la matière, ces tendances vont probablement perdurer.

[3] Ibid.

Figure 1. Raisons pour lesquelles la sécurité réseau est devenue plus difficile



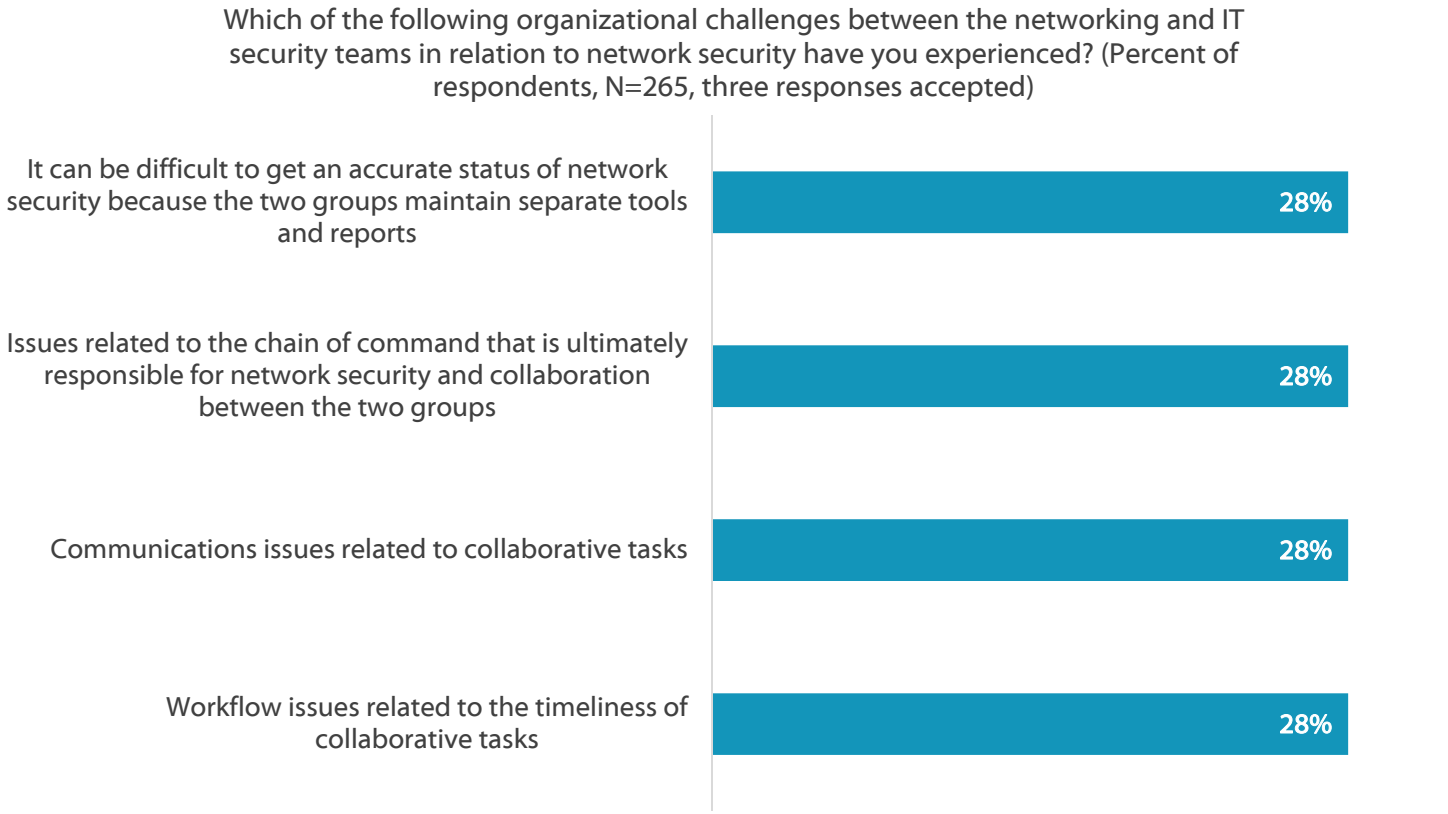
Source : Enterprise Strategy Group

Le fossé organisationnel entre la mise en réseau et la sécurité

La prévention, la détection et la résolution des menaces sont un effort collectif entre les équipes de sécurité et de mise en réseau, mais malheureusement, ces deux services ne travaillent pas toujours main dans la main. En fait, 44 % des organisations avouent que cette relation ne fonctionne pas toujours bien. En effet, les groupes gèrent des données/outils distinct(e)s, rendent des comptes à des hiérarchies indépendantes, communiquent de façon médiocre sur les tâches de collaboration et souffrent de problèmes de workflow liés à la rapidité des processus (voir figure 2) :[4]

[4] Source : Résultats principaux de l'étude d'ESG, *Network Security Trends* (Tendances de sécurité réseau), mars 2020.

Figure 2. Les quatre principaux défis organisationnels entre les équipes de mise en réseau et de sécurité



Source : Enterprise Strategy Group

Les données d'ESG dressent un tableau inquiétant : la sécurité réseau se complexifie et les deux principaux groupes chargés de gérer la sécurité réseau ne font pas toujours bon ménage. Si cette situation perdure, les cyberrisques vont monter en flèche, alors que les équipes chargées des réseaux et de la sécurité ont du mal à adapter les opérations quotidiennes, les processus de détection des menaces et la résolution des incidents. Pour empêcher ces perspectives alarmantes, les RSSI (responsables de la sécurité des systèmes d'information) doivent collaborer avec leurs homologues IT et réseau pour relever ces défis le plus rapidement possible.

La visibilité du réseau est la pierre angulaire des opérations de sécurité

Pour résoudre les difficultés liées à la sécurité réseau, les RSSI avisés savent qu'ils doivent surveiller tout le trafic aux points clés du réseau (c'est-à-dire les points d'entrée/sortie, les data centers, les clouds publics, etc.) Selon l'étude d'ESG, c'est déjà le cas : 87 % des entreprises utilisent des outils NTA pour la détection et la résolution des menaces, et 43 % déclarent que la NTA est une « première ligne de défense » pour la détection et la résolution des activités anormales/suspectes/malveillantes sur le réseau, telles que les mouvements latéraux, l'énumération des réseaux, le trafic C2 et l'exfiltration de données.[5] De nombreuses entreprises s'appuient également sur la visibilité réseau pour :

- **Établir une stratégie réseau et détecter les anomalies.** Pour citer le gourou du marketing Peter Drucker, « On ne peut gérer ce que l'on ne peut mesurer », et cette affirmation s'applique sans aucun doute à la sécurité réseau. Une visibilité réseau complète permet d'identifier les dispositifs indésirables qu'il peut abriter, de surveiller les schémas de trafic et d'en repérer les anomalies. Cela s'applique à tout le trafic : nord/sud et est/ouest, et

[5] Source : Résultats principaux de l'étude d'ESG, *The Threat Detection and Response Landscape* (Panorama sur la détection et la résolution des menaces), avril 2019.

s'étend également au trafic au sein de l'infrastructure du cloud public. Pour détecter les attaques complexes en plusieurs étapes, les RSSI doivent s'efforcer d'avoir une visibilité sur l'ensemble du trafic.

- **Obtenir des détails scientifiques approfondis.** Les principaux outils de visibilité réseau peuvent capturer l'historique des connexions en détaillant les ressources qui communiquaient, le moment où cette communication a eu lieu et ce qu'elle impliquait (ports, protocoles, charges utiles, etc.). Ce niveau de détail est essentiel pour la détection des menaces, le degré d'urgence des enquêtes et les enquêtes elles-mêmes. Lorsque les analystes de sécurité reçoivent une alerte provenant d'une technologie de détection (IDS/IPS, EDR, SIEM, etc.), ils se tournent généralement vers les outils de visibilité réseau, en fouillant dans les outils NetFlow/ipfix et de capture de paquets (PCAP) pour savoir ce qui s'est passé, quand cela s'est passé et quels nœuds du réseau étaient impliqués. À partir de là, les chasseurs de menaces peuvent utiliser les données de flux et de paquets pour un rappel fidèle des événements historiques. Pour garantir la disponibilité de ces données scientifiques approfondies, les organisations doivent surveiller et capturer des données de haute fidélité en permanence. La tentation de se contenter d'un simple échantillonnage de données (par souci de rapidité ou d'économie) est réelle, mais crée des lacunes importantes dans l'historique, qui peuvent être insurmontables et beaucoup plus coûteuses lorsqu'une analyse scientifique complète est indispensable.

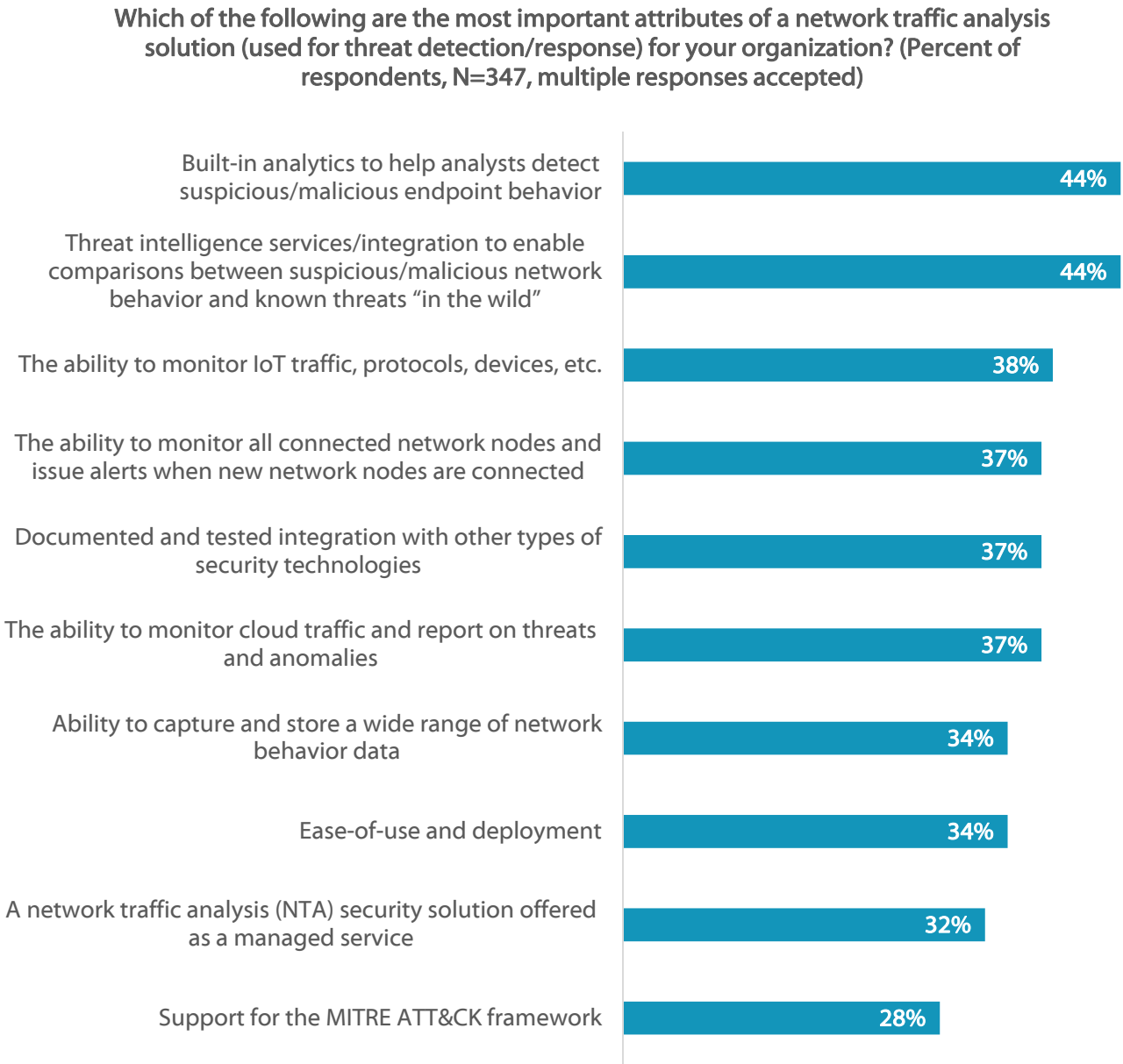
- **Créer un stratégie de sécurité.** Puisque la visibilité réseau ouvre une fenêtre sur les modèles de communication du réseau, les ingénieurs en sécurité peuvent utiliser ces données comme guide pour les projets en cours dans des domaines tels que la micro-segmentation et la confiance zéro. Cela peut contribuer à réduire la surface d'attaque pour atténuer les risques.

Comme nous l'avons déjà évoqué, la visibilité réseau est souvent soutenue par des outils d'analyse du trafic réseau (NTA). Selon l'étude d'ESG, la liste d'exigences des professionnels de mise en réseau et de la sécurité pour ce type de technologie est longue. Les caractéristiques les plus importantes des outils NTA sont notamment des analyses intégrées pour la détection des menaces, des renseignements sur les menaces pour l'enrichissement des données réseau, la capacité de surveiller les dispositifs/le trafic IoT ainsi que les nœuds du réseau afin de maintenir une hygiène de réseau sécurisée (voir la figure 3).[6]

Les principaux outils de visibilité réseau doivent également contribuer à combler le fossé entre les équipes chargées de la sécurité et celles chargées de la mise en réseau. Elles doivent fournir un référentiel de données commun prenant en charge les cas d'utilisation de la mise en réseau, tels que la gestion des performances réseau applicatives, et les cas d'utilisation de la sécurité, tels que la détection des menaces, la résolution des incidents et les enquêtes scientifiques, ainsi que la chasse aux menaces. Les meilleures solutions collecteront, traiteront et analyseront 100 % des données en des points stratégiques du réseau d'entreprise et du réseau cloud, fourniront une visibilité et des analyses à partir de plusieurs points d'observation du réseau et offriront ainsi des données complètes.

[6] Source : Résumé d'ESG, Caractéristiques clés d'une solution d'analyse du trafic réseau, septembre 2019.

Figure 3. Les caractéristiques les plus importantes des solutions NTA



Source : Enterprise Strategy Group

Riverbed pour la visibilité réseau

Les RSSI peuvent choisir parmi pléthore d'outils de visibilité réseau, mais un outil de sécurité de plus ne contribuera pas à créer une passerelle entre les équipes de sécurité et de mise en réseau. En revanche, les organisations pourraient trouver un avantage dans les outils de visibilité réseau qui peuvent prendre en charge les besoins et les cas d'utilisation des équipes de mise en réseau et de sécurité.

Forte de sa longue expertise dans le secteur, Riverbed propose une solution hybride pouvant satisfaire les besoins communs des équipes de sécurité et de mise en réseau. Une solution Riverbed peut être conçue à partir de ses produits NPM (surveillance des performances réseau) : NetProfiler pour les enregistrements de flux et AppResponse pour la capture complète des paquets. Grâce à cette combinaison, les organisations peuvent collecter des données sur l'ensemble du réseau afin d'obtenir une visibilité totale de toutes les activités du réseau. Cela leur donne également la possibilité de surveiller le réseau sous de multiples angles : au périmètre du réseau, dans les data centers dans le cloud et internes à entreprise, à l'intérieur du trafic est/ouest sur les réseaux internes, dans les bureaux distants connectés au WAN, etc. Au-delà de la seule visibilité, Riverbed fournit des fonctionnalités spécifiques pour la sécurité du réseau :

- **Détection active des menaces.** Pour améliorer la prévention et la détection des menaces, les solutions de sécurité Riverbed prennent en charge la liste noire IoC, consomment des flux de menaces pour l'enrichissement et la contextualisation et capturent l'établissement de références réseau pour la détection des anomalies.

- **Enquêtes scientifiques.** Lorsque les analystes de sécurité soupçonnent une cyberattaque, ils doivent pouvoir examiner l'activité détaillée sur le réseau, en temps réel et son historique. La NPM unifiée de Riverbed est conçue pour effectuer cette tâche. Elle fournit des données de flux et de paquets de haute fidélité pour des cas d'utilisation tels que les enquêtes de sécurité et la chasse aux menaces. Riverbed a même créé une API, permettant aux équipes SOC d'effectuer des captures de paquets sur la base de déclencheurs spécifiques, comme des connexions à des adresses IP inhabituelles ou des domaines Internet malveillants.

- **Détection et atténuation des attaques DDoS.** Riverbed va plus loin que beaucoup d'outils NTA en matière de détection et d'atténuation des attaques DDoS (déni de service distribué). En intégrant cette fonctionnalité à sa solution NPM unifiée, Riverbed peut contribuer à combler le fossé organisationnel entre les équipes de sécurité et des opérations réseau.

Grâce à une visibilité de haute fidélité, la NPM unifiée de Riverbed peut également aider les organisations à rassembler les communications réseau indiquant des cyberattaques « faibles et lentes » comme les menaces persistantes avancées (APT). Ces campagnes utilisent diverses tactiques, techniques et procédures (TTP) suivant une chaîne d'élimination pour compromettre les systèmes, se déplacer latéralement sur les réseaux, récolter des informations d'identification et finalement exfiltrer des données précieuses. Grâce à la visibilité de bout en bout, Riverbed permet également aux organisations de rendre opérationnel le cadre MITRE ATT&CK pour les cas d'utilisation typiques de MITRE ATT&CK tels que la détection des incidents, l'évaluation et l'ingénierie de la sécurité, l'analyse des renseignements sur les cybermenaces et l'émulation des adversaires. Enfin, la fonctionnalité de mise en réseau et de sécurité de la solution NPM unifiée de Riverbed peut aider les organisations à planifier, tester et mettre en œuvre des solutions architecturales pour la confiance zéro.

En conclusion

Les équipes de cybersécurité doivent soutenir les initiatives d'entreprise et informatiques tout en protégeant les actifs digitaux des cyberattaques. Bien que cette mission soit claire, elle devient de plus en plus difficile. L'équipe SOC ne peut tout simplement pas faire face à l'ampleur et à la complexité de son rôle sous le poids d'alertes de sécurité nébuleuses et d'une visibilité réseau morcelée. Au contraire, le personnel de sécurité doit se synchroniser avec les opérations réseau et disposer d'une visibilité claire et complète de tout ce qui se passe sur le réseau.

Bien que Riverbed ne soit généralement pas considérée comme un fournisseur de sécurité, un nombre croissant de nos clients utilisent aujourd'hui nos solutions de NPM unifiée pour la sécurité, car la combinaison de NetProfiler et d'AppResponse permet aux organisations d'obtenir une visibilité complète et fidèle de NetFlow/ipfix et des paquets (PCAP) sur le réseau. Dotés de ces outils, les clients de Riverbed peuvent identifier les comportements suspects, enrichir les données du réseau avec des renseignements sur les cybermenaces, bloquer les IoC malveillants et atténuer les attaques DDoS tout en prenant en charge les exigences de gestion des performances réseau. Cette combinaison pourrait constituer un complément précieux pour les équipes chargées de la sécurité et des opérations réseau en vue d'améliorer l'efficacité de la cybersécurité, de rationaliser les opérations et de renforcer la collaboration. En outre, ces mêmes données s'avèrent précieuses pour des analyses approfondies permettant de découvrir l'origine des problèmes, les points d'entrée et la chronologie des cyberattaques, ce qui est essentiel une fois l'attaque identifiée.

Enterprise Strategy Group est un cabinet d'analystes informatiques, de recherche, de validation et de stratégie qui fournit des données et des informations exploitables à la communauté IT mondiale concernant les marchés.

www.esg-global.com contact@esg-global.com +1 508.482.0188