Rapport sur les tendances mondiales des réseaux en 2020

Sommaire

Tendances des technologies réseau (suite)

Introduction : État des lieux des réseaux à l'ère numérique

Résumé de la section

Points clés

- La mondialisation, la transformation numérique, l'automatisation et la résilience de l'entreprise ainsi que le développement durable font partie des tendances imposant l'adoption d'un nouveau type de réseau.
- Avec l'émergence des modèles cloud natifs, l'Internet des objets (IoT), l'intelligence artificielle (IA), le mobile, les menaces de cybersécurité et les applications immersives, le contexte technologique connaît des évolutions influant considérablement sur les architectures et les opérations réseau.
- L'extrême ampleur, la complexité et la nature dynamique de ces exigences dépassent les capacités des seuls opérateurs humains.
- Les nouveaux réseaux s'appuient sur des technologies émergentes comme l'IA, l'apprentissage automatique et l'automatisation pour simplifier et sécuriser les opérations, accélérer l'adaptabilité et soutenir la prise de décision humaine.

Tendances métier et technologiques mondiales qui façonnent le nouveau réseau

700 M
de conteneurs hébergés en périphérie en 2021[1]

50 %
des charges applicatives en dehors du data center des entreprises en 2021[2]

14,6 Mrds
d'équipements IoT en 2022[3]

42 %
de croissance annuelle du trafic mobile professionnel de 2017 et 2022[3]

53 %
des attaques de cybersécurité entraînent plus de 500 000 USD de préjudices[4]

12 x
plus de trafic RA/RV d'ici 2022[3]

Résumé de la section (suite)

Conseils décisifs

- Les responsables IT et les architectes réseaux doivent procéder de manière graduelle pour faire évoluer chacun de leurs domaines réseau vers un modèle basé sur un contrôleur, en s'appuyant sur les technologies d'automatisation et d'intelligence artificielle.
- Les responsables IT doivent élaborer un plan stratégique et technologique axé sur les priorités métier et englobant l'architecture, la technologie, les opérations et les compétences réseau.
- Les architectes et ingénieurs réseaux doivent identifier des parcours de formation et d'évolution de carrière qui leur procureront les compétences nécessaires pour piloter cette transformation du réseau et mettre en valeur leur profil.

Prévision clé

« En 2025, les équipes réseau de pointe disposeront de réseaux intuitifs dans l'ensemble des domaines réseau : site principal, site distant, WAN, data center, cloud, opérateur et sécurité. Ces réseaux seront en mesure de comprendre les impératifs métier et applicatifs et de les traduire en politiques réseau et sécurité. Les gains d'agilité seront considérables grâce à l'automatisation intelligente du réseau, et les réseaux fonctionneront avec une boucle de rétroaction puissante fournissant les mécanismes de surveillance, d'assurance et d'optimisation continues. Le réseau intuitif veillera à ce que les services métier soient toujours fournis et protégés sur la totalité du réseau. Ces avancées procureront des avantages importants pour les entreprises et pour l'ensemble de la société ».

– John Apostolopoulos, CTO pour les réseaux d'entreprise, Cisco

Introduction : État des lieux des réseaux à l'ère numérique

Dans une série de mémos rédigés en 1962, J.C.R. Licklider, directeur au sein de l'agence des projets de recherche avancée du département américain de la Défense, proposait un « réseau informatique intergalactique » qui permettrait d'interconnecter les ordinateurs du monde entier afin d'assurer un accès sans frontières et rapide aux données et programmes[5].

À peine quelques années plus tard, en 1965, Leonard Kleinrock, Lawrence Roberts et Thomas Merrill établissaient une connexion entre quatre ordinateurs par le biais de lignes téléphoniques. Ils créaient ainsi le premier réseau étendu et dessinaient les prémices d'Internet[6].

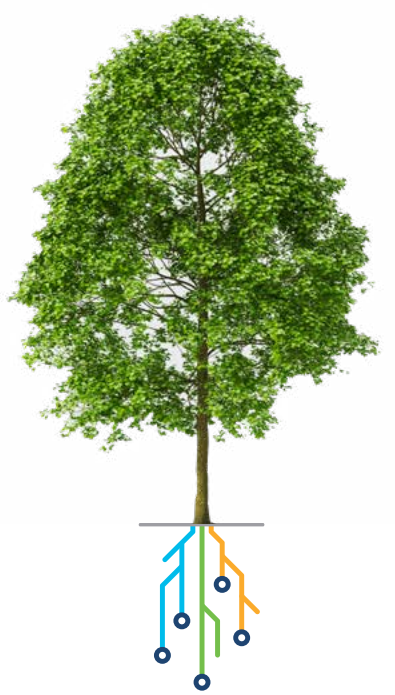
Plus de cinquante années se sont écoulées, et la vision de Licklider est toujours d'actualité : partout dans le monde, le réseau continue de connecter les consommateurs d'informations et de services à des applications et des sources de données.

Bien entendu, tout le reste a changé.

Évolution du rôle du réseau informatique

Porté par la croissance exponentielle des performances technologiques, le monde actuel devient de plus en plus connecté, digitalisé, distribué et diversifié. De plus, l'essor des objets capables de traiter des données pousse les modèles informatiques à devenir considérablement plus distribués et interconnectés en réseau. Et à mesure que s'y ajoutent des périphériques et des utilisateurs, la valeur et l'importance du réseau, telles que mesurées par la loi de Metcalfe, poursuivent leur croissance exponentielle.

L'entreprise numérique continue de favoriser les innovations en réseau. D'après les estimations d'IDC, 48,9 milliards d'appareils connectés seront utilisés dans le monde en 2023[7] et, selon les Prévisions complètes *2018 de l'indice Cisco VNI*, la quantité moyenne de données consommées par mois sur un réseau approchera les 60 Go par ordinateur personnel[3].

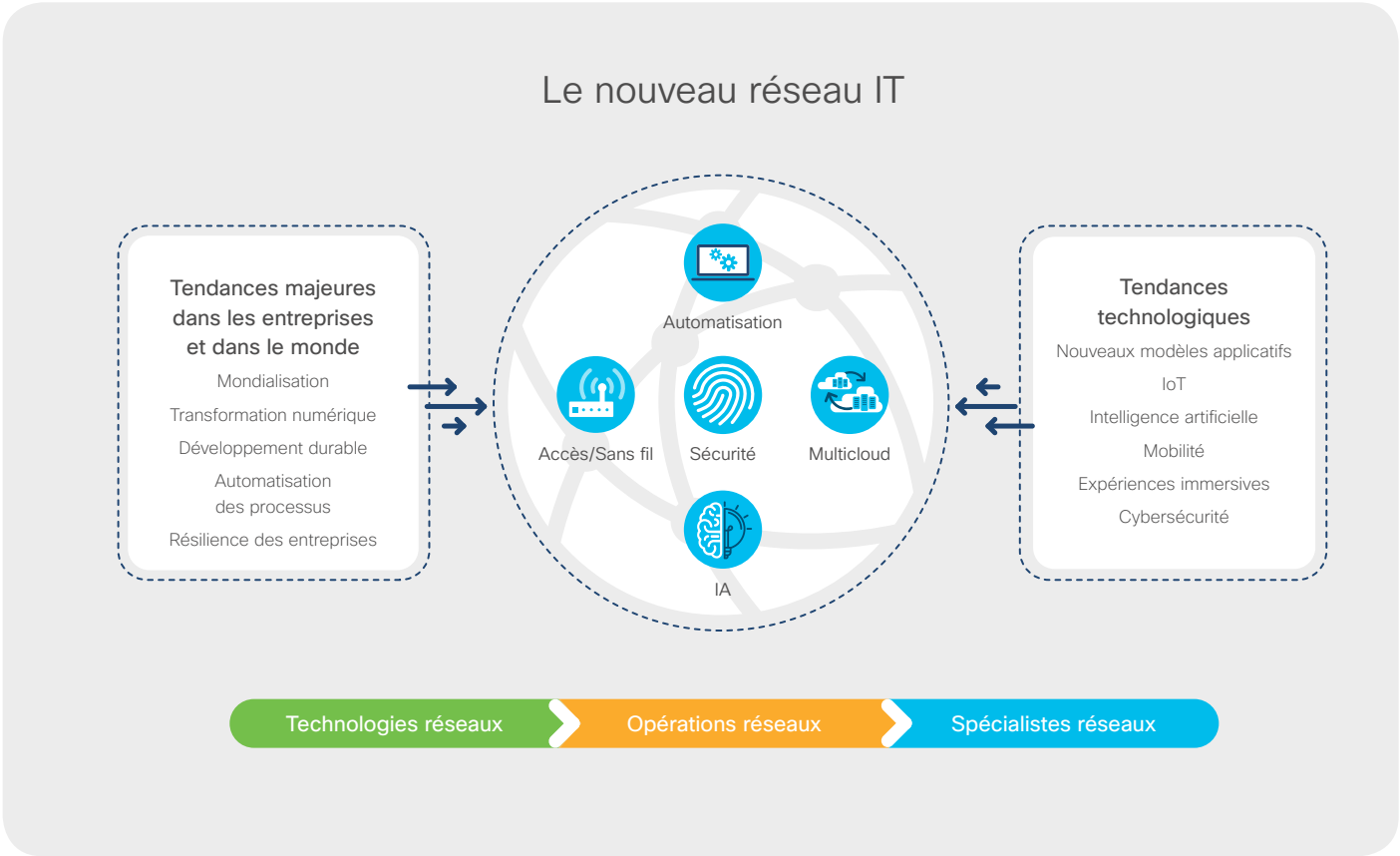


Face à cette croissance implacable, il n'est pas surprenant de constater que l'étendue et la complexité extrêmes des réseaux finissent par dépasser la capacité des équipes IT à les administrer et à les sécuriser efficacement. Il est nécessaire aujourd'hui de recourir à de nouveaux systèmes combinant des technologies telles que l'apprentissage automatique, le raisonnement machine et l'automatisation afin de simplifier les opérations et de soutenir la prise de décision humaine.

Nous nous trouvons aujourd'hui à l'orée d'une nouvelle ère du réseau, où les équipes IT peuvent rompre avec les méthodes traditionnelles de construction et d'exploitation des réseaux et embrasser un futur reposant sur des technologies capables de résoudre ces défis de manière largement novatrice.

Ce nouveau réseau se fonde sur plusieurs tendances émergentes influant sur les technologies, les opérations et les compétences réseaux. Mais avant de les étudier en détail, examinons brièvement les vecteurs technologiques et métier de cette évolution à l'échelle mondiale.

Figure 1 Tendances métier et technologiques mondiales qui façonnent le nouveau réseau



Tendances mondiales façonnant les exigences réseaux

Plusieurs tendances mondiales déterminent le rôle que joue le réseau dans une entreprise. S'ils maîtrisent ces tendances, les responsables IT peuvent se préparer à répondre aux attentes croissantes des responsables métier à l'égard du réseau.

60 %

Selon Gartner, d'ici 2023, plus de 60 % des entreprises placeront le réseau au cœur de leurs stratégies numériques. Aujourd'hui, elles ne sont que 20 % à envisager le réseau comme un instrument stratégique[8].

Un examen rapide de ces mégatendances mondiales permet d'identifier les exigences qu'ils sont susceptibles d'avoir dans ce domaine.

Mondialisation

Selon le Forum économique mondial, nous entrons dans une nouvelle ère de la mondialisation axée sur le numérique, la « mondialisation 4.0 ». Dans cette ère, les biens et services *numériques*, sous-tendus par des capacités numériques et l'intelligence artificielle (IA), constituent les principales exportations[9].

Impact sur le réseau

À l'heure où les connexions entre les systèmes, les personnes, les processus, les sites et les équipements deviennent de plus en plus distribuées et complexes, la valeur économique du réseau pour l'entreprise va s'accroître. En parallèle, la sécurisation et l'administration du réseau va devenir plus stratégique et plus difficile.

Transformation numérique de l'entreprise

De plus en plus d'entreprises recourent aux technologies numériques, comme l'analytique, la mobilité, les solutions cloud et l'Internet des objets (IoT), pour ancrer leur processus de transformation. Selon le rapport *Digital Vortex 2019* publié par IMD et Cisco, 88 % des cadres dirigeants estiment que la disruption numérique aura un impact majeur ou transformateur sur leur secteur d'activité, contre seulement 27 % en 2015[10].

Impact sur le réseau

L'imprévisibilité inhérente à l'activité d'une entreprise impose la mise en place d'un réseau capable de s'adapter rapidement à l'évolution de ses impératifs afin de proposer de nouveaux services, processus et modèles.

Automatisation métier

Dans les prochaines années, le recours à l'automatisation et à la robotique va continuer de progresser pour accompagner les efforts des entreprises visant, entre autres, à améliorer leur qualité, la productivité de leurs employés et la satisfaction de leurs clients. Selon les prévisions du Capgemini Research Institute, l'adoption généralisée de l'automatisation devrait permettre de réaliser 471 milliards de dollars d'économies d'ici 2022 dans les secteurs de l'automobile, de la vente au détail, de la distribution d'énergie et de la production industrielle[11].

Impact sur le réseau

Parce que l'automatisation des processus est urgente et stratégique, le réseau doit garantir une livraison fiable et ponctuelle des paquets.

Résilience de l'entreprise et des opérations

La mondialisation et la transformation numérique rendent les organisations dépendantes d'un ensemble toujours plus complexe de technologies, de systèmes, de processus, de chaînes logistiques et d'infrastructures. Pour être effectivement résiliente, l'entreprise doit évaluer ses risques opérationnels de manière continue et proactive, établir et auditer des plans d'urgence, et former ses équipes à la gestion des incidents.

Impact sur le réseau

Pour protéger les employés, les clients et les partenaires, mais aussi récupérer des données et rétablir rapidement les services et l'accès aux systèmes, une architecture réseau doit impérativement être agile, résiliente et sécurisée.

Développement durable

Dans un monde toujours plus interconnecté, les entreprises sont tenues de s'inscrire dans une stratégie de développement durable. Au-delà des indicateurs standard, elles seront jugées sur leur capacité à réduire les émissions de gaz à effet de serre, à préserver la biodiversité et les ressources naturelles et à concevoir des produits à même de minimiser les déchets ou de favoriser leur recyclage.

Impact sur le réseau

Les réseaux évolués laissent envisager des gains d'efficacité concernant pratiquement tous les aspects de l'entreprise, de la consommation d'énergie à l'utilisation des ressources et la réduction des émissions.

Tendances technologiques favorisant l'évolution du réseau

À l'heure actuelle, plusieurs tendances émergentes transforment profondément le panorama des technologies de l'information. Un examen plus poussé de ces tendances clés montre l'impact qu'elles peuvent avoir sur les réseaux d'entreprise.

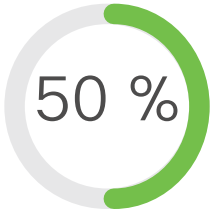
L'évolution des applications

Les applications et les données se trouvent évidemment au cœur de l'entreprise numérique et les modalités de développement, d'hébergement et de consommation des applications changent en permanence afin de répondre aux nouveaux impératifs métier.

Voici quelques-unes des évolutions que connaissent les applications, avec des conséquences sur le réseau :

Applications et données sortent des locaux de l'entreprise : les applications et les données sont modularisées en microservices et transférées dans de multiples clouds publics. Dans certains cas, elles sont également réparties à la périphérie du réseau. Et elles sont de plus en plus acquises auprès de différents fournisseurs SaaS (Software-as-a-Service).

Les applications sont modulaires et distribuées dans plusieurs environnements : bien souvent, les applications monolithiques se décomposent en microservices interconnectés, fournis à l'ensemble de l'entreprise par le biais de diverses charges virtuelles et physiques, y compris des conteneurs.

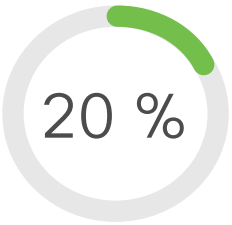


Selon l'Uptime Institute, la moitié de toutes les charges applicatives seront exécutées en dehors du data center de l'entreprise d'ici 2021, soit dans des infrastructures cloud et data center externes, soit à la périphérie du réseau[2].

Les applications sont générées en continu et rapidement : pour les applications développées et hébergées localement, l'IT doit accélérer ses propres processus de création et de déploiement de services d'infrastructure afin de répondre aux besoins des applications et des utilisateurs tout en limitant les coûts opérationnels.

Les applications migrent du physique au virtuel, aux conteneurs et au sans-serveur : avec l'essor des conteneurs, les paradigmes de

conception et de développement d'applications sont soumis à une disruption bien plus profonde, à savoir les architectures sans serveur. Les entreprises sont alors forcées de remettre à plat leurs méthodes de conception des applications, le rôle de leur infrastructure et leur conception des processus opérationnels.



À l'horizon 2021, les instances de conteneurs installées et utilisées devraient dépasser les 3,5 milliards et plus de 20 % d'entre elles devraient être exécutées à des emplacements distribués pour servir des charges applicatives IoT ou périphériques[1].

Impact sur le réseau

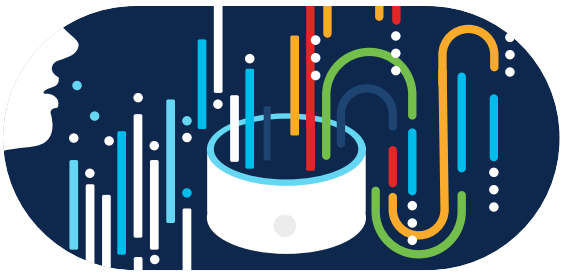
Avec l'apparition d'applications et de microservices dans tous les domaines, le réseau doit être envisagé davantage comme un ensemble croissant de « clusters nerveux » interconnectés et situés à proximité des données, c'est-à-dire en tout point du continuum périphérie-cloud. Le nouveau réseau doit être en mesure de sécuriser les liaisons au sein et entre ces « clusters nerveux », mais aussi de parfaitement comprendre le fonctionnement de ces nouveaux modèles applicatifs et d'appliquer les politiques applicatives de manière dynamique en tout point du réseau hébergeant les applications.

IoT

L'explosion des appareils et applications IoT, et de leurs données générées, favorise la création de nouveaux modèles informatiques distribués reposant sur une ampleur et un degré de complexité à la croissance exponentielle. Selon l'outil de synthèse des prévisions VNI de Cisco, les équipements intermachines (M2M) représenteront 51 % (14,6 milliards) de tous les appareils en réseau dans le monde en 2022[12].

Impact sur le réseau

En plus d'assurer la connectivité et la sécurité d'un ensemble extrêmement diversifié d'équipements IoT, les administrateurs réseau devront élaborer des méthodes efficaces et évolutives pour automatiquement identifier ces appareils, les classifier et leur appliquer des politiques. Il leur faudra aussi les surveiller pour garantir leur bon fonctionnement sans compromettre les autres services exécutés sur le réseau ou influer sur eux.



IA

L'émergence des applications optimisées par l'IA à destination des entreprises et des particuliers donne naissance à un nouvel univers constitué d'appareils connectés, intelligents et automatisés, aujourd'hui omniprésents.

Impact sur le réseau

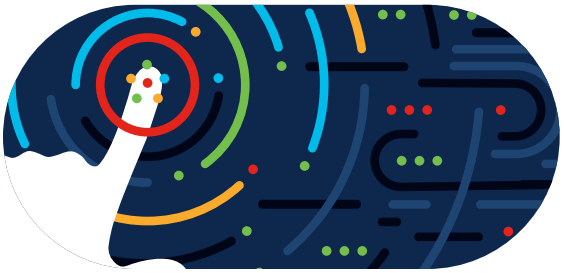
Pour exploiter tout le potentiel de l'IA en entreprise, une plus grande part du traitement informatique et de la prise de décision doit avoir lieu en périphérie. Selon les critères retenus en matière de performances, de capacité, de confidentialité et même de coûts, le traitement IA et les données seront placés dans le cloud, dans des data centers sur site ou à la périphérique du réseau.

Mobilité

Selon l'outil de synthèse des prévisions VNI de Cisco, le trafic mondial de données mobiles professionnelles va être multiplié par six entre 2017 et 2022, avec un taux de croissance annuel de 42 %[12]. Les utilisateurs mobiles professionnels garderont les mêmes attentes d'immédiateté, de performances et de connectivité permanente et omniprésente, avec tous les appareils en Wi-Fi et sur des réseaux 4G et 5G publics. En parallèle, les objets connectés se généraliseront au point d'intégrer tous les aspects du quotidien.

Impact sur le réseau

Lorsque des employés accèdent aux applications cloud sur des appareils professionnels ou privés en dehors du réseau de l'entreprise, les administrateurs réseau et sécurité se heurtent à un manque inédit de visibilité et de contrôle. De plus, la vague d'équipements IoT va amplifier les contraintes de connectivité sans fil en termes d'échelle, de diversité du trafic et de sécurité.



Sécurité

De plus en plus sophistiquées et dangereuses, les menaces de cybersécurité visent une surface d'attaque plus étendue et désormais affranchie d'un périmètre bien défini et défendu. En outre, avec le transfert des charges applicatives en dehors du site, l'IT court particulièrement le risque de perdre en visibilité.

Impact sur le réseau

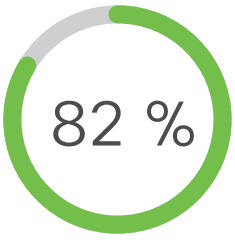
Certes, le réseau restera un allié puissant pour identifier et contenir les menaces, mais les équipes opérationnelles réseau et sécurité doivent partager leurs données et intégrer leurs outils et leurs workflows pour mieux lutter contre des attaques toujours plus nombreuses et complexes. En outre, le réseau peut étendre le rayon d'action de l'IT aux environnements cloud afin de mieux protéger les applications et les données, même si elles ne sont pas sous son contrôle direct.

Expériences immersives

L'utilisation croissante de la vidéo et l'émergence des réalités virtuelle (RV) et augmentée (RA) permettant d'améliorer la collaboration, la formation, la productivité et le télétravail, vont encore alourdir la demande de services réseau dans l'entreprise.

Impact sur le réseau

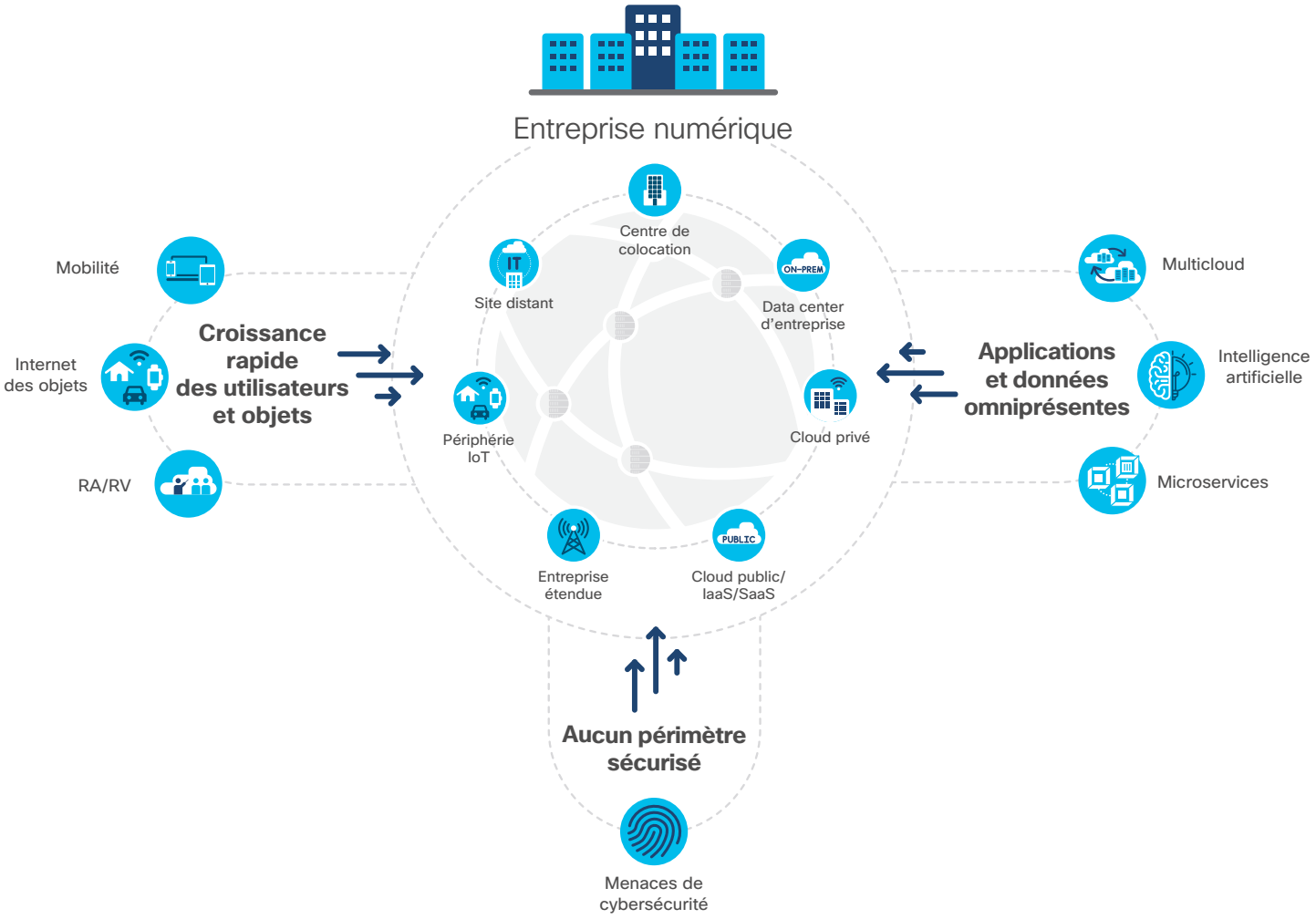
Le réseau devra fournir des liaisons de communication avec une bande passante de bout en bout et une faible latence, ainsi que des contrôles de performances dynamiques, tous adaptés à ce type d'expérience immersive.



En 2022, la vidéo sur Internet représentera 82 % de l'ensemble du trafic Internet des entreprises, le trafic RV/RA va être multiplié par douze et le trafic de vidéosurveillance par Internet par sept[13].

Ce contexte technologique dynamique n'est pas seulement une réalité pour toutes les entreprises et leurs clients, il est aussi le moteur de l'économie numérique. Il n'est pas surprenant que les départements IT ressentent fortement la nécessité de prendre en compte toutes ces tendances en mobilisant les bonnes stratégies technologiques, des modèles opérationnels fiables et les compétences adéquates.

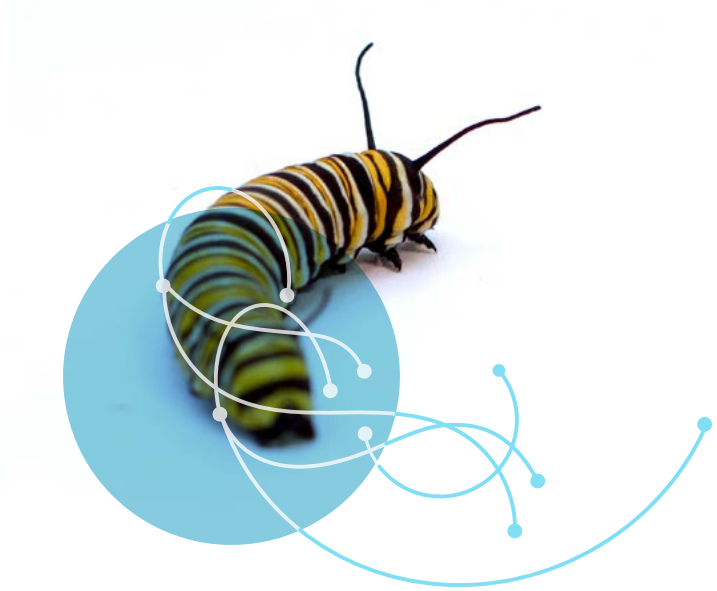
Figure 2 Les technologies qui boostent les nouvelles exigences réseau



Nécessité de proposer un nouveau type de réseau

Dans cet environnement de plus en plus exigeant, les responsables IT se doivent d'adopter une approche radicalement nouvelle du réseau.

Si l'entreprise veut prospérer dans l'économie numérique, son réseau doit être capable de s'adapter rapidement à l'évolution des impératifs métier. Il doit prendre en charge un ensemble de plus en plus varié et changeant d'utilisateurs, de périphériques, d'applications et de services. Il doit assurer l'intégration transparente et sécurisée de cette diversité d'équipements, et offrir une expérience utilisateur et applicative à la hauteur des attentes.



Il doit également fournir un accès rapide et sûr aux charges applicatives et entre elles, quel que soit leur emplacement. Et pour que le réseau offre un fonctionnement optimal, tous ces impératifs doivent être mis en œuvre de bout en bout entre les utilisateurs, les périphériques, les applications et les services dans chacun des domaines du réseau : site principal, site distant, bureau distant/domicile, WAN, opérateur, réseau mobile, data center, cloud hybride et multicloud.

Par conséquent, les entreprises ont besoin d'une nouvelle architecture intégrée pour chaque domaine réseau ; une architecture qui soit personnalisée pour répondre aux besoins précis du domaine tout en permettant de transmettre et d'appliquer des politiques homogènes à l'intégralité du réseau.

Figure 3 Les quatre principaux objectifs du nouveau réseau

Être en phase avec l'entreprise	Réduire la complexité	Garantir les performances	Réduire les risques
• Favoriser le lancement de nouvelles initiatives numériques pour l'entreprise • S'adapter de manière dynamique à des besoins applicatifs changeant rapidement	• Simplifier les opérations IT dans un contexte d'exigences croissantes • Permettre à l'IT de focaliser les ressources sur la création de valeur pour l'entreprise	• Toujours tenir les impératifs de performances des services et d'expérience utilisateur • Éviter les perturbations du réseau	• Prévenir ou circonscrire les menaces de sécurité avant qu'elles ne provoquent des dégâts • Respecter les exigences de conformité et les réglementations

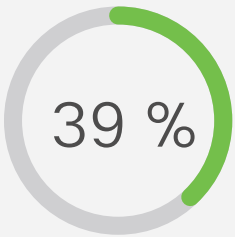
L'architecture réseau émergente envisagée par les experts Cisco

La majorité des réseaux actuels ne sont pas prêts à répondre aux exigences de cette nouvelle ère numérique. Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, nous avons constaté que si 39 % des responsables IT estiment que leurs réseaux sont tout à fait en phase avec les exigences de l'ère numérique, seuls 19 % des architectes réseaux ont la même conviction[14].

Il y a néanmoins des raisons d'être optimiste. John Apostolopoulos, CTO de Cisco pour les réseaux d'entreprise, s'attend à une transition relativement courte entre les infrastructures d'aujourd'hui, essentiellement rigides et pilotées manuellement, et les architectures plus agiles, pilotées par logiciel, capables de « s'adapter en permanence à une demande changeante d'applications et de services indispensables à l'entreprise ».

> « Les réseaux vont fonctionner comme un système doté d'une autonomie croissante, qui prendra en compte son propre état, l'état dynamique de tous les utilisateurs et applicatifs, et la grande variété des options envisageables ».
>
> – Ravi Chandrasekaran, VP senior de l'ingénierie des réseaux d'entreprise chez Cisco

À quoi ressemblera cette nouvelle architecture réseau ? Selon Ravi Chandrasekaran, VP senior de l'ingénierie des réseaux d'entreprise chez Cisco, « les réseaux vont fonctionner comme un système doté d'une autonomie croissante, qui prendra en compte son propre état, l'état dynamique de tous les utilisateurs et applicatifs, et la grande variété des options envisageables ».



Nous avons constaté que si 39 % des responsables IT estiment que leurs réseaux sont tout à fait en phase avec les exigences de l'ère numérique, seuls 19 % des architectes réseaux ont la même conviction[14].

Pour atteindre ce niveau d'autonomie, l'IA sera essentielle, puisqu'elle aidera les équipes IT à répondre rapidement aux changements de conditions du réseau, qu'il s'agisse de modifier automatiquement le routage du trafic, de demander plus de bande passante, d'exiger une modification de politique ou même de refuser une demande pour un nouveau service.

Avec le temps, en tirant parti de l'automatisation et des informations collectées à l'échelle du système, le réseau deviendra complètement transparent pour l'utilisateur. Il sera simplement présent, offrant une connectivité sécurisée aux services nécessaires à l'utilisateur, avec le niveau requis, partout et à tout moment.

Si M. Apostolopoulos admet qu'il reste beaucoup de chemin à parcourir avant que les réseaux acquièrent toute l'intelligence et la puissance

que suppose cette promesse, il est convaincu que les avancées techniques sont en bonne voie pour faire converger l'assurance de service reposant sur l'IA, l'automatisation basée sur un contrôleur, le traitement du langage naturel et une sécurité des réseaux fortement améliorée.

Cas d'usage du nouveau réseau

En 2025, un réseau d'entreprise de pointe sera capable de prendre en compte un besoin formulé en langage naturel par n'importe quelle entité de l'entreprise et de le convertir en un ensemble de politiques et d'automatismes assurant une réponse constante au besoin métier dans l'ensemble du réseau et ce, sans aucune incidence sur les services en place. Un réseau doté de telles capacités est communément qualifié d'intuitif.

Voici à quoi pourrait ressembler un cas d'utilisation pour un réseau intuitif.

Vue d'ensemble : Une entreprise souhaite utiliser des capteurs optiques IoT sans fil pour mettre en œuvre une innovation métier par le biais d'une application de réalité augmentée. Voici comment le besoin et l'intention métier pourraient être convertis en action réseau.

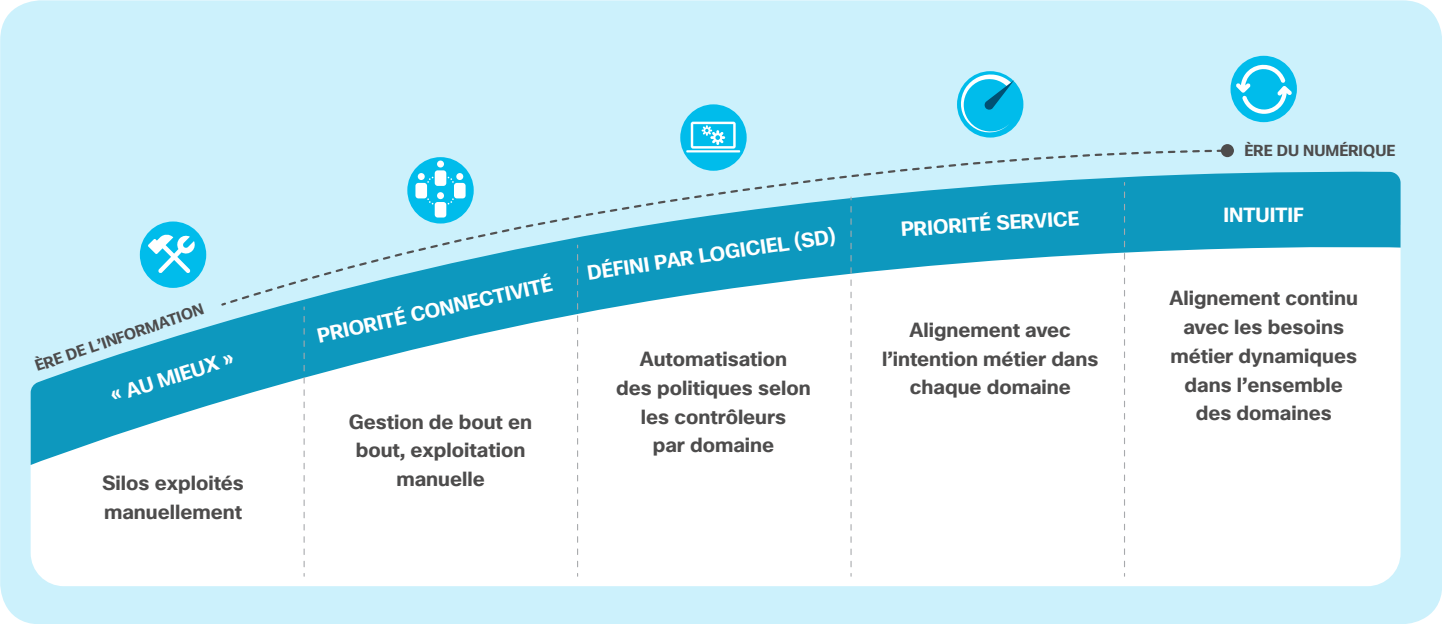
Figure 4 Cas d'usage du nouveau réseau

État de l'architecture réseau

Où se situent actuellement les entreprises sur le chemin menant à un réseau plus avancé, capable de répondre aux exigences de l'ère numérique ? Le modèle Cisco de préparation du réseau au numérique propose cinq stades de maturité pour aider les départements IT à évaluer le degré de préparation actuel de leur réseau et à déterminer l'objectif qu'elles doivent atteindre dans le futur.

Le modèle peut s'appliquer à plusieurs aspects de la préparation du réseau, comme l'architecture, l'accès, le WAN, l'assurance, la sécurité réseau, etc.

Figure 5 Modèle Cisco de préparation du réseau au numérique



Rapport sur les tendances mondiales des réseaux en 2020

Tendances des technologies réseau

Cinq tendances façonnent aujourd'hui le nouveau réseau.

À l'heure actuelle, plusieurs développements technologiques majeurs s'unissent pour poser les fondations d'un nouveau modèle de réseau. Les avancées réalisées dans cinq domaines technologiques particuliers, à savoir **l'automatisation, l'IA, les réseaux multicloud, le sans-fil** et **la sécurité réseau**, annoncent la plus forte vague de transformation du réseau depuis des décennies. Ces technologies visent à répondre aux attentes d'échelle, d'agilité et de sécurité exprimées par le marché et, ce faisant, elles alimentent les nouvelles tendances qui bouleversent le monde tel que nous le connaissons.

Domaines technologiques

- Automatisation
- IA
- Réseau multicloud
- Sans-fil
- Sécurité réseau

« Dans le monde entier, les entreprises se rendent compte de la nécessité de se transformer pour rester en phase avec le marché et répondre aux exigences de leurs employés, de leurs partenaires, de leurs clients et des entités qui les composent », explique Brandon Butler, analyste chercheur en chef d'IDC pour les réseaux d'entreprise. « En outre, les responsables IT comprennent que l'absence d'un réseau agile, sécurisé et robuste compromet la transformation numérique de leur entreprise, ce qui les encourage à remanier simultanément de nombreux aspects de leurs réseaux ».

Un état des lieux approfondi de chacune de ces technologies permet de comprendre leur impact sur le modèle réseau, leur niveau d'adoption actuel et les changements qu'elles devraient apporter dans un avenir proche.

Figure 6 Les cinq technologies qui favorisent la transformation réseau

Automatisation du réseau à grande échelle

Résumé de la section

Points clés

- La combinaison du réseau défini par logiciel (SDN), du réseau intuitif (IBN), de la virtualisation réseau, de la programmabilité et des contrôleurs de plateforme ouverte permet de concrétiser l'alignement automatisé des services réseau sur les besoins métier et les processus IT.
- L'IBN augmente les capacités d'automatisation du SDN avec la possibilité de convertir l'intention en politiques, de collecter des données, d'apporter de la visibilité, de résoudre les problèmes, et de vérifier que les politiques remplissent véritablement les objectifs.
- L'objectif de l'IBN est de mettre en place une application et une validation en continu des impératifs de performance des services, des politiques de sécurité et conformité, et des processus opérationnels de l' IT sur l'ensemble du réseau.
- Des interfaces de programmation d'application (API) placées sur un contrôleur de plateforme ouverte permettent à ce dernier de s'intégrer et d'échanger des informations avec des services IT et réseaux adjacents, d'autres domaines IT, des applications métier et des éléments d'infrastructure hétérogènes.

Conclusions clés

- Pour les responsables IT, l'automatisation réseau (25 %), le SDN (23 %) et l'IBN (16 %) font partie des technologies qui auront le plus d'impact sur les réseaux ces cinq prochaines années.
- 27 % des responsables IT reconnaissent qu'une conception en silos et une approche opérationnelle cloisonnée de l'accès, du WAN, du data center (DC), du cloud et de la sécurité constituent un frein à l'adoption des technologies réseau de pointe.
- 34 % des responsables IT soulignent l'importance d'une coordination et d'une intégration du réseau améliorées avec les autres équipes IT.
- Tandis que seuls 4 % des responsables IT et architectes réseaux qualifient déjà leur réseau d'intuitif, 35 % prévoient d'arriver à un réseau intuitif dans un délai de deux ans.

Résumé de la section (suite)

Conseils décisifs

- Les responsables IT doivent évaluer le degré de préparation de leur réseau afin de fournir les services nécessaires à l'activité métier en temps voulu.
- Élaborez une feuille de route permettant de mettre en œuvre une stratégie de réseau intuitif en boucle fermée sur chaque domaine réseau, avec des étapes successives qui procureront à l'entreprise le meilleur retour sur investissement.
- Identifiez et hiérarchisez les processus IT et applications métier qui bénéficieront le plus de l'intégration avec un contrôleur réseau de plateforme ouverte.

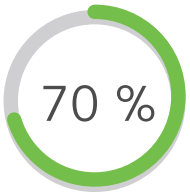
Prévision clé

« Envisagée depuis longtemps, l'application intuitive des politiques de bout en bout deviendra une réalité en 2025. Les équipes réseau pourront automatiser des politiques d'optimisation des services et de segmentation dynamique à grande échelle dans l'ensemble des domaines réseau (accès, WAN, data center, multicloud, IoT), d'un bout à l'autre de la liaison client-application et entre les charges distribuées ».

– Ronnie Ray, VP de l'expérience client pour les réseaux d'entreprise, Cisco

Automatisation du réseau à grande échelle

L'automatisation réseau consiste, comme son nom l'indique, à automatiser la configuration, la gestion, le test, le déploiement et l'exploitation des périphériques virtuels et physiques d'un réseau. L'optimisation du réseau peut elle-même être automatisée pour assurer l'amélioration continue des services.



Selon Gartner, « environ 70 % des tâches réseau d'un data center s'effectuent manuellement et se traduisent, par conséquent, par une perte de temps, des coûts supplémentaires et plus de probabilité de commettre des erreurs, mais également par une réduction de la flexibilité »[15].

L'automatisation peut améliorer la disponibilité du réseau et soulager les équipes d'opérations réseau (NetOps) de tâches quotidiennes laborieuses. Rien de surprenant, donc, que 25 % des responsables IT interrogés la désignent comme la technologie qui aura le plus fort impact sur le réseau au cours des cinq prochaines années[14].

Aujourd'hui, cette automatisation des réseaux se concrétise grâce aux innovations réalisées dans plusieurs domaines : réseau défini par logiciel ou SDN (Software-Defined Network), réseau intuitif ou IBN, virtualisation, programmabilité et contrôleurs de plateformes ouvertes.

25 % des responsables IT estiment que l'automatisation aura le plus fort impact sur le réseau au cours des cinq prochaines années[14].

Réseau défini par logiciel (SDN) : une première étape

Ces dernières années, le réseau défini par logiciel ou SDN (Software-Defined Network) a permis de réaliser un pas de géant dans l'automatisation à l'échelle du réseau. Avec le SDN, les équipes dédiées peuvent gérer les réseaux comme des systèmes de bout en bout, et ainsi gagner en flexibilité et en efficacité grâce à la séparation du plan de contrôle et du plan de commutation.

Dans ce système, le plan de contrôle devient directement programmable. Il abstrait l'infrastructure et les périphériques sous-jacents des applications et des services réseau. L'intelligence réseau est centralisée logiquement par le biais de contrôleurs SDN programmables.

À l'origine, le SDN a été proposé pour simplifier les environnements de data center complexes qui devaient prendre en charge des migrations de charges applicatives dynamiques et portables, ainsi que le trafic interserveur. Les mêmes principes sous-tendent l'accès défini par logiciel (SD-Access), qui contribue à une sécurisation plus efficace des accès utilisateur et périphérique, et le réseau étendu défini par logiciel (SD-WAN), qui peut améliorer l'expérience d'accès aux applications et services cloud pour les utilisateurs.

Réseau intuitif : boucler la boucle

L'objectif principal des équipes réseau est d'assurer la continuité de la performance et de la protection des services et des applications utilisés pour l'activité métier. Si le SDN offre d'importantes avancées en matière d'automatisation, il ne représente qu'une partie de la solution. Les entreprises ont aussi besoin d'une surveillance et d'une optimisation constantes du réseau afin d'appuyer des modèles économiques toujours plus dynamiques et digitalisés.

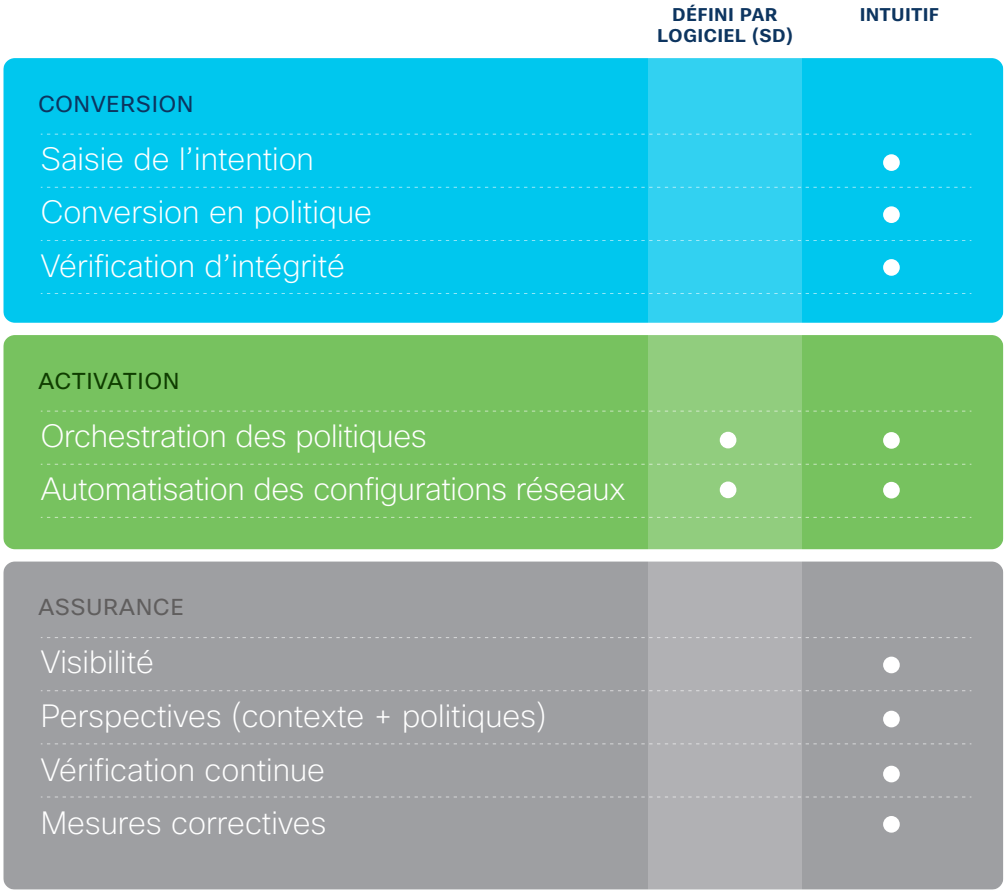
Pour y parvenir, les réseaux doivent comprendre l'intention évolutive de l'activité métier et surveiller leurs conditions dynamiques de manière à toujours s'adapter à cette intention. Selon un rapport préliminaire de l'Internet Engineering Task Force (IETF), « l'intention constitue une politique déclarative dont la portée s'étend à l'ensemble du réseau. Un opérateur humain définit l'attente et le réseau calcule une solution répondant aux impératifs »[16].

Le réseau intuitif est un modèle relativement récent, mis sur le marché pour la première fois en 2017 et largement adopté depuis par le secteur du réseau.

Pour être utile, le système doit vérifier en permanence que l'intention est respectée et, dans le cas contraire, fournir des conseils pour y remédier. Gartner indique que « les configurations par politiques vont se transformer en solutions de réseau

intuitif (IBN) grâce à une automatisation capable de s'autosurveiller pour s'assurer que le réseau respecte l'intention des politiques définies au moment de la configuration »[15].

Figure 7 Le réseau intuitif s'appuie sur les fondamentaux du SDN



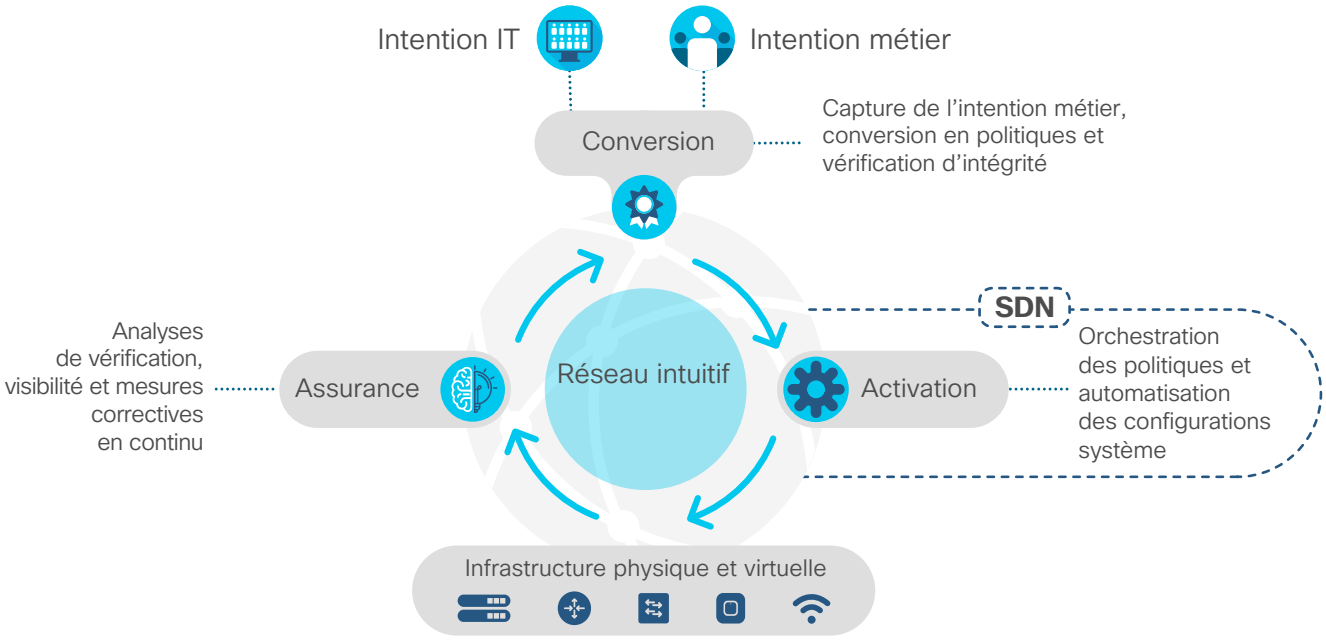
Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, nous avons constaté que 26 % des architectes réseaux considèrent le déploiement d'un réseau intuitif dans un ou plusieurs domaines comme une technologie prioritaire pour obtenir le réseau idéal. Et tandis que seuls 4,3 % des sondés qualifient déjà leur réseau d'intuitif, 35 % prévoient d'arriver à un réseau intuitif dans un délai de deux ans[14].

John Apostolopoulos explique qu'un contrôleur IBN s'appuie sur le SDN pour offrir un système plus complet, capable d'adapter constamment le réseau afin de réaliser l'intention métier voulue. Il augmente les capacités d'automatisation du SDN avec la possibilité de convertir l'intention en politique, de collecter des données, d'apporter de la visibilité et des perspectives pertinentes, puis de vérifier que le réseau accomplit véritablement ce qui a été prévu. L'IBN fournit une rétroaction en boucle fermée fondamentale pour obtenir les avantages souhaités[17].

Un réseau intuitif capture l'intention métier et s'appuie sur l'analytique, l'apprentissage automatique, le raisonnement machine et l'automatisation pour s'adapter de manière continue et dynamique à l'évolution des besoins métier, tout en prenant en compte les changements de charges réseau et d'autres paramètres environnementaux. Cela peut se traduire par une application et une validation continues des impératifs de performance des services, et des politiques concernant les utilisateurs, la sécurité, la conformité et les opérations IT sur l'ensemble du réseau.

Comment fonctionne un réseau intuitif ? Selon la définition de Cisco, le réseau intuitif se compose de trois piliers fonctionnels : conversion, activation et assurance[18].

Figure 8 Éléments d'un réseau intuitif



Les responsables IT sont tenus de fournir des services plus rapidement et plus efficacement en collaboration avec les services cloud, mais aussi en concurrence avec eux. D'un point de vue technologique, la puissance de traitement et de calcul ainsi que la maîtrise de l'IA, indispensables aux réseaux intuitifs, sont de plus en plus accessibles.

Rohit Mehra, d'IDC, explique : « Le réseau intuitif est une avancée considérable pour le secteur des réseaux. Non seulement il repousse les limites de la visibilité, de l'automatisation et de l'assurance, mais il constitue aussi la plateforme sur laquelle seront conçues les nouvelles fonctions de gestion réseau pilotées par l'apprentissage automatique »[19].

Virtualisation des fonctions réseau

Le modèle de virtualisation qui a totalement bouleversé les services de calcul a été transposé au réseau avec la virtualisation des fonctions réseau (NFV, Network Functions Virtualization). Il permet au NetOps de fournir ou modifier rapidement des services réseau et de procéder à leur déploiement et à leur administration à distance. Outre l'agilité de l'IT, le NFV permet une consolidation physique importante, avec des gains d'espace et de puissance et une réduction des points de défaillance potentiels.

Un réseau fondé sur la programmabilité

Pour que les contrôleurs et systèmes IBN soient évolutifs et délivrent leur plein potentiel, ils doivent être bâtis sur une infrastructure réseau virtuelle ou physique programmable. Les équipements et interfaces programmables ainsi que les circuits intégrés spécifiques

aux applications (ASIC) programmables forment la base d'un réseau intelligent.

Pour mettre en place des systèmes automatisés plus efficaces, les équipes IT abandonnent les approches de gestion manuelle par interface de ligne de commande (CLI), au profit d'interfaces pilotées par des modèles de données. Ces interfaces modélisées standard fournissent ainsi cohérence, ouverture, structuration et efficacité.

Ouvrant la voie vers un modèle opérationnel viable combinant cohérence et simplicité d'utilisation, les modèles normalisés de l'IETF tels que YANG offrent un ensemble complet d'interfaces de programmation ascendantes.

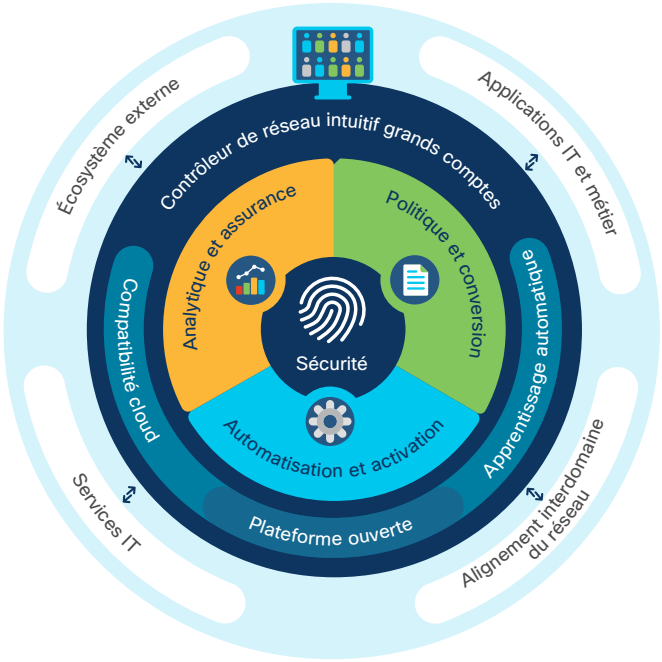
Contrôleurs IBN de plateformes ouvertes : intégration des processus IT et de l'activité métier

Des interfaces de programmation d'application (API) placées sur le contrôleur lui permettent de s'intégrer et d'échanger des informations avec des services IT et réseaux adjacents, d'autres domaines IT, des applications métier et des éléments d'infrastructure hétérogènes.

Ainsi devenu plateforme ouverte, le réseau peut accepter des spécifications de politiques issues des applications et périphériques, profiter de l'automatisation centralisée des politiques interdomaines et vérifier que le système répond aux besoins de l'activité métier. Et la fourniture des services IT s'améliore grâce à la rationalisation des workflows entre tous les domaines réseau, systèmes IT et processus métier auparavant gérés de manière indépendante.

Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, 34 % des responsables IT soulignent l'importance d'une coordination et intégration du réseau améliorées avec les autres équipes IT[14].

Figure 9 Contrôleur de plateforme ouverte pour l'intégration des applications métier, des services IT et des domaines réseau



La possibilité d'étendre le réseau en recourant à des API et des kits de développement réseau (SDK) permet à l'IT de mieux prendre en compte les besoins des applications IT et métier, de rationaliser les opérations et de veiller à la protection des investissements.

Alignement interdomaine des politiques et de l'assurance : du client à la charge applicative

Les équipes réseau doivent travailler main dans la main pour aligner le réseau et l'intention métier de bout en bout. Pour cela, il est nécessaire de créer une liaison transparente du point de connexion du client ou de l'objet au réseau jusqu'au point d'hébergement du service ou de l'application.

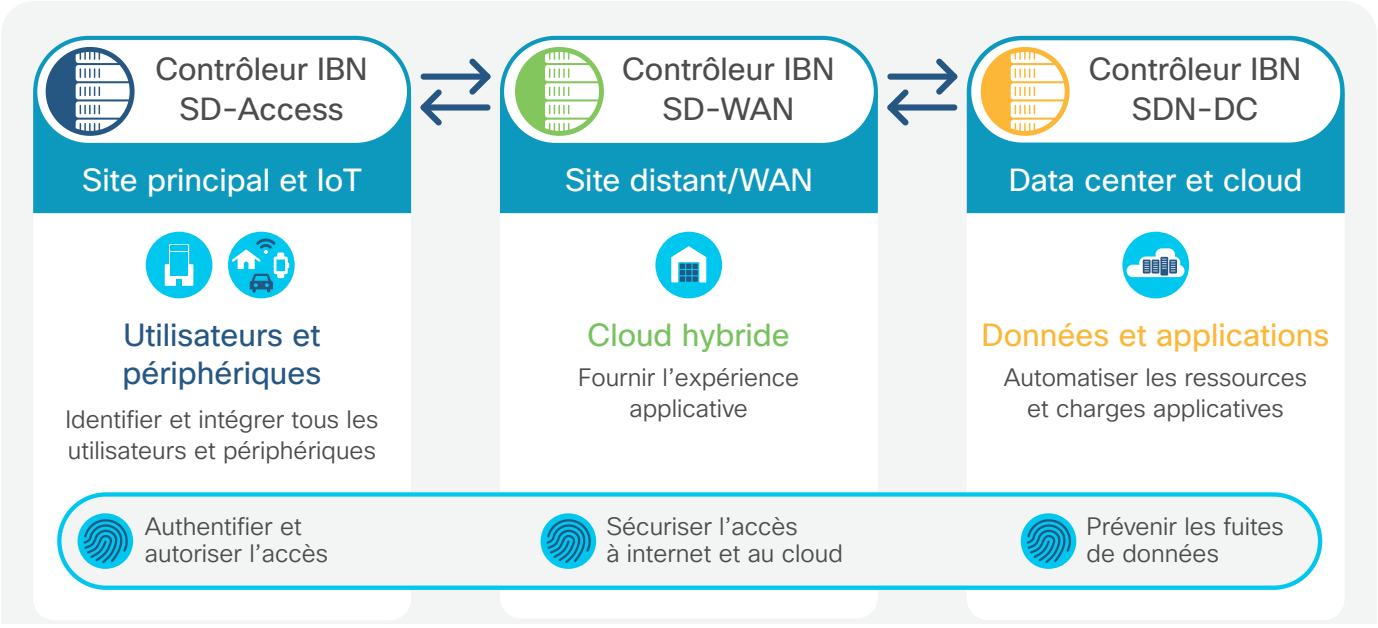
Analyse actuelle : pour mettre en place un réseau intuitif efficace, l'entreprise doit adopter l'automatisation au niveau du data center, du site principal, du réseau étendu et du site distant[20].

Cependant, cet objectif est souvent difficile à atteindre. Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, 27 % des responsables IT reconnaissent « qu'une conception en silos et une approche opérationnelle cloisonnée de l'accès, du WAN, du data center, du cloud et de la sécurité » constituent un frein à l'adoption des technologies réseau de pointe[14].

Habituellement, et pour de bonnes raisons, le réseau se décompose en plusieurs domaines, chacun articulé autour de son objectif principal. Néanmoins, pour véritablement atteindre une visibilité, un contrôle et une validation de bout en bout de l'intention métier, les fonctionnalités de politique et d'assurance doivent être orchestrées sur l'ensemble des domaines.

Les responsables IT prennent des mesures dans ce sens, puisque 26 % d'entre eux considèrent « l'application et la validation de politiques réseau multidomaines intégrées » comme une priorité d'investissement[14].

Figure 10 Politique et assurance : alignement sur l'ensemble des domaines IBN



Assurance basée sur l'IA

Résumé de la section

Points clés

- Avec l'AIOps, catégorie de l'IA dédiée aux opérations IT, l'intelligence artificielle devient un atout essentiel pour les opérations, la mise en œuvre des services et l'assurance réseau.
- Avec l'explosion du volume de trafic, des équipements mobiles et IoT et des applications et microservices interconnectés, ainsi que l'augmentation permanente des menaces de sécurité, les équipes réseau se trouvent débordées.
- Les quantités colossales de données, la télémétrie et les événements générés par des réseaux qui prennent en charge un nombre croissant de périphériques et de services dépassent la capacité d'action des seuls opérateurs humains.
- Composante fondamentale du modèle de réseau intuitif (IBN), l'IA exploite les innombrables données issues du réseau pour évaluer la complexité de l'environnement et propose des ajustements de manière dynamique.
- L'apprentissage automatique et le raisonnement machine se complètent pour fournir un traitement complexe des événements, des perspectives corrélées et des procédures de remédiation guidées.

Conclusions clés

- Plus de 50 % des architectes réseaux considèrent l'IA comme un investissement réseau prioritaire.
- Seuls 17 % des architectes réseaux pensent que la maturité insuffisante des technologies d'IA constitue un obstacle à la modernisation du réseau.
- Seuls 22 % des équipes réseau recourent aujourd'hui à une forme d'IA pour l'assurance réseau, sans doute parce que la disponibilité de véritables outils pilotés par IA est toute récente.
- 68 % des architectes réseaux projettent d'utiliser des perspectives prédictives ou une remédiation pilotées par IA dans un délai de deux ans.

Conseils décisifs

- Tirez parti de l'apprentissage IA dans le cloud : dans certains cas, il faudra envisager de modifier les politiques de données de l'entreprise pour profiter des avantages des outils d'IA basés dans le cloud.
- Imbrication de l'humain et de l'intelligence artificielle : définissez progressivement jusqu'où l'IA peut aller dans la prise de décision ou l'application de mesures avant qu'un humain intervienne pour surveiller, approuver ou modifier le processus.

Résumé de la section (suite)

- Maîtrise de l'IA : une connaissance pointue des réseaux constituera une compétence particulièrement précieuse pour vérifier que la mise en œuvre des objectifs IT et métier par l'IA est conforme aux attentes.

Prévision clé

« En 2025, les outils d'assurance réseau pilotés par IA permettront d'automatiser entièrement de nombreuses tâches précises et bien établies. Cependant, l'expertise et l'intervention d'opérateurs humains resteront indispensables pour la majorité des tâches opérationnelles exigeant une prise de décision plus souple et contextualisée ».

- J.-P. Vasseur, membre du conseil de Cisco, Cisco

Assurance basée sur l'IA

Dans de nombreux secteurs d'activité, l'IA engendre de profondes transformations et devient cruciale pour les opérations IT. Dans ce domaine, l'AIOps est désormais une spécialité bien établie.

Que sont l'IA, l'apprentissage automatique et le raisonnement machine ?

Pour faire simple, l'IA est une discipline accordant aux ordinateurs une intelligence semblable à celle des humains pour la réalisation de tâches précises. L'apprentissage automatique et le raisonnement machine sont deux des catégories principales de l'IA. L'apprentissage automatique peut être décrit comme la capacité à « tirer des leçons statistiques » des données sans programmation explicite. Le raisonnement machine se sert des connaissances acquises afin d'explorer un ensemble de solutions pouvant aboutir à un résultat optimal.

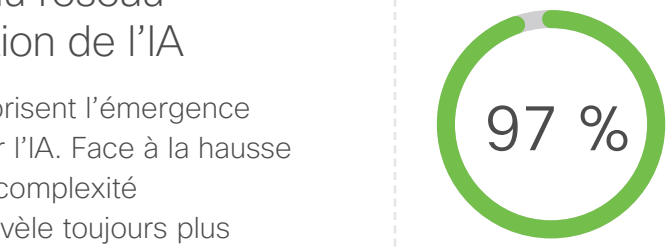
L'apprentissage automatique permet ainsi à un système de scruter les données et d'en déduire des connaissances. Il va au-delà du simple apprentissage ou de l'extraction de connaissances puisqu'il exploite le savoir et l'enrichit au fil du temps et de l'expérience. L'objectif de l'apprentissage automatique est essentiellement d'identifier les schémas cachés dans les données « d'entraînement » et de les exploiter.

Pour sa part, le raisonnement machine est parfaitement adapté à la résolution de problèmes nécessitant une expertise pointue. Pour que le raisonnement machine puisse s'appliquer à de nouvelles données, les humains doivent au préalable assembler toutes les connaissances nécessaires. Le raisonnement machine est donc un formidable complément de l'apprentissage automatique, puisqu'il peut travailler à partir des conclusions présentées par ce dernier, analyser les causes possibles et proposer différentes pistes d'amélioration.

La complexité du réseau renforce l'adoption de l'IA

Plusieurs facteurs favorisent l'émergence des réseaux basés sur l'IA. Face à la hausse sans précédent de la complexité des réseaux, l'IA se révèle toujours plus indispensable pour aider les équipes IT à fournir des niveaux constants de service et de performance réseau.

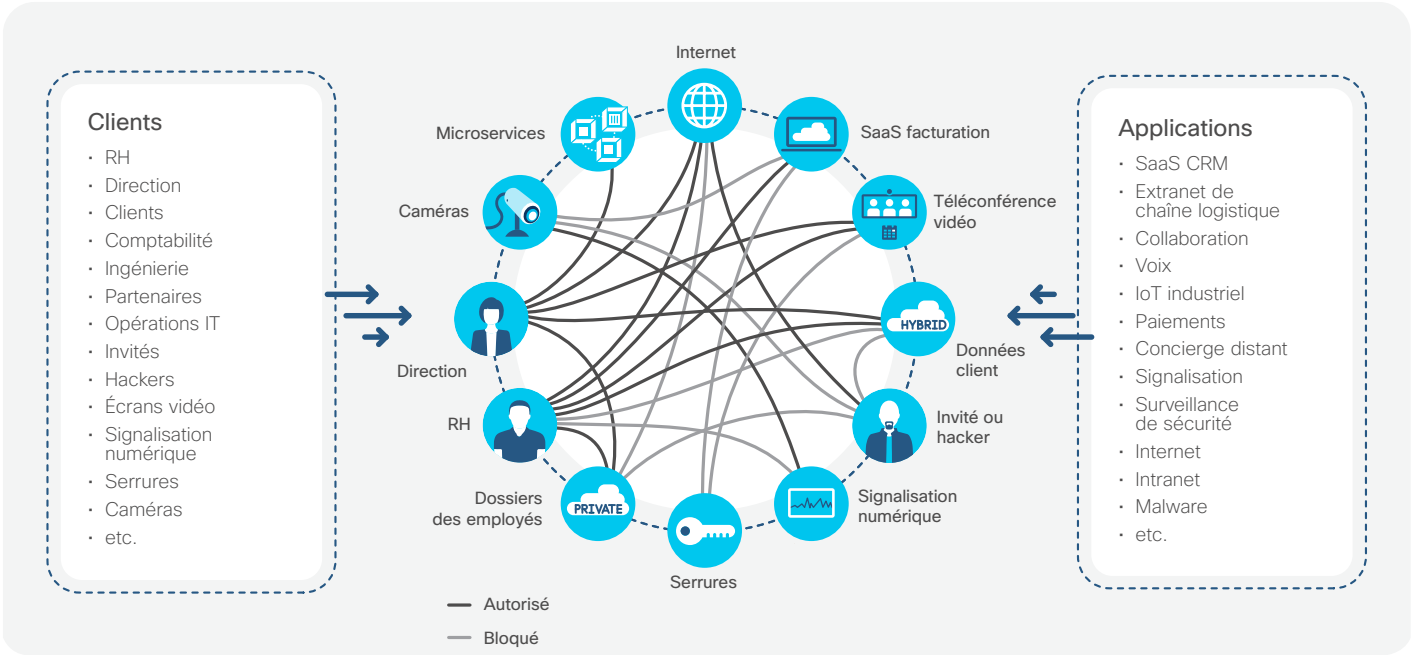
Les réseaux font face à une explosion du volume de trafic, des équipements mobiles et IoT connectés, et des applications et microservices interconnectés. Et ils génèrent désormais des quantités colossales de données que les seuls opérateurs humains ne sont pas en mesure de gérer, encore moindre de comprendre, dans les délais requis.



Le coût des coupures réseau

97 % des responsables IT mondiaux interrogés déclarent avoir rencontré des problèmes de performances touchant des applications stratégiques au cours des six mois précédents. Le coût moyen d'une telle coupure réseau s'élève à 402 542 USD aux États-Unis et 212 254 USD au Royaume-Uni[21].

Figure 11 Complexité du réseau dans les entreprises hyperconnectées



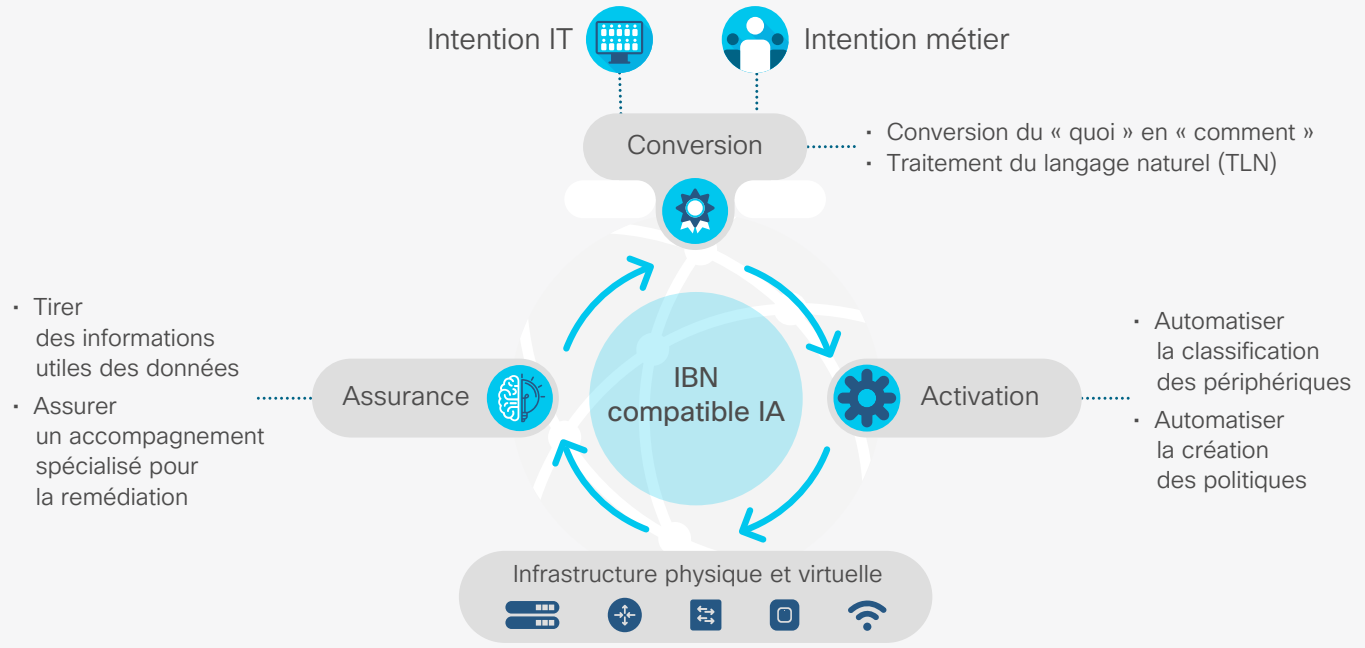
Grâce à l'IA, les équipes réseau peuvent envisager une meilleure utilisation des données afin de garantir un fonctionnement efficace des réseaux et une prise en compte permanente des besoins métier. Elle peut, par exemple, permettre de créer des bases de référence améliorées, prédire avec précision les problèmes et favoriser le dépannage des systèmes complexes.

Les architectes réseaux en font déjà le constat. Plus de 50 % d'entre eux considèrent l'IA comme un investissement prioritaire en vue d'atteindre le réseau idéal[14], tandis que 17 % seulement estiment que la maturité insuffisante des technologies d'IA constitue un obstacle à la modernisation du réseau[14].

Par l'exploitation des innombrables données tirées du réseau, l'IA cerne la complexité des communications et de l'environnement réseau et peut proposer des ajustements de manière dynamique. Cette faculté fait de l'IA un élément fondamental du modèle IBN.

L'IA et les technologies réseau de pointe comme l'IBN bousculent clairement le fonctionnement de l'IT, en particulier dans le domaine des opérations réseau. Avec elles, les nouvelles applications sont testées en quelques minutes au lieu de plusieurs semaines. La résolution des problèmes réseau devient beaucoup plus aisée dès lors qu'un moteur d'assurance peut en identifier les causes profondes et suggérer des correctifs. En effet, si l'opérateur réseau dispose de tableaux de bord puissants offrant des informations exploitables, il n'a plus besoin de passer au crible d'innombrables causes possibles, quelques vérifications suffisent.

Figure 12 Réseau intuitif reposant sur l'IA



Apprentissage automatique et raisonnement machine appliqués au réseau

Comme évoqué plus haut, l'assurance réseau est un élément important des opérations réseau et du réseau intuitif, car elle sert à vérifier continuellement la cohérence de l'état et du comportement du réseau avec l'intention choisie. L'apprentissage automatique et le raisonnement machine offrent des capacités exceptionnellement utiles aux opérateurs pour garantir les performances réseau désirées, en particulier dans les trois domaines suivants (voir figure 13 ci-dessous) :

Traitement complexe des événements : l'application de l'apprentissage automatique à la télémétrie du réseau permet d'établir des bases de référence dynamiques déterminant ce qui constitue les conditions de fonctionnement normal pour une intention donnée.

Perspectives corrélées : l'apprentissage automatique peut apporter des informations et une visibilité plus poussées sur le fonctionnement du réseau et aider à prédire à quel moment une anomalie est susceptible de survenir dans le futur. Le raisonnement machine renforce la puissance de l'apprentissage automatique en appliquant des connaissances pointues acquises lors de la résolution de problèmes similaires.

Remédiation : la remédiation permet la prise en compte permanente de l'intention en identifiant les mesures correctives les plus adaptées à partir des bases de connaissances obtenues, par exemple, avec le raisonnement machine[22].

État actuel et futur de l'IA appliquée à l'assurance réseau

Les données issues de notre *sondage sur les tendances mondiales des réseaux en 2019* montrent où en sont les entreprises dans l'adoption de l'assurance réseau pilotée par IA.

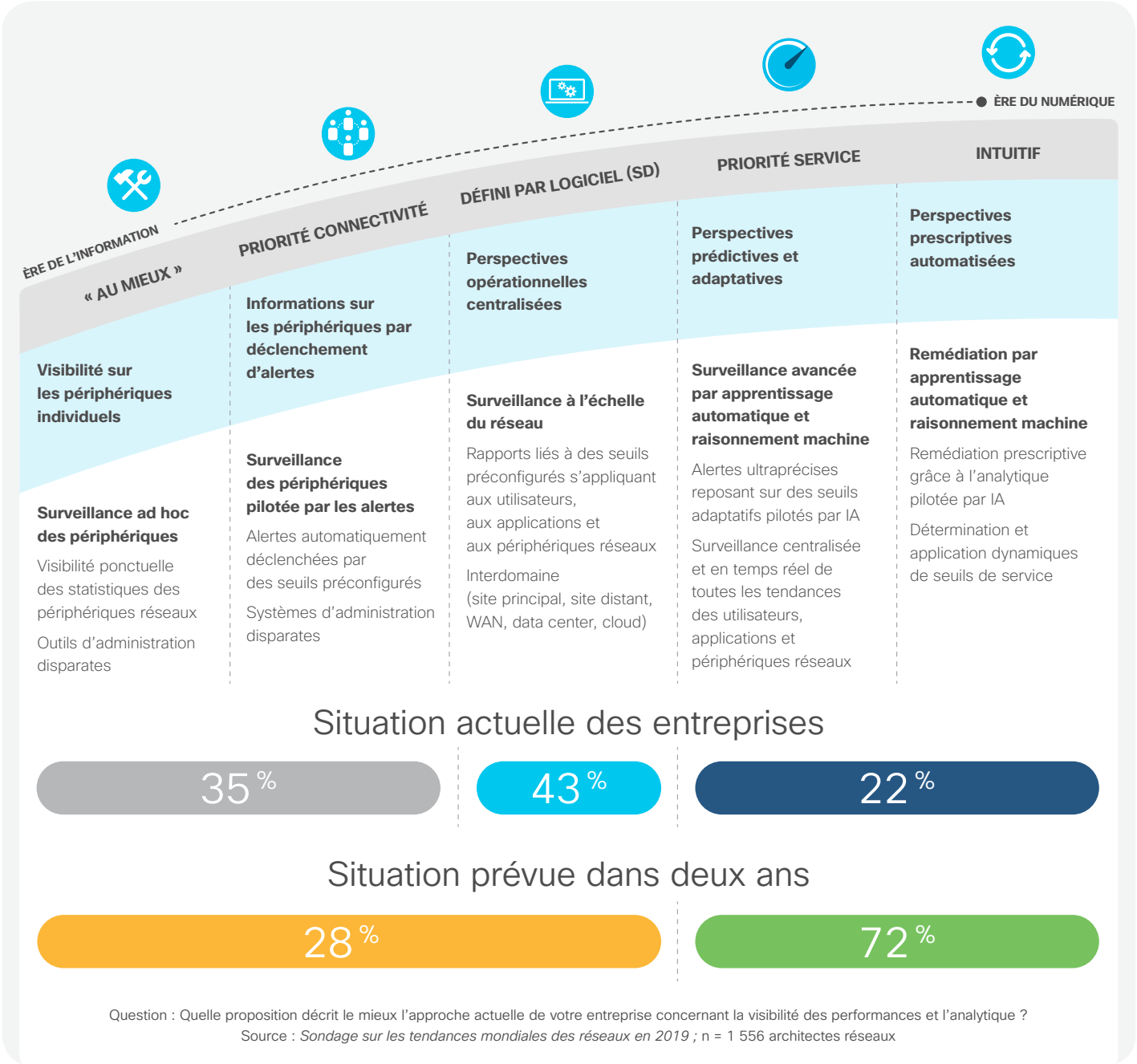
Suivant notre modèle standard à cinq stades servant à estimer le degré de préparation des entreprises, seuls 22 % des architectes réseaux interrogés déclarent utiliser l'IA dans le cadre de

Figure 13 Utilisation de l'apprentissage automatique et du raisonnement machine pour l'assurance réseau

	Apprentissage automatique	Raisonnement machine
Approche technologique	Modèle mathématique à partir d'importants jeux de données	Capture des connaissances humaines, logique symbolique
Applicabilité	Analyse prédictive, détection des anomalies, classification, régression	Mécanisation de workflows de décision
Fonction d'assurance réseau	• Constitution d'une base de référence et identification des problèmes en mode dynamique • Perspectives et visibilité • Analytique prédictive	• Résolution automatique des problèmes • Remédiation automatique

leur assurance réseau. Ce chiffre peut s'expliquer par le fait que les solutions d'assurance réseau véritablement pilotées par IA sont relativement récentes. Néanmoins, 72 % des sondés envisagent de mettre en place des perspectives prédictives ou une remédiation normative pilotées par IA dans un délai de deux ans[14].

Figure 14 Degré de préparation à l'assurance pilotée par IA



Question : Quelle proposition décrit le mieux l'approche actuelle de votre entreprise concernant la visibilité des performances et l'analytique ?
Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 1 556 architectes réseaux

Points à prendre en compte concernant le recours à l'IA

J.-P. Vasseur, membre du conseil de Cisco, recommande de tenir compte des éléments suivants lors de l'évaluation du recours à l'IA dans l'infrastructure réseau :

1. **Définition de pratiques exemplaires pour les opérations :** il ne suffit pas de comprendre toutes les **possibilités** qu'offre l'IA, il faut aussi déterminer ce qu'elle ne **peut pas** et ne **doit pas faire**. Au moment d'établir les domaines de l'entreprise qui peuvent tirer le plus grand parti de l'IA, veillez aussi à identifier les domaines pour lesquels elle constitue un risque élevé.

2. **Définition d'un objectif clair :** aucun algorithme ne peut extraire des faits intéressants d'un ensemble de données si l'équipe d'apprentissage automatique n'a pas clairement spécifié les objectifs. Il est absolument crucial de formuler clairement l'objectif et les indicateurs de performances avant de commencer la mise en œuvre de l'apprentissage automatique.

3. **Imbrication de l'humain et de l'intelligence artificielle :** il est indispensable, pour l'entreprise et pour que l'équipe réseau puisse garder la main, de définir jusqu'où l'IA peut aller dans la prise de décision ou l'application de mesures avant qu'un humain intervienne pour surveiller, approuver ou modifier le processus.

4. **Maîtrise de l'IA :** un recours croissant à l'IA est susceptible d'entraîner des connaissances lacunaires. Une connaissance pointue des réseaux constituera donc une compétence particulièrement précieuse pour vérifier que la mise en œuvre des objectifs IT et métier par l'IA est conforme aux attentes, et pour aider les opérateurs à faire le bon choix parmi les recommandations proposées par le système.

5. **Dépendance aux données :** la collecte des données doit être optimisée. Pour générer des perspectives exploitables, l'IA s'appuie sur des calculs mathématiques dont la valeur dépend entièrement de la qualité des données utilisées. Les spécialistes réseau devront donc travailler de manière transversale sur les fonctions et les domaines pour s'assurer de la fiabilité des données utilisées pour les projets d'IA.

6. **Où appliquer l'IA :** le choix dépendra de la performance, de la sécurité, de la capacité de données et de la confidentialité d'une application et de ses données. Bien qu'il existe des exemples d'entraînement des modèles sur site, l'apprentissage automatique dans le cloud reste le cas de figure le plus courant aujourd'hui. Le cloud offre la capacité de calcul et de stockage nécessaire pour mettre en œuvre l'apprentissage automatique sur de très grandes quantités de données anonymisées et agrégées à partir de plusieurs sources. Dans certains cas, des problèmes de confidentialité peuvent se poser concernant les entités autorisées à accéder aux données, voire le lieu de stockage des données. Tenez compte également des conséquences sur la latence que peut avoir l'analyse en temps réel de vastes ensembles de données, par exemple dans le cas de capteurs vidéo, qui génèrent des quantités de données considérables.

7. **Changement de paradigme dans l'entreprise :** dans l'idéal, les politiques de données de l'entreprise doivent évoluer de manière à tirer partir de l'IA basée dans le cloud. En rattachant des millions de systèmes à un seul et même moteur d'analytique IA, il est possible d'atteindre une taille d'échantillon de données qui fournira de bien meilleurs résultats qu'avec une technologie équivalente alimentée par les données tirées d'une seule expérience réseau. Les équipes IT peuvent dès aujourd'hui jouer un rôle déterminant dans la mise en place de politiques adaptées au cloud en vue du déploiement de l'IA.

Réseaux destinés aux données et applications dans des environnements multicloud

Résumé de la section

Points clés

- Toutes les entreprises auront besoin de services cloud, mais certaines données et charges applicatives devront toujours être maintenues sur site.
- Dans bien des cas, les applications monolithiques se décomposent en microservices interconnectés, fournis à l'ensemble de l'entreprise par le biais de diverses charges virtuelles et physiques, situées dans des conteneurs, sur site, dans le cloud et à la périphérie du réseau de l'entreprise.
- Un data center distribué ne fonctionne pas comme un data center traditionnel. Les départements IT doivent donc s'adapter pour répondre aux exigences d'applications et de connectivité réseau propres à cette nouvelle architecture.
- Pour veiller à ce que les services cloud répondent aux impératifs métier de manière efficace et dans des budgets raisonnables, plusieurs éléments d'architecture émergents sont aujourd'hui importants : le SD-WAN, l'accès cloud direct, les installations de colocation et les Cloud Exchanges, ainsi que les services 5G et haut débit à large bande passante proposés à un tarif plus abordable.

Conclusions clés

- Le SDN/NFV transporte déjà 23 % du trafic au sein des data centers d'entreprise, et ce taux devrait atteindre 44 % en 2021.
- 29 % des responsables IT et architectes réseaux estiment que d'ici deux ans, ils auront instauré des fonctionnalités de réseau intuitif sur l'ensemble de leurs environnements multicloud, cloud hybride et sur site.
- Le recours accru au cloud fait augmenter le trafic WAN : le trafic WAN IP d'entreprise dans le monde devrait doubler d'ici 2022 pour atteindre 5,3 exaoctets par mois.
- Plus de 58 % des entreprises dans le monde ont déjà déployé une forme de SD-WAN et plus de 94 % des sondés pensent qu'ils disposeront d'un SD-WAN intuitif de base ou avancé dans un délai de deux ans.

Conseils décisifs

- Identifiez les applications et services cloud les plus stratégiques et axez vos plans SD-WAN en priorité sur l'accès à ces applications et leur protection.
- Étendez la cohérence de l'automatisation par politique au cloud hybride et au multicloud, en prenant bien compte de l'ensemble des plateformes, des hyperviseurs ou

Résumé de la section (suite)

des frameworks de conteneurs, à tous les emplacements et pour toutes les charges (cloud natives, bare-metal, hyperviseur, conteneur et sans serveur).

- Cartographiez les services applicatifs, les charges et les composants de service sur le réseau « étendu » afin de bien identifier l'emplacement des applications, des services et des microservices au sein du réseau.
- Les équipes data center, cloud et réseau doivent collaborer pour favoriser la cohérence entre tous les domaines : site principal, site distant, data center, périphérie/IoT et fournisseurs de cloud public/SaaS.
- Les applications et services nécessiteront une intégration et une mise en œuvre en continu entre les charges cloud et sur site. Les entreprises qui implémenteront les processus opérationnels nécessaires à l'interconnexion et à la prise en charge de ce modèle bénéficieront en retour de la vitesse et de la flexibilité promises par le cloud.

Prévision clé

« En 2025, j'estime que 20 % des charges seront distribuées à la périphérie des réseaux en dehors des environnements de data center multicloud et d'entreprise. En d'autres termes, un cinquième du trafic normalement confiné à l'intérieur du data center devra désormais être protégé et validé dans l'ensemble du réseau d'entreprise et multicloud ».

– Vijoy Pandey, vice-président et directeur technologique du groupe Plateforme et solutions cloud, Cisco

Réseaux destinés aux données et applications dans des environnements multicloud

Les impératifs de vitesse et d'innovation poussent les départements IT à moderniser les applications existantes et à en développer de nouvelles pour offrir un accès permanent aux informations sur tout type de périphérique. Les développeurs d'applications et les utilisateurs apprécient l'agilité du cloud, son évolutivité et la possibilité de l'utiliser en libre-service.

Pourtant, si 85 % des départements IT envisagent de recourir au cloud public ou le font déjà, le passage au cloud est une affaire plus complexe[23]. L'expression elle-même, « passage au cloud » n'est pas totalement exacte. Vijoy Pandey, vice-président et directeur technologique du groupe Plateforme et solutions cloud chez Cisco, précise : « ces dernières années, avec le transfert de charges applicatives stratégiques vers le cloud public, il est devenu évident que nous n'étions pas face à une situation binaire. Certaines charges applicatives, mais surtout certaines données, devaient être conservées en local »[24].

Parmi les entreprises qui recourent au cloud public aujourd'hui, 85 % suivent une stratégie multicloud, et ce taux devrait atteindre 94 % d'ici 12 mois[25].

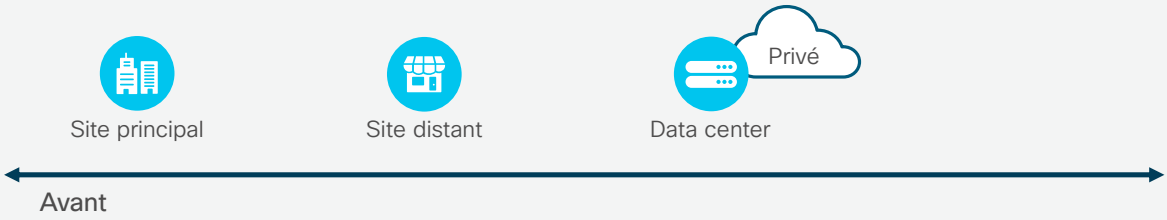
M. Pandey souligne également que la décision de maintenir les données sur site découle d'un certain nombre d'enjeux, notamment en termes de réglementation et de protection des données : « Si vous souhaitez obtenir un maximum de perspectives de vos données, vous devez les préparer et les modéliser convenablement. Pour toutes ces charges applicatives, il vous faut des capacités de calcul locales et des réseaux locaux. Certes, toutes les entreprises auront besoin de services cloud, mais les environnements sur site ne disparaîtront jamais. Je pense donc que miser sur le multicloud et l'hybride est une solution d'avenir ».

L'impact de l'évolution des modèles applicatifs sur le réseau

Traditionnellement, les performances d'un réseau se concentrent sur deux éléments principaux :

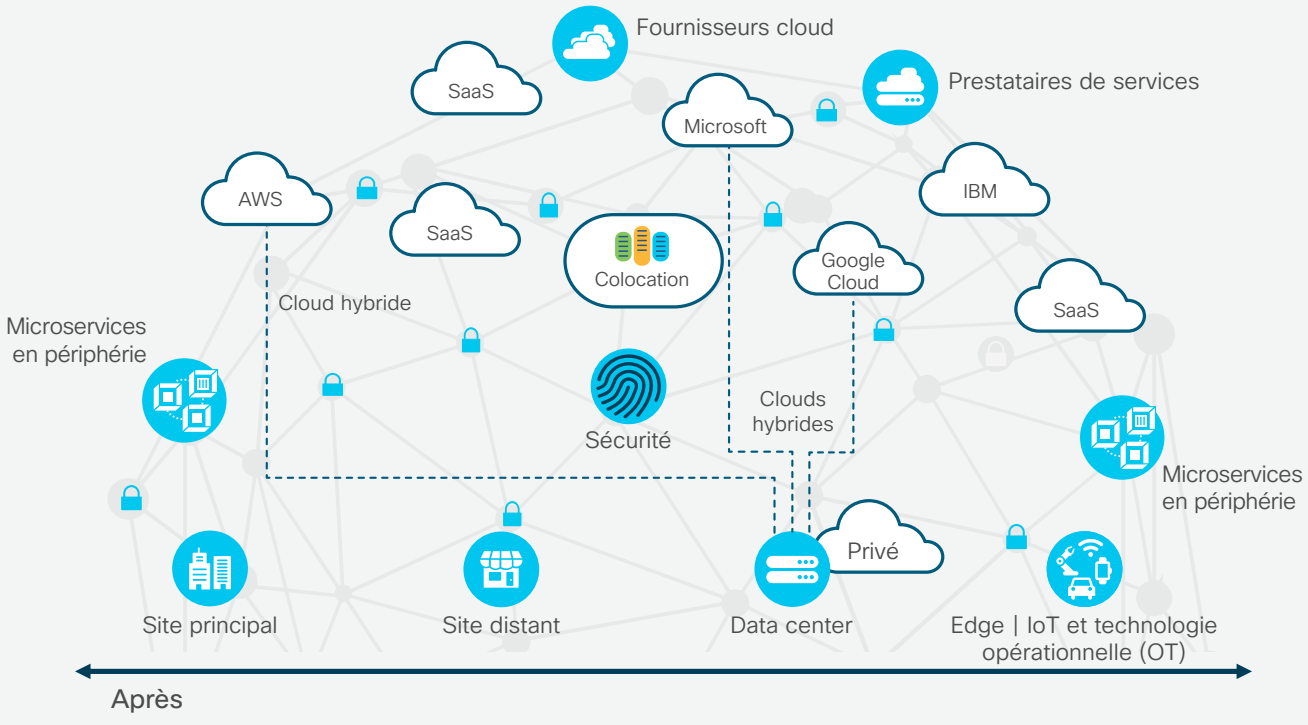
- Les communications entre le client et le service ou l'application monolithique, généralement hébergés dans un data center central
- Les communications au sein du data center, entre les serveurs et le stockage en réseau

Figure 15 Avant : communications du client au service et entre charges applicatives



Mais cette approche ne suffit plus puisque les équipes applications continuent d'adopter des modèles plus agiles, moins monolithiques, comprenant une multiplicité de charges applicatives ou de services qui ne sont pas toujours localisés au même endroit mais distribués, au-delà du data center et des environnements sur site.

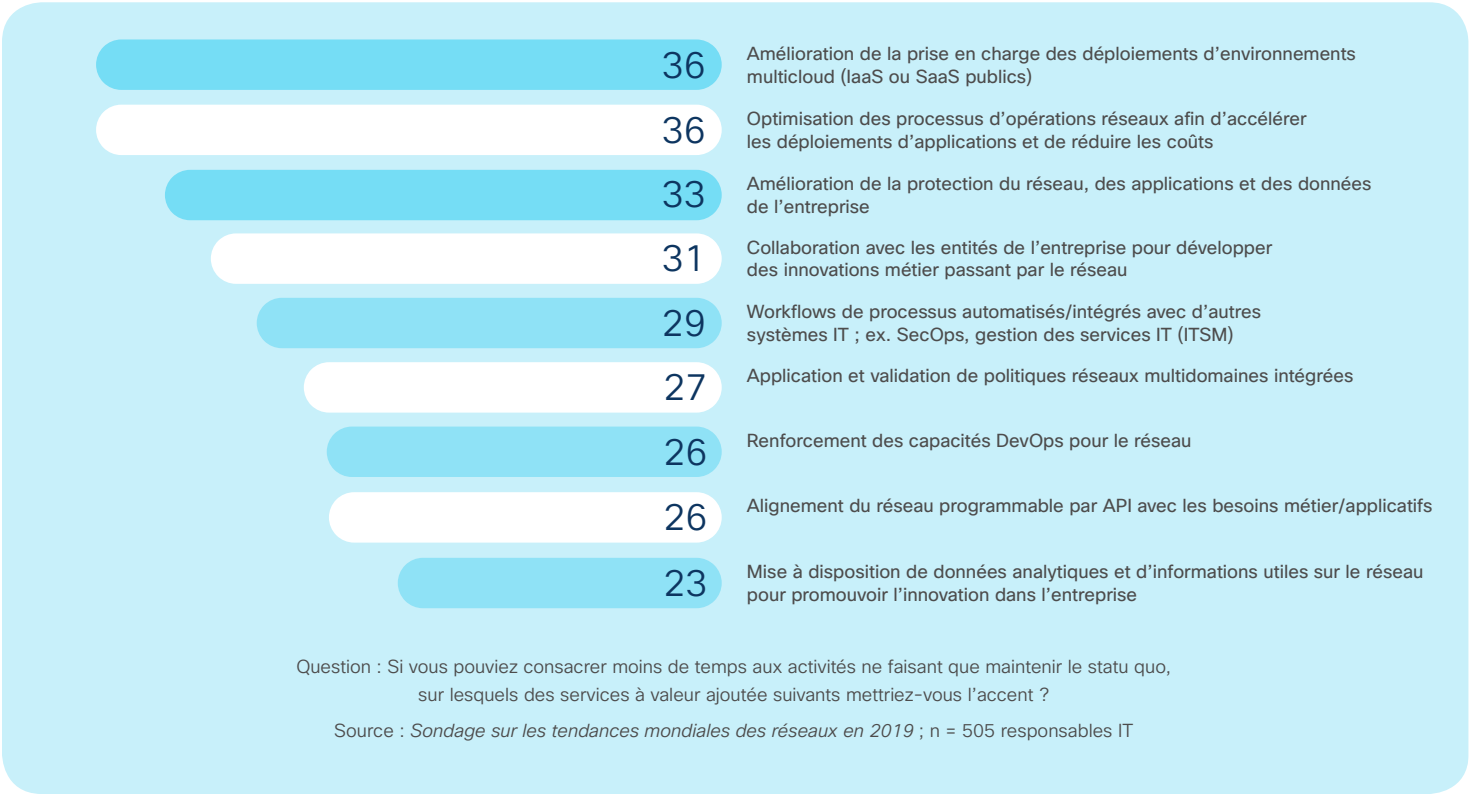
Figure 16 Après : communications du client au service et entre charges applicatives



Certaines équipes IT estiment qu'avec le passage au cloud le réseau devient moins important. Pourtant, il n'est en rien. Les équipes chargées du data center et du cloud ne peuvent plus travailler indépendamment des équipes réseau, et les responsables IT en ont déjà conscience.

Aujourd'hui, ils considèrent comme une priorité majeure les investissements réseau consacrés aux environnements multicloud (cloud public, infrastructure en tant que service [IaaS] ou logiciel en tant que service [SaaS])[14].

Figure 17 Les équipes IT privilégient les investissements réseau en faveur des environnements multicloud



Question : Si vous pouviez consacrer moins de temps aux activités ne faisant que maintenir le statu quo, sur lesquels des services à valeur ajoutée suivants mettriez-vous l'accent ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019* ; n = 505 responsables IT

Tom Edsall, directeur des technologies de data center et conseiller émérite chez Cisco, explique : « Les charges applicatives, les services et les données étant de plus en plus distribués sur tout le continuum périphérie-cloud, le département IT dans son ensemble est à présent tenu de s'assurer que la mise en œuvre des services est fiable, sécurisée et conforme aux performances attendues, quel que soit leur emplacement physique. Les spécialistes du data center doivent donc collaborer plus étroitement que jamais avec les équipes réseau en charge du site principal, du site distant et de la périphérie, et du WAN ».

Compte tenu de ces changements continus, sur quels aspects les responsables IT et réseau doivent-ils concentrer leurs efforts aujourd'hui ?

Le développement dans le cloud hybride et le multicloud implique de gérer des variables toujours changeantes (applications, données, utilisateurs et équipements) liées à tous les domaines de l'entreprise. Par conséquent, les équipes infrastructure et opérations (I&O) et les équipes réseau doivent aborder ensemble tous les aspects de cette mutation, des implications pour le réseau du recours à des fournisseurs de cloud public et SaaS, aux conséquences sur les environnements sur site.

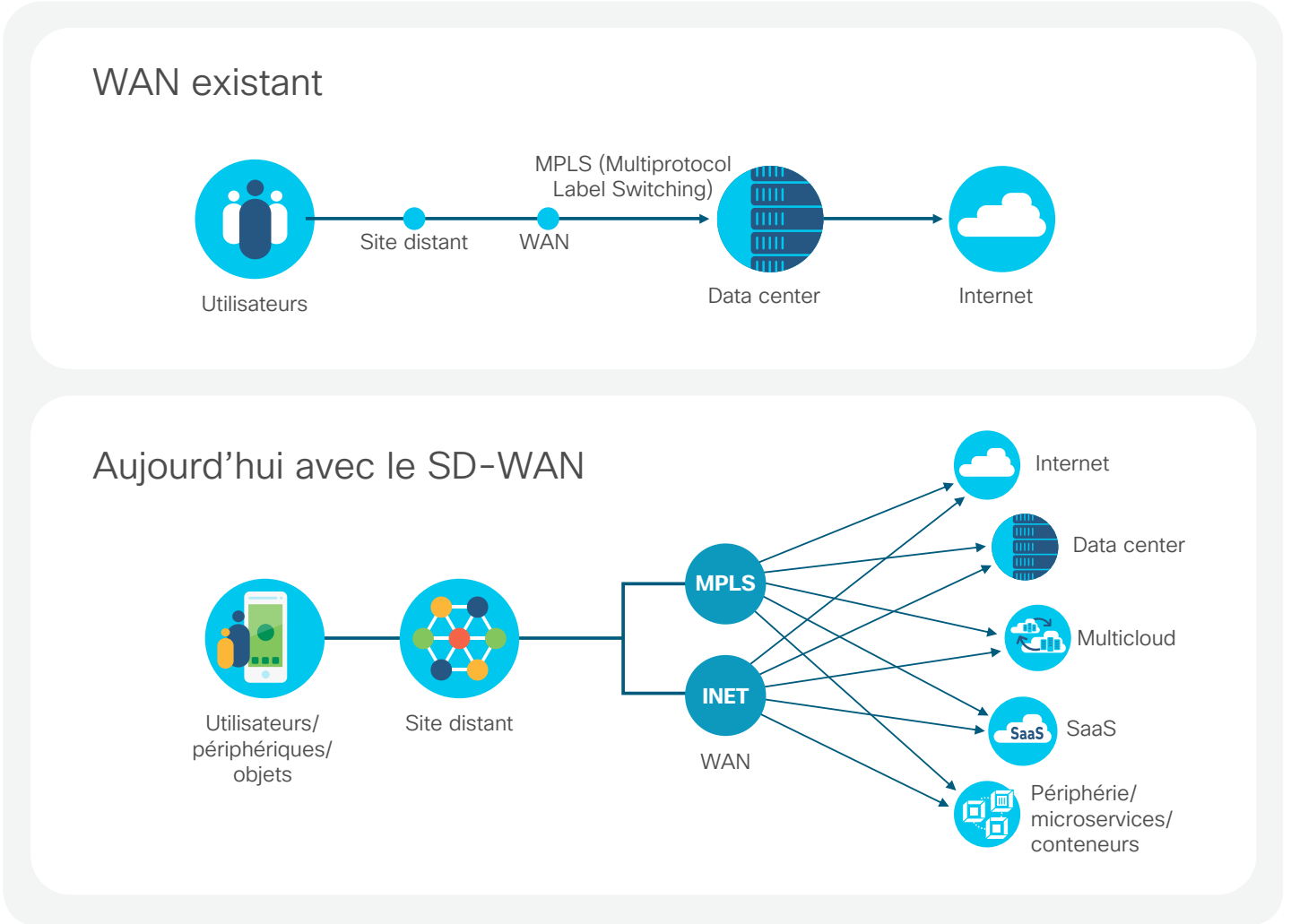
Pour faire la lumière sur ce défi à relever, nous allons examiner les impératifs réseau sous deux angles :

- Optimisation de la connectivité des utilisateurs au multicloud ;
- Mise en place d'un réseau adapté au data center omniprésent.

Optimisation de la connectivité des utilisateurs au multicloud

Avec la montée en puissance des services cloud, la connectivité à distance devient éminemment stratégique et les architectures WAN axées sur la connexion des sites distants aux data center centralisés ne sont plus optimales.

Figure 18 Évolution du WAN



Maintenant que l'hébergement du SaaS, de l'IaaS et des services distribués en périphérie est possible à tout emplacement offrant une connexion au réseau, l'architecture WAN traditionnelle en étoile peut être un frein pour les entreprises.

↑2 X Le recours accru au cloud fait également augmenter le trafic WAN : le trafic WAN IP d'entreprise dans le monde devrait doubler d'ici 2022 pour atteindre 5,3 exaoctets par mois[12].

Pour veiller à ce que les services cloud répondent aux impératifs métier dans des budgets raisonnables, plusieurs éléments d'architecture émergents sont aujourd'hui importants : le SD-WAN, l'accès cloud direct, les installations de colocation et les Cloud Exchanges, ainsi que les services haut débit à large bande passante proposés à un tarif abordable.

Les équipes IT doivent avoir le même degré de contrôle dans les environnements cloud qu'au sein de leurs propres réseaux si elles veulent continuer à fournir le service attendu par l'entreprise.

SD-WAN

Le SD-WAN, approche définie par logiciel de la gestion du réseau WAN, recourt à un contrôleur centralisé pour optimiser l'expérience applicative dans le multicloud tout en simplifiant considérablement les opérations réseau.

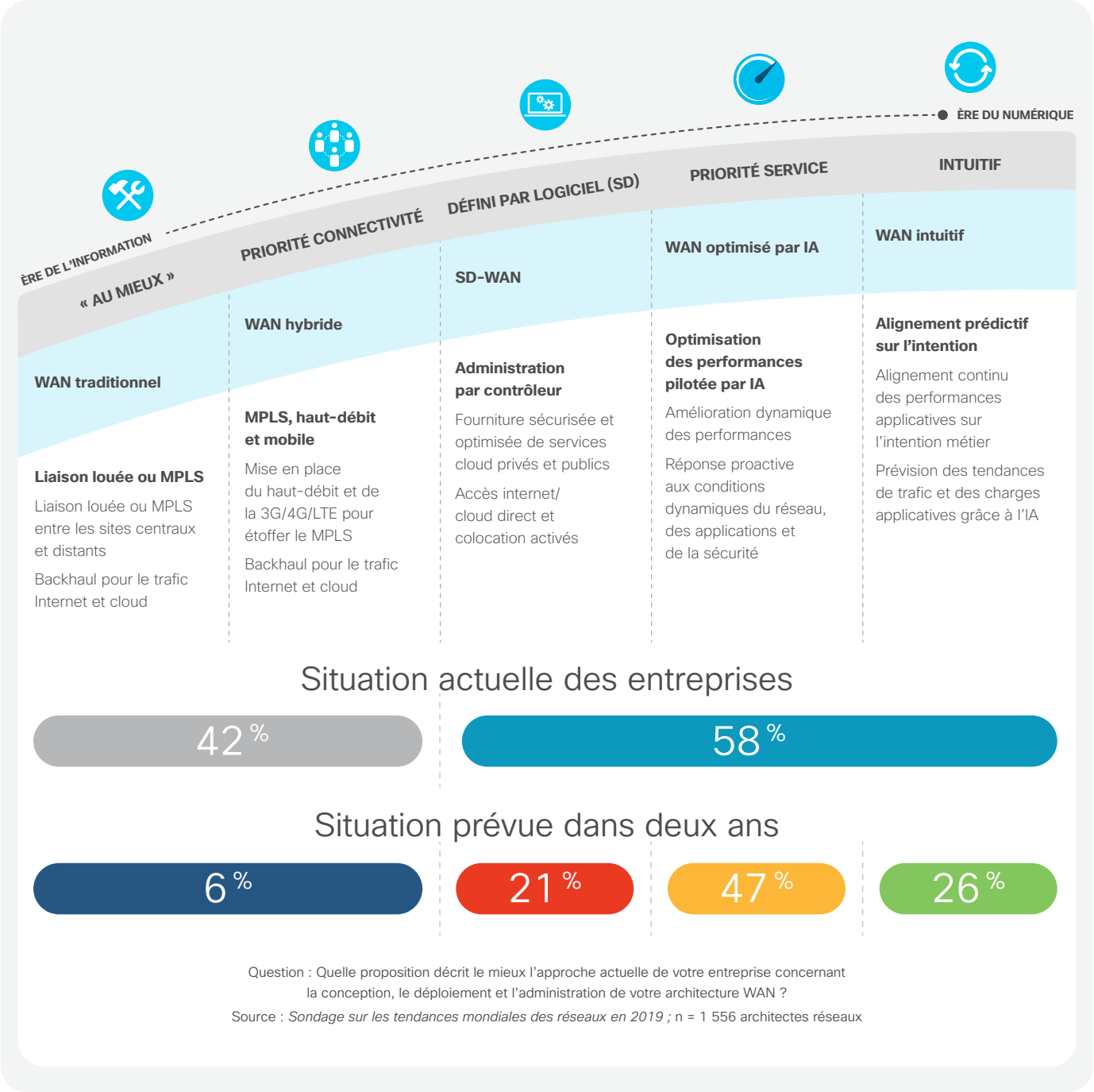
Le récent engouement pour ce type de réseau montre qu'il répond de plusieurs manières aux exigences croissantes du cloud. Et de fait, le cloud est le principal moteur de l'adoption du SD-WAN : dans le sondage d'IDC consacré au SD-WAN, près de 75 % des personnes interrogées indiquent que les services SaaS/cloud ont de l'importance (ou beaucoup d'importance) dans le choix des technologies WAN[26].

Ce chiffre n'est guère surprenant puisque les options et services traditionnellement utilisés pour la connexion au cloud privé virtuel proposé par des fournisseurs cloud, limitent le contrôle des équipes réseau d'entreprise dans un scénario multicloud.

Selon notre *sondage sur les tendances mondiales des réseaux en 2019*, plus de 58 % des entreprises dans le monde ont déjà déployé une forme de SD-WAN et plus de 94 % des sondés pensent qu'ils effectueront une implémentation SD-WAN de base ou avancée dans un délai de deux ans[14].

En outre, à mesure que les services 5G se généralisent, le SD-WAN va les intégrer de manière transparente dans un framework indépendant du transport pour combiner un maximum de flexibilité et de performances, une sauvegarde continue optimale et des coûts réduits.

Figure 19 Degré de préparation du WAN pour le multicloud



Question : Quelle proposition décrit le mieux l'approche actuelle de votre entreprise concernant la conception, le déploiement et l'administration de votre architecture WAN ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 1 556 architectes réseaux

Accès cloud direct

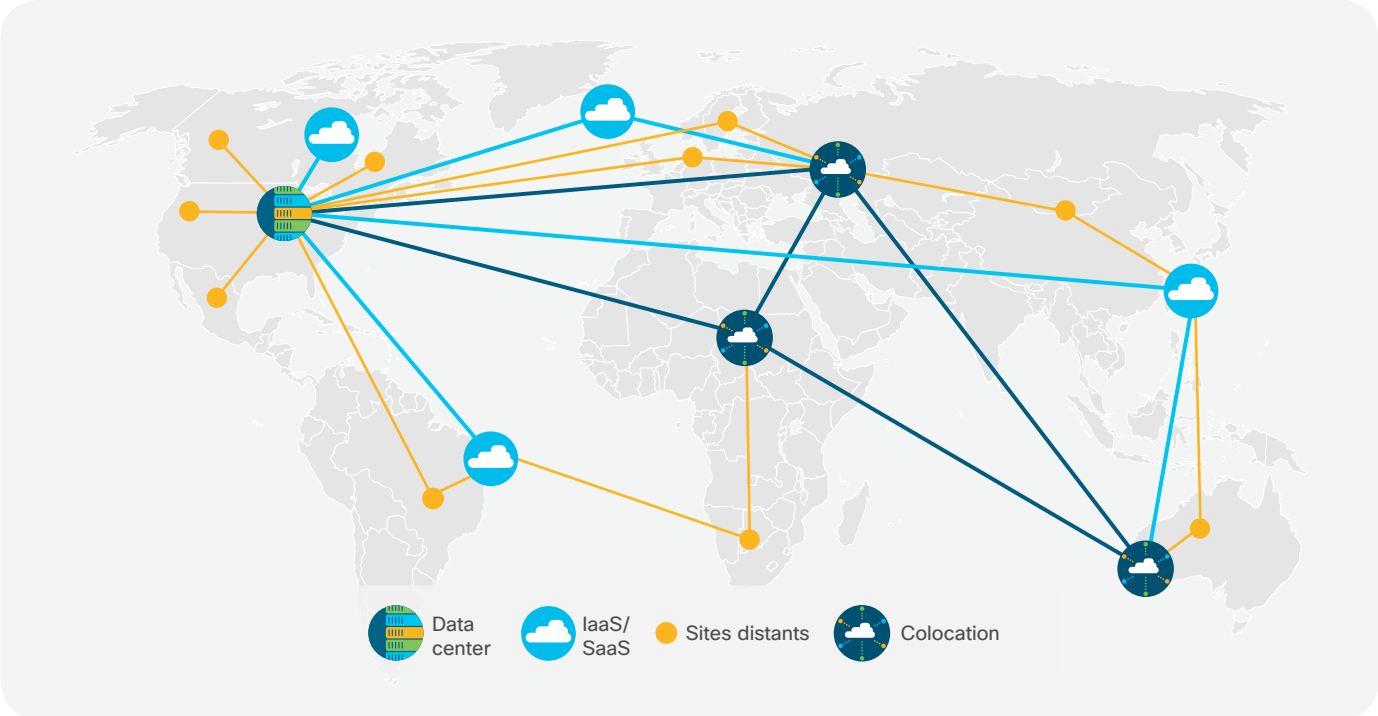
L'approche traditionnelle consistant à utiliser des circuits WAN coûteux pour établir une liaison de backhaul acheminant le trafic du site distant jusqu'au data center ou jusqu'à une passerelle Internet centralisée via une architecture en étoile peut ralentir la transition vers des services cloud. Et en plus d'accroître les dépenses, elle génère de la latence préjudiciable à l'expérience utilisateur.

Jusqu'ici, les architectes réseau étaient obligés de s'en tenir à cette approche en raison du coût et de la complexité de l'autre solution impliquant le déploiement et la gestion de fonctions de sécurité distribuées du type pare-feu, filtrage des URL et protection DNS sur chaque routeur de site distant.

Aujourd'hui, avec les capacités « accès direct cloud » ou « accès direct Internet », il est possible de sécuriser la connexion directe des utilisateurs du site distant jusqu'aux services

cloud. Cette évolution simplifie la gestion de la politique sur l'ensemble des sites distants et automatise le provisionnement rapide de nouveaux services réseau tout en appliquant une sécurité multicouche, avec chiffrement, authentification, segmentation, pare-feu et application du DNS.

Figure 20 SD-WAN sécurisé avec accès cloud direct et centres de colocation



Colocation et Cloud Exchanges

Certes, les installations de colocation neutre (colocation) ne sont pas nouvelles, mais elles prennent beaucoup d'ampleur à l'ère du multicloud et constituent un composant essentiel de la nouvelle architecture WAN optimisée pour le cloud. Par nature, les installations de colocation comme celles proposées par Equinix et d'autres services d'interconnexion constituent une extension du WAN d'entreprise, offrant visibilité, accès hautes performances et sécurité centralisée à de multiples fournisseurs SaaS et IaaS (voir figure 20 ci-dessus).

Mise en place d'un réseau adapté au data center omniprésent

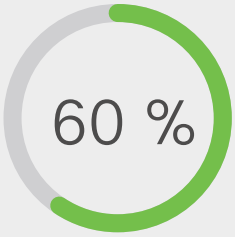
Aujourd'hui, les data centers ne sont plus monosites. Le nouveau « data center distribué » est apparu depuis que les applications et les données résident à la fois sur site et hors site, dans des environnements hybrides, multicloud et de périphérie. Il ne fonctionne pas de la même façon qu'un data center classique. Les départements IT doivent donc s'adapter et modifier leurs technologies et leurs opérations afin de répondre aux exigences des applications et de la connectivité réseau propres à cette nouvelle architecture.

Avec un data center omniprésent, les équipes IT doivent veiller à la cohérence des technologies et des opérations sur site, à la périphérie de l'entreprise et dans les environnements hybrides et multicloud.

Automatisation

Face à des data centers dont l'ampleur, la complexité et la portabilité des charges ne cessent de croître, les administrateurs réseau sont forcés de renoncer aux processus manuels et d'utiliser des outils d'automatisation pour la gestion des politiques réseau et de la connectivité.

L'adoption du réseau défini par logiciel, de l'automatisation et du NFV pour les services des couches 4 à 7 apporte aux réseaux de data center les capacités dont ils ont besoin pour prendre en charge un environnement cloud sur site agile. Il est alors possible d'appliquer au réseau et aux services de calcul et de stockage une orchestration centrée sur les charges. En réalité, on pourrait considérer comme dépassé un réseau de data center n'ayant pas encore adopté un modèle DevOps basé sur contrôleur et piloté par API.



Près de 60 % des responsables IT et architectes réseaux indiquent qu'ils ont déjà déployé une forme de SDN dans leur data center[14].

Près de 60 % des responsables IT et architectes réseaux indiquent qu'ils ont déjà déployé une forme de SDN dans leurs data centers[14]. Le SDN/NFV transporte désormais 23 % du trafic au sein des data centers d'entreprise, et ce taux devrait atteindre 44 % en 2021[23]. Quant aux data centers sans SDN, il va leur être difficile de prendre en charge des modèles applicatifs agiles et flexibles.

Réseau intuitif pour le data center

En s'appuyant sur les fondamentaux du SDN, le réseau intuitif permet aux équipes de data center de mettre en place une architecture globale de validation en boucle fermée, capable d'analyser le comportement du data center en temps réel au regard des politiques définies et d'établir une méthode fiable et efficace pour modifier le réseau. Les équipes IT peuvent ainsi rester en phase avec les changements dynamiques de charges et s'adapter en permanence aux besoins applicatifs de l'activité métier.

Dans un scénario de data center, il est également primordial de valider les politiques avant leur activation. L'IBN permet d'effectuer une vérification automatisée en continu, à l'échelle du réseau, avec des règles de conformité.

Extension de l'IBN aux environnements multicloud

Pour garantir les niveaux de service et la sécurité attendus dans les entreprises aujourd'hui, les équipes de data center doivent étendre le contrôle et la visibilité au-delà des environnements sur site. Les équipes IT peuvent appliquer les règles d'automatisation et d'application de l'IBN aux environnements multicloud pour que le déploiement des politiques soit cohérent entre toutes les charges, quel que soit leur emplacement.

D'ici deux ans, 29 % des participants à notre *sondage sur les tendances mondiales des réseaux en 2019* prévoient d'instaurer des fonctionnalités de réseau intuitif pour veiller à l'alignement sur l'intention métier grâce à l'automatisation d'actions réseau au sein des environnements multicloud[14].

Tom Edsall, directeur des technologies de data center chez Cisco, explique : « L'IBN est une initiative extrêmement audacieuse et universelle de la part du secteur des réseaux. Elle vise à créer un modèle de réseau systémique prenant en compte toutes les tendances technologiques actuelles et l'évolution rapide des besoins dans les organisations agiles ».

« L'IBN est une initiative extrêmement audacieuse et universelle de la part du secteur des réseaux. Elle vise à créer un modèle de réseau systémique prenant en compte toutes les tendances technologiques actuelles et l'évolution rapide des besoins dans les organisations agiles ».

– Tom Edsall, directeur des technologies de data center et conseiller émérite, Cisco

Pour réussir une implémentation sur site, multicloud ou hybride, la simplicité du système est primordiale. Les architectes réseau doivent donc tenir compte des points suivants :

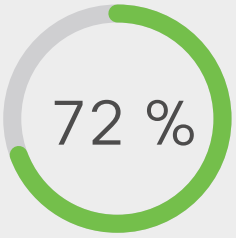
- Aucun réseau overlay dans le cloud ;
- Aucune dépendance à un agent, pour élargir l'applicabilité de toutes les charges ;
- Capacité d'adaptation à l'échelle du cloud.

Infrastructure réseau sous-jacente

Dans le data center, l'infrastructure réseau sous-jacente doit fournir une programmabilité ouverte et des fonctions de télémétrie afin de soutenir l'automatisation et l'analytique capitales dans les systèmes IBN. Elle doit aussi être en mesure de faire face à des hausses considérables du trafic alors que le trafic IP de data center

3 X Le trafic IP de data center à l'échelle mondiale devrait tripler au cours des cinq prochaines années[23].

à l'échelle mondiale devrait tripler au cours des cinq prochaines années. Dans l'ensemble, sa croissance annuelle devrait s'établir à 25 % (TCAC) jusqu'en 2021[23].



En 2021, le trafic au sein du data center représentera 72 % de l'ensemble du trafic de data center[23].

Les infrastructures réseau ont besoin de flexibilité et de capacité pour prendre en charge à la fois le trafic hautes performances entre client et application (nord-sud) et, de plus en plus, le trafic entre serveurs ou entre machines virtuelles (est-ouest). Pour ce faire, on recourt aujourd'hui à une architecture plate de type « spine-leaf » accompagnée d'un ou plusieurs protocoles overlay de couche de contrôle.

Selon le *Cisco Global Cloud Index*, en 2021, le trafic au sein du data center représentera 72 % de l'ensemble du trafic de data center et il dépassera largement le trafic entre le data-center et les utilisateurs (15 %) et le trafic entre data centers (14 %)[23].

Une augmentation continue des performances de commutation Ethernet sera forcément nécessaire pour faire face aux besoins accrus du trafic de calcul et du trafic de stockage en mode fichier, voire d'une partie du trafic de stockage en mode bloc.

Avec la généralisation du 400 Gbit/s commuté et alors que les spécifications IEEE pour le 800 Gbit/s, voire le 1,6 Tbit/s se préparent, Ethernet présente des avantages en termes d'investissement et d'exploitation qui vont inévitablement l'amener à remplacer la commutation Fiber Channel traditionnelle pour certaines charges.

Paramètres à prendre en compte lors de la conception de votre architecture réseau pour le multicloud

Dans cet environnement applicatif plus étendu et distribué, les architectes cloud et réseau, les responsables de data center et les équipes infrastructure et opérations doivent mettre au point une stratégie réseau visant à optimiser l'expérience applicative. Voici quelques points à prendre en compte dans un premier temps :

1. **Examiner la stratégie d'applications de l'entreprise :** tout commence par l'application. Les architectes IT et réseau doivent bien cerner l'empreinte grandissante de leurs charges applicatives et de leurs données.

2. **Collaborer pour apporter de la cohérence au multicloud :** les départements IT ont besoin d'un environnement multicloud (systèmes sur site compris) qui fonctionne comme un tout. Face à une telle complexité, les équipes data center et réseau doivent collaborer pour favoriser la cohérence entre tous les domaines : site principal, site distant, data center, périphérie/IoT et fournisseurs de cloud public/SaaS. Elles pourront ainsi optimiser les coûts, les performances, la visibilité, la sécurité et les expériences utilisateur.

3. **Étendre la cohérence de l'automatisation par politique au cloud hybride et au multicloud :** les équipes doivent envisager une automatisation par politique à l'ensemble des plateformes, des hyperviseurs ou des frameworks de conteneurs, à tous les emplacements et pour toutes les charges (cloud natives, bare-metal, hyperviseur, conteneur et sans serveur).

4. **Cartographier les services applicatifs, les charges et les composants de service sur le réseau étendu :** les architectes et ingénieurs réseaux doivent bien identifier l'emplacement des applications, des services et des microservices au sein du réseau.

5. **Privilégier les performances applicatives dans la stratégie SD-WAN :** identifiez les applications et services cloud les plus stratégiques et axez votre plan SD-WAN en priorité sur la prise en charge de ces applications.

6. **Établir des liaisons entre la politique d'accès et la politique applicative sur tous les silos du réseau :** pour mettre en œuvre une segmentation sécurisée pilotée par des politiques, réfléchissez à la manière dont les systèmes IBN peuvent lier des groupes et des politiques entre les différents domaines réseau, comme le WAN et le data center.

7. **Développer les compétences NetDevOps :** les charges applicatives et les services nécessitent des services réseau à la demande, non seulement au sein du data center mais également entre des emplacements distants ; la formulation de leurs besoins vis-à-vis du réseau doit donc être claire. Des compétences NetDevOps sont ainsi indispensables pour savoir faire le lien entre les impératifs applicatifs et les politiques réseau.

8. **Compléter le SDN avec les progrès de l'IA :** exploitez les capacités de l'IA afin d'accélérer la résolution des problèmes, d'améliorer la gestion des modifications et de veiller à la conformité.

Accès réseau et sans-fil

Résumé de la section

Points clés

- De nouvelles fonctionnalités comme OpenRoaming fourniront un roaming transparent, permanent et sécurisé à l'échelle mondiale entre différents réseaux Wi-Fi 6 et 5G publics.
- Les équipes réseau ont besoin de fonctionnalités pilotées par IA et de capacités analytiques améliorées pour la planification, la surveillance d'intégrité, le dépannage et la remédiation du sans-fil.
- Les équipes IT doivent gérer, administrer et propager une politique d'accès cohérente sur différents réseaux d'accès, de manière automatique, afin de mieux protéger les applications, les données, les utilisateurs et les périphériques.
- Les réseaux sans fil devront identifier les demandes d'applications multimédias immersives et d'équipements IoT, et les prendre en charge de manière dynamique.

Conclusions clés

- À l'échelle mondiale, les appareils sans fil représenteront 43 % de tous les équipements connectés en 2022.
- Les équipements IoT intermachine représenteront 51 % de tous les équipements connectés en 2022, et la grande majorité seront connectés en sans-fil.
- 35 % des architectes réseaux estiment que la résolution des problèmes réseau est l'activité la plus chronophage et laborieuse pour les équipes NetOps.
- 34 % des entreprises privilégient toujours une approche manuelle de la gestion des accès sur les réseaux filaires et sans fil.
- 40 % des entreprises mettent en œuvre une automatisation des politiques et une segmentation pour réduire la surface d'attaque, tandis que 15 % s'appuient sur des solutions d'accès pilotées par IA.
- 27 % des entreprises prévoient d'instaurer un modèle d'accès réseau intuitif d'ici deux ans.

Conseils décisifs

- Réfléchissez aux conséquences du Wi-Fi 6 et de la 5G sur les futurs impératifs métier de votre entreprise et définissez votre stratégie sans fil en conséquence.
- Élaborez une feuille de route pour automatiser l'intégration et la segmentation de tous les appareils mobiles et équipements IoT.
- Envisagez de recourir à la classification automatisée des périphériques pour permettre une intégration à grande échelle et sécurisée de tous les types d'équipements IoT.
- Examinez comment les services géolocalisés et l'analytique réseau peuvent bénéficier à l'activité de votre entreprise.

Résumé de la section (suite)

- Explorez la possibilité de gérer les technologies sans fil spécialisées indispensables à certains cas d'usage uniques ou exigeants (ex. Bluetooth, Zigbee et Thread) par le biais d'une couche de gestion commune.

Prévisions clés

« En 2025, l'omniprésence de fédérations du sans-fil telles qu'OpenRoaming permettra aux départements IT et aux fournisseurs de service de recourir à des systèmes d'accès Zero-Trust et de partager des identifiants en toute sécurité, mais aussi aux utilisateurs de passer d'un réseau d'accès sans fil à un autre, public ou privé, en toute transparence et sécurité. L'expérience utilisateur sera fluide, encadrée par des politiques, et donc optimale pour tous les utilisateurs, quel que soit leur lieu de connexion ».

– Matt MacPherson, directeur des technologies sans fil, Cisco

---

« D'ici 2025, les réseaux Wi-Fi 6 basés sur la norme IEEE 802.11ax, ainsi que les extensions Wi-Fi 6 planifiées, seront le type de réseau Wi-Fi dominant à l'échelle mondiale. Ce n'est qu'autour de 2024 que la prochaine génération de Wi-Fi, basée sur la norme IEEE 802.11be aujourd'hui en développement (et qui sera probablement baptisée Wi-Fi 7) fera son apparition sur le marché ».

– Andrew Myles, administrateur et ancien président de la Wi-Fi Alliance, et directeur technique Cisco

Accès réseau et sans-fil

À l'échelle mondiale, le trafic IP d'entreprise atteindra 63,3 exaoctets par mois en 2022, soit le triple du trafic enregistré en 2017[3]. Issu des tout premiers réseaux locaux partagés aux performances relativement modestes, comme l'Ethernet (10 Mbit/s), le Token Ring (16 Mbit/s) et le FDDI (100 Mbit/s), l'accès filaire a bénéficié d'innovations continues dans le domaine du silicium et de l'optique pour aboutir au cœur de réseau Ethernet 400 Gbit/s commuté, aujourd'hui utilisé par les clients pour déployer des environnements réseau locaux et métropolitains.

La poursuite des innovations permet d'envisager l'Ethernet Terabit et de nouvelles capacités avancées comme le TSN (Time-Sensitive Networking) pour les applications IoT déterministes dans un futur relativement proche. Néanmoins, dans notre monde actuel privilégiant le mobile, l'accès sans fil est au centre de toutes les attentions. L'accès réseau sans fil via un réseau local sans fil (Wi-Fi) ou un réseau mobile public continue de transformer notre quotidien d'une manière difficilement prévisible.

« Nous constatons que l'innovation pour l'entreprise numérique exige et stimule les avancées dans le domaine du sans-fil, et en même temps, les innovations du sans-fil ouvrent de nouvelles possibilités d'innovation pour l'entreprise. C'est un cercle vertueux ».

– Guillermo Diaz, VP senior de la transformation client, Cisco

« Aujourd'hui, "l'expérience" est le maître-mot des entreprises et l'évolution de la connectivité sans fil sera le vecteur de nombreuses expériences nouvelle génération. En combinant le meilleur du Wi-Fi 6 et de la 5G, les équipes réseau ont les moyens de leur donner vie ».

– Matt MacPherson, directeur des technologies sans fil, Cisco

À l'échelle mondiale, les périphériques sans fil représenteront 43 % de tous les équipements connectés en 2022, et les smartphones 24 % (6,7 milliards). En parallèle, les équipements IoT intermachine seront 14,6 milliards, soit 51 % de tous les équipements connectés en 2022, et ils seront en grande majorité connectés en sans-fil[12].

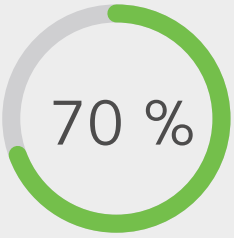
Mettre en place une expérience utilisateur mobile de grande qualité

Partout dans le monde, les gens se sont accoutumés aux applications mobiles telles qu'Uber, Waze et Webex, et au réel confort qu'elles leur apportent dans leur vie aussi bien professionnelle que personnelle. Pour eux, l'expérience mobile doit être immédiate, toujours disponible, sans attache et omniprésente. Elle doit aussi être satisfaisante, c'est-à-dire offrir un accès ininterrompu et stable à la vidéo 4K, une navigation fulgurante et des communications vocales sur IP d'une clarté parfaite.

Il est tout aussi important que les réseaux sans fil soutiennent les innovations métier. À l'heure où les entreprises recourent de plus en plus aux applications multimédias immersives, comme la vidéo haute définition, la réalité augmentée et la réalité virtuelle, les responsables métier veulent être sûrs que le réseau offre les performances, les capacités, la prise en charge et la sécurité indispensables à ces nouveaux projets numériques, de manière à agir rapidement lorsqu'une opportunité se présente.

« Imaginez qu'un acheteur potentiel reçoive une expérience pertinente et personnalisée grâce à la géolocalisation et la réalité augmentée », explique Matt MacPherson, directeur des technologies sans fil chez Cisco. « Ou qu'un entrepôt puisse être équipé de millions de capteurs permettant à des robots et des véhicules électriques autonomes de préparer des commandes et d'expédier des produits ».

Les nouveaux réseaux Wi-Fi 6 et 5G (pour le mobile public) promettent des gains de performances considérables pour répondre à de telles exigences. Le Wi-Fi 6 apporte des débits de données plus élevés, une latence plus faible, une densité d'équipements accrue et des performances globales bien meilleures. De même, en 2022, les réseaux publics mobiles 5G, dont le déploiement commercial est prévu en 2020 dans certains pays, offriront des vitesses de connexion plus de quatre fois supérieures à celles de la 4G[12].



Le Wi-Fi est largement utilisé comme un mécanisme de déchargement du mobile et il sera encore plus indispensable avec la 5G. D'après les prévisions, la 5G déchargera 70 % de son trafic, quand les réseaux 4G en déchargent 59 %[27].

Les utilisateurs mobiles veulent aussi bénéficier d'une expérience transparente pour l'accès aux applications d'entreprise, aux applications cloud et aux applications Internet publiques, sans oublier l'intégration aux nouveaux réseaux et le roaming.

Si le Wi-Fi 6 vient en complément de la 5G, les utilisateurs bénéficieront d'une expérience transparente et permanente dans les lieux privés et publics, en intérieur comme en extérieur. Et cela vaudra aussi pour les nouvelles applications gourmandes en données, susceptibles d'épuiser rapidement les forfaits de données mobiles de bien des utilisateurs.

Afin de concrétiser cette vision, OpenRoaming s'appuie sur la technologie Passpoint de la Wi-Fi Alliance[28]. En dépit de sa jeunesse, la fondation OpenRoaming, consortium constitué de plusieurs leaders du sans-fil dont Cisco, s'est fixé un objectif ambitieux : permettre un roaming véritablement transparent et sécurisé entre les réseaux sans fil privés et publics.

Cette technologie offre aux utilisateurs une itinérance facile et sécurisée entre différents réseaux Wi-Fi 6 et 5G publics via une fédération basée dans le cloud de réseaux d'accès et de fournisseurs d'identité, dont des opérateurs mobiles. La présentation d'OpenRoaming a remporté un réel succès lors d'un récent salon mondial de la téléphonie mobile[28].

Avec des appareils bimodaux comme les smartphones et les tablettes, les utilisateurs pourront passer automatiquement d'un réseau Wi-Fi privé domestique ou professionnel à des points d'accès Wi-Fi et réseaux 5G publics.

« Avec OpenRoaming, les utilisateurs mobiles n'auront plus à identifier le bon réseau Wi-Fi, à passer par un portail de connexion captif, ni à saisir un identifiant et un mot de passe non sécurisés. Où qu'ils aillent, ils seront connectés et pourront effectuer des téléchargements, utiliser le streaming, discuter par messagerie vidéo, jouer, et même travailler, à leur gré ».

– Matt MacPherson, directeur des technologies sans fil, Cisco

Préparer l'IT à sa réussite sans fil

Les équipes NetOps doivent anticiper ces nouveaux impératifs métier afin de fournir les expériences utilisateur mobiles voulues, car les approches traditionnelles de déploiement et de maintenance des réseaux sans fil ne seront plus viables.

En particulier, la résolution des problèmes de réseaux sans fil a toujours été une activité réactive, complexe et gourmande en ressources pour la plupart des équipes réseau. Sans surprise, les responsables réseau estiment d'ailleurs que la résolution des problèmes réseau est l'activité chronophage par excellence des équipes NetOps[14].

La situation est d'autant plus complexe que, au-delà de l'émergence des réseaux Wi-Fi 6 et 5G, les équipements IoT peuvent communiquer via de multiples protocoles sans fil de niche, comme BLE, Zigbee et Thread. Pour l'IT, le défi sera donc de veiller à ce que les efforts de gestion réseau ne soient pas scindés sur ces différents réseaux.

De nombreux cas d'usage IoT vont converger sur les réseaux Wi-Fi 6 et 5G dominants, mais les équipes IT doivent réfléchir à la manière dont elles peuvent gérer les technologies sans fil plus spécialisées, requises par des cas d'usage précis et uniques, via une couche de gestion commune.

Pour anticiper, les équipes NetOps doivent adopter une approche plus proactive de la planification, de la surveillance, du dépannage et de la remédiation du sans-fil. Il leur faut donc tirer profit du gain de visibilité considérable sur les performances et l'intégrité du réseau sans fil apporté par l'analytique et la surveillance par IA.

État actuel et futur de la préparation des accès réseau

Pour prendre en charge les utilisateurs mobiles, l'IT ne peut pas s'en remettre aux opérations réseau traditionnelles en accès manuel. Elles doivent recourir à une approche pilotée par logiciel couvrant l'ensemble des domaines réseau.

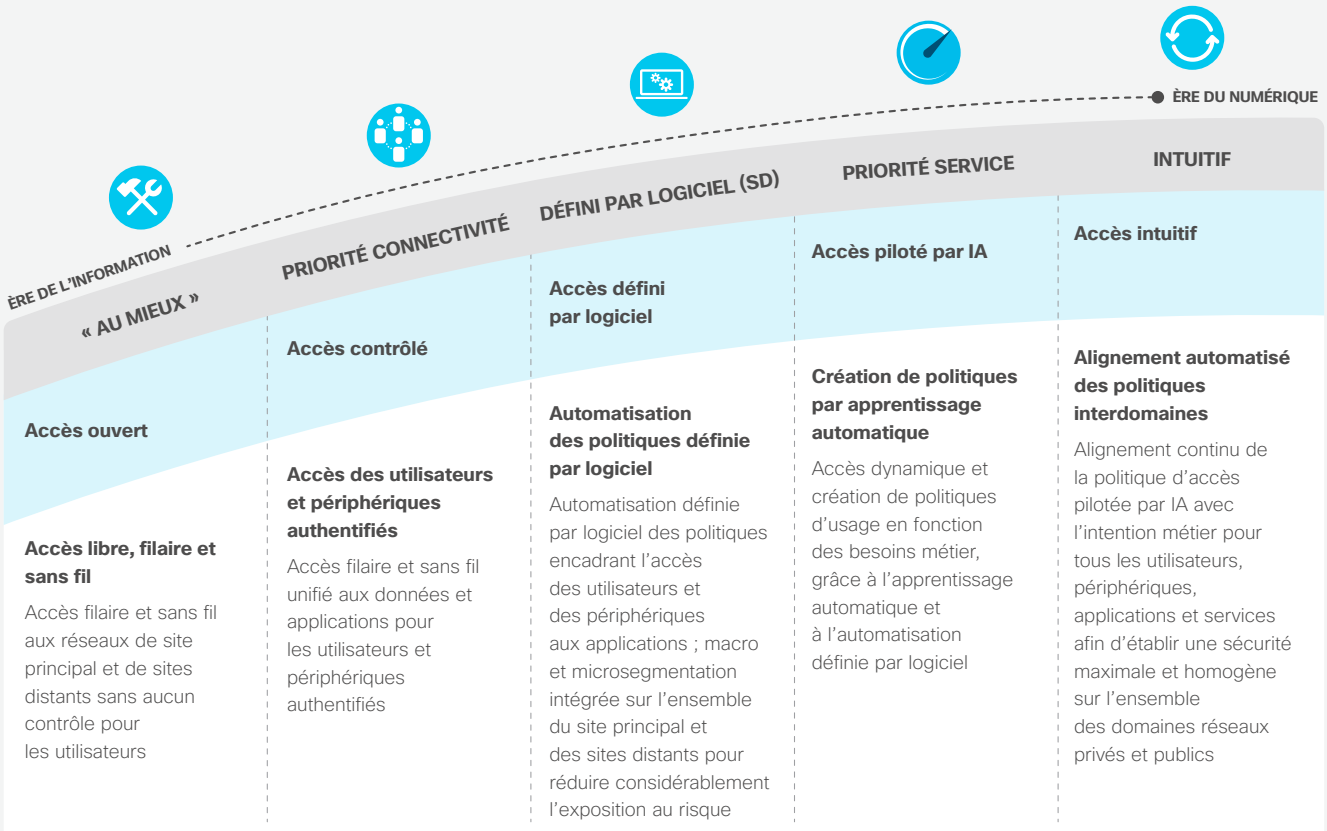
Le système de gestion réseau doit être capable d'administrer et de propager une politique d'accès cohérente sur différents réseaux d'accès, de manière automatique, même lorsque les utilisateurs et les charges applicatives se déplacent. Il doit révéler les données et perspectives qui permettront à l'IT de soutenir l'activité métier en temps réel et d'employer l'IA pour mieux prédire les problèmes et automatiser les tâches de routine. Et compte tenu de la prévalence croissante des applications IoT, il est important que le réseau puisse automatiquement reconnaître les équipements IoT, les classifier et leur appliquer les politiques pertinentes.

Toutes capacités réunies permettront aux employés, aux clients et aux responsables métier de tirer pleinement parti du Wi-Fi 6 et de la 5G. En même temps, elles donneront à l'IT la possibilité de faire face au déluge de

connectivité sans fil, tout en veillant à la sécurité et à la qualité optimale de l'expérience utilisateur dans un monde mobile.

Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, nous avons demandé aux architectes réseaux où ils en étaient dans l'adoption d'une architecture d'accès sécurisée, parmi les cinq stades de notre modèle. 72 % des sondés prévoient de déployer un accès intuitif ou piloté par IA dans un délai de deux ans, et 18 % seulement le font déjà aujourd'hui. Cette adoption leur permettra de créer et modifier dynamiquement les politiques et, à terme, d'aligner les politiques d'accès sur l'intention métier de bout en bout, entre les utilisateurs et les services, quels que soient leur emplacement et leurs déplacements[14].

Figure 21 Degré de préparation à l'accès sécurisé



Question : Quelle proposition décrit le mieux l'approche actuelle de votre entreprise concernant la sécurité du réseau ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 1 556 architectes réseaux

Points à prendre en compte pour la mise en œuvre de l'accès et du sans-fil à l'ère numérique

1. **Des outils d'assurance sans-fil sont indispensables :** dans la plupart des secteurs, le sans-fil devient la connectivité d'accès prédominante pour les terminaux clients comme pour les objets. Les architectes réseaux doivent disposer de systèmes et d'outils d'assurance sans-fil pour être en mesure d'assurer la cohérence des expériences sur l'ensemble des réseaux d'accès IT et IoT.

2. **La segmentation par politique du filaire et du sans-fil va lever de nombreuses difficultés :** l'automatisation par politique sur l'ensemble des réseaux d'accès, de sites principaux et de sites distants permet de créer et de gérer des segments et des microsegments de manière dynamique en se fondant sur des groupes d'utilisateurs et d'applications. Les réseaux forment alors une barrière Zero-Trust dynamique contre les attaques et les menaces.

3. **Procéder à une classification des équipements pilotée par IA avant de déployer l'IoT à grande échelle :** il n'est pas viable, économiquement, de protéger des équipements IoT peu onéreux, comme des capteurs ou des dispositifs de contrôle, avec des solutions de sécurité qui, elles, coûtent cher. En revanche, le recours à la classification automatisée des équipements et à l'automatisation par politique permet de créer et gérer des segments et microsegments IoT en fonction de groupes d'équipements et d'applications.

4. **Se préparer au Wi-Fi 6, à la 5G et à OpenRoaming :** pour établir leurs feuilles de route, les responsables réseau doivent prendre en compte la complémentarité du Wi-Fi 6 et de la 5G, et choisir les équipements, les opérateurs Wi-Fi et les fournisseurs de services qui permettront de proposer des capacités OpenRoaming.

5. **Envisager des services géolocalisés :** de nombreux dirigeants métier des secteurs de la vente au détail, des soins de santé et de l'éducation tirent déjà parti des atouts des services géolocalisés en intérieur pour améliorer l'expérience des clients. Dans notre sondage, 51 % des personnes interrogées ont déjà recours au sans-fil géocontextuel pour proposer une expérience client plus personnalisée via des applications mobiles. Et parmi les autres, 40 % étudient cette possibilité[14].

6. **Se préparer à l'exécution de microservices sur des périphériques réseau en périphérie :** Grâce à Kubernetes et d'autres capacités de gestion et d'orchestration dédiées aux charges applicatives basées sur des conteneurs, les équipes applications sont de plus en plus attirées par l'hébergement de composants de services réseau ou applicatifs sur des équipements réseau compatibles situés en périphérie. Imaginez l'impact que cette pratique aura sur les impératifs de politique, de performance, de sécurité et de segmentation de votre réseau.

Évolution du rôle de la sécurité réseau

Résumé de la section

Points clés

- Avec le transfert des applications, des données et des identités dans le cloud ou en périphérie du réseau, la sécurité périmétrique seule ne peut plus offrir une protection efficace contre les menaces actuelles.
- Face à la grande variété des périphériques et des mobinautes se connectant depuis divers emplacements à des applications réparties sur tout le réseau, de nouveaux défis apparaissent, comme la perte de visibilité et de contrôle.
- L'intégration de la sécurité et des fonctionnalités de réseau intuitif crée une puissante combinaison rationalisant l'application effective des politiques, la protection et la remédiation sur l'ensemble du réseau.

Conclusions clés

- Les architectes réseaux placent la sécurité au second rang des domaines dans lesquels investir en priorité, juste derrière l'IA.
- 43 % des équipes réseau identifient l'amélioration des capacités de sécurité réseau embarquées comme une priorité.
- En 2019, 48 % des RSSI identifiaient le « délai de remédiation » comme un indicateur de performance clé (KPI), contre seulement 30 % en 2018.
- Près de 75 % des responsables réseau estiment qu'ils utiliseront un processus de définition et d'application des politiques piloté par IA et adaptatif ou automatisé d'ici deux ans.

Conseils décisifs

- Développez des fonctionnalités de sécurité réseau dans cinq domaines essentiels : visibilité et détection des menaces, accès Zero-Trust, protection en continu, infrastructure réseau digne de confiance et intégration des workflows SecOps et NetOps.
- Veillez à inclure une stratégie de sécurité Zero-Trust dans tous les plans d'assurance et d'automatisation du réseau afin de gérer efficacement les menaces de sécurité en tout point du réseau distribué.
- Lors de la mise à niveau de l'infrastructure et des processus, les équipes réseau doivent tenir compte des impératifs de fiabilité pour être sûres que le réseau lui-même soit inviolable.
- Les équipes SecOps et NetOps doivent réfléchir à une mise en commun de leurs données et intégrer leurs outils afin de rationaliser les workflows de prévention, de détection et de résolution des menaces.

Résumé de la section (suite)

Prévisions clés

« En 2025, certains départements IT d'avant-garde auront entièrement automatisé un petit nombre de workflows de sécurité basée sur le réseau, avec lesquels ils pourront accélérer la remédiation et réduire la charge de travail de l'équipe SecOps. Le gain de maturité des plateformes IBN et des technologies d'IA et d'apprentissage automatique, ainsi que l'intégration des outils de sécurité et d'opérations réseau, permettront d'automatiser certains cas d'usage bien définis et sans aucun risque pour le dispositif de sécurité de l'entreprise et son reseau ».

– Wendy Nather, responsable de l'équipe Advisory CISO, Cisco

« En 2025, l'informatique quantique n'en sera encore qu'à ses débuts. En revanche, des programmes s'efforceront déjà de faire face à un nouveau danger : le recours à l'informatique quantique pour contrer les méthodes de chiffrement actuelles ».

- David McGrew, membre du conseil Cisco, Cisco

Évolution du rôle de la sécurité réseau

L'adoption des modèles mobiles, multicloud et IoT soulève de nouveaux enjeux de sécurité réseau et offre de nouvelles opportunités. Le périmètre traditionnel du réseau d'entreprise n'est plus désormais qu'un simple élément d'un modèle plus distribué, dans lequel les identités de tous les utilisateurs, objets et applications doivent être vérifiées, qu'ils se trouvent sur le site principal ou un site distant, et connectés à un VPN, à un réseau public ou au cloud.

Les équipes IT doivent exploiter la puissance combinée du réseau et de la sécurité pour s'attaquer efficacement aux enjeux de cybersécurité. Les architectes réseaux reconnaissent volontiers l'importance d'un investissement dans la sécurité réseau. Lorsque nous leur avons demandé comment les équipes réseau pouvaient mieux répondre aux besoins métier, les participants à notre *sondage sur les tendances mondiales des réseaux en 2019* ont placé la sécurité au 2e rang des domaines dans lesquels investir, derrière l'IA. Et 43 % d'entre eux identifiaient l'amélioration des capacités de sécurité réseau embarquées comme une priorité[14].

La convergence de la sécurité et d'un modèle de réseau intuitif permet aux départements IT d'appliquer des politiques en fonction des rôles dans l'entreprise et de répondre plus rapidement aux menaces sur l'ensemble des services réseau.

Dans ce contexte inédit, les équipes NetOps et les réseaux qu'elles contrôlent ont un rôle vital à jouer sur cinq aspects clés de la sécurité :

Visibilité : le maintien de la visibilité est une préoccupation majeure des RSSI dans ce nouveau modèle d'applications et de données distribuées.

Accès Zero-Trust : le réseau est un élément essentiel de la mise en œuvre d'un modèle de confiance cohérent, dans lequel tous les utilisateurs, périphériques et applications sont considérés avec le même niveau de suspicion, indépendant de leur point d'accès au réseau.

Selon Forrester Research, un modèle réseau Zero-Trust doit remplir trois fonctions[29] :

1

Segmenter les réseaux afin d'appliquer des contrôles granulaires tout en empêchant les déplacements latéraux.

2

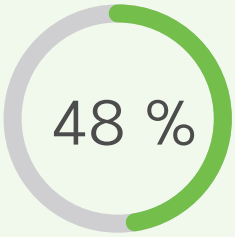
Fournir une visibilité et une analyse granulaires du réseau favorisant la détection et la résolution des menaces.

3

Apporter une capacité de gestion consolidée de la sécurité réseau et poser les bases de l'automatisation.

Protection continue : le réseau doit être à la fois une force de détection distribuée et une force d'application des règles, toutes deux capables de prendre des mesures rapides afin de confiner les périphériques infectés.

Infrastructure réseau digne de confiance : face à la menace croissante des acteurs malveillants cherchant à acquérir des informations précieuses ou à perturber le fonctionnement des réseaux, les entreprises doivent sécuriser le système réseau, et ses différents périphériques, contre les attaques.



En 2019, 48 % des RSSI identifiaient le « délai de remédiation » comme un indicateur de performance clé, contre seulement 30 % en 2018[30].

Transparence des workflows SecOps et NetOps : les RSSI estiment que leurs équipes SecOps et NetOps travaillent ensemble, puisque 95 % d'entre eux déclarent qu'elles sont très ou extrêmement collaboratives[30]. Cependant, elles ont tendance à utiliser des sources de données, des workflows et des outils distincts pour la collecte et l'analyse des données. Les équipes SecOps et NetOps doivent donc repenser leurs workflows de manière à les rationaliser, à mettre en commun leurs données et à intégrer leurs outils afin d'atteindre un but commun : une automatisation de la prévention, de la détection et de la résolution des menaces.

Selon une étude de Gartner, « pour l'équipe SecOps, l'accès au trafic réseau appuie l'analyse rétrospective des flux de trafic, l'identification des tentatives d'exfiltration, l'analyse forensique et les workflows de microsegmentation »[31].

Enjeux de sécurité réseau

Échelle et complexité accrues

L'IT doit protéger l'organisation et ses données face à des environnements toujours plus grands, plus complexes et plus changeants, à la prédominance du cloud et du mobile et à des menaces de sécurité de plus en plus difficiles à contrer.

Charges applicatives : avec le transfert des applications, des données et des identités dans le cloud ou sur Internet, le modèle IT continue de se développer en dehors du périmètre traditionnel de l'entreprise. L'essor du cloud hybride, du multicloud et des microservices hébergés en périphérie impose également de réajuster les méthodes de sécurisation des charges applicatives. La sécurité périmétrique seule ne peut plus offrir une protection efficace contre les menaces actuelles.

Clients : la complexité s'accroît également en raison des nombreux types d'équipements (appareils utilisateur et équipements IoT interconnectés) et des différentes catégories d'utilisateurs (employés, sous-traitants, tierces parties) se connectant depuis divers emplacements à des applications réparties sur tout le réseau[30].

Infrastructure : enfin, la complexité des menaces évolue et les attaquants cherchent de plus en plus à subvertir l'infrastructure sous-jacente de commutation et de routage afin d'espionner, de dérober des informations ou de manipuler les données pour ensuite lancer des attaques contre d'autres parties du réseau[32].

« Comme toute autre grande entreprise, nous devons faire face à une complexité à grande échelle. Nous inspectons 47 To de trafic Internet, nous analysons 28 milliards de flux et nous consignons 1 200 milliards d'événements de sécurité par jour ».

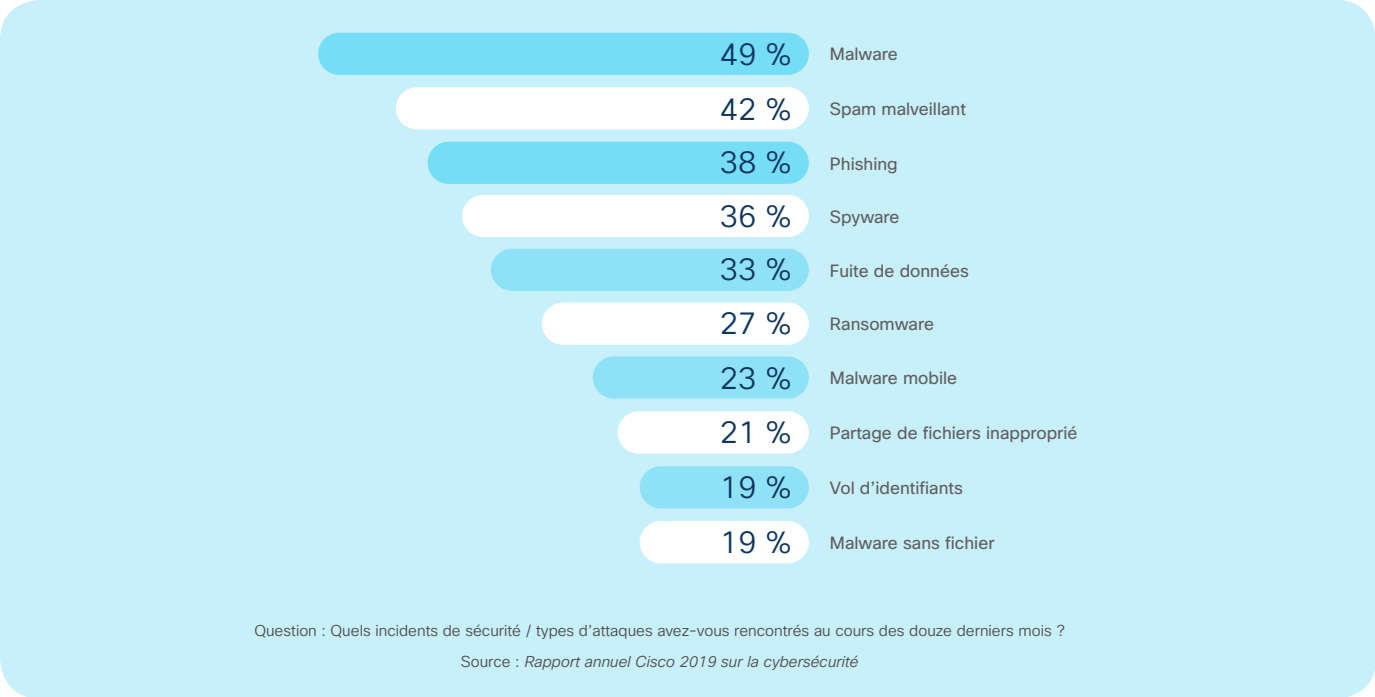
– Marisa Chancellor, directrice de la sécurité de l'infrastructure, Cisco

Le paysage des menaces : innovation continue des attaquants

Alors que la rentabilité potentielle des attaques de cybersécurité est de plus en plus alléchante, ces dernières deviennent de plus en plus sophistiquées. Voici quelques-unes des tendances les plus inquiétantes :

- Ransomware installé au sein du réseau et capable de s'autopropager ;
- Attaques par malware dissimulé dans le trafic chiffré, qui représentent 70 % de toutes les attaques malveillantes en 2017[4] ;
- Botnets IoT déployés sur des équipements non corrigés et non surveillés.

Figure 22 Menaces actuelles pesant sur la cybersécurité



Question : Quels incidents de sécurité / types d'attaques avez-vous rencontrés au cours des douze derniers mois ?

Source : *Rapport annuel Cisco 2019 sur la cybersécurité*

Pour obtenir les toutes dernières informations sur l'évolution des menaces, consultez le rapport Cisco sur les menaces de cybersécurité[33].

Conformité

Les équipes de sécurité doivent également composer avec de nouvelles réglementations, en s'assurant et en démontrant que des politiques de sécurité efficaces sont en place.

Imposant une approche proactive de la confidentialité des données, le règlement général européen sur la protection des données (RGPD) est entré en vigueur en 2018. De plus, certains secteurs d'activité, comme les soins de santé, les services bancaires et la vente au détail, ainsi que les agences du gouvernement fédéral aux États-Unis, sont soumis à des normes de conformité supplémentaires, avec de lourdes sanctions en cas de manquement.

Prolifération des équipements IoT : la surface d'attaque s'accroît

Les équipements IoT connectés continuent de se généraliser sans mesure de sécurité adaptée, essentiellement parce que, dans bien des cas, ils échappent à la connaissance ou à la détection du département IT. Chaque équipement connecté accroît la surface d'attaque de l'entreprise. À l'échelon du réseau, les équipements IoT peuvent faire l'objet d'attaques de déni de service distribué (DDoS), d'usurpation d'identification par radiofréquence (RFID) et de programmes malveillants visant les mots de passe.

Visibilité lacunaire

La prolifération des nouvelles applications cloud et des microservices peut créer des angles morts dans la visibilité de l'IT et sa maîtrise de la surface d'attaque. Aujourd'hui, les utilisateurs peuvent installer et activer eux-mêmes des applications qui ne sont pas forcément sûres ou exigent des autorisations d'accès excessives.

« De nombreux équipements IoT ont très peu de mécanismes de sécurité intrinsèques, ils utilisent rarement des certificats numériques ou des identifiants et peuvent très facilement être compromis. Pour prévenir ou contenir les incidents de sécurité, il est donc primordial d'automatiser la reconnaissance des équipements et leur classification, ainsi que l'activation des politiques d'accès réseau sur ces appareils ».

– Tim Szigeti, ingénieur en chef, Cisco IoT

Le nombre et la diversité des appareils mobiles (appartenant à l'entreprise ou aux utilisateurs) continuent de croître et la tendance BYOD (Bring Your Own Device), multipliant les accès d'appareils personnels tels que les smartphones, portables et autres tablettes aux applications stratégiques, aggravent là encore le manque de visibilité et de contrôle.

Répondre aux enjeux de sécurité grâce à un réseau intelligent

Avec un réseau intelligent, l'équipe NetOps fournit à l'équipe SecOps un allié puissant pour défendre sans relâche la sécurité de l'entreprise et de ses données. En adoptant un modèle de réseau intuitif dans lequel les fonctionnalités de sécurité sont fondamentales, le département IT peut mobiliser le système réseau pour détecter automatiquement l'apparition d'éléments nouveaux, importants et inhabituels, partout dans le réseau distribué.

En définitive, la combinaison du réseau intuitif et de la sécurité apporte une visibilité et un contrôle permanents sur les utilisateurs et les composantes du réseau. Elle contribue également à la mise en œuvre d'un modèle d'accès Zero-Trust et renforce la prévention, la détection et la résolution rapide des menaces au sein même du réseau, plutôt que de l'extérieur, pour une protection permanente et omniprésente (voir figure 23 ci-dessous).

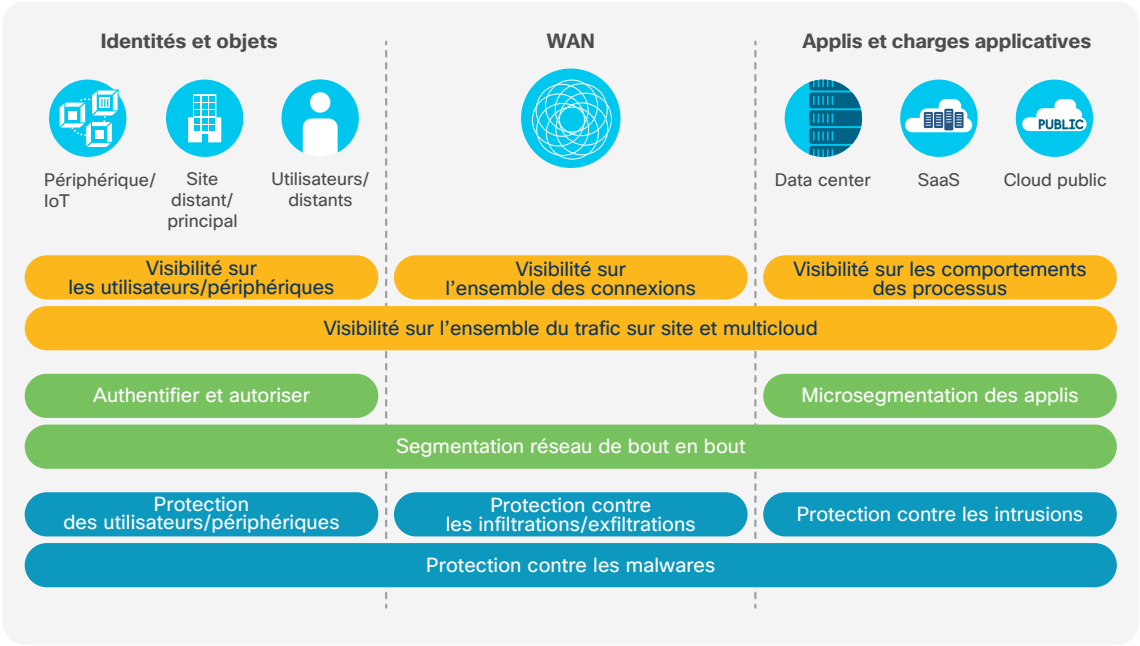
Visibilité du réseau et détection des menaces

Certains disent que l'on ne peut protéger ce que l'on ne voit pas, et c'est particulièrement le cas aujourd'hui. Pour protéger les ressources réseau et les informations, les équipes IT ont fondamentalement besoin de visibilité et ce, sur les utilisateurs, les périphériques, les applications et les objets, quel que soit leur emplacement, afin de détecter toute activité anormale et de définir une politique.

« Nous sommes confrontés à un mouvement de grande ampleur vers le SaaS et nous perdons la visibilité et le contrôle que nous avions par le passé ».

– Marisa Chancellor, directrice de la sécurité de l'infrastructure, Cisco

Figure 23 Modèle de sécurité réseau intégrée



Une vue complète de tous les réseaux (accès, WAN, data center, multicloud et IoT) permet de cartographier tous les flux traversant le réseau, et ainsi d'établir une base de référence des comportements réseau normaux. Avec un réseau intelligent offrant une visibilité totale, l'équipe réseau dispose d'une précieuse ressource pour aider l'équipe sécurité à détecter et résoudre les menaces plus rapidement et plus précisément, y compris dans le trafic chiffré.

Accès Zero-Trust

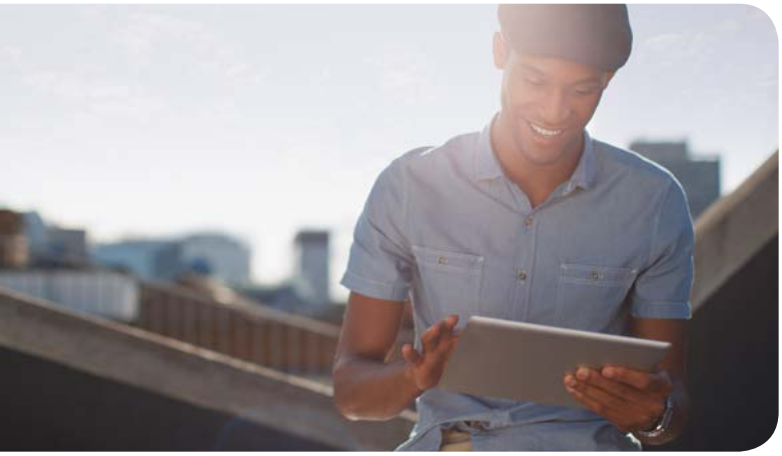
Fondé sur une visibilité avancée, un modèle global de sécurité Zero-Trust permet aux équipes NetOps de gérer les accès indépendamment du type et de l'emplacement des périphériques et charges concernés. S'il est appliqué convenablement, il permet de protéger les charges et les données au sein du cloud privé ou public, pour tous les utilisateurs, même quand ils sont hors réseau. Les principales fonctions du modèle Zero-Trust sont les suivantes :

Sécurisation de l'accès réseau : dans un modèle d'accès Zero-Trust, le département IT contrôle avec précision les connexions au réseau filaire et sans fil pour savoir quels utilisateurs ou objets y ont été autorisés, à quel moment, depuis quel emplacement et de quelle manière. L'approche Zero-Trust peut aussi passer par des contrôles basés sur des règles de groupes et par une segmentation de bout en bout de la liaison client-application, afin de restreindre l'accès aux ressources du réseau.

Mesures proactives pour maîtriser les failles des applications : le personnel IT peut limiter les déplacements latéraux non autorisés entre les charges applicatives au sein du data center et au-delà, et ainsi réduire la surface d'attaque lorsque l'attaquant a déjà pénétré le réseau.

Limitation du risque d'accès non autorisé aux applications : lorsqu'un utilisateur, quel qu'il soit, (employé, sous-traitant, tierce partie, etc.) se connecte à une application sur site ou hors site, il doit s'identifier via

un mécanisme d'authentification bifactorielle et vérifier la sécurité de son appareil. Cette étape permet d'éviter le risque d'accès non autorisé aux applications et aux données à cause d'un mot de passe volé ou faible.



Protection constante en tout point du réseau

Pour fournir une protection à l'ensemble des utilisateurs et systèmes de l'entreprise, le réseau doit s'adapter aux évolutions et étendre ses dispositifs de défense au-delà de son périmètre traditionnel. Les architectures intuitives telles que le SD-WAN offrent une plateforme centralisée permettant de déployer et de gérer une structure de sécurité complète en périphérie, et d'étendre la protection à tous les points d'infiltration ou d'exfiltration du réseau. Pour que la protection soit intégrale, cette structure doit inclure la segmentation du réseau, un pare-feu, une passerelle web sécurisée, une protection contre les malwares et une sécurisation de la couche DNS.

Si un fichier malveillant parvient à s'infiltrer, la détection des malwares peut rapidement ordonner au réseau de placer automatiquement les périphériques infectés dans un segment du réseau confiné ou mis en quarantaine. De plus, en actualisant en continu l'intelligence réunie sur les menaces de manière à bloquer les fichiers malveillants, et en transmettant cette information aux terminaux et à l'environnement cloud, le système est en mesure de prévenir les récidives.

Constituer une infrastructure réseau digne de confiance

À mesure que les entreprises basculent dans le numérique et que les menaces s'accentuent, il devient plus pressant de vérifier la sécurité et l'intégrité de l'infrastructure réseau et des différents périphériques réseau.

La constitution d'une infrastructure réseau « digne de confiance » impose de mettre en œuvre une solution de sécurité globale sur l'intégralité du cycle de vie produit. Elle contribue à la protection contre les altérations et les manipulations pendant la fabrication, la distribution, le déploiement et l'exploitation continue des produits, et répond ainsi à une nécessité majeure, car des acteurs externes, comme les revendeurs, les intégrateurs système ou les prestataires de services gérés interviennent souvent dans ces processus.

Lors de la mise à niveau des équipements, les équipes réseau doivent rechercher plusieurs fonctionnalités importantes : le démarrage sécurisé ancré dans le matériel, les identifiants de périphériques uniques et sécurisés, et la possibilité de détruire les clés et d'activer la restauration de la configuration d'usine.

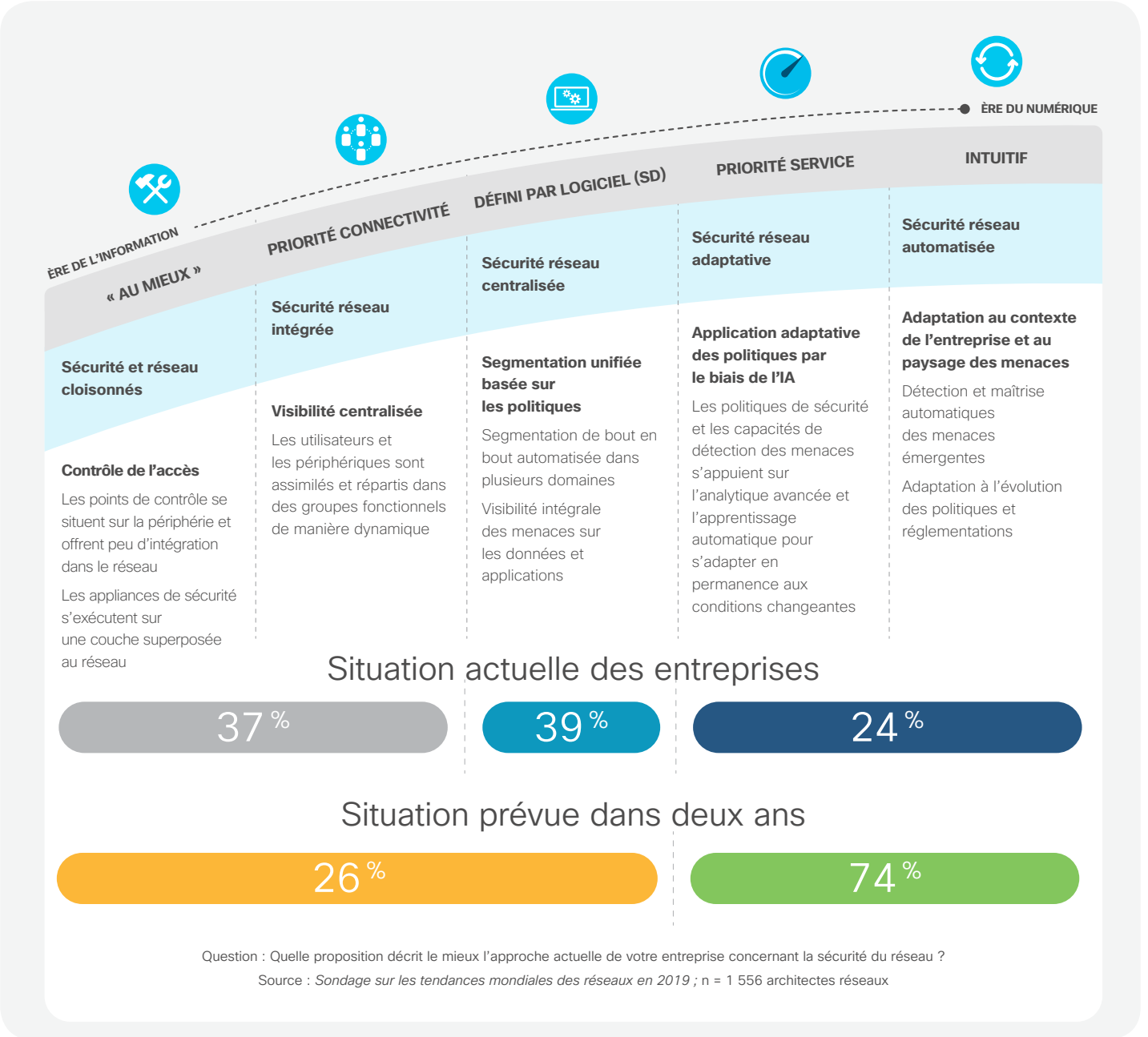
En résumé, les réseaux ont de plus en plus la capacité de se prémunir contre les menaces actuelles et futures. Il revient donc aux équipes NetOps et SecOps de prendre les mesures nécessaires pour intégrer ces fonctionnalités dans la conception et les opérations réseau afin d'obtenir ensemble une visibilité, une protection et une fiabilité continues.

État actuel et futur de la sécurité réseau

Où en sont les entreprises aujourd'hui dans l'élaboration d'un modèle de sécurité globale du réseau permettant d'obtenir une protection continue ?

Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, nous avons demandé aux responsables réseau d'évaluer leur approche actuelle de la sécurité réseau en se référant aux cinq stades de notre modèle. Si la répartition actuelle des entreprises entre les différents stades est relativement équilibrée, près des trois quarts estiment qu'elles utiliseront un processus automatisé et piloté par IA de définition et d'application des politiques de sécurité au terme de la période considérée[14].

Figure 24 Degré de préparation de la sécurité pour le réseau intuitif



Question : Quelle proposition décrit le mieux l'approche actuelle de votre entreprise concernant la sécurité du réseau ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 1 556 architectes réseaux

Rapport sur les tendances mondiales des réseaux en 2020

Tendances des opérations réseau

Passer de la réaction à l'optimisation métier

Résumé de la section

Points clés

- Dans un contexte de hausse constante des exigences numériques, les modèles traditionnels ne permettent pas aux opérations réseau une prise en charge viable des services métier requis.
- Les équipes IT modernisent les opérations IT et adoptent des approches DevOps afin de tirer le meilleur parti des systèmes basés sur contrôleur et des outils IA qui automatisent ou éliminent de nombreuses tâches répétitives des réseaux classiques.
- De nouvelles plateformes évoluées de réseau ouvert offrent une meilleure intégration dans les autres systèmes IT et de sécurité et les processus opérationnels. Elles présentent également de nouvelles opportunités pour les développeurs d'applications métier.
- Dans cette nouvelle ère des opérations réseau, les responsables et les équipes seront plus à même d'abandonner les modèles opérationnels réactifs et de fournir en permanence les services dont l'entreprise a précisément besoin.

Conclusions clés

- 73 % des équipes consacrent plus de la moitié de leur temps à préserver l'état actuel du réseau.
- Si les responsables IT pouvaient décharger les équipes réseau de certaines tâches de simple maintenance quotidiennes, ils pourraient affecter des ressources en priorité au multicloud, aux déploiements d'applications et à la protection du réseau, des applications et des données.
- Plus d'un tiers des responsables IT estime qu'il est primordial d'améliorer la coordination et l'intégration des opérations réseaux avec les autres équipes IT et entités de l'entreprise.

Résumé de la section (suite)

Conseils décisifs

- Pour adopter des modèles d'assurance et d'automatisation basés sur des contrôleurs, les équipes réseau doivent se concentrer sur trois domaines de processus stratégiques : la gestion du cycle de vie, la gestion de la politique et la gestion de l'assurance.
- Afin d'améliorer la qualité de service, les coûts, l'agilité et la sécurité, les administrateurs réseau doivent se détourner de la gestion individuelle des périphériques et concentrer leur attention sur le contrôleur réseau pour gérer, à travers lui, le système réseau dans son ensemble.
- Les équipes réseau doivent adopter une approche de plateforme ouverte axée sur le DevOps afin d'intégrer le réseau dans les processus IT et de rationaliser les workflows de bout en bout de manière à gagner en efficacité et à mieux répondre aux besoins métier.
- Les équipes NetOps doivent se doter des nouvelles capacités AIOps pour booster l'efficacité de leur réseau et les résultats de leur entreprise.

Prévisions clés

Relation entre les équipes métier et IT : « Les équipes vont réduire le temps passé à maintenir les réseaux pour tourner leur attention vers l'activité de l'entreprise et faire en sorte que le réseau réponde mieux à ses besoins tout en soutenant l'innovation métier. De nouvelles fonctions opérationnelles vont être identifiées en convertissant l'intention métier et les exigences applicatives en politiques réseau ».

Extension de la surveillance NetOps dans le cloud : « Avec la généralisation des services métier multicloud, les équipes NetOps étendront la visibilité et la surveillance prédictive aux réseaux WAN, aux réseaux publics et au point de présence cloud. Pour étoffer encore les perspectives, les systèmes de réseau intuitif d'entreprise commenceront à intégrer des données issues des systèmes des fournisseurs cloud et des prestataires de services afin de maintenir la qualité de l'expérience sur les services cloud ».

– Rich Plane, CTO de Cisco Customer Experience

Passer de la réaction à l'optimisation métier

D'après une étude Cisco, la transformation numérique des entreprises est conduite par les décideurs IT. Pour la mener à bien, ils pilotent une autre transformation, tout aussi importante : la modernisation de l'infrastructure et des opérations IT pour répondre aux nouvelles attentes de l'ère numérique[34].

Du fait de l'adoption d'une approche de plateforme ouverte axée sur le DevOps, les équipes réseau ont pour la première fois les outils et technologies nécessaires pour intégrer le réseau dans les processus IT et rationaliser les workflows de bout en bout de manière à gagner en efficacité et à mieux répondre aux besoins métier.

Cette approche permet également d'établir des liens opérationnels entre les domaines réseau et d'effectuer une intégration directe avec les applications afin de mieux prendre en charge les besoins changeants des entités de l'entreprise.

En appréhendant différemment les opérations réseau et en adoptant de nouveaux modes de travail, les responsables IT et leurs équipes seront mieux placés pour fournir des services répondant précisément aux besoins des entités de l'entreprise, que ce soit par l'amélioration des services existants ou par la création de services orientés métier.

63 %

D'après notre *sondage sur les tendances mondiales des réseaux en 2019*, 63 % des responsables IT prévoient, dans un délai de trois ans, de mettre en place des réseaux avancés capables d'apporter une réponse dynamique aux besoins métier[14].

État actuel et futur des opérations réseau

Préparation opérationnelle de la transformation numérique

Lors de notre *sondage sur les tendances mondiales des réseaux en 2019*, nous avons demandé aux responsables IT et aux architectes réseaux de qualifier le degré de préparation de leurs opérations réseau du point de vue de la gestion de l'assurance suivant un modèle de maturité à cinq stades, allant de la réaction à l'optimisation métier.

Seulement 23 % des sondés considèrent qu'ils se trouvent actuellement au stade de la prédiction ou de l'optimisation métier, quand 71 % prévoient d'y être dans deux ans. Ces chiffres soulignent donc que les entreprises ressentent bien l'urgence de se préparer à l'accroissement des exigences réseau[14].

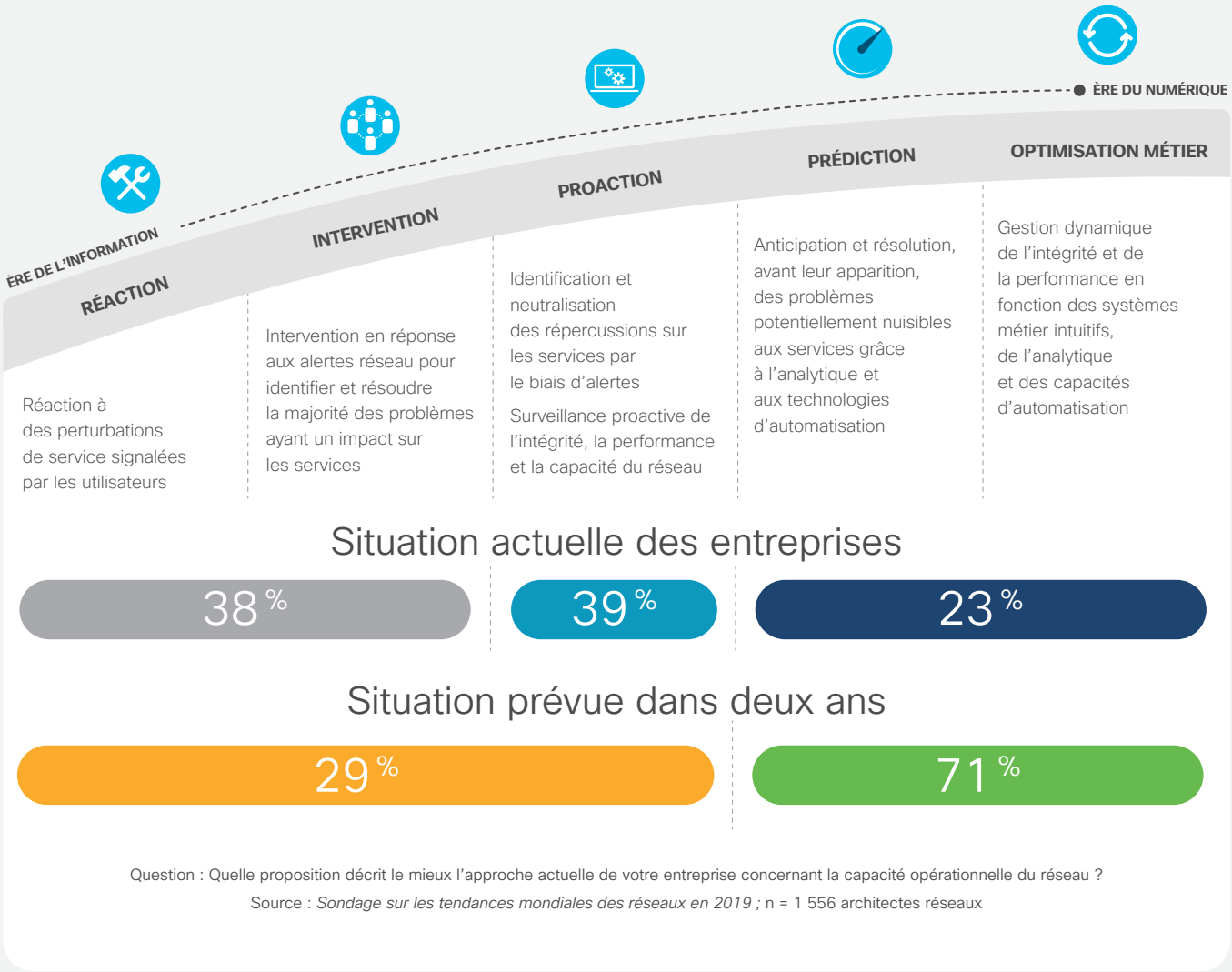
Impacts des avancées réseau sur les opérations réseau

La récente vague de technologies réseaux avancées va bouleverser les opérations réseaux sous presque tous leurs aspects et des changements majeurs devraient survenir dans les domaines suivants :

Intégration des opérations réseau dans le processus IT

Le temps où les réseaux étaient exploités en silos technologiques par des ingénieurs essentiellement spécialisés dans un seul domaine sera bientôt révolu. Dans notre étude, près d'un tiers des responsables IT insistent sur l'importance d'améliorer la

Figure 25 Préparation des opérations réseau : gestion de l'assurance



Question : Quelle proposition décrit le mieux l'approche actuelle de votre entreprise concernant la capacité opérationnelle du réseau ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 1 556 architectes réseaux

coordination et l'intégration réseau avec d'autres équipes IT, tandis que 26 % indiquent qu'il est important d'améliorer leur capacité à interagir avec les entités de l'entreprise[14]. En outre, 27 % des sondés reconnaissent qu'une conception en silos et une approche opérationnelle cloisonnée des divers domaines du réseau constituent un frein pour eux[14].

Grâce aux interfaces ouvertes des contrôleurs réseau intuitifs, les équipes NetOps vont sortir de leur isolement pour devenir une part

intégrante des processus IT. Pour 34 % des responsables IT, ce changement pourrait aider l'équipe réseau à mieux répondre aux besoins de l'entreprise[14].

Néanmoins, pour atteindre l'agilité désirée et toujours rester en phase avec l'intention métier, les équipes NetOps devront améliorer l'intégration avec l'ensemble des domaines réseau (accès, WAN, data center, cloud, etc.) et avec d'autres domaines IT, comme la gestion des services IT (ITSM) et les systèmes SecOps.

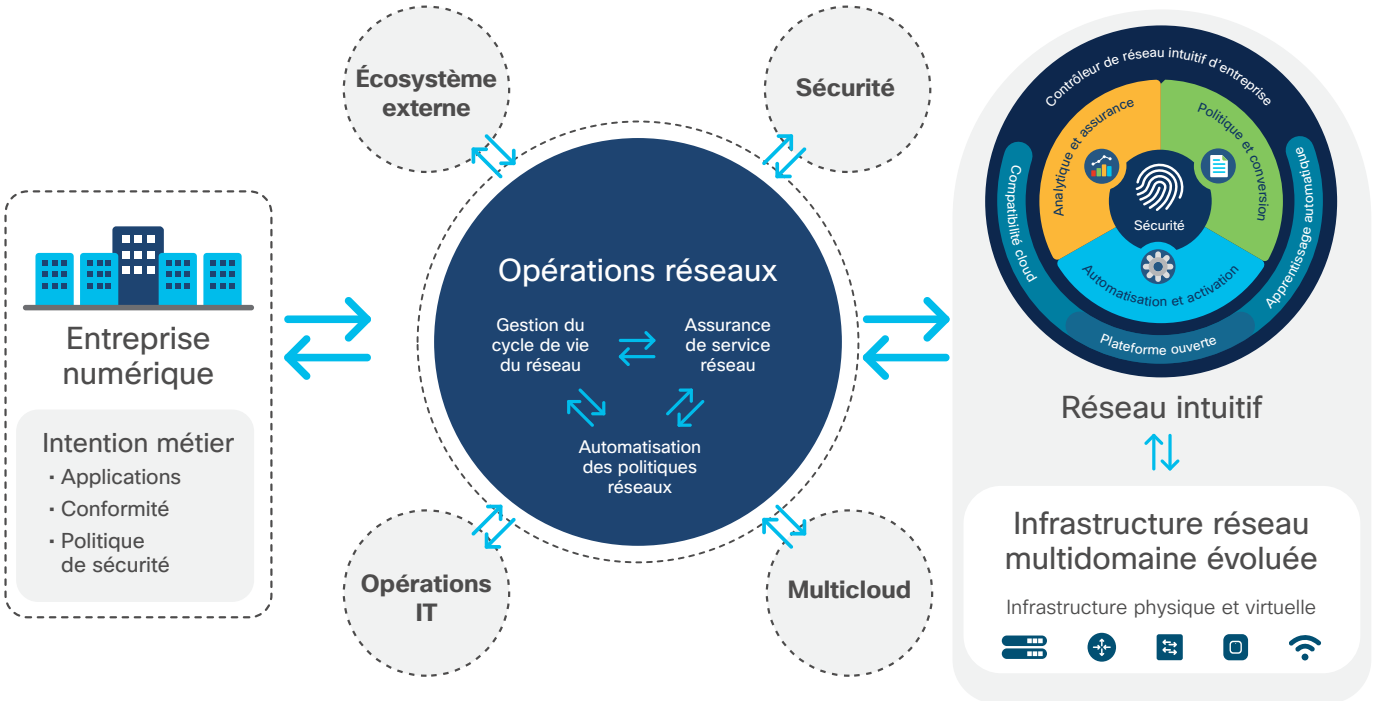
Cette figure montre comment les équipes NetOps peuvent tirer parti d'une approche réseau DevOps avec une plateforme ouverte afin d'intégrer les technologies et processus réseau à d'autres systèmes internes, voire externes.

Alignement intégral avec l'intention métier et IT

Fondamentalement, le réseau sert à fournir des services utiles aux employés, aux clients et aux partenaires, c'est-à-dire des services nécessaires au fonctionnement de l'entreprise. Mais dans la réalité, les approches traditionnelles d'exploitation manuelle ne permettent pas de répondre aux besoins dynamiques de l'entreprise. Cette situation est sur le point de changer.

Avec les réseaux intuitifs, les opérations réseau seront beaucoup plus automatisées et dynamiques, et directement déterminées par l'intention métier et IT, comme les besoins de performance pour les applications, les politiques de sécurité et de conformité, ou encore les processus IT.

Figure 26 Possibilités d'intégration avec une approche DevOps réseau reposant sur une plateforme ouverte



Avec le temps, la conversion de l'intention métier et IT en politique réseau deviendra une composante à part entière du cahier des charges des opérations réseau.

Automatiser pour simplifier les opérations réseau

Indiscutablement, l'automatisation des tâches opérationnelles révolutionne les opérations réseau. Pour un quart des responsables IT et architectes réseaux, l'automatisation est la technologie qui aura le plus d'impact sur leurs stratégie et conception réseau ces cinq prochaines années[14].

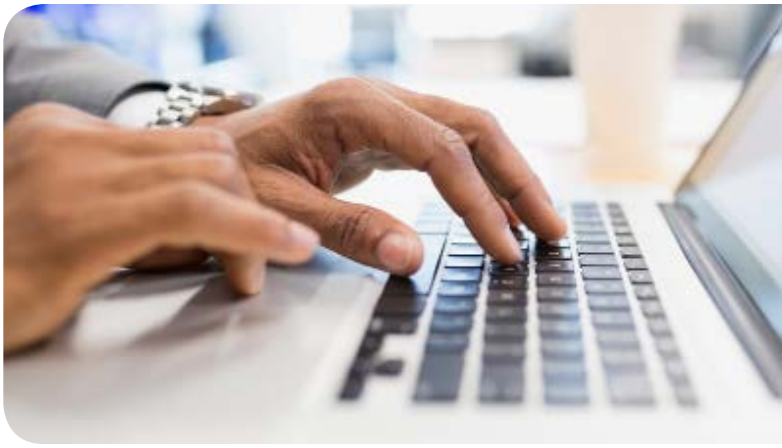
Cependant, une telle évolution implique l'abandon des approches traditionnelles de la configuration et de la maintenance réseau, axées sur les interventions manuelles. Certaines équipes seront de toute évidence perturbées par ce changement, puisque 20 % des responsables IT indiquent que la réticence des équipes NetOps à adopter les technologies d'automatisation et d'IA constitue le principal obstacle à la modernisation[14].

Gestion des problèmes et incidents : réaction ou prévention ?

Comme souligné précédemment, de nombreuses entreprises se situent au stade réactif de la préparation opérationnelle. Or, 25 % des sondés indiquent qu'une approche opérationnelle réactive les empêche d'atteindre leurs objectifs réseau[35]. L'enjeu est donc de taille, mais là encore, la situation est sur le point de changer. En utilisant l'IA et en intégrant les opérations réseau avec d'autres systèmes IT, les équipes NetOps pourront accéder à la maintenance prédictive, et ainsi anticiper les problèmes et les corriger bien avant qu'ils ne provoquent des incidents ou ne pèsent sur les services.

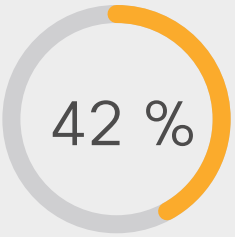
Conjuguer intelligence humaine et intelligence artificielle

Les ingénieurs réseau ont besoin de toute l'aide qu'ils peuvent trouver pour faire face à la complexité du réseau.



C'est pourquoi les équipes NetOps complètent leur arsenal avec des capacités opérationnelles pilotées par IA (AIOps). L'apprentissage automatique et le raisonnement machine permettent par exemple d'affiner les références de performance, la détection des anomalies, l'analyse automatisée des causes profondes, les conseils de remédiation et les perspectives prédictives.

Au lieu de passer au crible des milliers d'événements, les équipes NetOps s'appuieront de plus en plus sur ces technologies pour mettre au jour les événements les plus importants, et les possibilités de remédiation les plus pertinentes. L'équipe AIOps pourra aussi affiner les résultats, enrichir le contenu et intégrer les connaissances obtenues dans les systèmes clés de gestion des services et de l'activité métier.



L'assimilation de l'IA dédiée aux opérations informatiques (AIOps) s'accélère, puisque 42 % des responsables IT estiment que l'intelligence artificielle aura un impact maximal sur l'automatisation des opérations dans les années à venir[35].

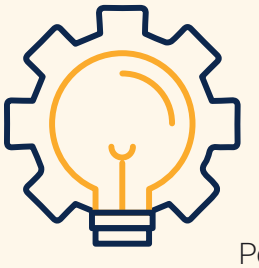
Apporter la connectivité des technologies opérationnelles aux opérations réseau

Aujourd'hui considérés comme des ressources de l'entreprise, les équipements IoT génèrent des données essentielles aux opérations métier. Il est donc évident que la gestion de l'infrastructure doit être abordée avec de nouvelles approches.

- Dans des scénarios IoT tels que la surveillance en temps réel, les problèmes opérationnels peuvent avoir de graves conséquences, voire mettre en danger des vies.
- Si les réseaux de grande envergure peuvent compter des millions d'équipements IoT, l'automatisation est le seul moyen de les gérer efficacement.
- Dans certains cas, il n'y a pas de garantie de connexion permanente entre le site principal et les équipements IoT distants (ce qui pousse à investir dans l'analytique en périphérie ou géodistribuée).

Un nouveau cadre de travail pour les opérations réseau nouvelle génération

Pour aider les entreprises à se préparer à des opérations réseau pilotées par réseau intuitif, les experts technologiques de Cisco Customer Experience ont élaboré un cadre de travail proposant des conseils stratégiques, des pratiques exemplaires, des conceptions validées, des processus éprouvés et des recommandations d'ajustement.

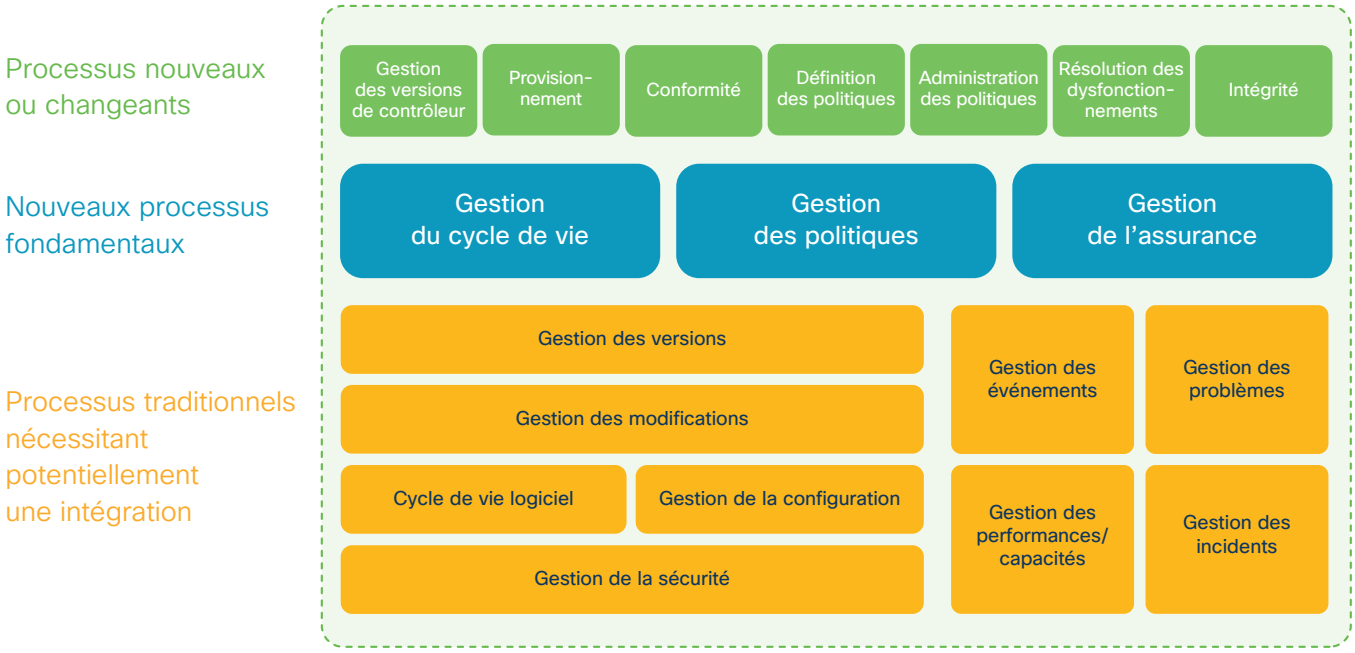


Changement de perspective : gérer le réseau sur le contrôleur

Pour Jake Hartinger, architecte de solutions Cisco Customer Experience, l'un des changements les plus profonds que va connaître le domaine des opérations réseau sera le recentrage sur le contrôleur. Jusqu'ici, pour provisionner et collecter des informations sur le réseau, les administrateurs réseau se connectaient généralement aux périphériques.

Avec les modèles d'automatisation et d'assurance basés sur des contrôleurs, les administrateurs vont avant tout gérer le contrôleur, les intégrations et les processus se rapportant au contrôleur. Plus une entreprise est en mesure d'effectuer cette transition, plus vite elle pourra améliorer la qualité de ses services, ses coûts, son agilité et sa sécurité[36].

Figure 27 Modèles opérationnels émergents pour le nouveau réseau



Au cœur de ce modèle se trouvent trois domaines de processus critiques : la gestion du cycle de vie, la gestion de la politique et la gestion de l'assurance. L'IBN propose une simplification opérationnelle permettant de planifier et d'élaborer une transformation à partir de ces processus fondamentaux.

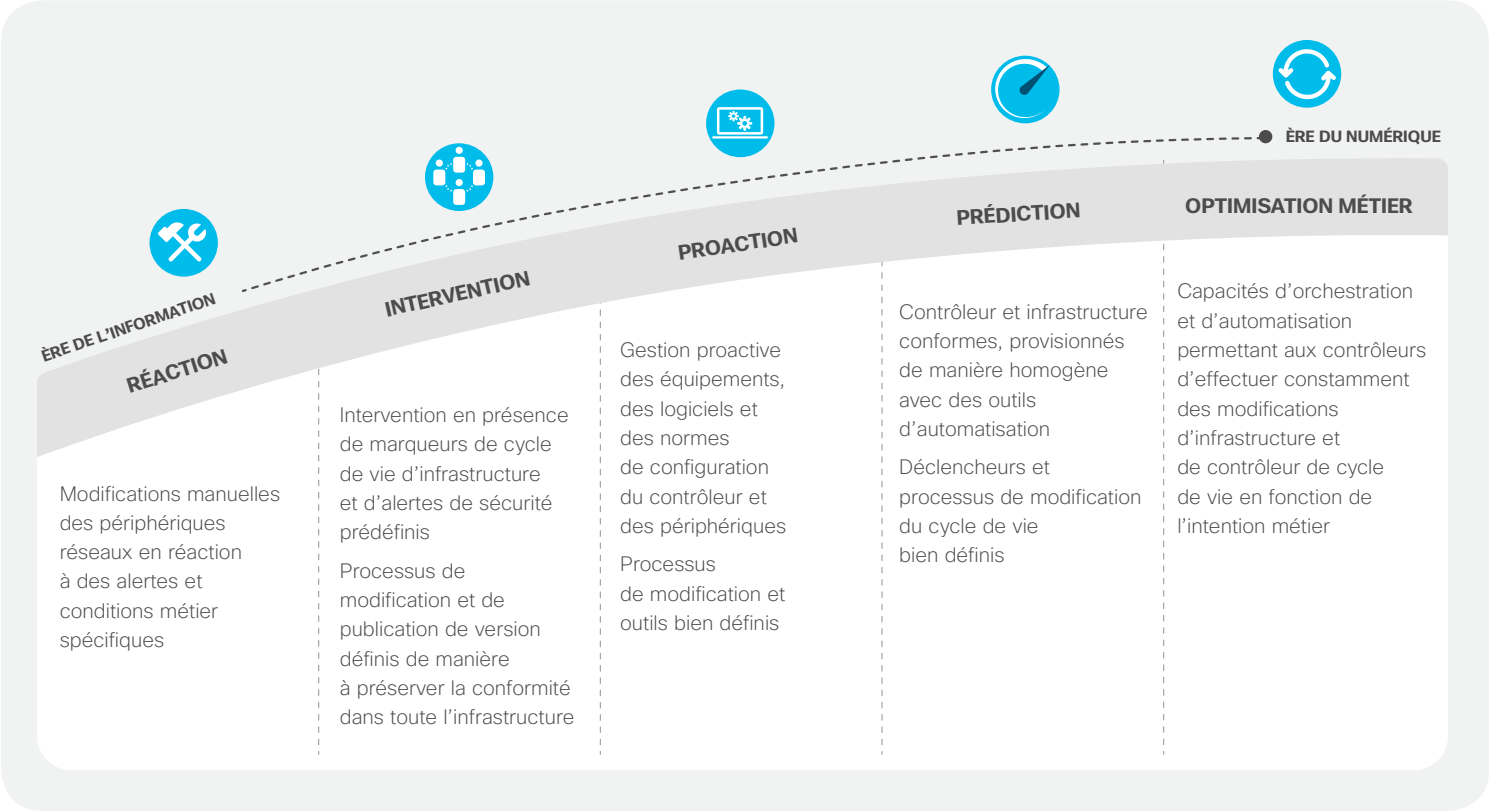
Gestion du cycle de vie

L'adoption de systèmes de provisionnement et d'automatisation pilotés par contrôleur impose un respect beaucoup plus strict des normes encadrant le matériel, les logiciels et la sécurité. Si un utilisateur effectue une modification par ligne de commande, il pourra constater dans les mises à jour suivantes que le contrôleur l'a écrasée parce qu'elle ne figurait pas au rang des politiques définies.

Pour éviter ce cas de figure, l'entreprise doit bien définir ses pratiques de gestions des versions et des changements, en particulier lorsque les automatisations s'appliquent au réseau ou au service en tant que système.

En d'autres termes, la gestion du contrôleur réseau implique l'administration de nouveaux matériels, logiciels, points d'intégration et API dédiés au contrôleur, ainsi que la configuration d'interface utilisateur administrant les fonctionnalités de politiques et d'assurance. Et comme les capacités des contrôleurs vont évoluer continuellement, au moins dans un avenir proche, il est capital de définir un processus unique pour la gestion du cycle de vie du contrôleur réseau et des intégrations.

Figure 28 Préparation des opérations réseau : gestion du cycle de vie

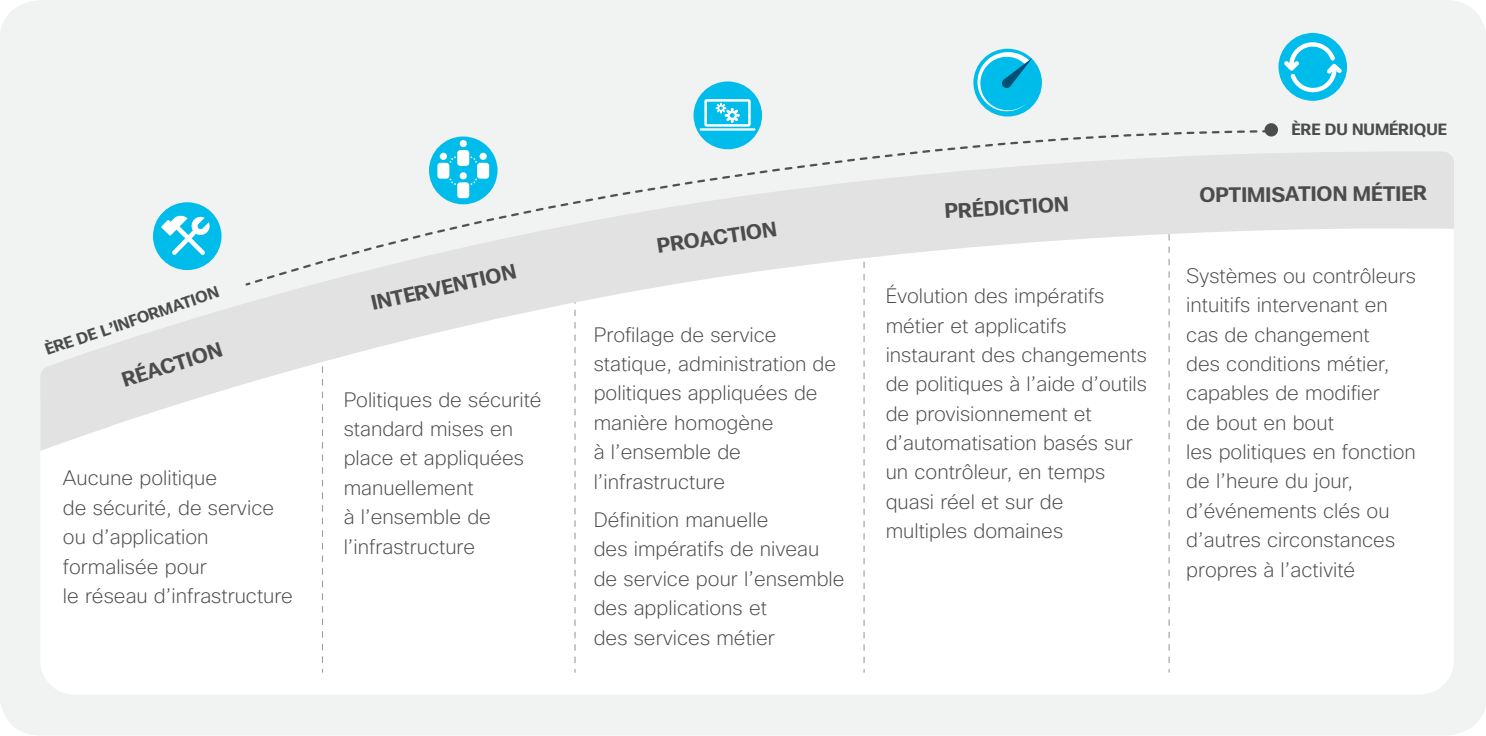


Gestion des politiques

Il est également essentiel de gérer la politique réseau. Pour combiner efficacité et durabilité, les contrôleurs réseau doivent en effet reposer sur des normes et directives plus strictes concernant le matériel, les logiciels et les configurations de périphériques réseau, voire les intégrations. La politique doit être définie, puis mise à jour. Elle doit également être configurée au sein des contrôleurs réseau pour garantir un provisionnement en continu des normes définies. Il convient aussi de valider la politique avec des méthodes de vérification de la conformité.

Les changements de politique peuvent avoir une empreinte considérable et leur activation concerner les configurations de milliers de périphériques. Par conséquent, ces changements doivent être prescriptifs par nature, afin qu'ils puissent être testés, validés et approuvés. À terme, avec la généralisation des modèles de vérification permettant de simuler tout changement de politique avant activation, les options de configuration offriront davantage de souplesse.

Figure 29 Préparation des opérations réseau : gestion de la politique



Gestion de l'assurance

Les opérations manuelles permettent aisément de gérer de petits réseaux, mais face à des architectures complexes, elles se révèlent vite insuffisantes sans l'aide d'outils, de données sur le réseau et de processus bien définis. Aujourd'hui, près d'une équipe Opérations sur cinq peut recourir à l'analytique avancée pour potentiellement identifier et anticiper les problèmes ayant un impact sur les services[14].

Avec le modèle de réseau intuitif basé sur l'IA, la gestion de l'assurance améliore ces ressources et les combine à l'analytique, aux intégrations d'API, aux fonctionnalités de corrélation, à l'inventaire et aux rapports avancés, et à l'enrichissement. L'analytique et l'enrichissement apportent notamment des détails supplémentaires sur les défaillances réseau et permettent ainsi de résoudre rapidement les incidents et d'améliorer l'intégrité du réseau. Et comme l'IA devrait permettre au système de continuer à s'améliorer grâce aux apprentissages tirés de très nombreux déploiements supplémentaires, les équipes Opérations continueront d'en tirer profit.

Pour les réseaux de grande envergure, cette évolution se traduit par une amélioration de la qualité de service, une accélération de la résolution des problèmes et des gains d'efficacité opérationnelle. Une équipe AIOps pourrait se concentrer sur le filtrage, l'enrichissement et des API en lien avec des systèmes de gestion des services et de l'activité métier afin d'automatiser totalement les workflows d'assurance.

Outre ces trois domaines de processus fondamentaux, nous recommandons d'envisager d'éventuelles interactions avec les processus ITSM traditionnels, les domaines IT et d'autres systèmes afin d'identifier d'autres possibilités d'intégration.

L'avenir des opérations réseau à l'horizon 2025

Pour Rich Plane, CTO de Cisco Customer Experience, d'ici à cinq ans, les équipes chargées des opérations réseau (NetOps) seront en mesure de répondre bien plus efficacement aux attentes de leurs entreprises. Voici ses prévisions.

1. **Assurance de bout en bout :** les équipes NetOps pourront recourir à la détection prédictive des problèmes et à l'analyse des causes profondes pour tout client ou périphérique et tout service métier, où qu'il soit hébergé, et déterminer rapidement si le réseau est à l'origine d'une quelconque dégradation de performance du service, et à quel endroit.

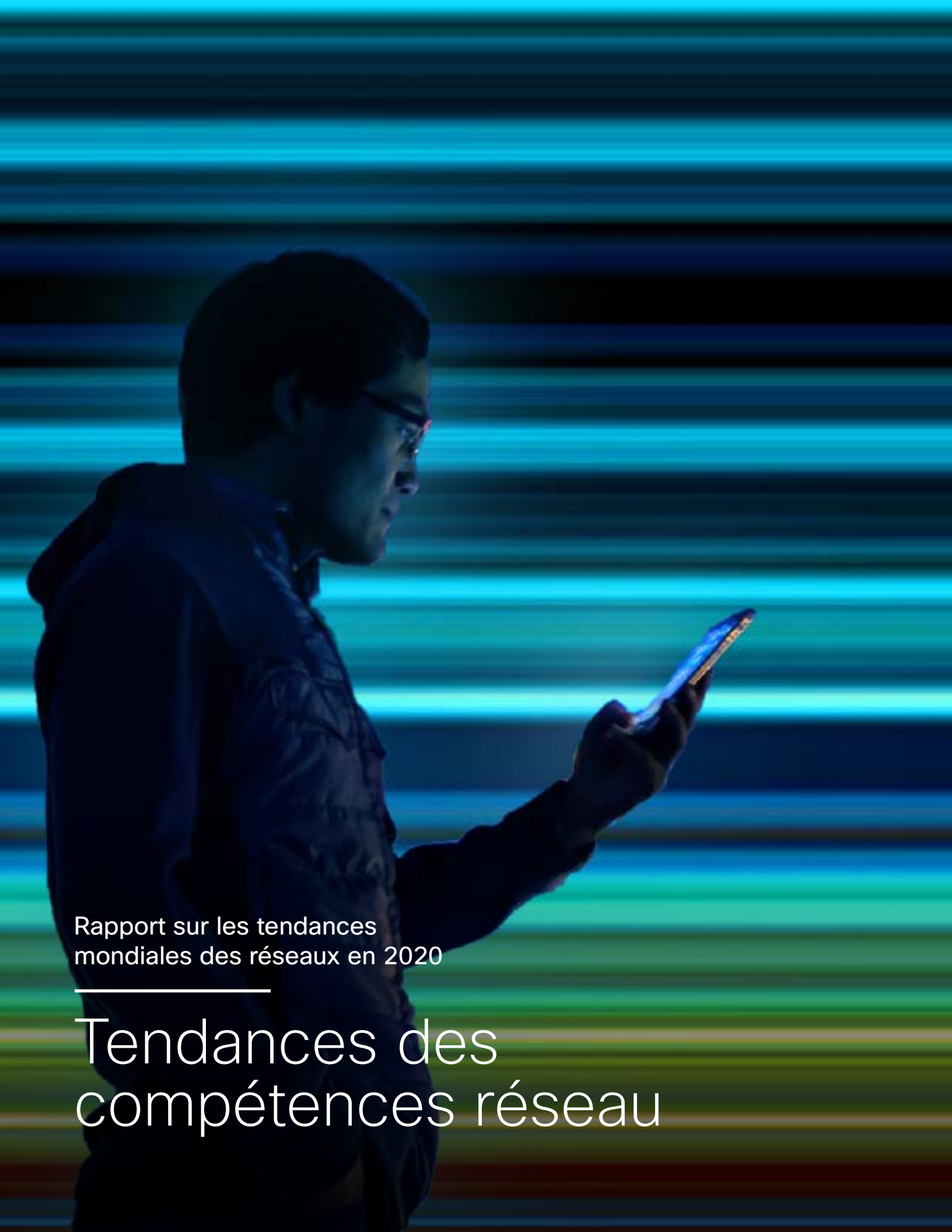
2. **Passerelle entre activité métier et IT :** les équipes NetOps pourront rééquilibrer leurs priorités. Au lieu de se consacrer presque exclusivement à la surveillance et à la résolution des problèmes du réseau, elles pourront aussi tenir compte de l'activité métier et faire en sorte que le réseau réponde au mieux à ses besoins. De nouvelles fonctions opérationnelles vont être identifiées en cernant l'intention métier et les exigences applicatives, et en les convertissant en politiques réseau.

3. **Source unique de références pour NetOps et SecOps :** les équipes NetOps et SecOps développeront des workflows intégrés et rationalisés en partageant leurs données, en automatisant la mise à disposition et en favorisant les interactions entre plateformes et outils.

4. **Extension de la surveillance NetOps dans le cloud :** avec la généralisation des services métier multicloud, les équipes NetOps étendront la visibilité et la surveillance prédictive à l'ensemble des réseaux WAN et publics, ainsi qu'au point de présence cloud. Pour étoffer encore les perspectives, les systèmes IBN d'entreprise commenceront à intégrer des données issues des systèmes des fournisseurs cloud et des prestataires de services afin de maintenir la qualité de l'expérience sur les services cloud.

5. **Gestion des changements basée sur la modélisation :** des processus NetOps plus évoluées, comme une analyse « What-If » de tout changement apporté au réseau, s'étendront au-delà du data center et se généraliseront.

6. **Autopilotage et autoréparation des workflows :** certains workflows de moindre impact seront entièrement automatisés pour permettre au réseau de prendre des mesures de remédiation ou de gestion du cycle de vie sans intervention humaine. Cette approche pilotée par les données et l'intention aura pour résultat d'accroître fortement la continuité de service, puisque les possibilités d'erreurs seront minimisées.



Rapport sur les tendances mondiales des réseaux en 2020

Tendances des compétences réseau

De nouvelles compétences pour le réseau moderne

Résumé de la section

Points clés

- Les nouvelles technologies permettent d'éliminer de nombreuses tâches manuelles dans nombre de secteurs d'activité, et l'IT ne fait pas exception à la règle.
- La bonne nouvelle pour le département informatique et les équipes réseau tient à une demande de travail toujours aussi forte pour ceux qui acquièrent des compétences aujourd'hui très recherchées, comme celles spécialisées dans la programmabilité du réseau.
- Avec l'autonomisation croissante des opérations réseau, les administrateurs réseau vont assumer des fonctions répondant aux nouvelles pratiques en lien avec la gestion du cycle de vie, la politique et l'assurance réseau.
- Les architectes réseaux auront quant à eux des missions hautement tactiques : être plus en phase avec l'activité de l'entreprise, s'intégrer aux processus IT, améliorer la sécurité et optimiser l'exploitation des données.

Conclusions clés

- Une équipe réseau consacre en moyenne 55 % de son temps et de ses ressources aux tâches de maintenance du réseau.
- 27 % des responsables IT évoquent l'absence des compétences nécessaires comme un obstacle majeur à la transition vers un réseau évolué.
- 22 % des responsables IT préfèrent opter pour la requalification en investissant dans la formation, l'apprentissage continu et la certification.
- Pour les architectes réseaux, les principaux domaines dans lesquels les compétences doivent être renforcées sont l'IA, l'intégration IT/OT, l'automatisation et le DevOps réseau.

Conseils décisifs

Architectes : envisagez d'acquérir une expertise technique, métier et logicielle vous permettant d'évoluer vers les spécialités suivantes **:**

- L'interprète métier se chargera d'aligner les performances IT avec l'intention métier.
- Le gardien du réseau établira des passerelles entre les architectures réseau et sécurité.
- L'architecte de données réseau se concentrera sur l'exploitation de l'analytique et de l'IA pour le réseau.
- L'architecte d'intégration réseau centrera son action sur l'intégration du réseau et des domaines IT.

Résumé de la section (suite)

Ingénieurs : développez de manière proactive un ensemble de compétences techniques et logiciels vous permettant d'évoluer dans l'un ou plusieurs de ces nouveaux domaines :

- Le commandeur réseau axera son action sur la gestion du cycle de vie du réseau.
- L'orchestrateur réseau se concentrera sur la conversion et l'automatisation des politiques.
- Le détective réseau se focalisera sur l'assurance des services et la sécurité du réseau.

Responsables : tenez compte de ces recommandations pour composer l'équipe réseau du futur :

- Entretenez une culture de l'apprentissage continu.
- Trouvez le juste équilibre entre requalification et recrutement.
- Investissez davantage dans la formation et le développement.
- Proposez des rotations de postes pour développer le sens des affaires.
- Favorisez un environnement de travail inclusif.

Prévision clé

« En 2025, 75 % des équipes réseau consacreront moins d'un tiers de leur temps à préserver l'état du réseau, et les deux autres tiers à l'innovation et à la création de valeur pour l'entreprise ».

– Joe Clarke, ingénieur émérite, Cisco

De nouvelles compétences pour le réseau moderne

Au cours des deux prochaines années, les technologies réseaux avancées vont modifier presque toutes les fonctions réseau. L'IT joue un rôle plus central dans la transformation de l'entreprise et les professionnels IT doivent s'adapter.

60 % des responsables métier pensent que l'IT mène la stratégie de transformation de l'entreprise. Pourtant, 93 % des cadres indiquent que la pénurie de compétences les empêche d'agir suffisamment vite[34].

Lorsqu'une entité de l'entreprise déploie une nouvelle application IoT, un nouveau service cloud ou une nouvelle politique de conformité, les professionnels IT doivent identifier les attentes vis-à-vis du réseau et le rôle qui leur revient s'ils veulent fournir les services réseau requis à temps et de manière sécurisée.

Dans cette partie du rapport, nous allons examiner les trois principales fonctions du département IT : l'architecte réseaux, l'ingénieur réseaux et le responsable IT. Nous verrons comment elles changent et identifierons les nouvelles compétences que ces professionnels doivent acquérir pour superviser un environnement réseau d'entreprise qui évolue rapidement.

Responsable IT

- Supervision globale du réseau et de l'IT
- Supervision de l'architecture et du budget réseau

Intitulés de postes : DSI, VP infrastructure IT, directeur IT

Architecte réseaux

- Chargé de définir la stratégie, la feuille de route et l'architecture du réseau, ainsi que les technologies à privilégier

Intitulés de postes : stratège réseau, architecte réseau/IT, responsable réseau

Ingénieur réseaux

- Chargé du déploiement, de la configuration, de la maintenance et de la résolution des problèmes du réseau

Intitulés de postes : ingénieur réseau, administrateur réseau, ingénieur de support réseau

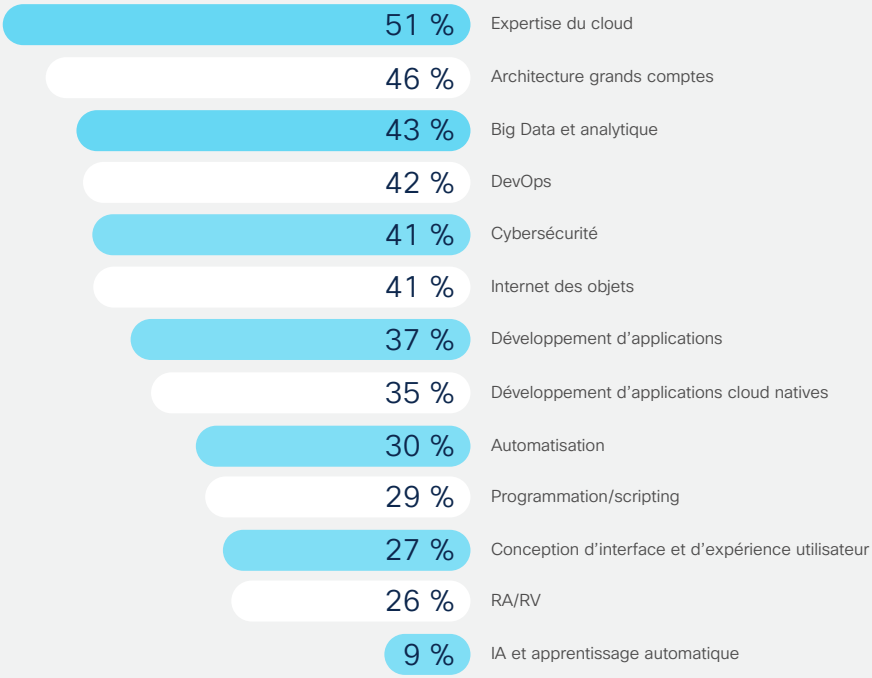
Se préparer à l'évolution des compétences réseau

Ce ne sera une surprise pour personne : la mutation du réseau d'entreprise va de pair avec l'évolution des compétences nécessaires à sa conception et à sa gestion. Dans deux sondages récents, les responsables IT et les architectes réseaux mettent en lumière les écarts de compétences qu'ils constatent, parfois dans des domaines inattendus.

Principales pénuries de compétences dans les technologies de l'information

Les données issues de notre sondage sur les compétences IT montrent que, dans l'IT en général, les technologies avancées telles que le cloud, l'architecture d'entreprise, le Big Data et l'analytique, le DevOps, ainsi que la cybersécurité figurent au sommet de la liste des compétences et spécialisations qui font défaut[34]. Incidemment, le besoin de compétences dans les quatre premiers de ces domaines (cloud, architecture d'entreprise, analytique des données et DevOps) illustrent parfaitement l'évolution que subissent les fonctions IT.

Figure 30 Principales pénuries de compétences IT



Question : Quelles sont les principales compétences ou expertises technologiques nécessaires à votre département IT pour soutenir la transformation de l'entreprise ?

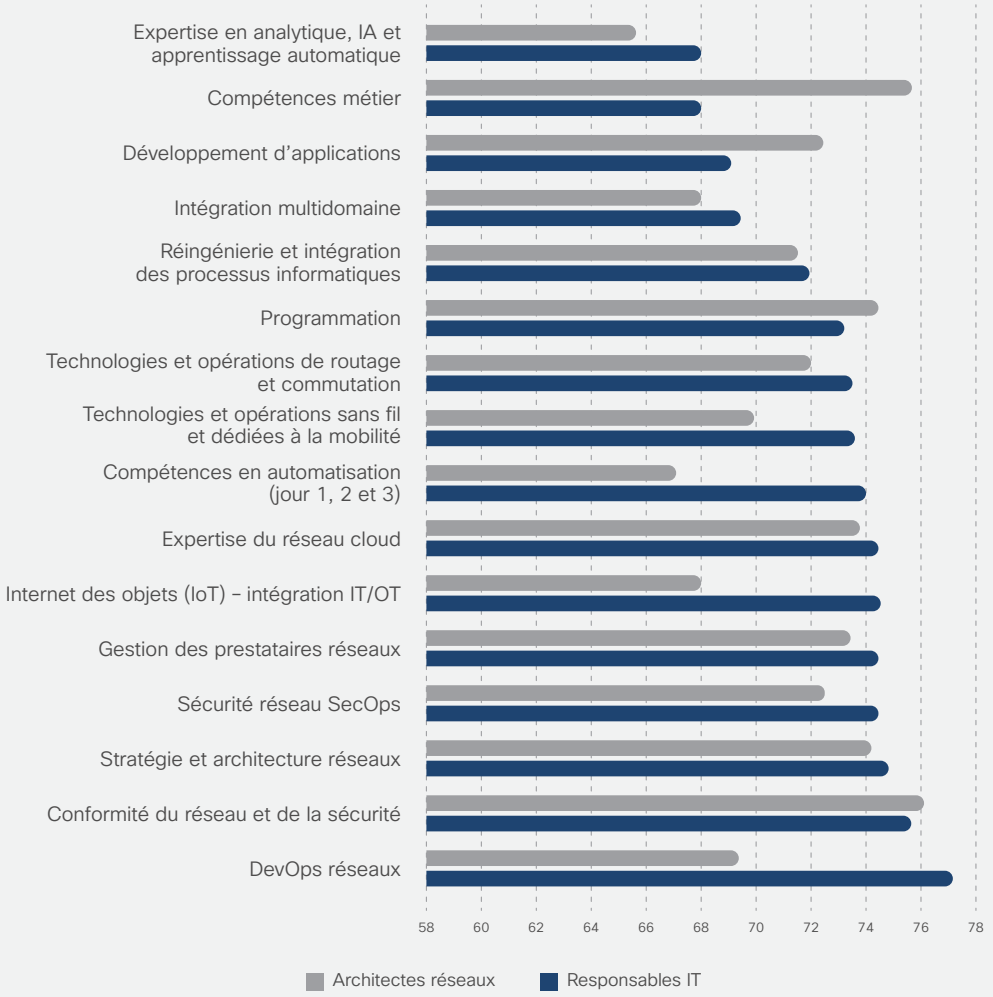
Source : *Stratégies de compétences IT nouvelle génération*, Cisco, octobre 2018 ; n = 600 cadres IT et métier

Principales pénuries de compétences dans le domaine des réseaux

Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, nous avons demandé aux responsables IT et architectes réseaux d'évaluer le degré de préparation de leurs équipes pour la conception et la maintenance d'un réseau répondant aux exigences futures de leur entreprise.

Dans l'ensemble, responsables et architectes se disent confiants dans les capacités de leurs équipes réseaux. Pour les responsables IT, l'analytique et l'IA sont les domaines nécessitant le plus d'attention, ainsi que les compétences métier et les compétences en développement d'applications. Les architectes réseaux reconnaissent aussi une pénurie de compétences en analytique et en IA, tout en citant d'autres domaines à améliorer : intégration IT/OT, automatisation et DevOps réseau[14].

Figure 31 Confiance dans la préparation des équipes réseau sur différents types de compétences



Question : Compte tenu des compétences et capacités actuelles de votre équipe réseaux, comment noteriez-vous le degré de préparation de cette équipe pour concevoir et maintenir un réseau à la hauteur des futures exigences de votre entreprise dans chacun des domaines suivants ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 2 061 (505 responsables IT ; 1 556 architectes réseaux)

Besoin croissant de compétences métier et humaines

Notre propre sondage sur les compétences IT montre que le sens des affaires est la compétence la plus rare dans l'IT aujourd'hui[34]. Il est essentiel que les entreprises comblent cette pénurie pour faire la transition vers des réseaux intuitifs. En parlant le langage des affaires, l'IT peut effectivement convertir les objectifs métier, ou l'intention métier, en politiques IT de haut niveau qui, à leur tour, peuvent déterminer les configurations d'infrastructure et d'équipement.

Figure 32 Le sens des affaires, l'une des principales pénuries de compétences

Question : Quels sont les principaux domaines de compétence et d'expertise IT qui vous font défaut pour soutenir les initiatives de transformation de l'entreprise ?
Source : *Stratégies de compétences IT nouvelle génération*, Cisco, octobre 2018 ; n = 600 cadres IT et métier

La méthode Cisco pour développer le sens des affaires

Chez Cisco, nous avons créé « Customer Zero », un programme qui place les professionnels de l'IT dans un environnement de développement de produit, où ils peuvent acquérir le sens des affaires et des compétences humaines comme la pensée critique et la capacité à résoudre des problèmes profonds. Les employés sont ainsi encouragés à s'adapter et à évoluer, ce qui nous aide à rester compétitifs.

Future prééminence des fonctions transversales

Dans un avenir proche, certaines fonctions IT vont devenir transversales et englober plusieurs domaines. Par exemple, les administrateurs réseau qui complètent leur profil avec des compétences en programmation ou en analytique des données pourront occuper une fonction émergente et ainsi élargir leur contribution et accroître la valeur de leur travail.

Ces fonctions transversales nécessiteront des combinaisons rares et très recherchées de savoir-faire techniques et de maîtrise des langages. Par exemple, les ingénieurs pourront programmer le réseau via des API et divers langages de programmation. Ou encore, les équipes NetOps et SecOps pourront collaborer pour mettre au point des workflows opérationnels rationalisés et communs.

« Nous avons besoin d'ingénieurs réseau et infrastructure qui ont la volonté de concevoir, de mettre sur pied et d'exploiter des infrastructures stratégiques. Nous avons besoin de développeurs logiciels prêts à coder des applications novatrices qui s'exécutent sur l'infrastructure et automatisent les workflows et les tâches. Les entreprises les plus efficaces disposeront d'équipes composées d'experts en logiciel et de spécialistes en infrastructure capables de collaborer »[37].

– Susie Wee, VP sénior et CTO, Cisco DevNet

Nouvelles fonctions des architectes réseaux

Incontestablement, la mission la plus urgente des architectes réseaux est d'élaborer une feuille de route pour aboutir efficacement et avec un minimum de risque à une architecture réseau plus agile et en phase avec l'activité métier. Ils devront également optimiser l'IT en créant des catalogues de libre-service réseau, en intégrant le réseau dans les processus IT, en intégrant les workflows NetOps et SecOps, et en faisant converger l'IT et les technologies opérationnelles (OT). Les entreprises auront besoin d'aide pour concevoir des innovations métier mises en œuvre par le réseau, comme la personnalisation géolocalisée, l'optimisation du taux d'utilisation de l'espace de travail, ou encore les applications d'expertise à distance.

Architecte du futur : apporter de la valeur au-delà du réseau

Pour Joe Clarke, ingénieur émérite chez Cisco, l'architecte réseaux remplira un rôle englobant de plus en plus de fonctions totalement étrangères à ses responsabilités générales actuelles. Les architectes réseaux vont probablement évoluer vers l'une ou plusieurs des spécialités suivantes :

L'**interprète métier**, chargé d'aligner les performances IT avec l'intention métier :

L'interprète s'efforcera de convertir au mieux les besoins de l'entreprise en impératifs de niveaux de service pouvant être appliqués et surveillés dans l'ensemble du réseau. L'interprète cherchera aussi à mieux utiliser le réseau et les données réseau au profit de l'activité métier et de l'innovation.

Compétences métier : déterminer les impératifs métier et les convertir en impératifs réseau.

Compétences DevOps : comprendre comment les API de plateforme réseau et les technologies de traitement du langage naturel peuvent créer une passerelle entre l'intention métier et l'IT.

L'**architecte d'intégration réseau**, centré sur l'intégration du réseau et des domaines IT :

L'intégrateur réalisera l'intégration du réseau dans le processus IT et les systèmes externes. L'intégrateur sera également chargé de l'intégration des différents domaines réseau pour garantir que l'intention est mise en œuvre dans tous les domaines pertinents.

Réingénierie et intégration des processus IT : comprendre les processus et workflows de l'IT pour modifier et intégrer les opérations réseau de manière à gagner en efficacité.

Opérations de services ITSM : comprendre les processus ITIL (Information Technology Infrastructure Library) pour établir des liens efficaces entre les systèmes d'assurance réseau et les fonctionnalités ITSM.

Compétences DevOps : développer sa connaissance des API proposées par une plateforme réseau ouverte et comprendre comment elles peuvent apporter des workflows intégrés à d'autres systèmes IT.

Le **gardien du réseau**, chargé d'établir des passerelles entre les architectures réseau et sécurité :

Le gardien va incorporer l'intelligence distribuée du réseau dans l'architecture de sécurité et les processus SecOps. Il jouera un rôle essentiel dans la convergence du réseau et de la sécurité.

La méthode Cisco : parcours de formation IT continue

Chez Cisco, nous avons mis au point plusieurs parcours de formation informatique sur des thèmes comme les spécificités des grandes entreprises, la sécurité, le data center, les prestataires de service, la collaboration et le DevNet, afin de donner aux ingénieurs la possibilité d'acquérir des compétences de pointe. Nous proposons aussi une formation continue à plusieurs échelons (Associate, Specialist, Professional et Expert), ainsi que des cours et certifications gratuits ou remisés pour les employés.

Compétences sécurité : définir des architectures de sécurité réseau, déployer les technologies de sécurité réseau et comprendre en quoi le réseau contribue à la sécurité globale.

Compétences DevOps : comprendre comment les API de plateforme réseau peuvent favoriser l'intégration aux systèmes SecOps.

L'**architecte de données réseau**, centré sur l'exploitation de l'analytique et de l'IA pour le réseau :

L'architecte de données réseau s'efforcera de valoriser les vastes quantités de données transitant par le réseau et les nouveaux outils d'intelligence artificielle afin d'améliorer les services IT et d'apporter de l'information utile à l'entreprise.

Compétences en analytique et IA : collecter des données pour accélérer et améliorer la prise de décision. Maîtriser les technologies d'IA et comprendre comment elles peuvent s'appliquer à l'assurance réseau et s'intégrer à d'autres systèmes IT pour renforcer l'assurance globale des services.

Compétences métier stratégiques : connaître l'activité de l'entreprise et comprendre comment elle peut s'appuyer sur les données accessibles par le réseau pour étayer ses décisions et créer des opportunités.

Nouvelles fonctions des ingénieurs réseaux

Alors que la transformation numérique devient un élément central de la stratégie de l'entreprise, les ingénieurs réseaux devront accorder moins d'attention aux tâches de gestion répétitive pour se concentrer davantage sur les services à valeur ajoutée qui appuient les objectifs métier. Cette transition sera facilitée par l'automatisation croissante des réseaux avancés aboutissant à la disparition de certaines des tâches les plus laborieuses des ingénieurs IT.

Ingénieurs réseau du futur : apporter de la valeur au-delà de la connectivité

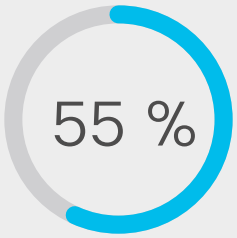
Avec la généralisation des réseaux intuitifs, les fonctions d'ingénieurs réseaux vont évoluer vers la prise en charge d'un ou plusieurs piliers des opérations réseau : cycle de vie, processus ou assurance. Dans un tel scénario, les ingénieurs réseaux devront développer les compétences nécessaires pour assumer une ou plusieurs de ces fonctions potentielles :

> « Aujourd'hui, un bon ingénieur réseau est celui qui sait intégrer les nouvelles technologies aux anciennes et faire le lien entre gestion réseau et développement logiciel. Ce profil exige à la fois une mentalité de DevOps et une connaissance pointue des liens entre les technologies et les objectifs métier ».
>
> **– Joe Clarke, ingénieur émérite, Cisco**

Le **commandeur réseau**, centré sur la gestion du cycle de vie du réseau :

Le commandeur prendra en charge les processus et les pratiques permettant de maintenir l'intégrité globale et le fonctionnement constant du contrôleur réseau et du réseau sous-jacent.

Compétences requises : exploiter, maintenir et ajuster un contrôleur assurant l'automatisation et l'orchestration dans des environnements de réseaux intuitifs. Veiller à la viabilité des intégrations de la plateforme dans d'autres systèmes. Comprendre le cycle de vie de ces contrôleurs et veiller constamment à l'intégrité, la sécurité, la conformité et la stabilité des contrôleurs et du réseau sous-jacent.



Les tâches de gestion répétitives peuvent actuellement mobiliser jusqu'à 55 % du temps et des ressources des ingénieurs réseaux[14].

L'**orchestrateur réseau**, centré sur la conversion et l'automatisation des politiques :

L'orchestrateur doit comprendre comment les besoins métier se transposent en politiques réseau, puis gérer l'automatisation de ces politiques. Il est également chargé de l'alignement des politiques avec les autres domaines réseau et IT.

> **Compétences requises :** savoir parfaitement employer les outils d'automatisation de l'infrastructure, les protocoles d'automatisation et les modèles de données. Maîtriser Linux, Python et les outils de développement pour la programmabilité réseau. Comprendre les formats de données courants. Se familiariser avec les méthodologies agiles de développement logiciel et être à l'aise avec l'utilisation d'API et de boîtes à outils pour interfacer avec les contrôleurs et périphériques réseau.

Le **détective réseau**, centré sur l'assurance du réseau et des services :

Le détective sera versé en utilisation et paramétrage des outils d'assurance réseau qui s'appuient sur l'analytique avancée et l'IA pour veiller à ce que le réseau soit à la hauteur de l'intention métier. Il devra s'intégrer dans les processus de gestion des services IT et travailler étroitement avec l'équipe SecOps pour que les anomalies réseau soient signalées et les failles de sécurité comblées.

> **Compétences requises :** identifier et prioriser les tendances en fonction des perspectives obtenues par IA, afin que l'entreprise puisse prendre des mesures proactives. Affiner les systèmes analytiques et commenter les résultats de façon à améliorer constamment la détection des anomalies et la remédiation. Intégrer les processus de détection et de résolution des problèmes réseau dans les processus IT et de sécurité.

Responsables IT : agir pour combler la pénurie de spécialistes réseau

Il est urgent de renforcer les compétences techniques pour réussir la transformation numérique le moment venu. Dans notre *sondage sur les tendances mondiales des réseaux en 2019*, nous avons invité les responsables IT à nous faire part de leurs actions en cours pour développer les compétences. La requalification, l'expansion et le rééquilibrage sont les principales approches choisies.

Figure 33 Approches privilégiées pour combler les pénuries de compétences réseau

Question : Quelle approche la direction IT de votre entreprise devrait-elle privilégier afin d'acquérir les talents qui lui manquent pour planifier, déployer et maintenir son réseau de demain ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 505 responsables IT

Bien que les responsables émettent des réserves concernant la requalification, cette approche est celle qu'ils privilégient, tant pour les compétences métier de l'IT que pour les compétences techniques.

Figure 34 Principales réserves concernant la requalification

Question : Quelles sont vos principales préoccupations concernant les éventuels plans de requalification de votre entreprise visant au développement et à la prise en charge d'un réseau plus évolué ?

Source : *Sondage sur les tendances mondiales des réseaux en 2019 ;* n = 505 responsables IT

Recommandations pour les responsables IT : composer l'équipe réseau du futur

Pour Guillermo Diaz, VP senior de la transformation client chez Cisco, ces cinq stratégies permettent aux responsables de composer une équipe réseau capable de soutenir l'entreprise après sa transformation numérique.

1. **Entretenir une culture de l'apprentissage continu :** il est absolument crucial que les responsables IT entretiennent une telle culture. L'apprentissage en continu permettra aux ingénieurs et aux architectes réseaux d'acquérir de manière régulière les compétences dont ils ont besoin pour s'adapter aux nouvelles technologies et aux nouveaux processus opérationnels. Pour ce faire, il est possible de combiner des opportunités de développement en interne et en externe offrant à vos équipes une variété de formations, d'expériences pratiques et de mises en situation.

2. **Trouver le juste équilibre entre requalification et recrutement :** d'après notre étude, les responsables recourent de plus en plus à la requalification pour combler les pénuries de compétences. Dans le domaine des nouvelles technologies, il semble toutefois que ce soit le contraire. De nombreuses entreprises cherchent à attirer de nouveaux spécialistes pour occuper les postes technologiques émergents, en particulier ceux liés à l'IA et à l'apprentissage automatique. Le juste équilibre entre développement des compétences et recrutement dépendra des objectifs métier et opérationnels, et de l'avancement de la transformation de votre réseau.

> « Il est moins coûteux de requalifier que de recruter un nouveau spécialiste à l'extérieur, indiscutablement du fait du salaire supplémentaire et des frais de recrutement, mais aussi des coûts liés à l'intégration du nouvel employé, au transfert des connaissances tacites de l'entreprise et à la familiarisation avec les processus. Vos collaborateurs en place ne disposent pas forcément de toutes les nouvelles compétences requises, mais ils ont bien des atouts pour vous mettre sur la bonne voie »[38].
>
> – Colin Seward, CIO Europe, Moyen-Orient, Afrique et Russie, Cisco

3. **Investir davantage dans la formation et le développement :** dans un récent sondage réalisé auprès de responsables IT, nous avons découvert que les entreprises qui réussissent le mieux leur transformation numérique dépensent presque 10 % de plus dans la formation et le développement du personnel IT[34]. Si le département IT est capable d'évoluer au même rythme que les technologies, il peut prendre des décisions plus rapides, plus judicieuses et plus avisées pour soutenir les objectifs de l'entreprise.

Répondre aux besoins nouveaux : offre étendue de certifications Cisco

Pour accompagner ces nouveaux besoins de formation, les cursus et certifications dédiés aux réseaux, comme ceux proposés par Cisco, se mettent rapidement à jour[37].

4 **Encourager les rotations de postes pour développer le sens des affaires :** des échanges de postes de courte durée entre les personnels IT et métier contribuent à développer la compréhension de l'entreprise, à faciliter la mise en contexte et à optimiser les interactions ultérieures. Plus spécifiquement, des rotations entre les unités réseau, application et métier permettent de cumuler des compétences liées aux technologies, à la programmabilité et au sens des affaires.

5 **Favoriser un environnement professionnel inclusif :** si les recommandations précédentes se focalisent sur les spécialistes, n'oublions pas qu'un milieu professionnel hautement inclusif permet de tirer pleinement parti des compétences disponibles en interne. Les entreprises privilégiant la diversité et l'inclusion dans leur mode de recrutement, de gestion, de développement et de reconnaissance des employés se révèlent plus performantes que celles, parmi la concurrence, qui ne le font pas. À l'initiative des dirigeants, cette démarche passe par la mise en œuvre de normes, de programmes, de politiques et de formations comportementales créant les conditions d'un environnement professionnel inclusif. L'entreprise IT nouvelle génération se doit de prêcher cette culture de la diversité et de l'inclusion par l'exemple dans son fonctionnement quotidien.

La méthode Cisco : attirer de nouvelles compétences

La découverte de nouveaux talents ne tient pas du hasard. Nous avons donc recours à des programmes spécifiques : la Cisco Networking Academy, notre université des technologies de l'information, et notre programme international de stages permettent de repérer et recruter de jeunes spécialistes. En outre, avec le programme Cisco dédié aux vétérans, nous proposons une formation débouchant sur un emploi à d'anciens militaires souhaitant poursuivre une carrière dans les technologies.

À propos de ce rapport

Le *rapport sur les tendances mondiales des réseaux en 2020* fournit aux responsables, architectes et ingénieurs IT une analyse des tendances actuelles et futures des réseaux des grandes entreprises. Il propose également des conseils décisifs concernant les technologies, les opérations et les compétences réseau. Ce rapport s'appuie sur des études menées par Cisco et réunit des données inédites issues du *sondage sur les tendances mondiales des réseaux en 2019*, réalisé auprès de 2 061 responsables et architectes IT dans 13 pays différents. Dans ces pages, des dirigeants, des membres du conseil et des ingénieurs émérites de Cisco exposent leurs points de vue d'experts et leurs recommandations pour les entreprises en cours d'adoption de technologies réseau avancées.

Dédié à Cliff Apsey, ce rapport s'est inspiré de son attachement à proposer à nos clients des expériences numériques optimales pour vous présenter ce rapport sous une forme plus enrichissante. Le temps passé à ses côtés nous est précieux et il va beaucoup nous manquer.

Sources

1. *Rapport FutureScape d'IDC : L'infrastructure des entreprises dans le monde à l'horizon 2018*, IDC, 2017.
2. *Étude annuelle du Uptime Institute sur les data center*, 2019.
3. *Prévisions complètes 2018 de l'indice Cisco VNI,* Cisco, 2018.
4. *Rapport annuel Cisco 2018 sur la cybersécurité,* Cisco, 2018.
5. « J.C.R. Licklider », Le temple de la renommée d'Internet, 2013.
6. « Histoire de la formation en ligne », The Quad, 2019.
7. *Évolution de la datasphère planétaire des périphériques et données IoT, 2019–2023*, IDC, mai 2019.
8. Dennis Smith, Dale Kutnick, Lisa Pierce, Investir dans ses réseaux d'entreprise pour réussir à l'ère numérique, Gartner, mai 2019.
9. « Bref historique de la mondialisation », Forum économique mondial, janvier 2019.
10. *Rapport Digital Vortex 2019 : un changement continu et connecté,* IMD, 2019.
11. *Réinventer le futur* (sondage sur les cas d'usage de l'automatisation), Capgemini Research Institute, 2018.
12. « Outil de synthèse des prévisions VNI », Cisco, 2017.
13. *Cisco Visual Networking Index : prévisions et tendances, 2017–2022 (livre blanc),* Cisco, février 2019.
14. *Sondage sur les tendances mondiales des réseaux en 2019,* Cisco, 2019.
15. Jonathan Forest, Neil Rickard, Feuille de route stratégique 2019 pour les réseaux, Gartner, 10 avril 2019.
16. *Faire la distinction entre intention, politique et modèles de services*, IETF, 3 mai 2018.
17. « Pourquoi le réseau intuitif est-il une bonne nouvelle pour le réseau défini par logiciel (SDN) ? » Cisco, 1er juin 2018.
18. *Réseau intuitif : Jeter des ponts entre l'activité métier et l'IT,* Cisco, janvier 2018.
19. *Réseau intuitif : Évolution du réseau principal d'entreprise*, IDC, juin 2018.
20. « Sans véritable engagement sur la voie de l'automatisation, les entreprises ne peuvent pas réussir », IT Connection, 21 juillet 2017.
21. « La montée en puissance de l'AIOps : Comment les données, l'apprentissage automatique et l'IA vont transformer la surveillance des performances », AppDynamics, 17 décembre 2018.
22. « L'assurance réseau grâce au raisonnement machine et à l'apprentissage automatique », Cisco, 25 juillet 2019.
23. *Indice mondial du cloud Cisco : Prévisions et méthodologie, 2016–2021 (livre blanc),* Cisco, 19 novembre 2018.
24. « Prévisions 2019 pour l'infrastructure », Cisco, 11 février 2019.
25. *Le multicloud comme nouvelle norme*, IDC, mars 2018.
26. *SD-WAN : La sécurité, l'expérience applicative et la simplicité opérationnelle sont les moteurs de croissance du marché,* IDC, avril 2019.
27. « Connecter ce qui ne l'est pas : la 5G et le Wi-Fi 6 joueront un rôle central dans la réduction de la fracture numérique », Cisco, 19 mars 2019.
28. « OpenRoaming : Roaming automatique et transparent entre Wi-Fi 6 et 5G », Cisco, 29 avril 2019.
29. *L'écosystème Zero Trust eXtended : Réseaux*, Forrester, 2 janvier 2019.
30. *Anticiper les inconnues : Étude comparative des Responsables de la sécurité des systèmes d'information,* Cisco, mars 2019.

31. Sanjit Ganguli, Lawrence Orans, Aligner les objectifs des outils NetOps et SecOps avec des cas d'usage commun, Gartner, 24 juillet 2018.
32. *Des attaques de cybersécurité organisées par l'État russe ciblent des équipements d'infrastructure réseau,* CISA, 16 avril 2018.
33. « Série de rapports Cisco sur la cybersécurité », Cisco, 2019.
34. *Stratégies des compétences IT nouvelle génération,* Cisco, octobre 2018.
35. *À l'heure de la transformation des opérations IT,* Cisco Connected Futures, 2018.
36. *Opérations réseau nouvelle génération,* Cisco, septembre 2019.
37. « Programmes de certifications et DevNet Cisco : les pratiques et compétences logicielles appliquées au réseau », Cisco, 10 juin 2019.
38. *Évolution de l'équipe IT,* Cisco, 2019.