Perspective

L'union fait la force

Réseau et sécurité : six arguments en faveur d'une stratégie d'achat unifiée

verizon business

Réseau + sécurité

Les avantages métiers et techniques d'un achat et d'une gestion harmonisés

David Bailey
Global Solutions Executive

Depuis plus de 20 ans, David Bailey aide de grandes entreprises internationales et des acteurs du secteur public à définir et à satisfaire leurs besoins en matière d'infrastructure et de sécurité. Ses domaines de compétences comprennent notamment les réseaux filaires et sans fil pour l'Internet des objets (IoT), ainsi que les infrastructures agiles et intelligentes qui sous-tendent les applications les plus exigeantes, notamment l'IA.

À l'heure où les cyberattaques évoluent et où les infrastructures réseau se complexifient, il devient urgent pour les entreprises d'intégrer réseau et cybersécurité afin de bâtir des systèmes plus résilients, plus efficaces et plus sécurisés. Seule cette fusion leur permettra à la fois de protéger leurs actifs critiques et d'atteindre leurs objectifs métiers. La croissance phénoménale de l'IA et des volumes de données qu'elle consomme n'a fait qu'exacerber cet impératif.

Propriétaire de l'un des réseaux IP les plus étendus de la planète, Verizon est déjà l'un des opérateurs Tier 1 les plus réputés du marché. Côté cybersécurité, nous sommes également un prestataire leader, avec une offre de services allant du conseil à la Threat Intelligence, en passant par la réponse à incident (IR), les audits de conformité et les analyses forensiques. Nous sommes également les auteurs du Verizon Data Breach Investigations Report (DBIR), un rapport cyber annuel qui célèbre sa 18e édition et compte parmi les plus complets du marché. Ce capital d'expérience nous place dans une position unique pour concevoir, piloter et sécuriser votre infrastructure.

Que ce soit pour notre dorsale mondiale, nos offres Internet haut débit grand public ou les milliers de réseaux WAN que nous gérons pour de grandes entreprises internationales, nous avons la conviction que réseau et sécurité sont inextricablement liés. Cet article vous explique les avantages d'une gestion unifiée de ces deux services en entreprise.

1 Renforcez vos défenses

Lorsqu'elles travaillent chacune de leur côté, les équipes réseau et cybersécurité opèrent souvent en vase clos, avec les décalages que cela entraîne sur les plans de la communication et de la stratégie. De même, les écarts dans leurs configurations respectives peuvent créer des vulnérabilités.

> Les équipes réseau et sécurité qui opèrent séparément peuvent pâtir d'un manque de visibilité et de communication qui crée des failles dans les défenses et ralentit la réponse à incident.

La fusion de ces deux fonctions permet d'assurer une surveillance continue et une détection des menaces en quasi temps réel sur toutes les couches du réseau. De même, la gestion de la configuration des équipements (routeurs, commutateurs, etc.) et l'application des politiques peuvent être harmonisées dans toute l'entreprise. Cette stratégie cohésive facilite une démarche plus préventive face aux menaces, de manière à réduire le risque de compromission et à accélérer l'identification et la correction des vulnérabilités.

- **Améliorez votre modèle opérationnel**
  Cette approche unifiée peut faire émerger une posture cyber plus résiliente. Quant à l'efficacité du nouveau modèle opérationnel, elle génère des économies à plusieurs niveaux : réduction des doublons d'activités, rationalisation de l'affectation des effectifs, réduction de la charge de communication et simplification des systèmes et licences. La disparation des silos technologiques aide également à réduire les problèmes d'intégration et d'interopérabilité.

- **Réduisez les interruptions de services et le risque tiers**
  Ces améliorations peuvent s'étendre au helpdesk de manière à optimiser le service aux collaborateurs, à réduire les pertes de temps et à booster la productivité. Elles permettent aussi d'identifier les écarts et problèmes dans les processus, tant au niveau des collaborateurs que des partenaires, deux catégories dont les attaquants cherchent à détourner les identifiants pour accéder aux systèmes.

- **Optimisez l'efficacité des contrôles**
  Un pilotage centralisé du réseau et de la sécurité peut améliorer la détection des vulnérabilités. A contrario, une gestion cloisonnée peut omettre certains aspects de l'infrastructure et laisser ainsi des vulnérabilités échapper à toute détection. De fait, une identification et une remédiation plus rapides et plus complètes des vulnérabilités aident à fermer la fenêtre d'attaque.

- **Faites un meilleur usage des données et de la Threat Intelligence**
  Pas de cybersécurité efficace sans une bonne Threat Intelligence. Or, les équipes peuvent faire meilleur usage de cette veille cyber quand la sécurité et le réseau sont gérés comme un tout. En ce sens, les solutions intégrées peuvent analyser le trafic réseau et les événements de sécurité en temps réel pour identifier les indicateurs de menaces potentielles, et ainsi réduire le risque d'attaque.

2 Améliorez votre efficacité et réduisez vos coûts

L'achat et la gestion séparés de solutions réseau et de cybersécurité se traduit souvent par un surcoût et un manque d'efficacité. En unifiant ces services, vous pouvez :

- **Réduire les coûts**
  Une gestion unifiée de ces fonctions peut simplifier la budgétisation et la planification financière, offrir une aperçu plus clair des dépenses technologiques et générer des économies.

- **Résorber la pénurie de ressources**
  L'élimination des silos contribue aussi à résoudre les problèmes de ressources. Les professionnels des réseaux et de la cybersécurité doivent en effet souvent maîtriser des compétences qui se recoupent. D'où l'intérêt d'unifier les deux fonctions pour concevoir des programmes de formation couvrant les deux domaines. Quand un même collaborateur est capable d'effectuer des tâches réseau et de sécurité, son temps est beaucoup mieux utilisé. Cela s'avère d'autant plus important lorsque vos équipes doivent assurer un service H24 dans le monde entier. Côté satisfaction et rétention aussi, les indicateurs sont au beau fixe, car vos collaborateurs apprécient de pouvoir étendre leurs compétences et d'accéder à divers rôles au sein de l'organisation.

3 Intégrez de multiples clouds et accélérez la transformation digitale en toute sécurité

La plupart des projets de transformation digitale s'articulent autour de services cloud. Or, toute migration d'applications vers ces environnements exige une intégration étroite entre réseaux et sécurité. Ensuite, lorsque l'entreprise est déjà bien implantée dans le cloud, elle tend à évoluer vers une architecture multicloud, souvent sous la forme d'un cloud hybride. Une approche unifiée du réseau et de la sécurité peut aider à mieux maîtriser ces environnements complexes :

- **Optimisez la gestion de vos environnements multicloud**
  En connectant l'infrastructure cloud au moyen de fonctionnalités réseau intelligentes, les équipes obtiennent une meilleure visibilité sur les workloads, les performances et les schémas d'utilisation. Elles bénéficient ainsi d'une gestion simplifiée tout en accélérant la résolution des problèmes.

- **Appliquez des politiques de sécurité homogènes sur vos ressources on-prem et cloud**
  Grâce aux contrôles unifiés, les données restent conformes et protégées où qu'elles soient, les erreurs de configuration reculent et les failles de sécurité disparaissent.

- **Simplifiez la gestion des environnements hybrides et multicloud**
  Les solutions intégrées permettent aux équipes IT d'orchestrer les services et politiques depuis une plateforme centralisée. Elles peuvent ainsi tourner la page des systèmes disparates pour rationaliser leurs opérations, développer l'automatisation et améliorer leur efficacité et leur agilité.

4 Améliorez la scalabilité et la flexibilité

Les entreprises doivent pouvoir s'adapter rapidement aux mutations rapides des technologies et des besoins de leurs clients. Tout retard dans ce domaine peut se traduire par une baisse de compétitivité, une perte d'opportunités et, in fine, l'obsolescence de votre offre.

- **Maintenez l'intégrité de vos défenses au fil de l'évolution de l'infrastructure réseau**
  Une approche intégrée de la cybersécurité aide les entreprises à répondre plus rapidement aux incidents. À mesure qu'elles se développent, adoptent de nouveaux business models et apportent des modifications à leur infrastructure réseau, une stratégie réseau et sécurité intégrée leur permet de maintenir des défenses robustes.
- **Évitez de dupliquer les efforts et les technologies**
  Des équipes cloisonnées sont susceptibles d'investir dans des outils et services séparés, alors qu'une solution unifiée s'avérerait à la fois moins chère et plus facile à gérer. Par contraste, des équipes intégrées collaborent plus efficacement, réduisant ainsi le temps et les ressources engagés dans le déploiement de nouveaux services et la résolution de problèmes.

5 Accélérez la réponse à incident et réduisez les interruptions de service

En cas d'incident de sécurité, une approche unifiée du réseau et de la cybersécurité favorise une réponse plus robuste et mieux coordonnée.

- **Atténuez l'impact des incidents de sécurité**
  La gestion unifiée du réseau et de la sécurité permet de mieux coordonner les procédures IR pour fluidifier la collaboration entre les équipes, et ainsi accélérer l'intervention et atténuer l'impact des attaques.
- **Identifiez et isolez plus rapidement les menaces**
  En unifiant les services, les entreprises peuvent mettre en place un suivi proactif du réseau pour détecter les menaces et vulnérabilités. Elles renforcent ainsi leur sécurité tout en réduisant les risques d'interruption.
- **Automatisez et accélérez la réponse à incident**
  Une approche intégrée facilite le déclenchement de mécanismes de réponse automatisés qui réduisent les temps de neutralisation et de résolution des incidents. Une gestion unifiée, c'est aussi une analyse plus efficace des incidents pour aider les entreprises à en tirer les enseignements et à renforcer leur posture de sécurité.

6 Simplifiez la conformité et le reporting

La conformité est généralement associée à des secteurs très réglementés comme la finance et la santé. Toutefois, la plupart des entreprises sont soumises à des obligations draconiennes en matière de protection des données. Toute entreprise qui traite des paiements par carte ou qui manipule des données à caractère personnel doit ainsi être en capacité de démontrer sa conformité aux normes de cybersécurité en vigueur. Cette tâche coûteuse et chronophage le devient encore plus dans des environnements IT complexes.

- **Améliorez l'homogénéité des contrôles de sécurité**
  En gérant le réseau et la cybersécurité comme un tout, les entreprises peuvent simplifier leur mise en conformité en harmonisant l'application et la documentation des configurations réseau et des contrôles de sécurité.

> Les outils de reporting automatisés sont plus efficaces lorsque la cybersécurité et le réseau sont pilotés ensemble.

- **Créez un point de responsabilité unique**
  Une gestion unifiée, c'est aussi un référent unique pour toutes les questions de conformité. Cette centralisation facilite le suivi et le reporting au regard de lois et réglementations telles que :
  - Le Règlement général sur la protection de données (RGPD)
  - Le Health Insurance Portability and Accountability Act (HIPAA)
  - Le Payment Card Industry (PCI) Data Security Standard (DSS)
  - Le California Consumer Privacy Act (CCPA)

Gestion des accès d'entreprise : comment choisir la bonne option
Cet autre article de la série vous invite à découvrir à quel point le choix du fournisseur influence les performances et les résultats pour votre entreprise. Une décision d'autant plus cruciale pour les applications sensibles à la latence, très présentes dans les cas d'usage de l'IA.

Temps de lecture : 15 minutes

Pourquoi choisir Verizon ?

C'est très simple : qui dit réseau, dit Verizon. Nos millions de kilomètres de fibre sous-tendent une grande partie de la dorsale Internet. Nous sommes ainsi en mesure de vous offrir la visibilité, la performance et la fiabilité dont les autres opérateurs osent à peine rêver.

Mais le réseau n'est qu'une partie de l'équation. Nos équipes de sécurité comptent aussi parmi les plus étendues et les plus expérimentées de la planète, avec des domaines de compétences allant de la Threat Intelligence à la réponse à incident, en passant par les analyses forensiques, la conformité et plus encore. Chaque année, elles accomplissent plus de 1 000 missions GRC (gouvernance, risque et conformité).

Notre passion pour la data et sa sécurité aurait de quoi interpeller si elle ne vous apportait pas tant d'avantages. Pour l'édition du Data Breach Investigations Report (DBIR) de cette année, nous avons ainsi analysé plus d'un demi-million d'incidents de sécurité issus de nos propres missions de réponse et de nos quelque 60 contributeurs, parmi lesquels des acteurs clés de la puissance publique et du secteur de la cybersécurité dans le monde entier. Chaque année, nous traitons également des milliers de milliards d'événements de sécurité sur nos réseaux et ceux de nos clients, constituant ainsi un immense corpus de données sur lesquelles nous entraînons nos modèles d'intelligence artificielle.

Au-delà des chiffres, notre vraie différence se situe au niveau de notre réseau et de nos équipes. Pour la connectivité de votre entreprise, la sécurité de vos systèmes et la performance de vos applications, nous avons l'expertise qu'il vous faut.

Alors pourquoi se contenter de moins ?

23 000+ Md
Nous traitons en moyenne 23 000 milliards d'événements de sécurité chaque année.

550 000+
Nous gérons plus d'un demi-million d'équipements réseau, de sécurité et d'hébergement

1 000+
Nous menons chaque année plus de 1 000 missions de gouvernance, risque et conformité (GRC)

Échangeons

De l'IoT à l'IA et à l'analytique temps réel, Verizon vous offre des technologies de pointe pour surveiller, gérer et améliorer vos opérations. Pour toute question ou renseignement, n'hésitez pas à nous contacter à l'adresse : verizon.com/business/fr-fr/contact-us

Série Network Procurement

Cet article s'inscrit dans le cadre d'une série qui explore les pressions croissantes qui pèsent sur le réseau et dresse la liste des questions essentielles à poser aux fournisseurs durant le processus d'achat. Il vise ainsi à guider les entreprises dans le choix d'une solution réellement à la hauteur de leurs enjeux actuels et futurs.

Prêt pour le déferlement annoncé ?

Données **IoT** **IA**

Cet article explore les principaux ressorts de l'explosion des volumes de données collectées par les entreprises et ses implications pour la planification réseau.
verizon.com/business/resources/articles/iot-genai-data-explosion.pdf

Accès réseau : explorer les options

Performances

De nombreuses décisions entrent en jeu lors de l'achat de solutions réseau. Pour évaluer les options disponibles, il est impératif de bien comprendre les trois couches qui composent Internet. Cet article explique leur importance pour la performance et la sécurité des réseaux.
verizon.com/business/resources/articles/tier-1-isp-enterprise-connectivity.pdf

Peering réseau

Cloud **Performances** **Fiabilité**

Composante essentielle aux performances du réseau, le peering est tout autant indispensable pour les applications d'entreprise, notamment dans le cloud. Malgré cela, ce sujet figure rarement au cahier des charges des processus d'achat. Ce court article vous aide à rectifier le cap.
verizon.com/business/resources/articles/network-peering.pdf

Quelle visibilité sur vos performances ?

Données **Performances** **Gestion simplifiée**

Découvrez comment un achat séparé des composants physiques (underlay) et logiciels (overlay) du réseau peut impacter les performances, la visibilité et la simplicité de gestion.
verizon.com/business/resources/articles/overlay-underlay-network-procurement.pdf

L'union fait la force

Sécurité **Performances** **Gestion simplifiée**

Dans un contexte de prolifération et de sophistication des cybermenaces, cet article offre six raisons de mieux intégrer la cybersécurité et les réseaux, parmi lesquelles une protection renforcée, une baisse des coûts et une réduction de la charge de travail.
verizon.com/business/resources/articles/unified-network-security-services.pdf

Boostez vos applications IA

IA **Performances**

L'intelligence artificielle (IA) s'annonce comme la technologie la plus disruptive depuis la démocratisation d'Internet, il y a près de 30 ans. Cet article souligne l'importance cruciale des performances réseau pour concrétiser les promesses des applications d'IA.
verizon.com/business/resources/articles/network-infrastructure-ai-platforms.pdf

verizon
business