The bridge to possible

Rapport de 2021 sur les tendances réseau dans le monde

Édition spéciale sur la résilience de l'entreprise : découvrez les cinq tendances qui favorisent l'agilité et la résilience en temps de crise.

Contents

Introduction – La résilience

Introduction : de la continuité de l'activité à la résilience de l'entreprise

Personne ni aucune entreprise ne pouvait anticiper une telle crise mondiale à long terme comme celle de la COVID-19 ni était prêt à y faire face. Presque du jour au lendemain, des équipes entières se sont mises à travailler à distance. Des entreprises ont dû rapidement mettre leurs produits et services en ligne, quand d'autres ont dû confier leurs chaînes d'approvisionnement stratégiques à de nouveaux fournisseurs ou travailler avec de nouveaux pays.

Cette pandémie a été un électrochoc pour toutes les nations, municipalités et entreprises. Mais qu'est-ce qui a changé ? Après tout, ce n'est pas la première fois que les entreprises font face à un défi majeur. 7 entreprises sur 10 ont affronté au moins une crise grave au cours des 5 dernières années et 95 % d'entre elles pensent que ce ne sera pas la dernière.[1]

Nombre d'entreprises ayant affronté au moins une crise grave au cours des 5 dernières années.

Source : enquête de PwC sur la crise mondiale de 2019

Les crises d'origine humaine comme les cyberattaques, les obligations réglementaires et les crises sociales sont de plus en plus courantes. Partout dans le monde, nous subissons les effets dévastateurs d'ouragans, d'incendies, d'inondations et d'**autres catastrophes naturelles** à un rythme qui s'accélère.

Pour faire face aux crises futures, il est important que les responsables IT adoptent un nouvel état d'esprit. Ils doivent notamment privilégier l'agilité IT afin d'assurer la **résilience de l'entreprise** plutôt que de persévérer dans l'approche normative et réactive sur laquelle s'appuie la planification de la **continuité de l'activité classique**. Contrairement aux mesures de continuité de l'activité actuelles, la résilience de l'entreprise permet de parer à toutes les éventualités même les plus inattendues.

[1] PwC, enquête de PwC sur la crise mondiale de 2019.

Continuité de l'activité ou résilience de l'entreprise

Continuité de l'activité : la capacité d'une entreprise à continuer à fournir des produits ou des services à des niveaux acceptables prédéfinis à la suite d'un incident. *

Résilience de l'entreprise : la capacité d'une entreprise à faire face et à s'adapter à un environnement en plein bouleversement afin de poursuivre ses objectifs, de survivre et de prospérer. **

* International Organization for Standardization, « Sécurité et résilience-Vocabulaire », ISO 22300-2018

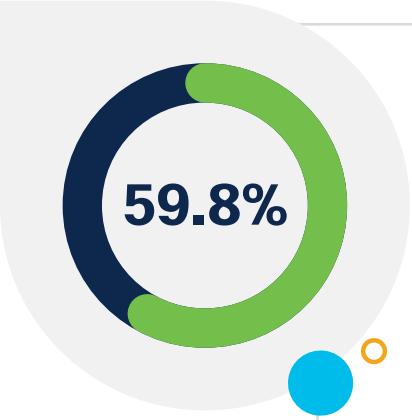
** International Organization for Standardization, « Sécurité et résilience-Vocabulaire – Résilience organisationnelle – Principes et attributs », ISO 22316-2017

Figure 1. De la continuité de l'activité à la résilience de l'entreprise

Cinq tendances en matière de réseau

Le réseau : 5 tendances pour assurer la résilience de l'entreprise

Les processus commerciaux vitaux dépendent d'un tissu de plus en plus complexe de technologies numériques qui sont indispensables pour assurer la résilience organisationnelle.



59,8 % d'experts de la continuité de l'activité estiment que la résilience IT est le facteur le plus important pour répondre à la pandémie actuelle.

Source : BCI, l'avenir de la continuité d'activité et de la résilience

Étant la seule plateforme qui relie et protège des utilisateurs et des équipements de plus en plus dynamiques et distribués, ainsi que des applications et des workloads de plus en plus dispersés, le réseau joue un rôle central pour assurer la résilience des entreprises.

Il ne suffit plus de se contenter d'assurer la connectivité et le fonctionnement du réseau. Les entreprises ont besoin d'une plateforme réseau avancée qui leur confère la résilience nécessaire pour réagir rapidement à toutes les situations, mettre en œuvre de nouveaux modèles et services opérationnels, intégrer des processus IT et protéger leurs collaborateurs, leurs activités principales, leurs clients et leur marque, ce même réseau à l'origine de la réussite des initiatives de transformation numérique.

Résilience du réseau ou réseau au service de la résilience de l'entreprise

Résilience du réseau : la capacité de fournir et de garantir un niveau de service acceptable en dépit des défaillances et des problèmes nuisant au fonctionnement normal d'un réseau de communications donné en fonction des installations prévues.*

Réseau au service de la résilience de l'entreprise : réseau conçu pour permettre aux entreprises de réagir rapidement, en toute sécurité et efficacement aux incidents attendus et inattendus.

* Union internationale des télécommunications : Exigences pour la résilience des réseaux et leur reprise.

Assurer agilité et résilience pour les collaborateurs, l'espace de travail, les workloads et les opérations

Nous avons sélectionné cinq tendances que les responsables réseau doivent prendre en compte pour mettre en œuvre les plans de résilience de leur entreprise. Il s'agit principalement de renforcer la résilience dans quatre domaines clés : **les collaborateurs, l'espace de travail, les workloads et les opérations IT** .

Figure 2. Base réseau pour la résilience des collaborateurs, de l'espace de travail, des workloads et des opérations IT

Protéger les collaborateurs travaillant à distance

Tendance 1 : les collaborateurs – Étendre la sécurité aux collaborateurs travaillant à distance

La plupart des entreprises commencent à réaliser que les modes de travail de leurs collaborateurs vont évoluer pour devenir plus flexibles.

En moyenne 4,7 fois plus de personnes travaillent de chez eux par rapport à la situation avant la pandémie. De nombreuses équipes IT ont des difficultés à faire évoluer leur réseau pour répondre à la croissance soudaine de la demande.

Source : rapport de Freeform Dynamics sur l'espace de travail moderne commandité par Cisco, juillet 2020

Par conséquent, les équipes IT doivent satisfaire de nouveaux besoins :

- Soutenir la productivité et la collaboration partout
- Optimiser les performances, le coût et la sécurité de l'infrastructure IT pour chaque collaborateur
- Étendre les opérations et la gouvernance IT de l'entreprise à leur domicile

Mais répondre à ces besoins présente des difficultés. La **sécurité des** télétravailleurs, ainsi que le **comportement des utilisateurs** font partie des préoccupations permanentes de la majorité des départements IT.

4 principales difficultés liées à l'IT pour mettre en œuvre le télétravail :

Sécurité (65 %)

Comportement des utilisateurs (52 %)

Performance des applications (43 %)

Opérations IT (35 %)[2]

[2] Étude Cisco 2020 sur le réseau au service de la résilience de l'entreprise

Les télétravailleurs sont particulièrement vulnérables aux cyberattaques lorsqu'ils accèdent aux applications et aux données de l'entreprise via leurs équipements et connexions personnels. Beaucoup contournent le VPN et se connectent directement aux services et applications dans le cloud public, qui reste l'environnement le plus difficile à défendre.[3]

Considérations relatives au réseau : pour mettre en œuvre des modèles de télétravail sécurisés à grande échelle, les équipes IT doivent adopter certaines ou l'ensemble des approches suivantes :

- **Mettre à l'échelle les VPN pour protéger les télétravailleurs :** les VPN d'entreprise restent l'un des moyens les plus rapides et efficaces pour offrir le même niveau de contrôle et de protection à la maison que sur le lieu de travail.
- **Utiliser l'authentification multifacteur (MFA) pour protéger les applications :** l'authentification MFA, qui vérifie l'identité de chaque utilisateur avant de lui permettre d'accéder au réseau ou aux applications et données sensibles, est essentielle pour protéger l'entreprise.
- **Déployer une solution SASE (Secure Access Services Edge) pour protéger l'accès mulitcloud :** la sécurité basée dans le cloud et SASE offrent une protection contre les attaques sur Internet, quels que soient la connexion, l'équipement ou l'environnement cloud.

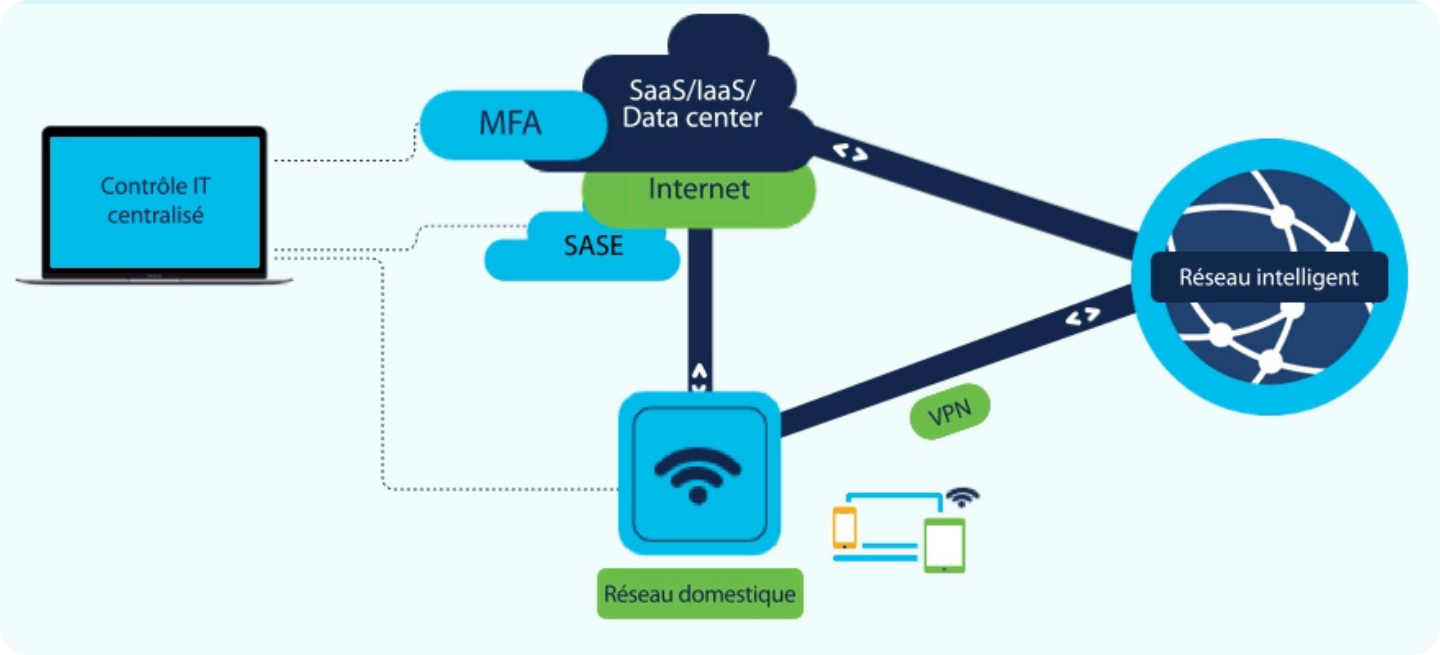


Figure 3 : Sécuriser les télétravailleurs avec le VPN, l'authentification MFA et SASE

Découvrez comment connecter et sécuriser vos collaborateurs travaillant à distance

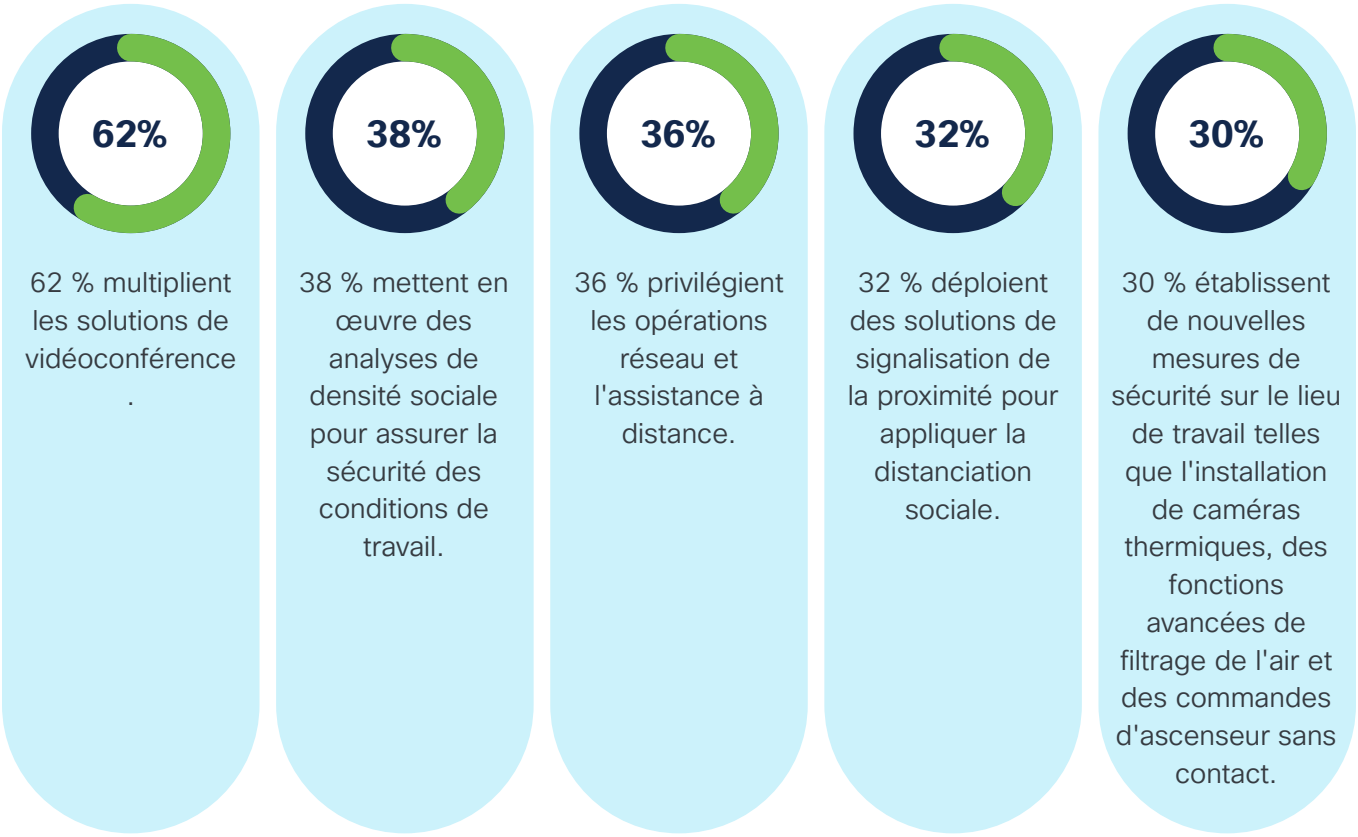
[3] Cisco Umbrella, rapport 2019 sur les tendances en matière de cybersécurité.

Sécuriser l'espace de travail

Tendance 2 : l'espace de travail – Assurer la sécurité des collaborateurs qui retournent au bureau

Bien que de nombreuses questions demeurent, il est certain que les lieux et les espaces de travail continueront à évoluer suite à la pandémie. Un grand nombre d'entreprises travaillent à optimiser les services existants tels que la vidéoconférence et le Wi-Fi géodépendant. D'autres déploient de nouveaux services et protections, telles que la surveillance de la distanciation physique, la signalisation de proximité, l'automatisation accrue de l'espace de travail et même des robots qui soutiennent la productivité humaine et facilitent la communication.

Comment les équipes réseau se préparent pour un retour au bureau sécurisé



Source : « Étude Cisco 2020 sur le réseau au service de la résilience de l'entreprise »

Considérations relatives au réseau : un réseau moderne et agile est un facteur essentiel pour faciliter le retour des collaborateurs sur leur lieu de travail en toute sécurité et sans difficulté.

- **Tester le réseau :** dans de nombreux cas, le réseau est resté inactif pendant plusieurs semaines. Il est possible qu'il n'assure plus le même niveau de services sans fil et filaires.
- **Automatiser l'accès sécurisé basé sur l'identité :** les entreprises doivent pouvoir gérer, sécuriser et segmenter en permanence l'intégration des utilisateurs et des équipements ainsi que l'accès aux services, quel que soit le réseau de connexion, un réseau public, celui de l'entreprise ou du domicile.
- **Renforcer la sécurité des collaborateurs et des clients via l'analyse géodépendante :** mettre en œuvre des solutions de surveillance, de génération d'alertes et de collecte d'informations sur le lieu de travail pour protéger la santé et la sécurité des collaborateurs, des partenaires, des invités et des clients en tirant parti des réseaux Wi-Fi existants.

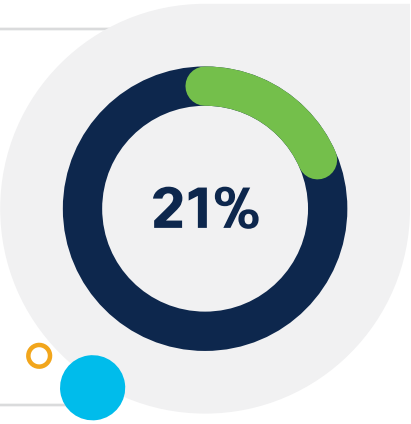
Découvrez comment créer un espace de travail sécurisé

Workload et multicloud

Tendance 3 : les workloads – Privilégier le multicloud pour renforcer la résilience

Suite à la pandémie mondiale, les responsables IT utilisent les services cloud pour améliorer la résilience de leur entreprise. Nombre d'entre eux adoptent un modèle multicloud, qui permet de répartir les applications, les workloads et les données entre différents data centers sur site et fournisseurs de cloud public, afin de réduire les coûts, d'augmenter la flexibilité, de prévenir les risques de pannes et d'empêcher leur propagation.

> "21 % des entreprises transfèrent des workloads supplémentaires dans le cloud public en raison des problèmes de CapEx liés à la pandémie. "
>
> IDC, étude sur l'impact de la pandémie de la COVID-19, Wave 5, 2020



Considérations relatives au réseau : pour offrir un niveau d'expérience cohérent aux utilisateurs et aux équipes de développement, les entreprises doivent élaborer une stratégie réseau multicloud proactive qui tient compte des priorités en matière de cloud, de sécurité et d'opérations IT.

Les stratégies de réseau multicloud efficaces reposent sur trois piliers :

- **Les workloads :** adopter un modèle opérationnel basé dans le cloud pour simplifier les politiques, la sécurité et la gestion des workloads et des services dans les data centers sur site, les divers types de cloud et d'autres environnements informatiques.
- **L'accès :** adopter des approches SD-WAN et SASE afin de sécuriser en permanence l'accès multicloud (notamment SaaS) pour les utilisateurs et les équipements sur des réseaux professionnels et publics, depuis un réseau local, une succursale, en déplacement ou à domicile.
- **La sécurité :** réduire les risques associés aux utilisateurs, équipements et applications répartis dans plusieurs clouds et d'autres environnements informatiques.

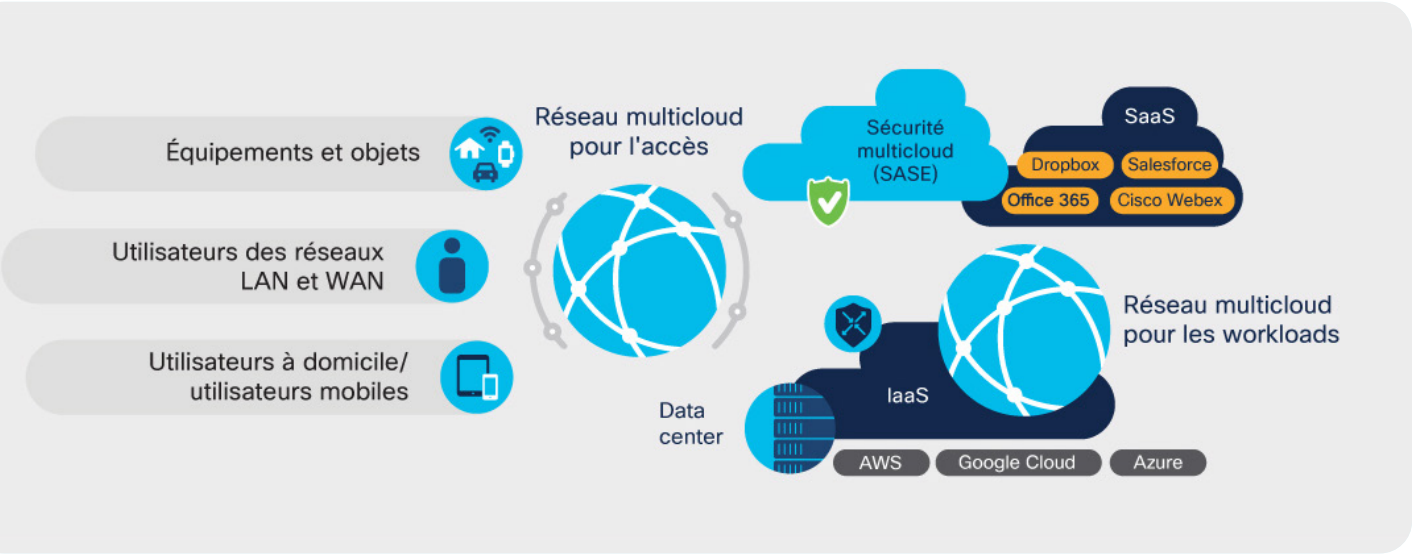


Figure 4 : Réseau multicloud : workloads, accès et sécurité

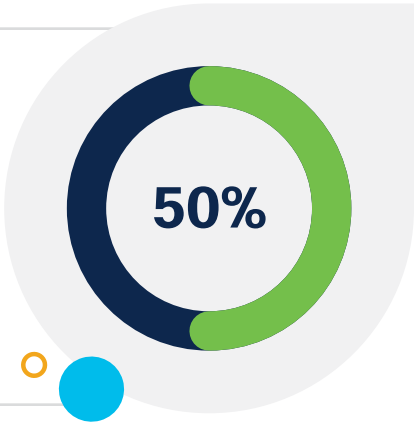
Découvrez comment créer une stratégie de réseau multicloud sécurisée et efficace

Opérations automatisées

Tendance 4 : les opérations – Automatiser les opérations pour une reprise plus rapide

L'explosion du nombre de télétravailleurs dispersés n'est pas le seul facteur de tension pour les équipes en charge du réseau. La pandémie a également donné lieu à des niveaux de fluctuation sans précédent du nombre de clients, ainsi qu'à une évolution des modèles de trafic applicatif et à des nouvelles utilisations telles que la formation à distance, la vidéoconférence, les événements virtuels, les soins à distance, l'automatisation des processus et d'autres services réseau.

> "50 % privilégient l'automatisation du réseau pour répondre aux perturbations actuelles. "
>
> Étude Cisco 2020 sur le réseau au service de la résilience de l'entreprise



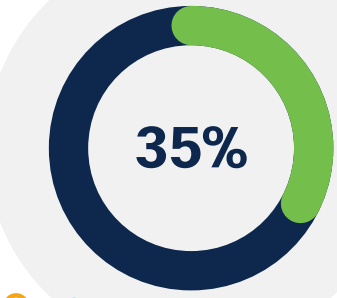
Il n'est donc pas surprenant que la moitié des experts des technologies réseaux estiment que l'automatisation du réseau est indispensable pour garantir le niveau de performance des services pendant une crise.

Source : rapport Cisco de 2020 sur les tendances réseau dans le monde

Considérations relatives au réseau : les équipes en charge du réseau obtiennent de meilleurs résultats et répondent rapidement à l'augmentation des incidents et des menaces en adoptant une approche progressive :

- **Automatiser les tâches administratives répétitives** comme le provisionnement et la configuration du réseau, ainsi que la gestion des images afin de réduire la charge administrative et d'améliorer la conformité dans chaque domaine.
- **Automatiser l'accès réseau, l'intégration et la segmentation** pour protéger les groupes d'utilisateurs et d'objets distribués et réduire la propagation des cyberattaques.
- **Automatiser les politiques réseau dans le data center de l'entreprise** avec une segmentation qui protège les applications et les données et qui suit les workloads.
- **Automatiser les politiques du data center au cloud** avec un modèle opérationnel du cloud qui applique la même politique aux applications dans les environnements sur site et cloud hybride.
- **Automatiser la segmentation de bout en bout multidomaine basée sur une politique** pour établir un modèle d'accès de type zero-trust intégral et cohérent couvrant les utilisateurs, les équipements et les workloads.

> “35 % des entreprises prévoient de mettre en œuvre un réseau intuitif de bout en bout d’ici 2022 et au-delà, contre seulement 4 % en 2019. ”
>
> Rapport Cisco de 2020 sur les tendances réseau dans le monde



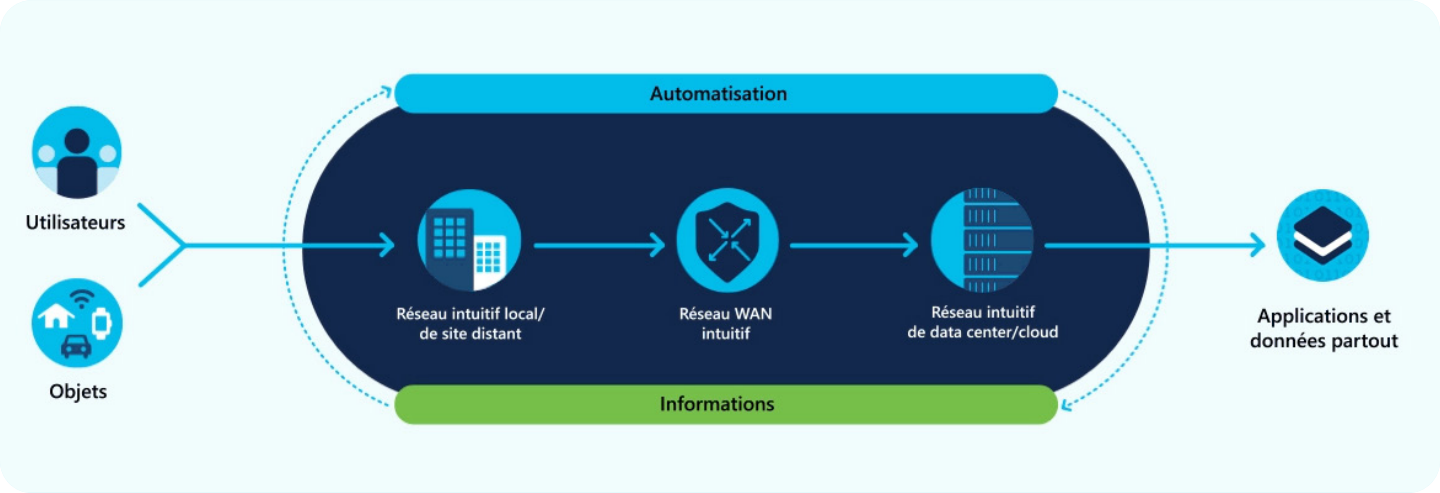


Figure 5 : Automatisation et informations, de l’utilisateur aux workloads, partout

Découvrez comment automatiser les politiques sur plusieurs domaines réseau

Opérations optimisées par l'IA

Tendance 5 : les opérations – Optimiser les analyses réseau avec l'IA pour obtenir des données plus pertinentes

Gérer la complexité et l'ampleur des réseaux modernes ainsi que le volume d'événements et de problèmes à traiter en conséquence sur diverses plateformes de surveillance est à la fois ardu et inefficace, surtout en cas de catastrophe.

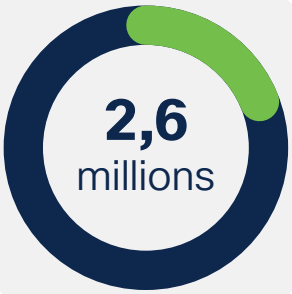
"4 400 : nombre moyen d'événements mensuels liés aux connexions sans fil sur le réseau d'une entreprise. * "

Source : Télémétrie Cisco : Cisco DNA Center, 2020

* Basé sur plus de 600 réseaux d'entreprises. Les événements incluent les échecs/délais d'intégration, le débit radio et le temps de réponse/les échecs DHCP. La collecte dynamique des performances de référence optimisée par l'IA a déjà permis de réduire ces événements.

Les équipes en charge du réseau doivent s'appuyer sur des analyses avancées pour prendre des décisions opportunes et avisées.

Avec les analyses réseau optimisées par l'IA et les techniques d'apprentissage automatique, ces équipes ont moins de problèmes à gérer.



"Em nível global, o Cisco AI Network Analytics, uma aplicação do Cisco DNA Center, resolve 2,6 milhões de "eventos" mensais em 15.080 "problemas" acionáveis – uma redução de 99,4%. *"

Source : Télémétrie Cisco : Cisco DNA Center, 2020

* Basé sur plus de 700 réseaux d'entreprises dans le monde.

Grâce à cette réduction, les équipes concentrent leurs efforts sur les problèmes sérieux qui risquent d'avoir un impact négatif sur l'activité.

Et cela ne se limite plus aux réseaux d'entreprises. Comme désormais la majorité des transactions émanent du réseau d'entreprise classique ou aboutissent en dehors de celui-ci, les équipes en charge du réseau ont besoin de visibilité et d'analyses sur les réseaux publics auxquelles elles se connectent, en particulier pendant les périodes de tension inhabituelles, comme la pandémie actuelle.

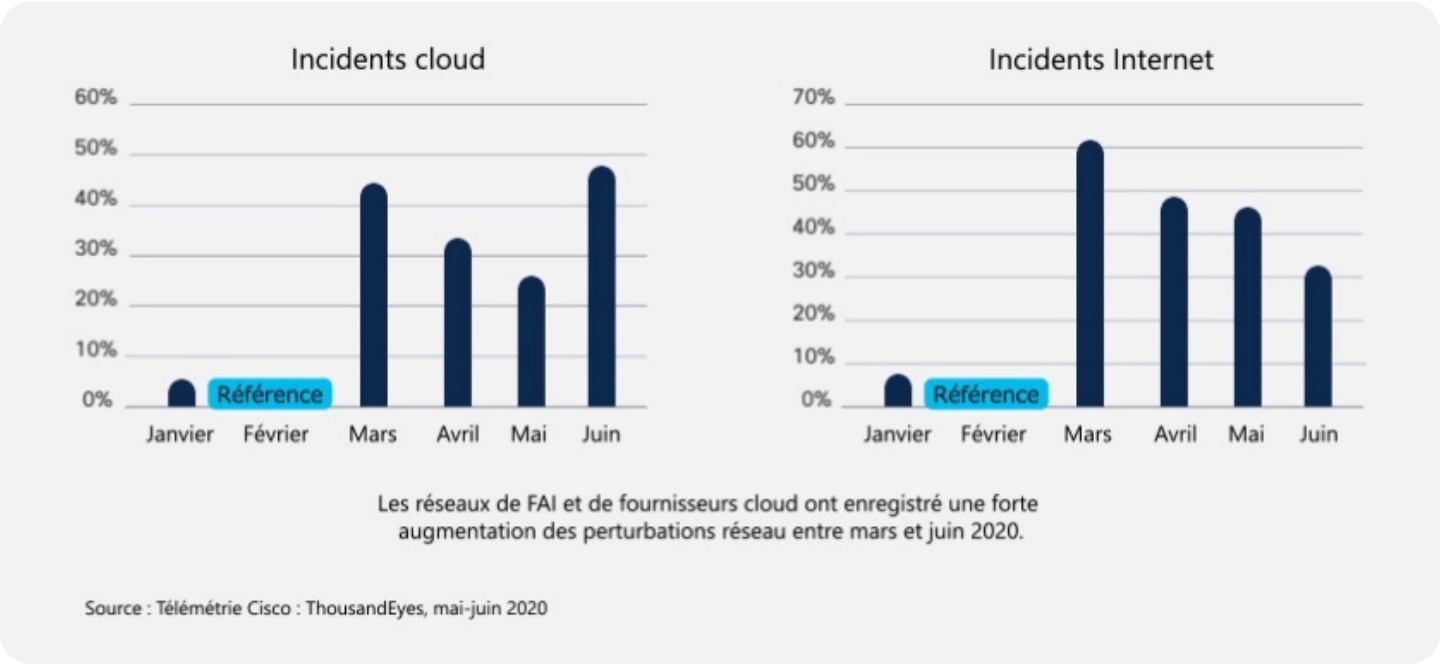
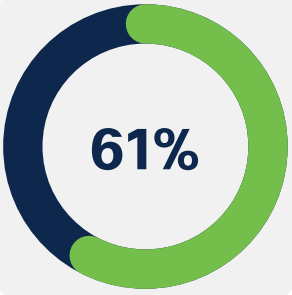


Figure 6 : L'augmentation des interruptions de service sur Internet et dans le cloud pendant la pandémie

"Cisco ThousandEyes a identifié une augmentation de 61 % du nombre d'incidents sur les réseaux de FAI et de 44 % sur les réseaux de fournisseurs cloud entre février et mars 2020. "



Rapport 2020 de Cisco ThousandEyes sur les performances Internet et l'impact de la COVID-19

Considérations relatives au réseau : afin de réussir à gérer l'explosion du nombre d'incidents, les équipes en charge du réseau doivent tirer parti d'analyses optimisées par l'IA pour :

- **Améliorer la précision des détections :** améliorer la précision de la détection automatisée des anomalies et des problèmes dans les différents domaines du réseau.
- **Accélérer la remédiation :** mettre les événements en corrélation pour détecter et décrire précisément la cause la plus probable des problèmes et des anomalies.
- **Automatiser la gestion des politiques :** identifier les équipements, les applications et les tendances et offrir des mises à jour recommandées.
- **Réduire les détériorations de service :** identifier les tendances et les modèles et fournir des informations contextuelles pour accélérer le déclenchement d'actions proactives de correction et de prévention.
- **Partager des informations :** fournir des informations et des analyses permettant aux administrateurs réseau de comparer les performances de leur réseau à des tests régionaux, sectoriels et mondiaux.

Découvrez comment tirer parti des informations générées par l'IA pour mieux gérer vos réseaux :

Network Insights pour le data center

Conclusion

Conclusion : améliorer la résilience de l'entreprise avec une plateforme réseau avancée

Tout au long de notre vie professionnelle nous seront confrontés à des événements graves qui mettront à mal nos entreprises et nos réseaux. Il est donc temps de repenser l'impact de votre **stratégie réseau** sur votre **stratégie de résilience** de l'entreprise et de privilégier de nouvelles capacités réseau qui vous permettront d'anticiper la prochaine catastrophe.

L'automation et les informations générées par l'IA du réseau intuitif fournissent une plateforme puissante pour vous aider à vous adapter à toutes les situations. Elles offrent l'agilité, la sécurité, les données et le débit requis pour assurer la résilience de l'ensemble de l'entreprise :

- **Les collaborateurs :** leur offrir un accès sécurisé et performant à leurs applications depuis leur domicile, au bureau et partout ailleurs
- **L'espace de travail :** assurer la sécurité des collaborateurs qui retournent au bureau grâce à une surveillance, des alertes et des informations optimisées par le Wi-Fi
- **Les workloads :** faciliter les modèles de résilience multicloud et protéger les données et les applications où que se trouvent les workloads, dans les clouds publics et les data centers sur site
- **Les opérations :** automatiser les politiques réseau de bout en bout et la segmentation, simplifier les tâches administratives, améliorer la visibilité, réduire les alertes et accélérer la remédiation

Il s'agit, après la crise, de disposer d'un réseau capable de s'adapter, quel que soit l'avenir. Au moment de définir votre stratégie de résilience de l'entreprise, réfléchissez au rôle central que doit y tenir votre réseau.

Pour plus d'informations sur la résilience de l'entreprise

Autres sujets susceptibles de vous intéresser

Résilience de l'entreprise | Webinars

Cisco Digital Network Architecture (Cisco DNA)

C96-744697-00 01/21