**Réponse de suivi au Comité permanent de la Chambre des communes Comité permanent des opérations gouvernementales et des prévisions budgétaires (OGGO)**
**Pratiques d'approvisionnement au sein de Services partagés Canada**
**Le 28 avril 2021**

1. **Renseignements supplémentaires sur les documents confidentiels du Cabinet et la sécurité liées aux centres de données? – (Julie Vignola (BQ) et Matthew Green (NPD))**

**Réponse :**

L'objet du privilège relatif aux « documents confidentiels du Cabinet » est de protéger la divulgation des discussions et des délibérations des ministres du Cabinet fédéral sur des questions qui font l'objet, ou qui ont fait l'objet, de discussions lors des réunions du Cabinet ou entre les ministres du Cabinet. Le privilège relatif aux « documents confidentiels du Cabinet » existe pour assurer la confidentialité de ces délibérations afin que les ministres puissent tenir des discussions ouvertes et franches sans devoir se préoccuper de la perception du public concernant leurs délibérations, qui sont essentielles à un bon gouvernement.

À la suite de la comparution du 28 avril 2021, Services partagés Canada (SPC) a demandé des conseils supplémentaires sur le caviardage fait au rapport Gartner. Le conseil a mené à la reconnaissance qu'une erreur avait été commise par les fonctionnaires du Ministère au cours de l'examen original du rapport. Plus précisément, il en a résulté une mauvaise interprétation de la définition d'un document confidentiel du Cabinet, qui s'est produite en raison du caractère unique de la circonstance, à savoir qu'un tiers, en l'occurrence Gartner plutôt que le gouvernement, spéculait sur un éventuel processus du Cabinet. En bref, l'avis supplémentaire reçu par le ministère a confirmé que l'information figurant à la page 78 du rapport n'est pas un document confidentiel du Cabinet et n'aurait pas dû être caviardé par les fonctionnaires pour des raisons de confidentialité du Cabinet. Il convient de noter que le caviardage initial de la page 78 était le seul caviardage fondé sur un document confidentiel du Cabinet (les autres rédactions étaient fondées sur la sécurité et les renseignements personnels). Un rapport révisé qui n'expurge pas cette section de la page 78 est joint à la présente réponse.

De plus, sur la question de la sécurité liée aux centres de données, les conseils supplémentaires demandés ont confirmé de nouveau le fait que pour des raisons de sécurité, la combinaison de l'information est ce qui crée le risque pour la sécurité – par exemple, la nature du travail effectué, la mise à niveau de l'équipement ou son remplacement, les détails de configuration, et les plans d'avenir sont tous des exemples d'éléments d'information, qui, lorsque mis ensemble, créent un risque pour la sécurité. Le caviardage du nom du centre de données dans le rapport Gartner atténue ce risque et permet au ministère de fournir la plus grande diffusion possible d'informations liées à l'engagement du Comité d'examiner les pratiques d'approvisionnement de SPC.

**2. Renseignements supplémentaires pour expliquer pourquoi les coordonnées de Gartner ont été retirées à la fin du document? – (Kelly McCauley (PCC))**

**Réponse :**

En ce qui a trait au caviardage des coordonnées des employés de Gartner, le fait de révéler ces renseignements constituerait une violation aux termes de la *Loi sur la protection des renseignements personnels*. Le gouvernement est tenu de protéger les renseignements personnels, y compris ceux des tiers, contre leur divulgation au public, notamment les noms et les coordonnées des employés de Gartner qui ont collaboré au rapport. La communication de ces renseignements porterait aussi atteinte au lien de confiance qui existe entre le gouvernement et les tiers, comme Gartner, représentant une explication valide de ces caviardages. Gartner a en outre confirmé que ces renseignements ne doivent pas être divulgués étant donné qu'ils ne sont pas communiqués publiquement ni publiés sur le site Web de Gartner.

**3. Renseignements supplémentaires sur l'accès à la documentation au sein de SPC? – (Caroline Desbiens (BQ))**

**Réponse :**

Les renseignements auxquels un fonctionnaire aura accès sont déterminés par son niveau d'autorisation de sécurité et par son rôle. L'accès à de tels renseignements doit être nécessaire afin d'exercer les fonctions officielles de son rôle et d'atteindre les objectifs établis.

Les fonctionnaires qui ont ou ont eu accès à la version non caviardée du rapport de Gartner détiennent l'autorisation de sécurité appropriée et y avaient accès en cas de nécessité absolue afin d'accomplir leur travail.

**4. Renseignements supplémentaires sur l'accès de Gartner / attestation de sécurité? – (Matthew Green (PCC) et Caroline Desbiens (BQ))**

**Réponse :**

Le mode d'approvisionnement utilisé pour conclure un contrat avec Gartner est un vaste mode de services professionnels mis en place par Services publics et Approvisionnement Canada (SPAC). Étant donné que ce mode est utilisé dans l'ensemble du gouvernement et pour un éventail de tâches, l'exigence de sécurité prévue dans le mode d'approvisionnement se situe à un niveau de fiabilité. Certaines entreprises dans leur ensemble détiennent différents niveaux d'autorisation de sécurité. Par exemple, Gartner, en tant qu'entreprise, a une autorisation de sécurité lui permettant d'accomplir des travaux au niveau Secret.

Les exigences de sécurité ci-après ont été appliquées et font partie intégrante de l'offre à commandes, pour les services d'analyse comparative.

a) L'entrepreneur ou l'offrant doit détenir en permanence, pendant l'exécution du contrat ou de l'offre à commandes, une attestation de vérification d'organisation désignée (VOD) en vigueur, délivrée par le Programme de sécurité des contrats (PSC) de SPAC.
b) Les membres du personnel de l'entrepreneur ou de l'offrant devant avoir accès à des renseignements ou à des biens ou à des lieux de travail délicats protégés doivent tous détenir une cote de fiabilité délivrée ou approuvée par le PSC de SPAC.
c) L'entrepreneur ou l'offrant ne doit pas emporter de renseignements ou de biens protégés hors des établissements visés et l'entrepreneur ou l'offrant doit s'assurer que son personnel est au courant de cette restriction et qu'il la respecte.
d) Aucun contrat de sous-traitance comportant des exigences relatives à la sécurité ne doit être attribué sans l'autorisation écrite préalable du PSC de SPAC.

L'entrepreneur ou l'offrant doit respecter les dispositions : i) de la Liste de vérification des exigences relatives à la sécurité et du guide de sécurité (s'il y a lieu, en pièce jointe à l'annexe C); et ii) du Manuel de la sécurité industrielle (dernière édition).

**5. Préciser les raisons pour lesquelles une demande de renseignements sur le site achats et ventes fourni les adresses des centres de données, mais que ces renseignements ont été supprimés dans le rapport? - (Rachel Harder (PCC))**

**Réponse :**

SPC remercie le Comité de nous avoir signalé cette situation. Il semble qu'au moment de la publication de la demande de renseignements, les détails sur l'emplacement ont été fournis par inadvertance sur le site Achats et ventes. Une demande à Services publics et Approvisionnement Canada a été faite de supprimer cette information et cette divulgation accidentelle a depuis été corrigée.

La pratique habituelle consiste à ne pas divulguer les renseignements de cette nature pour des raisons de sécurité. Tandis que la divulgation de la ville d'un centre de données en soi n'est pas préoccupante, la combinaison de l'emplacement et des détails sur l'endroit où sont conservées les données à cet emplacement ou l'infrastructure ou les systèmes de TI particuliers peuvent fournir suffisamment de renseignements pour constituer un risque pour la sécurité. Ces caviardages sont requis pour protéger la sécurité du centre de données, et la sécurité des données et des renseignements qu'ils contiennent, ainsi que toute amélioration ou rénovation à venir dans ces centres.

Depuis que ce problème identifié, Services partagés Canada a déterminé l'existence d'incohérences dans l'application de cette pratique dans l'ensemble du Ministère. SPC a lancé un examen interne de nos pratiques ministérielles afin d'assurer qu'une telle divulgation ne survienne pas à l'avenir.

# Matrice de référence pour les décisions relatives à la sélection de fournisseurs de réseau
# Rapport final

Préparé pour : Services partagés Canada (SPC)
4 février 2021 330 068 737



Gartner®

# SPC a demandé l'aide de Gartner pour évaluer sa stratégie en matière de réseau, examiner les cas d'approvisionnement actuels et passés où les services de fournisseurs de réseaux ont été retenus, et élaborer un cadre décisionnel reproductible pour l'acquisition ultérieure de services de réseau fondée sur les pratiques exemplaires.

## Notre compréhension de la situation actuelle

- SPC procède actuellement à la sélection d'un ou plusieurs fournisseurs pour soutenir l'installation de réseaux de centres de données (RCD) dans ses centres de données.
- Dans le cadre de la sélection des fournisseurs, SPC doit déterminer les principaux critères de décision liés à l'état du réseau des centres de données ainsi qu'aux risques et à la valeur qui y sont associés.
- SPC a besoin qu'un examen des exigences relatives au réseau soit effectué afin d'établir les conditions dans lesquelles le fait de renouveler le contrat d'un fournisseur existant est la seule option viable, et les conditions dans lesquelles un processus d'appel d'offres ouvert est possible.

## Approche de Gartner

- SPC a demandé l'aide d'un partenaire indépendant et impartial pour la création d'une matrice de référence pour les décisions relatives à la sélection de fournisseurs de réseau et de services de sécurité pour les centres de données. Pour ce faire, Gartner devra suivre les étapes suivantes :
  - Évaluer/comparer 3 ou 4 exemples précis d'approvisionnement en matière de réseaux et de services de sécurité.
  - Participer à des ateliers avec des intervenants (y compris à l'approvisionnement, aux activités, aux opérations et à l'exécution de projets) afin d'établir les résultats optimaux sur le plan opérationnel, technique et des achats, les contraintes, etc.
  - Faire fond sur les données de référence de Gartner, les pratiques exemplaires et les observations des analystes.
- Les livrables de ce mandat comprendront ce qui suit :
  - Un examen comparatif de la **stratégie en matière de réseau et d'approvisionnement** actuelle de SPC.
  - Une analyse des **cas d'approvisionnement passés et actuels**
  - Un **guide de décision** pour les futurs approvisionnements liés aux réseaux fondé sur les risques et les impératifs opérationnels, techniques, de sécurité et d'approvisionnement mis en lumière, la stratégie en matière de réseau et de sécurité de SPC, des cas d'approvisionnement étudiés, les données de référence de Gartner ainsi que les pratiques exemplaires du secteur.
  - Des **recommandations** sur les approches susceptibles d'aider à équilibrer les risques opérationnels, techniques, de sécurité et d'approvisionnement afin d'optimiser le résultat global.
  - Une séance d'information à l'intention des cadres supérieurs.

01 **Sommaire de gestion**

02 **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 **Analyse de cas d'approvisionnement**

05 **Annexe**




Gartner

# Sommaire de gestion – Examen de la stratégie en matière de réseau

## La demande

Examiner l'ébauche de la documentation relative à la stratégie en matière de réseau et de sécurité de SPC pour s'assurer qu'elle correspond aux pratiques exemplaires et décrit adéquatement l'état souhaité afin qu'elle puisse être communiquée à l'industrie.

## Approche de Gartner

- Comparer la stratégie en matière de réseau de SPC aux pratiques exemplaires publiées par Gartner.
- Effectuer un examen et une analyse approfondis du document afin de déterminer s'il permet de communiquer efficace la stratégie en matière de réseau.
- Formuler des recommandations visant à améliorer le document.

## Principales leçons à tirer

- Gartner a déterminé que les **objectifs** exposés dans le document sur la stratégie en matière de réseau **correspondent bien** aux objectifs et buts d'autres gouvernements, mais les **liens** avec le contexte actuel, la stratégie opérationnelle et d'autres stratégies de TI **pourraient être renforcés**.
- SPC a déterminé **les technologies à venir qui cadrent avec les recherches actuelles de Gartner**, mais ce document **ne fournit pas suffisamment d'orientation** pour lui permettre d'élaborer un plan pour le déploiement de ces solutions par rapport aux autres stratégies du secteur de service.
- La structure du document stratégique de SPC, qui repose sur trois piliers fondamentaux, crée des redondances, des chevauchements et des divergences au sein du texte qui pourraient être évités si l'on suivait un **cadre stratégique normalisé** pour l'industrie.

# Sommaire de gestion – Outil d'aide à la décision pour la sélection de fournisseurs de réseaux

## La demande

Gartner a été chargé de mettre au point une matrice de référence pour les décisions relatives à l'approvisionnement en matériel de réseau.

## Approche de Gartner

- Organiser des ateliers à l'intention des intervenants afin de comprendre les buts et contraintes des parties prenantes dans la sélection des fournisseurs de réseaux.
- Utiliser les recherches publiées par Gartner pour élaborer un outil d'aide à la décision qui s'harmonise avec les pratiques exemplaires de l'industrie.
- Fournir un aperçu général des fournisseurs selon les travaux de Gartner Research.

## Principales leçons à tirer

- Gartner a créé un **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux** visant à faciliter les démarches relatives à la sélection de fournisseurs de réseaux.
- Pour les trois types de réseau (RL, RÉ, RCD), Gartner a recommandé l'établissement de **normes technologiques au moyen de processus d'approvisionnement ouverts et concurrentiels** et a fourni des paramètres pour ces normes qui encouragent le recours au processus concurrentiel tout en limitant la charge de travail.
- Gartner a proposé l'établissement de deux normes technologiques pour le RCD et d'une seule norme pour le RÉ de l'ensemble de ses CDE, ainsi qu'une norme pour le réseau local (RL) de chaque installation.
- Pour les environnements existants comptant un fournisseur établi (norme de facto), mais aucune norme technologique établie, Gartner recommande d'examiner les **exceptions d'approvisionnement propres au fabricant d'équipement d'origine (FÉO)** dans les cas où la mise à niveau est urgente et essentielle.

# Sommaire de gestion – Analyse des cas d'approvisionnement

## La demande

Trois cas d'approvisionnement ont été fournis à Gartner afin de mieux comprendre les décisions actuelles de SPC quant à la sélection de fournisseurs de RL, de RÉ et de RCD.

1) CDE [redacted] Mise à niveau du RÉ et principale composante du RCD

2) Centre de données CCM/CDSL [redacted] – Migration des charges de travail au CDE

3) Édifice Lester B. Pearson – RL de l'immeuble, phase 1

## Approche de Gartner

- Définir les buts et contraintes des intervenants quant à la sélection des fournisseurs de réseaux.
- Effectuer un examen comparatif et une analyse approfondie des cas d'approvisionnement.
- Utiliser et valider l'outil d'aide à la décision pour la sélection de fournisseurs de réseaux que Gartner a créé pour SPC en se fondant sur les pratiques exemplaires.
- Évaluer l'incidence commerciale de l'utilisation de l'outil d'aide à la décision pour les projets en cours.
- Documenter les constats

## Principales leçons à tirer

- Gartner a mis au point un outil d'aide à la sélection de fournisseurs de réseaux pour les cas d'approvisionnement actuels et futurs en fonction des buts et contraintes définis par les intervenants.
- Gartner a évalué l'emploi de l'outil d'aide à la décision par rapport aux trois cas d'approvisionnement; tandis que les **cas d'approvisionnement 1 et 3 se prêtent entièrement à** l'utilisation de l'outil d'aide à la décision pour la sélection de fournisseurs de réseaux, le **cas d'approvisionnement 2** (CCM) ne s'y prête que **partiellement**, puisque la décision d'approvisionnement pour les composantes du RCD ne correspond pas à l'orientation prescrite.
- En consultation avec les intervenants, Gartner a documenté les **répercussions opérationnelles** qui découleraient de l'utilisation de l'outil d'aide à la décision pour la sélection de fournisseurs de réseaux pour les composants du RCD dans le cas d'approvisionnement 2, **fournissant ainsi des renseignements éclairés sur la prise de décision** aux membres de la direction de SPC afin de déterminer le processus adéquat en matière d'approvisionnement.

# Recommandations à court terme

1. Mettre à jour et **améliorer la stratégie en matière de réseau** afin d'y inclure les éléments manquants de première importance de manière à ce qu'elle puisse servir de référence pour la planification à court et à moyen termes ainsi que d'outil de communication.
2. Officialiser l'**adoption d'une approche pour la prise de décision en matière d'approvisionnement** pour l'acquisition d'équipement de réseau, y compris les domaines technologiques et les paramètres relatifs aux normes technologiques. Envisager d'étendre la pratique à d'autres secteurs technologiques.
3. Créer **des mécanismes d'examen et des processus d'approbation** permettant de déroger de l'approche établie pour la prise de décisions relatives à la sélection de fournisseurs. Ce processus doit comprendre **la consultation des parties concernées** ainsi que la consignation des **contraintes et des répercussions opérationnelles** ayant mené à la décision.

**La consignation, la normalisation et la communication de la stratégie en matière de réseau de SPC favoriseront la responsabilisation et la transparence.**

01 **Sommaire de gestion**

02 **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 **Analyse de cas d'approvisionnement**

05 **Annexe**

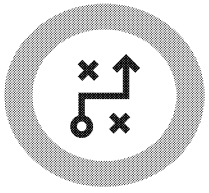



Gartner

# Gartner Research a déterminé les principales composantes d'une stratégie en matière de réseau réussie.

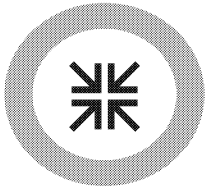
La planification stratégique du réseau est essentielle pour nous permettre de relever les défis associés aux initiatives comme l'infonuagique, la mobilité, l'approvisionnement et Internet des objets (IdO) tout en maintenant la sécurité et en réduisant les coûts.

**Les stratégies efficaces en matière de réseau comportent plusieurs éléments fondamentaux essentiels.**



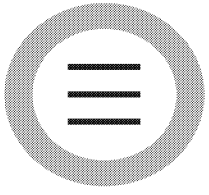
### Stratégie opérationnelle

Utiliser la stratégie opérationnelle, et non la technologie, pour la mise en œuvre de la stratégie en matière de réseau.



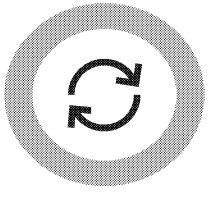
### Rouages internes de la stratégie

Élaborer une stratégie en matière de réseau qui tient compte de l'état actuel, de l'état souhaité, de l'analyse des lacunes et du plan d'action.



### Établissement des priorités/risques

Établir les priorités des projets de réseautage en fonction des investissements requis et de leur importance à l'égard de la réussite opérationnelle et des risques.



### Mettre à jour la stratégie chaque année

Mettre à jour la stratégie en matière de réseau chaque année ou à mesure que les priorités opérationnelles changent.




Gartner

# L’examen de Gartner tient compte des travaux actuels de Gartner Research et des discussions tenues avec les membres de l’équipe de SPC au cours des dernières années.

Gartner a suivi les étapes suivantes et fourni des renseignements généraux et des recommandations dans les diapositives suivantes.

Étapes suivies par Gartner

- Examen de la stratégie en matière de réseau et de sécurité
- Examen des mesures/initiatives actuelles/futures
- Améliorations possibles du libellé de la stratégie
- Examen du document de discussion sur la modernisation du réseau

### Examen de la « stratégie en matière de réseau et de sécurité de SPC »

- Rédigée initialement en mai 2020
- Version : 1,8, mise à jour en novembre 2020, avec les commentaires de SPC, du CST, du CCC et du SCT

### Améliorations possibles du libellé

- Gartner a indiqué certaines améliorations qui pourraient être apportées au libellé du document de la stratégie afin de permettre à SPC de communiquer plus effectivement ses besoins.

### Examen des initiatives actuelles et des activités à venir de SPC

- Gartner a souligné la nécessité d’intégrer les initiatives actuelles et les activités à venir en une seule structure cohérente.

### Examiner le document de discussion sur la modernisation du réseau de SPC

- Ce document de discussion s’appuyer davantage sur la stratégie en matière de réseau et de sécurité de SPC.

01 **Sommaire de gestion**

02 **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 **Analyse de cas d'approvisionnement**

05 **Annexe**




Gartner

# Gartner a comparé la stratégie en matière de réseau et de sécurité de SPC aux pratiques exemplaires de Gartner Research.

- La stratégie en matière de réseau et de sécurité de SPC (stratégie de SPC) vise à améliorer l'expérience de l'utilisateur final tout en protégeant l'information du gouvernement.
  - Gartner constate que les objectifs de SPC s'harmonisent avec ceux d'autres gouvernements et de grandes entreprises clientes.

- La stratégie de SPC comprend un examen des avantages des solutions de réseau et de sécurité émergentes.
  - Les solutions émergentes abordées dans la **stratégie de SPC s'harmonisent avec les technologies** dont traite Gartner Research.
  - La stratégie de SPC ne fournit pas un plan de déploiement complet pour ces solutions.

- SPC a conçu une nouvelle structure de documents de stratégie composée de « colonnes » et de « lignes » pour communiquer avec ses intervenants.
  - Gartner croit que cette nouvelle structure de documents de stratégie crée des redondances, des chevauchements et des lacunes dans le texte. Par exemple, la confiance zéro est abordée à la fois dans les colonnes et les lignes, et certaines lacunes sont observées en ce qui concerne la gestion des services. (La présente section comprend des exemples précis.)
  - Gartner recommande que la stratégie de SPC suive l'approche adoptée par l'industrie pour la consignation de stratégies. * L'état actuel et l'état souhaité devraient être présentés de façon globale et non compartimentée en « piliers » (structure recommandée par Gartner à la page 36).
  - Le sommaire de la stratégie de SPC devrait fournir un aperçu de toutes les composantes de la stratégie et comprendre une définition de l'état actuel, de l'état souhaité et des activités prévues.

**Dans les diapositives suivantes, Gartner commente la façon dont les stratégies en matière de réseau de SPC s'harmonisent avec les travaux de Gartner Research.**




*Voir section des notes afin d'obtenir de plus amples détails.

# Gartner compare le document sur la stratégie en matière de réseau de SPC à celui de Gartner Research.

| Pilier 1<br>Connectivité | Stratégie en matière de réseau et de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **Réseau intra-immeubles** | ▪ Le GC a adopté une stratégie « sans-fil d'abord » pour les appareils des utilisateurs finaux et l'IdO.<br>▪ À moyen terme, les appareils continueront d'utiliser la connectivité Wi-Fi et cellulaire (3G/4G) jusqu'à ce que la technologie de réseau 5G s'améliore.<br>▪ Capacité à recenser de façon fiable les appareils et les utilisateurs qui utilisent le ressources du réseau du GC. | ▪ Conforme aux résultats des travaux de Gartner Research – Dans *Top 10 Trends for the Communications Service Provider Industry in 2021, published 9 March 2021*.<br>▪ Gartner définit la technologie de réseau 5G comme une plateforme destinée aux solutions d'entreprise.<br>▪ Les activités de SPC liées aux services sans fil ne sont pas définies. |
| **Réseau inter-immeubles** | ▪ La dépendance à l'égard de l'infrastructure d'immeuble traditionnelle diminuera.<br>▪ Les principaux services inter-immeubles demeureront probablement les mêmes dans la région de la capitale nationale. | ▪ Les initiatives liées aux réseaux inter-immeubles ne sont pas traitées dans cette section. |
| **Réseaux de centres de données (réseau les réseaux définis par des logiciels [réseau logiciel])** | ▪ Les réseaux de centres de données feront la transition à la technologie de réseau les réseaux définis par des logiciels afin d'accélérer l'approvisionnement en services de réseau et la mise en œuvre des changements.<br>▪ Le réseau étendu défini par logiciel (les réseaux étendus réalisés par logiciel) servira de nouvelle couche transport pour l'accès à Internet dans les centres de données de petite à moyenne taille.<br>▪ AIOps automatisera les changements en vue d'élimination de menaces et de gestion du rendement. | ▪ Gartner considère le réseau les réseaux définis par des logiciels comme un terme générique commercial qui a perdu tout sens spécifique.<br>▪ Gartner recommande que SPC définisse ses attentes particulières quant à la valeur des réseaux définis par des logiciels et harmonise la stratégie avec ces exigences.<br>▪ Gartner recommande l'adoption d'une solution misant sur AIOps dans l'annexe – Gartner Research. |
| **Connectivité du réseau externe** | ▪ Les données Protégé B seront accessibles au moyen de la solution de connectivité d'activation et de défense du nuage sécurisé (ADNS).<br>▪ Un plus grand nombre de clients tirent parti des solutions les réseaux étendus réalisés par logiciel afin de permettre l'accès à Internet et aux services SaaS à partir du nuage.<br>▪ On mettra en œuvre l'accès direct à des applications SaaS comme Microsoft Office 365, sans RPV, afin d'optimiser la capacité et de réduire la latence, ce qui, en bout de ligne, enrichira l'expérience utilisateur. | ▪ Gartner fait remarquer que SPC a défini une initiative particulière (ADNS) pour appuyer l'accès sécurisé aux services infonuagiques.<br>▪ SPC doit élaborer une stratégie d'accès Internet intégrée pour accéder aux services infonuagiques publics, y compris l'utilisation des solutions les réseaux étendus réalisés par logiciel et SASE. |

# Gartner compare le document stratégie en matière de réseau de SPC à celui de Gartner Research.

| Pilier 2 Contrôle d'identité et d'accès | Stratégie en matière de réseau et de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **Périmètre virtuel** | ▪ Passer d'une approche traditionnelle de la sécurité du périmètre à un « périmètre virtuel »; s'appuyer sur le concept de la vérification systématique (confiance zéro) (*Zero Trust*) et de la microsegmentation.<br>▪ La sécurité du périmètre traditionnelle pourra encore servir de première ligne de défense, mais le dispositif et l'utilisateur feront continuellement l'objet de vérification, d'authentification et d'autorisation. | ▪ S'harmonise avec Gartner Research sur le déploiement du modèle à vérification systématique (MVS) (*Zero Trust Architecture – ZTA*).<br>▪ SPC doit établir certaines attentes relativement au déploiement du MVS, p. ex., « d'ici X ans… ».<br>▪ Résumé de Gartner Research sur la vérification systématique (confiance zéro) en annexe |
| **Active Directory** | ▪ Rétablir le contrôle d'un environnement Active Directory compromis en maintenant un environnement de bastion distinct reconnu pour ne pas être affecté par les attaques malveillantes. | ▪ S'harmonise avec les pratiques exemplaires. |
| **Comptes privilégiés** | ▪ Isoler l'utilisation des comptes privilégiés pour amoindrir le risque de vol de ces justificatifs. | ▪ S'harmonise avec les pratiques exemplaires. |
| **Gestion des secrets** | ▪ Il faut assurer un service de gestion des secrets étroitement lié aux mécanismes de contrôle d'accès afin de permettre l'automatisation et l'orchestration. | ▪ Seule référence à la gestion des secrets dans la Stratégie |
| **Outils d'évaluation de risque intelligent** | ▪ Les outils d'évaluation de risque « intelligents » entraîneront des exigences supplémentaires en matière de capacité pour la collecte et le traitement des métadonnées sur les utilisateurs finaux et les dispositifs. | ▪ Gartner définit le marché de la gestion de l'accès comme des technologies qui utilisent des moteurs de contrôle d'accès (fournisseurs d'identité, serveurs d'autorisation, serveurs de politiques, etc.) pour fournir des capacités de base. |
| **Gestion des données** | ▪ Établir une gouvernance appropriée des données, une gestion des données de référence, et des mesures de protection contre les fuites de données. | ▪ La gouvernance des données est devenue plus difficile à mesure que les données sont reproduites dans de multiples environnements informatiques : en périphérie de réseau, sur place et infonuagiques. De plus, de nouveaux règlements stimulent la demande pour une gouvernance efficace des données. |

# Gartner compare le document stratégie en matière de réseau de SPC à celui de Gartner Research.

| Pilier 3<br>Contrôle | Stratégie en matière de réseau et de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **Outils de surveillance** | ▪ SPC devra passer de l'utilisation d'outils et de processus de surveillance autonomes à un ensemble intégré de technologies appuyé par un dépôt centralisé de données appelé « lac de données SPC » et offrant une meilleure visibilité. | ▪ SPC doit définir les lacunes relatives aux outils actuels.<br>▪ La stratégie de SPC ne précise pas les types d'outil de surveillance qu'elle prévoit déployer. |
| **Intelligence artificielle (IA)** | ▪ SPC devra mettre en œuvre l'IA, l'automatisation et l'orchestration pour améliorer l'efficacité avec laquelle il sécurise l'infrastructure de TI. Une initiative est en cours à SPC pour aborder la question de l'IA pour les Opérations (« AIOps »). | ▪ L'IA promet de révolutionner le fonctionnement des TI, mais la plupart des équipes de TI ont du mal à voir au-delà du tapage publicitaire et à trouver des cas d'utilisation pragmatiques et les bons outils. Les professionnels techniques des I et O doivent utiliser ce chemin de solution pour préciser l'adoption d'AIOps en superposant les outils, les plateformes et les caractéristiques d'AIOps. |
| **Regroupement des centres de données** | ▪ Le regroupement des centres de données s'avérera primordial pour faciliter le regroupement des outils de surveillance et du lac de données de SPC. Cela comprendra l'établissement d'une solution de surveillance centralisée au sein des Centres de données d'entreprise (CDE), qui formera le fondement d'une capacité de surveillance centralisée pour le GC. | ▪ SPC doit expliquer la dépendance entre les outils de regroupement et de surveillance des centres de données et les lacs de données. |
| **GIES de nouvelle génération** | ▪ L'amélioration de la capacité de GIES sera crucial pour mieux comprendre la situation dans l'ensemble des environnements du GC et améliorer la rapidité et la coordination des interventions en cas d'incident. Cela doit comprendre une solution GIES de prochaine génération intégrée. | ▪ SPC doit fournir sa définition de « solution de GIES de prochaine génération », et préciser l'utilisation de lacs de données. |




Gartner

# Gartner compare le document stratégie en matière de réseau de SPC à celui de Gartner Research.

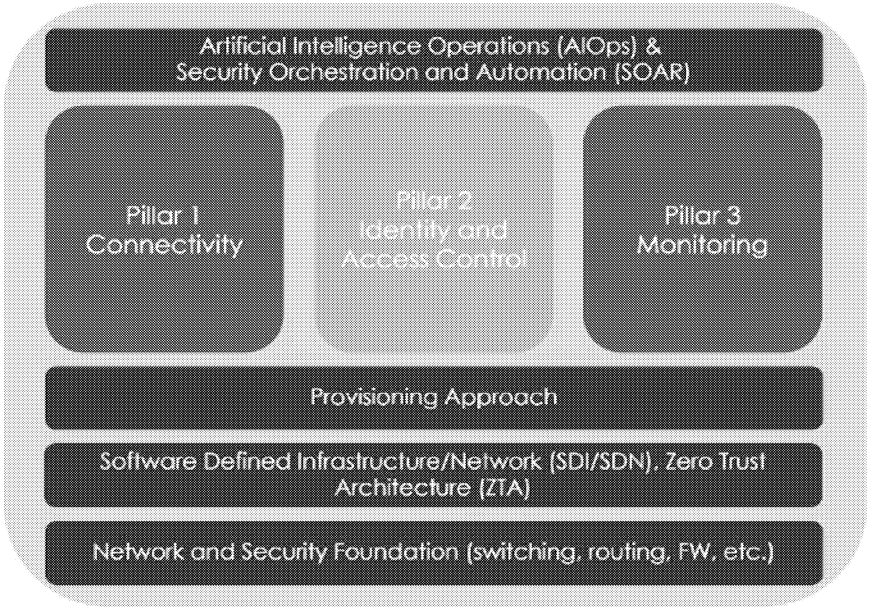
| Approvisionnement | Stratégie en matière de réseau et de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **Réseaux définis par des logiciels/Infrastructure logicielle** | ▪ Mettre en œuvre un réseau et une infrastructure définis par logiciel (les réseaux définis par des logiciels/l'infrastructure logicielle), intégrés au réseau et aux plateformes de sécurité sur place. | ▪ ***Alors que les solutions véritablement fondées sur le les réseaux définis par des logiciels ne sont pas encore largement adoptées par le marché****, le développement du les réseaux définis par des logiciels et la menace qui pèse sur les acteurs établis du marché ont eu un effet profond et positif sur l'évolution ultérieure du marché.*<br>▪ En 2021, nous voyons actuellement l'infrastructure logicielle passer à une technologie de silo propre au fournisseur (et non un lecteur de service hétérogène) et, par conséquent, désuète en qualité de normes interopérables multifournisseurs.<br>**Nota : Détaillé dans la diapositive suivante** |
| **Infrastructure hyperconvergente** | ▪ Utiliser les réseaux définis par des logiciels/l'infrastructure logicielle, intégré à l'infrastructure sur place, telle qu'une infrastructure hyperconvergente. | ▪ Il s'agit de la seule référence à une « infrastructure hyperconvergente » dans la stratégie.<br>▪ SPC doit ajouter du contexte et préciser les mesures à prendre. |
| **Approvisionnement en nuage** | ▪ L'infonuagique hors-lieu permettra l'approvisionnement rapide de services de réseau, de sécurité et de calcul. | ▪ SPC doit expliquer comment il compte tirer parti de l'« approvisionnement infonuagique ». |
| **Modèle opérationnel** | ▪ SPC devra apporter un changement fondamental à son modèle de fonctionnement à mesure qu'il effectuera la transition vers l'infonuagique et les nouvelles capacités de réseau et de sécurité. Pour ce faire, il faudra modifier : La structure organisationnelle de SPC, les compétences requises, les processus opérationnels, et les capacités de gestion des fournisseurs. | ▪ La stratégie de SPC ne décrit pas un nouveau modèle opérationnel.<br>▪ SPC n'a pris aucune initiative de modifier sa structure organisationnelle. |
| **Nouveaux rôles** | ▪ Architecte en infrastructures et réseaux définis par logiciel<br>▪ Architecte MVS<br>▪ Gestion des fournisseurs<br>▪ Accent supplémentaire sur la gestion des relations avec les partenaires dans tous les rôles | ▪ SPC doit définir les rôles en termes plus généraux, y compris l'architecture de réseau et celle de sécurité.<br>▪ La stratégie de SPC doit aborder la façon dont elle améliorera la collaboration avec ses partenaires et ses fournisseurs. |

# Gartner compare le document stratégie en matière de réseau de SPC à celui de Gartner Research.

| | Stratégie en matière de réseau et de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **Réseaux définis par des logiciels** | ▪ Mise en œuvre de technologies habilitantes, comme les réseaux et l'infrastructure définis par logiciel, intégrés au réseau et aux plateformes de sécurité sur place | ▪ Bien que les réseaux définis par des logiciels soient manifestement désuets sur le marché, de nombreuses organisations citent encore les réseaux définis par des logiciels comme une pierre angulaire de leur stratégie et leur architecture futures. Ce qui est crucial pour les entreprises, c'est de comprendre ce qu'elles essaient d'accomplir lorsqu'elles pensent aux « réseaux définis par des logiciels ». Nous recommandons ce qui suit :<br>▪ Ne vous laissez pas séduire et obnubiler par la publicité tapageuse et les affirmations du fournisseur selon lesquelles les produits commerciaux sont des réseaux définis par des logiciels, et ne participez à aucune discussion ou planification du déploiement de réseaux définis par des logiciels. les réseaux définis par des logiciels n'est pas la réponse à un quelconque défi de mise en réseau d'entreprise aujourd'hui.<br>▪ Concentrez-vous sur les résultats souhaités que vous essayez d'obtenir, comme l'automatisation accrue, la segmentation virtuelle, l'orchestration externe, le contrôle et la programmabilité du réseau, ou le découplage du matériel physique des systèmes d'exploitation du commutateur logiciel.<br>▪ Choisissez d'abord un cadre de travail opérationnel ou d'automatisation, puis choisissez les fournisseurs et les produits de réseautage. Le matériel et les logiciels découplés et les superpositions de réseaux indépendants offrent un moyen d'établir des modèles opérationnels à long terme qui sont indépendants du matériel sous-jacent s'il s'agit du résultat souhaité.<br>▪ Évaluez les approches tant de l'infrastructure matérielle que de la superposition de logiciels. Évaluez non seulement les promesses des fournisseurs, mais aussi les exigences opérationnelles à respecter pour obtenir un avantage. Tenez tout fournisseur considéré ou établi responsable pour l'obtention des résultats souhaités, et ne croyez en rien à la publicité excessive entourant les revendications liées aux réseaux définis par des logiciels. Évaluez les comptes de référence et accordez une attention particulière à la mise en œuvre et aux coûts et investissements opérationnels continus afin de vous assurer qu'il est possible d'atteindre de façon réaliste les avantages promis.<br>▪ Élaborez une collaboration interfonctionnelle et étudiez des méthodologies permettant de mieux intégrer les équipes de serveur, de virtualisation, de réseau, de sécurité et d'application. Ces équipes peuvent aider à cerner les principaux cas d'approvisionnement, à la fois à court terme, comme les environnements de réalisation libre-service et la microsegmentation, et à long terme, en intégrant plus largement la mise en réseau dans l'orchestration des centres de données.<br>▪ Allouez du temps et des ressources à l'évaluation des technologies et d'une courte liste de fournisseurs pertinents, tant titulaires que non titulaires, afin d'en arriver à la solution qui répond le mieux aux besoins de l'organisation interfonctionnelle. |

# Structure des documents de la stratégie de SPC

- La structure des documents de la stratégie de SPC comprend des **concepts qui se chevauchent** et un certain nombre de **lacunes** particulières. Si la structure définit les « piliers » plus largement, ils pourraient couvrir tous les aspects de la stratégie.
- **Pilier 1 – Connectivité**
  - Chevauchement concernant les principaux éléments du réseau (dans la rangée 3) et englobe des éléments des couches 1 à 3 de la pile ISE, y compris les câblés (cuivre, fibre de verre) et sans fil (4G, 5G, Wi-Fi 6, satellite) de commutation, de routage, et de protocoles connexes (IP, MPLS, etc.).
- **Pilier 2 – Contrôle des justifiants et de l'accès**
  - Une composante de la sécurité qui est reprise dans la vérification systématique (architecture de confiance zéro), dans la rangée 2.
  - Ce deuxième pilier devrait s'intituler « Sécurité » et couvrir tous les aspects de la sécurité des réseaux.
- **Pilier 3 – Surveillance**
  - Une composante de la gestion des services, tout comme l'approvisionnement (rangée 1), et AIOps (dans la rangée 0), la gestion de la configuration (BDGC)
  - Ce troisième pilier devrait s'intituler Gestion des services et traiter de tous les composants, tels que les définit la BITI.



01 **Sommaire de gestion**

02 **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

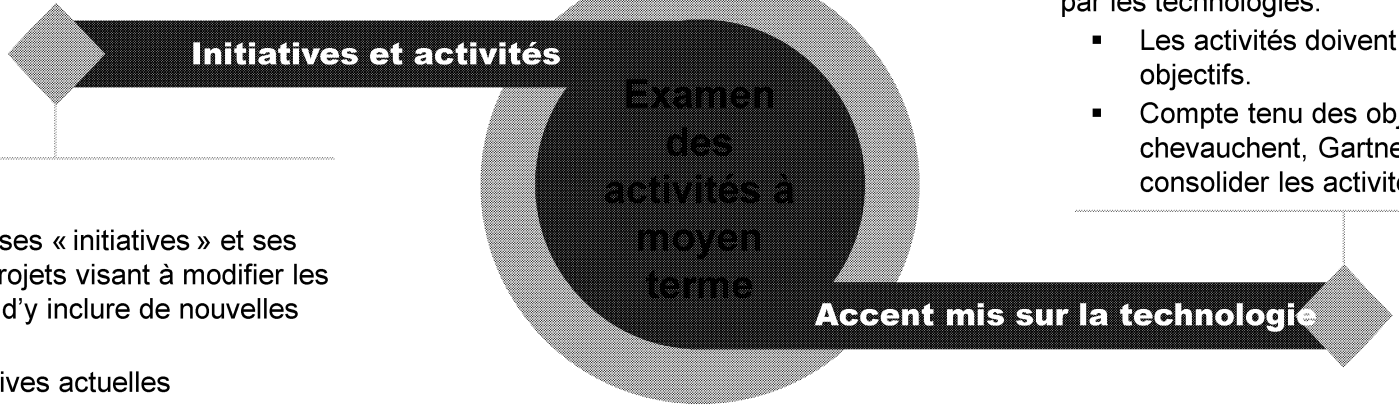
04 **Analyse de cas d'approvisionnement**

05 **Annexe**




Gartner

# Gartner a terminé un examen des activités à moyen terme de la documentation actuelle sur la stratégie en matière de réseau de SPC.




## Intégration

- SPC doit intégrer ses « initiatives » et ses « activités » aux projets visant à modifier les plans actuels afin d'y inclure de nouvelles solutions :
  - Initiatives actuelles
  - Activités à court terme
  - Activités à moyen terme

## Définitions

- Les activités de SPC sont généralement définies par les technologies.
  - Les activités doivent s'harmoniser avec les objectifs.
  - Compte tenu des objectifs qui se chevauchent, Gartner voit une occasion de consolider les activités à moyen terme.

**Dans les diapositives suivantes, Gartner explique comment les définitions des activités de SPC s'harmonisent avec celles de Gartner Research.**

# Stratégie en matière de réseau et de sécurité de SPC – Activités à moyen terme

| Activités | stratégie en matière de réseauet de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **1. Automatisation et orchestration** | • Augmentation continuelle de l'automatisation et des outils d'orchestration — Laissez de côté l'automatisation tout court et pensez aux outils qui fonctionnent en synergie. | ▪ Gartner reconnaît l'importance et la valeur des outils d'automatisation et d'orchestration.<br>▪ La stratégie de SPC doit fournir des détails sur la sélection des outils ou les plans de déploiement. |
| **2. Mettre à jour la BDGC** | ▪ Continuer de mettre à jour la BDGC en fonction de l'infrastructure de SPC, mais on doit envisager l'approvisionnement d'outils de découverte automatique . | ▪ La base de données de gestion des configurations définit l'inventaire des biens d'infrastructure et est cruciale pour une gestion efficace des services.<br>▪ SPC doit définir des buts d'achèvement. |
| **3. Déterminer les exigences relatives au lac des données de SPC** | ▪ Déterminer les besoins relatifs au lac des données de SPC pour la journalisation de tous les services d'infrastructure de SPC. SPC aura-t-il besoin de plus de renseignements que ce que fournira la GIES traditionnelle – Service central de journalisation (CLS)? | Gartner définit les lacs de données comme un outil important de GIES. Les organisations qui réussissent utilisent souvent la GIES avec leur lac de données de sécurité.<br>• GIES pour l'analyse en temps quasi réel; un lac de données de sécurité pour la gestion étendue des journaux<br>• GIES pour l'analyse à court terme; un lac de données de sécurité pour l'analyse historique à plus long terme<br>• GIES pour la détection en temps réel; un lac de données de sécurité pour mettre à l'essai et affiner les règles et les modèles de données<br>• GIES pour certains cas d'approvisionnement de sécurité; un lac de données de sécurité pour d'autres cas d'approvisionnement appelant à la collecte de données qui ne cadrent pas dans une GIES |
| **4. Amorcer la stratégie relative aux justificatifs** | ▪ Commencer la mise en œuvre de la stratégie relatives aux justificatifs, y compris leur conception, les plans et le déploiement. | ▪ Les justificatifs sont le fondement du modèle de vérification systématique (architecture de confiance zéro).<br>▪ Intégrer avec l'activité № 11 du modèle de vérification systématique (architecture de confiance zéro). |

# Stratégie en matière de réseau et de sécurité de SPC – Activités à moyen terme

| | stratégie en matière de réseauet de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **5. Faire évoluer les réseaux définis par des logiciels, l'infrastructure logicielle, le périmètre défini par logiciel** | ▪ Faire évoluer le réseau défini par logiciel du Centre de données à l'état final (CDE) avec une infrastructure de sécurité intégrée, un périmètre défini par logiciel et une microsegmentation. | ▪ La stratégie de SPC doit fournir des détails de base sur ses plans.<br>▪ Redéfinir et restructurer cette activité pour qu'elle s'harmonise avec les buts définis, en évitant les termes désuets sans définition claire. |
| **6. Évaluer le CDDL** | ▪ Preuve de service du centre de données défini par logiciel (CDDL) dans les centres de données à l'état final. | ▪ La stratégie de SPC doit comprendre un processus approximatif pour cette évaluation.<br>▪ Intégrer avec l'activité 5 ci-dessus. |
| **7. Mettre en œuvre Microsoft Office 365** | ▪ Mise en œuvre d'Internet commercial pour les systèmes M365 et SaaS dans les immeubles à bureaux, où et si jugée faisable pendant l'étude. | ▪ SPC doit redéfinir cette activité en « Stratégie d'accès Internet » pour appuyer les applications SaaS. |
| **8. Évaluer le SASE** | ▪ Évaluer la feuille de route du SASE (*Security Access Service Edge* – service d'accès sécurisé en périphérie de réseau) et son intégration avec d'autres services de sécurité et de réseau. | ▪ On décrit le SASE comme une « tendance », mais non une « stratégie », c'est-à-dire pourquoi il est important et comment il améliorerait les opérations de SPC.<br>▪ Intégrer à la stratégie d'accès Internet |
| **9. Mettre en œuvre les réseaux étendus réalisés par logiciel** | ▪ Concevoir et mettre en œuvre un RÉ défini par logiciel (les réseaux étendus réalisés par logiciel). | ▪ Définir le lien aux plans SASE dans une stratégie.<br>▪ Intégrer à la stratégie d'accès Internet |
| **10. Mettre en œuvre du RL défini par logiciel** | ▪ Concevoir et mettre en œuvre un RL réalisés par logiciel – conception d'une infrastructure WI-FI et d'un RL d'après les solutions déterminées dans le cadre du projet ENM. | ▪ Redéfinir l'activité lié au RL réalisés par logiciel pour l'harmoniser avec les objectifs clairs du projet ENM.<br>▪ Cela devrait-il s'intitulé « Initiative liée au réseau de l'immeuble » ou « Modernisation du réseau local »? |

# Stratégie en matière de réseau et de sécurité de SPC – Activités à moyen terme

| | stratégie en matière de réseauet de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **11. Évaluer les points de service (PDS) fondés sur le modèle de la vérification systématique (architecture de confiance zéro)** | ▪ Concevoir et mettre en œuvre une preuve de service de la vérification systématique (architecture de confiance zéro). | ▪ La vérification systématique (architecture de confiance zéro) revêtira une grande valeur pour SPC et le GC.<br>▪ Assurer la coordination avec la stratégie d'accès Internet. |
| **12. Établir une feuille de route pour la vérification systématique (architecture de confiance zéro).** | ▪ Déterminer une feuille de route et un plan détaillés pour la vérification systématique (architecture de confiance zéro) selon la preuve de service. | • Intégration avec « Évaluer les points de service (PDS) fondés sur la vérification systématique (architecture de confiance zéro) », ci-dessus. |

# On doit consolider les initiatives à moyen terme de SPC grâce aux initiatives à court terme

| Sections à moyen terme de la stratégie de SPC | Structure recommandée par Gartner |
|---|---|
| 1. Automatisation et orchestration | Automatisation et orchestration |
| 2. Mettre à jour la BDGC | Mettre à jour la BDGC |
| 3. Déterminer les exigences relatives au lac des données de SPC | Déterminer les exigences relatives au lac des données de SPC – Lien vers la GIES |
| 4. Amorcer le déploiement des justificatifs | Initiative du modèle à vérification systématique (confiance zéro) (reliée à l'accès à Internet) |
| 5. Faire évoluer les réseaux définis par des logiciels, l'infrastructure logicielle, le périmètre défini par logiciel | Les initiatives ont besoin d'une définition plus claire. – Doit-on les relier? |
| 6. Évaluer le CDDL | |
| 7. Mettre en œuvre Microsoft Office 365 | Accès à Internet et aux SaaS |
| 8. Évaluer le SASE | |
| 9. Mettre en œuvre les réseaux étendus réalisés par logiciel | |
| 10. Mettre en œuvre les réseaux locaux réalisés par logiciel | Les initiatives ont besoin d'une définition plus claire. |
| 11. Évaluer les points de service (PDS) fondés sur le modèle de la vérification systématique (architecture de confiance zéro) | Initiative du modèle à vérification systématique (confiance zéro)<br>Relié au SACI et aux initiatives « Accès à Internet et aux SaaS » |
| 12. Établir une feuille de route pour la vérification systématique (architecture de confiance zéro). | |

# Les initiatives actuelles de SPC doivent s'intégrer aux activités futures.

| Esprit d'initiative | Définition | Activités futures connexes |
|---|---|---|
| GIES | Gestion de l'information et des événements de sécurité | Lacs de données |
| VSST | Visibilité, sensibilisation et sécurité à l'égard des terminaux | Intégrer aux plans de SPC pour 2021-2024 |
| EVCM | Gestion de la vulnérabilité et de la conformité de l'entreprise | Intégrer aux plans de SPC pour 2021-2024 |
| RGC | Réseau de gestion centralisée | Intégration aux plans de SPC pour les réseaux étendus réalisés par logiciel |
| DCAM | Gestion des comptes de justificatifs d'identité en répertoire | Intégrer aux plans de SPC pour 2021-2024 |
| SCAA | Service de contrôle d'accès administratif | Lien vers le modèle à vérification systématique (confiance zéro) |
| ADR (*NDA*) (maintenant GCVC [*CLM*]) | Authentification des dispositifs de réseau/Gestion du cycle de vie de la cryptographie | Lien vers le modèle à vérification systématique (confiance zéro) |
| SACI | Service d'authentification centralisé interne | Lien vers le modèle à vérification systématique (confiance zéro) |
| GCCAR | Gouvernement du Canada — Contrôle d'accès réseau | Lien vers le modèle à vérification systématique (confiance zéro) |
| ENM | Modernisation du Réseau des économies mondiales dynamiques et émergentes (*EDGE*) | SD-LAN |
| SPE | Sécurité du périmètre d'entreprise (SPE) | Faire évoluer le « périmètre défini par logiciel (SDP) » |
| SRAM | Gestion de l'accès à distance sécurisé | Accès à Internet et aux SaaS/Vérification systématique (confiance zéro) |
| SICR | Stratégie d'interconnexion des centres régionaux | Lien vers d'autres activités |
| ADNS | Activation et défense du nuage sécurisé | Accès à Internet et aux SaaS/Vérification systématique (confiance zéro) |

# Stratégie en matière de réseau et de sécurité de SPC – Autres références

| Solution | Stratégie en matière de réseau et de sécurité de SPC | Gartner Research + Commentaires |
|---|---|---|
| **5G** | ▪ La cinquième génération de services cellulaires (5G), qui est prête à changer fondamentalement la prestation des services de réseau aux consommateurs et aux entreprises.<br>▪ La stratégie et l'approche « sans-fil d'abord » simplifieront la connectivité des utilisateurs, réduiront les coûts d'aménagement et enrichiront l'expérience utilisateur. | ▪ La stratégie de SPC doit suggérer l'utilisation potentielle de la 5G au cours des trois prochaines années. (Moyen terme)<br>▪ SPC doit élaborer des plans de déploiement des services 5G. |
| **Wi-Fi 6** | ▪ Des technologies comme le Wi-Fi 6 et la 5G fourniront une occasion de moderniser et d'enrichir l'expérience utilisateur. | ▪ La stratégie de SPC doit définir ses attentes concernant le déploiement du réseau Wi-Fi 6.<br>▪ La stratégie de SPC doit indiquer où elle préférerait utiliser le Wi-Fi 6 et la 5G. |
| **Infrastructure hyperconvergente** | ▪ Mise en œuvre de technologies habilitantes, comme les réseaux définis par des logiciels, intégrées à l'infrastructure sur place, comme l'infrastructure hyperconvergente. | ▪ La stratégie de SPC doit définir les possibilités d'utiliser l'infrastructure hyperconvergente.<br>▪ SPC doit établir une « activité à moyen terme » pour atteindre des buts précis d'ici trois ans. |
| **Compétences** | ▪ La stratégie de SPC signale et définit le besoin de nouvelles compétences. | ▪ La stratégie de SPC doit établir et exposer toute initiative à moyen terme pour combler cette lacune. |
| **Interopérabilité** | ▪ Stratégie de SPC – « Soutient une transition vers des normes ouvertes sans égard au fournisseur. »<br>▪ La stratégie de SPC ne tient pas compte de l'interopérabilité. | ▪ La stratégie de SPC doit énoncé les mesures qu'elle prendra pour assurer l'interopérabilité et l'utilisation de normes ouvertes à l'avenir. |

01 | **Sommaire de gestion**

02 | **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 | **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

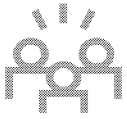
04 | **Analyse de cas d'approvisionnement**

05 | **Annexe**



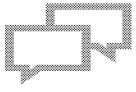

Gartner

# Gartner a terminé l'examen du document de la stratégie de SPC et a émis des recommandations pour l'amélioration du texte.



Aperçu général – Passage de la voix passive à la voix active et utilisation de formulations positives plutôt que négatives

Accent mis sur « l'état actuel » – Présentation d'un aperçu plus équilibré des réussites et des possibilités de SPC



Attention accrue aux « exigences » – SPC doit envisager d'ajouter des exigences supplémentaires

Attention accrue à la « gestion des services » – Utilisation de la structure de la BITI pour cerner les lacunes dans la stratégie de service

**Dans les diapositives suivantes, Gartner aborde plus en détail le contenu de la documentation de SPC et la façon dont il s'harmonise avec les travaux de Gartner Research.**

# Stratégie en matière de réseau et de sécurité de SPC – Examen des documents
# Aperçu général

| Stratégie en matière de réseau et de sécurité de SPC<br>Observations | Recommandations de Gartner |
|---|---|
| ▪ On a rédigé le sommaire de la stratégie de SPC de façon passive, alors qu'on aurait pu le faire à la voix active au moyen d'activités définies.<br>▪ Exemples :<br>  ▪ « SPC devra réfléchir à la manière dont il peut créer une proposition de valeur qui attire des ensembles de compétences de valeur et permet leur maintien. »<br>  ▪ « Envisager d'investir dans l'automatisation et l'orchestration… » | ▪ La rédaction de la stratégie de SPC à la voix active communiquerait la confiance. La Stratégie doit privilégier les activités prévues.<br>▪ Suggestion –<br>  ▪ « SPC créera une proposition de valeur qui attirera des ensembles de compétences de valeur et permettra leur maintien. »<br>  ▪ « SPC investira dans l'automatisation et l'orchestration… » |
| ▪ La stratégie de SPC fait de vagues références négatives à l'état actuel de SPC.<br>▪ Exemple : « Veiller à ce que les projets actuels et futurs soient guidés et réalisés non pas en silos, mais en tenant compte de tous les services dans l'optique de la vision et de la stratégie en matière de réseauet de sécurité. » | ▪ La stratégie de SPC doit accentuer la façon dont elle améliorera la prestation des services.<br>▪ Suggestion : « Les dirigeants de SPC travailleront avec les équipes de projet afin d'assurer l'harmonisation avec la stratégie en matière de réseauet de sécurité de SPC. » |
| ▪ Certaines solutions abordées dans la stratégie ne font pas partie des activités à moyen terme, p. ex., le déploiement de la 5G. | ▪ SPC doit définir les activités à moyen terme associées à ces activités. |
| ▪ Certaines solutions définies à titre d'activités à moyen terme ne figurent pas dans la Stratégie, p. ex., la mise à jour de la BDGC. | ▪ Le sommaire de gestion doit mettre en évidence les mesures que prendra SPC, en s'harmonisant avec les activités à court et à moyen termes. |

# Stratégie en matière de réseau et de sécurité de SPC – Examen des documents
# Accent mis sur l'état actuel

| Stratégie en matière de réseau et de sécurité de SPC<br>État actuel – Observations | Recommandations de Gartner |
|---|---|
| On a rédigé l'**analyse de l'état actuel** comme une accusation de SPC.<br><br>« Plus de 500 projets individuels sont prévus ou en cours pour maintenir, actualiser ou remplacer ces environnements sans stratégie globale ou intégrée. » | ▪ En réalité, SPC dispose bel et bien d'une stratégie, mais mal documentée.<br>▪ SPC doit présenter une vision équilibrée de la situation actuelle.<br>▪ SPC doit renvoyer aux indicateurs qu'il a améliorés ou espère améliorer. (Des exemples figurent en annexe, page 102.) |
| « la technologie évolue trop rapidement pour que nous puissions en suivre le rythme » | ▪ Hyperbole – Une phrase inutile<br>▪ Est-ce clair que SPC prend du retard? Comment le mesure ou l'aborde-t-on? |
| « Les progrès technologiques dépassent les compétences requises disponibles. » | ▪ Hyperbole – Une phrase inutile<br>▪ Compétences disponibles : à SPC, au GC, au Canada? |
| « Le personnel ne peut pas répondre assez rapidement, puisqu'il n'a pas accès aux bons renseignements. » | ▪ Hyperbole – Une phrase inutile<br>▪ Quelles sont les données manquantes? Comment abordera-t-on ces problèmes? |
| « SPC requiert une nouvelle approche de gestion et de fonctionnement de son environnement de réseau et de sécurité. » | ▪ Quelle est cette approche?<br>▪ La Stratégie n'a-t-elle pas clairement défini cette approche? |
| La Stratégie évoque les « impacts négatifs sur les délais d'approvisionnement ». | ▪ Sont-ce des indicateurs pour les délais d'approvisionnement? Ces indicateurs sont-ils en train d'empirer?<br>▪ L'utilisation de mesures, d'indicateurs et de tendances précis fournit un contexte important. |
| « risques accrus associés à l'effort manuel » | ▪ Exemples où les risques augmentent? Où les efforts manuels subiront-ils leur remplacement? |

# Stratégie en matière de réseau et de sécurité de SPC – Examen de documents
# Attention accrue aux exigences

| Stratégie en matière de réseau et de sécurité de SPC<br>Exigences du gouvernement du Canada – Observations | Recommandations de Gartner |
|---|---|
| **Utilisateurs finaux**<br>• La Stratégie renvoie à 400 000 utilisateurs finaux. | ▪ SPC ne tient pas compte de l'expérience utilisateur actuelle et des indicateurs connexes.<br>▪ SPC ne s'occupe pas des problèmes d'accès à distance comme la latence.<br>▪ SPC ne répond pas aux besoins particuliers des employés et des citoyens. |
| **Applications**<br>• Bien que fonctionnelles, les applications RPV ou de bureau à distance traditionnelles n'ont généralement pas subi de mise à l'échelle pour que la majorité des effectifs puisse les mettre à profit simultanément.<br>• Des efforts sont en cours pour accorder à nouveau la connectivité externe avec les applications SaaS infonuagiques existantes et à venir prochainement, comme Office 365 de la stratégie en matière de réseauet de sécurité de SPC. | ▪ SPC ne définit pas quels « efforts sont en cours pour accorder à nouveau la connectivité externe ».<br>▪ Gartner s'attend à ce que les ministères du GC utilisent davantage d'applications SaaS à l'avenir, mais la stratégie de SPC n'aborde pas cette croissance. |
| **Charge de travail**<br>• « les charges de travail qui effectuent la transition vers le nuage public » | ▪ La stratégie de SPC ne documente aucune mesure ni aucun indicateur présumés associés aux changements de charge de travail, y compris la migration vers le nuage. |
| **Incidence de la COVID-19**<br>• À la suite de la COVID-19, la plupart des organisations se sont vu forcer d'adopter le travail à domicile et un modèle de travail par accès à distance. Ce changement d'emplacement du travail a mis en charge et contraint ces services jusqu'au point de rupture. | ▪ SPC a-t-il réussi à s'adapter au travail à domicile?<br>▪ Qu'est-ce qui est arrivé jusqu'au point de rupture? Comment a-t-on abordé ce problème?<br>▪ Quelles leçons a-t-on apprises?<br>▪ Comment cela s'est-il répercuté sur la stratégie de SPC? |
| **Dispositions prévues pour l'après-COVID-19**<br>• Quelle incidence le travail à domicile aura-t-il sur la stratégie de SPC après la COVID-19? | ▪ Quelles hypothèses SPC formule-t-il au sujet de l'environnement de travail post-COVID-19?<br>▪ La planification de SPC repose-t-elle sur un plus grand nombre d'utilisateurs travaillant à domicile?<br>▪ Quelle incidence cela a-t-il sur les dispositions que prévoit SPC pour les réseaux intra-immeubles? |

# Stratégie en matière de réseau et de sécurité de SPC – Examen de documents
# Attention accrue à la gestion des services (1 de 2)

| Stratégie en matière de réseau et de sécurité de SPC<br>Gestion des services – Observations | Recommandations et commentaires de Gartner |
|---|---|
| **Gestion des services** – Les 25 premières pages de la Stratégie se consacrent uniquement à la surveillance et à l'approvisionnement. | ▪ Le sommaire de gestion doit comprendre une référence à la gestion des services, et la Stratégie doit en traiter dès les quelques premières pages. |
| **Gestion des configurations**<br>« Des ingénieurs et opérateurs de systèmes au sein de SPC et d'autres ministères ont principalement effectué les configurations manuellement, ce qui peut entraîner des incohérences dans ces dernières. » | ▪ La stratégie de SPC s'attaque à une partie de la gestion des configurations en page 37 – « Établir et mettre à jour la BDGC avec toute l'infrastructure de SPC ». |
| **Approvisionnement** – Mettre en œuvre les réseaux définis par des logiciels/l'infrastructure logicielle et l'approvisionnement en nuage<br>« SPC devra apporter un changement fondamental à son modèle de fonctionnement à mesure qu'il effectuera la transition à l'infonuagique et aux nouvelles capacités de réseau et de sécurité. » | ▪ SPC doit définir les mesures et indicateurs d'approvisionnement actuels ou prévus en fonction d'utilisateurs, d'applications, d'actualisation de l'infrastructure, etc.<br>▪ La stratégie de SPC doit comprendre l'amélioration des mesures et indicateurs d'approvisionnement par voie d'activités à moyen terme. |
| **Surveillance** – SPC considère la surveillance comme un « pilier » de la Stratégie.<br>« SPC devra passer d'outils et de processus de surveillance autonomes à un ensemble intégré de technologies appuyé par un dépôt de données centralisé. » | ▪ Voir « Pilier 3 – Surveillance » à la page 9 du présent rapport Gartner. (ci-dessus) |
| **Gestion de la capacité**<br>Le réseau sur demande fournira « une meilleure planification de la capacité », mais le réseau sur demande est défini comme une « tendance », et non comme une stratégie. | ▪ SPC doit définir une stratégie pour aborder la gestion de la capacité. |
| **Entretien**<br>L'infrastructure, l'équipement et le câblage des réseaux intra-immeubles ont de multiples responsables, ce qui entraîne la complexité des modèles opérationnels avec des stratégies disparates pour les technologies, les fournisseurs, le déploiement, l'entretien et le fonctionnement. | ▪ La stratégie de SPC doit définir les programmes d'entretien ou toutes initiatives visant à améliorer l'entretien de l'infrastructure. |

# Stratégie en matière de réseau et de sécurité de SPC – Examen de documents
# Attention accrue à la gestion des services (2 de 2)

| Stratégie en matière de réseau et de sécurité de SPC<br>Gestion des services – Observations | Recommandations de Gartner |
|---|---|
| **Gestion du changement**<br>• La stratégie de SPC fait référence au besoin de gestion du changement.<br>• « Élaborer les processus de gestion du changement pour gérer le changement opérationnel (très important) selon les pratiques exemplaires de la GSTI. » | ▪ SPC doit définir des activités précises afin d'aborder la gestion du changement. |
| **Gestion des incidents**<br>« Les plateformes opérationnelles d'intelligence artificielle (AIOps) permettront à SPC d'obtenir des perspectives et renseignements approfondis et de favoriser une intervention automatisée en cas d'incident. » | ▪ SPC doit indiquer clairement, dès le départ, comment elle améliorera la gestion des incidents. L'utilisation de mesures et indicateurs attirerait l'attention sur les buts de SPC. |
| **Gestion des problèmes**<br>« L'incohérence des équipes de surveillance et de soutien des dispositifs qui travaillent en silos ajoute davantage aux couches de complexité qui nuisent à la résolution rentable et en temps opportun des problèmes. » | ▪ SPC doit définir des stratégies pour améliorer la gestion des problèmes, au-delà des améliorations de la surveillance. |

01 **Sommaire de gestion**

02 **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

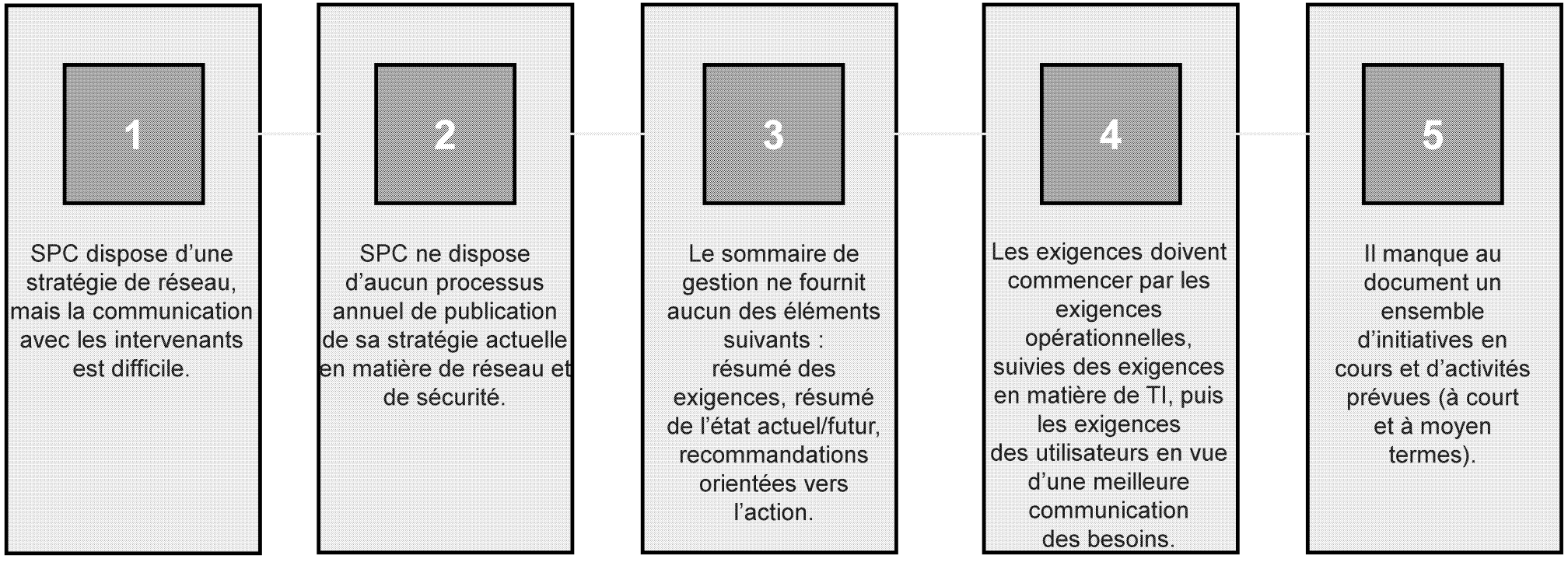
04 **Analyse de cas d'approvisionnement**

05 **Annexe**




Gartner

# Gartner a cerné cinq lacunes clés en comparant le document de discussion sur la modernisation du réseau de SPC au modèle de stratégie en matière de réseau de Gartner.




**Dans les diapositives suivantes, Gartner traite de la façon dont SPC peut corriger les lacunes relevées dans le document sur sa stratégie en matière de réseau.**




Gartner

# Structure du document sur la stratégie recommandée par Gartner

## Gartner Research : *Creating a Business-Relevant Network Strategy*, 5 janvier 2016

| Sections | Objet | Description |
|---|---|---|
| **Résumé** | ▪ Résumé de toutes les sections ci-dessous, dans l'ordre | ▪ Résumé autonome des principaux points |
| **Facteurs opérationnels et de TI** | ▪ Répond aux exigences connues | ▪ Relié aux stratégies opérationnelles et de TI établies |
| **Environnement de TI** | ▪ Environnement de TI actuel | ▪ Définition des contraintes, y compris les solutions existantes |
| **Environnement utilisateur** | ▪ Types d'utilisateur et expérience utilisateur | ▪ Répondre aux principaux indicateurs relatifs aux besoins des utilisateurs et à l'expérience utilisateur |
| **Évaluation de l'état actuel** | ▪ Ce qui fonctionne bien et ce qui ne fonctionne pas | ▪ À quoi faut-il s'attaquer? |
| **État futur souhaité** | ▪ Comment le service fonctionnerait-il mieux? | ▪ Buts et objectifs établis sur une période fixe |
| **Analyse d'écarts et de lacunes** | ▪ Hypothèses et dépendances | ▪ Quels facteurs externes influeront sur la stratégie? |
| | ▪ Évaluation des risques | ▪ Quels sont les risques liés aux solutions de rechange, y compris l'inaction? |
| | ▪ Contraintes | ▪ Qu'est-ce qui limitera l'exécution du plan? |
| **Plan d'action/ Feuille de route** | ▪ Recommandations approfondies | ▪ Que peut-on faire? Quand? Qui peut l'accomplir? |
| | ▪ Feuille(s) de route pour la mise en œuvre | ▪ Initiatives particulières – Comment atteindra-t-on l'état souhaité? |

# Gartner a comparé le « Document de discussion sur la modernisation du réseau de SPC » à son modèle de stratégie en matière de réseau

| Stratégie en matière de réseau | Modèle de stratégie en matière de réseau de Gartner | Document sur la modernisation du réseau de SPC | Commentaires de Gartner |
|---|---|---|---|
| **Aperçu** | ▪ **Gartner Research —** *Creating a Business-Relevant Network Strategy*; 5 janvier 2016, G00294550 | ▪ SPC « Document de discussion sur la modernisation du réseau - décembre 2020 » | ▪ Le document de discussion doit définir son auditoire cible et son mode d'utilisation. On doit relever et solliciter les partenaires du GC pour obtenir leurs commentaires.<br>▪ Le document de discussion doit adopter un ton positif et éviter de respirer une position défensive. |
| **Sommaire de gestion** | ▪ Résumé des exigences | ▪ SPC utilise une section « ce que les partenaires demandent » afin d'énumérer les exigences connues. | ▪ SPC doit déterminer toute exigence propre au gouvernement du Canada et à ses employés (p. ex., latence du réseau)? |
| | ▪ Résumé de l'état actuel | ▪ Il y a dix ans, « cette infrastructure était vieillissante, coûteuse à entretenir et incapable de prendre en charge des services modernes ». | ▪ Si cette infrastructure n'a subi aucune mise à jour depuis 2011, il s'agirait d'une lacune majeure dans l'état actuel.<br>▪ Autrement, la pertinence de ce point n'est pas claire. |
| | ▪ Résumé de l'état souhaité | ▪ « SPC conçoit actuellement la solution d'état futur. » | ▪ Bien que SPC en soit encore à concevoir son état futur, la stratégie doit documenter les initiatives actuelles qui définissent en fait l'architecture de réseau future de SPC.<br>▪ Les exemples comprendraient les nouveaux RL de centre de données. |
| | ▪ Recommandations orientées action | ▪ Ce document ne traite d'aucune initiative particulière. | ▪ SPC doit communiquer ses principales initiatives en matière de réseau dans le cadre d'une stratégie en matière de réseauannuelle. |

# Gartner a comparé le « Document de discussion sur la modernisation du réseau de SPC » à son modèle de stratégie en matière de réseau

| Stratégie en matière de réseau | Modèle de stratégie en matière de réseau de Gartner | Document sur la modernisation du réseau de SPC | Recommandations de Gartner |
|---|---|---|---|
| **Facteurs opérationnels et de TI** | ▪ Priorités opérationnelles<br>▪ Stratégies du DPI<br>▪ Plan des RH et des compétences | ▪ Priorités opérationnelles – traite de la prise en charge du travail à domicile.<br>▪ Stratégies du DPI – Traite de la migration des applications au nuage.<br>▪ La référence au document Vision de la sécurité est utile.<br>▪ Plan des RH et des compétences – Le document de SPC manque de clarté sur le plan des compétences requises à l'avenir. | ▪ Établir un processus visant à définir les priorités opérationnelles sur une base annuelle.<br>▪ Énoncer les priorités opérationnelles particulières et uniques du GC.<br>▪ Insérer un lien vers le document de discussion sur la stratégie en matière de réseau et de sécurité de SPC et d'autres stratégies de SPC.<br>▪ SPC reconnaît la nécessité de nouvelles compétences, et doit fournir des exemples. |
| **Environnement de TI** | ▪ Architecture<br>▪ Infrastructure/Gouvernance<br>▪ Approvisionnement<br>▪ Mesures et indicateurs utilisés | ▪ Architecture – Diagramme d'architecture de réseau de haut niveau.<br>▪ Gouvernance – Aucun processus décisionnel clairement défini et prévu.<br>▪ Approvisionnement – SPC reconnaît le besoin de mettre à jour sa stratégie d'approvisionnement existante.<br>▪ Mesures et indicateurs non compris | ▪ Architecture – Le diagramme d'architecture de réseau de haut niveau doit s'appuyer de texte descriptif.<br>▪ Approvisionnement – Les processus d'approvisionnement amélioreront la transparence, la responsabilisation et l'efficacité.<br>▪ Mesures et indicateurs – Ajouter une référence à l'utilisation des mesures et indicateurs pour suivre les améliorations. |
| **Environnement utilisateur** | ▪ Planification de l'effectif<br>▪ Capacités souhaitées<br>▪ Plan des installations | ▪ Plan de l'effectif – Mentionne l'incidence de la COVID-19, mais ne définit pas les écarts associés.<br>▪ Capacités souhaitées – Définies en termes génériques sans référence à une quelconque exigence particulière du GC.<br>▪ Plan des installations – Répercussions de la COVID-19 abordées et évolution de l'utilisation des lieux de travail. | ▪ Les attentes pour les environnements de travail durant et après la période de la COVID-19 doivent être établies dans une stratégie en matière de réseau.<br>▪ Le plan des installations doit exposer les attentes relatives aux besoins de soutien du réseau (RL) des bâtiments du GC.<br>▪ La stratégie doit comporter un renvoi pour améliorer les processus visant à définir les besoins des utilisateurs des ministères clients. |

# Gartner a comparé le « Document de discussion sur la modernisation du réseau de SPC » à son modèle de stratégie en matière de réseau

| Stratégie en matière de réseau | Modèle de stratégie en matière de réseau de Gartner | Document sur la modernisation du réseau de SPC | Recommandations de Gartner |
|---|---|---|---|
| **Évaluation de l'état actuel** | ▪ Budget et finances<br>▪ Niveaux de service<br>▪ Technologie<br>▪ Organisation et dotation<br>▪ Évaluation des fournisseurs | ▪ Budget – Ne comprend aucune analyse des dépenses courantes.<br>▪ Niveaux de service – Ne fournit aucun renvoi aux mesures et indicateurs de rendement actuels.<br>▪ Évaluation des fournisseurs – Ne tient aucun compte des hauts et des bas actuels des relations avec les fournisseurs.<br>▪ Technologie – Comporte la liste des fournisseurs pour chaque catégorie de réseau, mais aucun détail sur la solution.<br>▪ Le diagramme d'architecture de réseau de haut niveau ne s'appuie d'aucun texte descriptif. | ▪ Fournir des mesures et indicateurs de la consommation actuelle des services pour montrer la tendance vers la demande future de services.<br>▪ Présenter des indicateurs d'efficacité mesurables clés harmonisés avec les rapports budgétaires publics du GC et de SPC.<br>▪ Définir des indicateurs de rendement utiles et mesurables, par exemple : temps de disponibilité, latence, panne ou défaillance d'équipement ou de matériel.<br>▪ Technologie – Ajouter une mesure de l'utilisation future prévue de nouvelles technologies – Qui? Où?<br>▪ Organisation – Comment SPC s'est-il organisé pour répondre aux besoins du GC en matière de réseaux?<br>▪ Fournisseurs – Comment mesure-t-on le rendement des fournisseurs? |
| **État futur souhaité** | ▪ Services futurs offerts<br>▪ Tendances technologiques futures<br>▪ Changements à l'état actuel | ▪ État futur non encore défini – « SPC conçoit actuellement la solution de l'état souhaité ».<br>▪ La référence aux tendances technologiques ne comprend pas la référence à l'applicabilité ou aux avantages mesurables.<br>▪ Le document de SPC comprend une « approche d'approvisionnement théorique », qui se limite à la sélection des fournisseurs.<br>▪ SPC prévoit une plus grande utilisation du service de fibre noire et des services par satellite. | ▪ Bien que SPC en soit encore à concevoir son état futur, la stratégie doit documenter les initiatives actuelles qui, en fait, sont en train de définir un avenir. Les exemples comprendraient les nouveaux RL de centre de données.<br>▪ SPC doit établir des attentes relatives à l'utilisation du service de fibre noire et des services par satellite. |

# Gartner a comparé le « Document de discussion sur la modernisation du réseau de SPC » à son modèle de stratégie en matière de réseau

| Stratégie en matière de réseau | Modèle de stratégie en matière de réseau de Gartner | Document sur la modernisation du réseau de SPC | Commentaires de Gartner |
|---|---|---|---|
| **Analyse des écarts et des lacunes** | ▪ Hypothèses et dépendances | ▪ Le document de discussion suppose que SPC appuiera le travail actuellement fait à domicile en raison de la COVID-19, mais n'aborde pas d'autres efforts d'intervention.<br>▪ SPC n'a pas défini de dépendances. | ▪ Une fois que SPC aura défini sa stratégie de réseau, il voudra définir toutes hypothèses et dépendances. |
| | ▪ Évaluation des risques | ▪ Les énoncés de risque ne sont pas clairs. Exemple : « Normaliser deux produits ou plus – ….. atténue le risque que le GC ne veuille plus traiter avec un fournisseur particulier pour des raisons opérationnelles ou de sécurité. » | ▪ SPC doit déterminer le risque qui aura une incidence sur sa capacité de fournir et d'améliorer des services.<br>▪ SPC doit déterminer le risque qui aura une incidence sur sa capacité de fournir et d'améliorer des services. |
| | ▪ Contraintes | ▪ Contraintes – Manque de précisions sur les causes des contraintes. | ▪ SPC doit tenir compte des principales contraintes qui pourront limiter sa capacité de fournir des services. |
| **Plan d'action/ Feuille de route** | ▪ Recommandations approfondies<br>▪ Feuille(s) de route pour la mise en œuvre | ▪ SPC n'a pas défini de recommandations claires.<br>▪ Feuille de route – Les échéanciers du projet sont abordés, mais il n'y a pas de feuille de route claire en ce qui a trait aux déploiements. | ▪ Le document de discussion doit comporter des recommandations précises provenant de la stratégie en matière de réseau et de sécurité de SPC.<br>▪ Le document de discussion doit comprendre une feuille de route quinquennale pour les grandes initiatives et faire mention des ressources nécessaires pour atteindre l'état souhaité. |

01 | **Sommaire de gestion**

02 | **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 | **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 | **Analyse de cas d'approvisionnement**

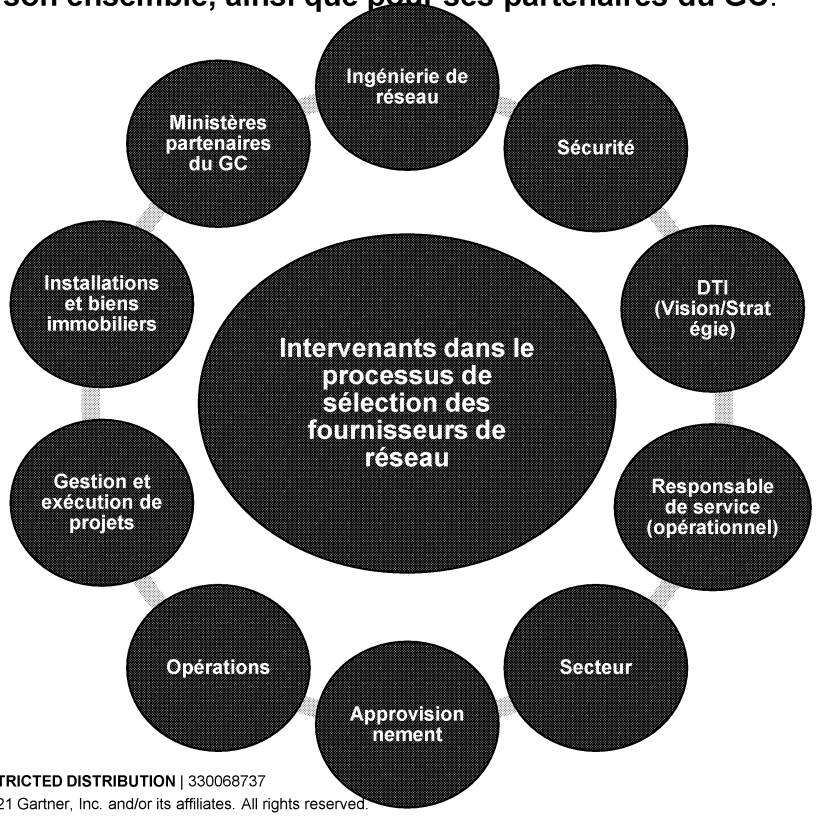
05 | **Annexe**




Gartner

# Des ateliers de découverte ont été tenus pour discuter des buts et des contraintes des intervenants en matière de sélection de fournisseurs de réseau et orienter de l'approche en la matière

Leurs commentaires ont permis de définir une approche de prise de décisions relatives à la sélection de fournisseurs qui **concilie les buts et les contraintes souvent concurrents des intervenants**. À mesure que des décisions seront prises quant à la sélection de fournisseurs ou que des exceptions seront faites, Gartner recommande de tenir compte de la position de chaque intervenant **afin d'atteindre le résultat optimal pour SPC dans son ensemble, ainsi que pour ses partenaires du GC**.




## Perspectives

La normalisation des processus et des fournisseurs est un but clé aux yeux de plusieurs intervenants.

Les obligations juridiques et d'approvisionnement imposent des contraintes de taille.

Le budget, les compétences et la taille de l'effectif sont devenus des contraintes aux yeux de nombreux intervenants.

Les intervenants du secteur et de SPC ont pour but d'accroître la transparence.

Les anciens réseaux existent et persistent dans les activités de SPC.

Les contraintes de sécurité (p. ex. : certifications, intégrité de la chaîne d'approvisionnement) sont immuables pour certains approvisionnements sélectionnés.

# Aperçu des intervenants

| Ingénierie de réseau | Approvisionnement | Sécurité |
|---|---|---|
| ▪ **Buts :** Normalisation, soutenabilité, interopérabilité dans l'écosystème existant<br>▪ **Contraintes :** Normes sectorielles et de SPC, capacité (p. ex., essai d'interopérabilité), possibilités existantes (compétences) | ▪ **Buts :** Modalités acceptables, respect des échéances, budget, besoins opérationnels, ouverture et transparence<br>▪ **Contraintes :** Règles et règlements d'approvisionnement de SPC, règles et règlements du CIIT, aspects juridiques, capacité (personnel), affectations de fonds | ▪ **Buts :** Fonctions de sécurité de réunion<br>▪ **Contraintes :** Certifications sectorielles (p. ex. : FIPS, CC), harmonisation et conformité avec le CSTC, exigences en matière d'intégrité de la chaîne d'approvisionnement |

| Opérations | DTI (vision/stratégie) |
|---|---|
| ▪ **Buts :** Simplicité de gestion, préservation et amélioration des niveaux de service<br>▪ **Contraintes :** Possibilités existantes (compétences), capacité opérationnelle | ▪ **Buts :** Harmonisation avec la vision et la stratégie établies<br>▪ **Contraintes :** On n'en a relevé aucune pendant l'entrevue exploratoire. |

# Aperçu des intervenants

| Gestion et exécution de projets | Responsable de service (opérationnel) | Installations/Biens immobiliers |
|---|---|---|
| ▪ **Buts :** Budget, calendrier, portée<br>▪ **Contraintes :** Détenteur du pouvoir de dépenser pour le projet, processus d'approvisionnement | ▪ **Buts :** Optimisation des ressources, maintien et amélioration de la gamme de services, amélioration continue du service, gestion du cycle de vie de chaque service, gestion du rendement des fournisseurs<br>▪ **Contraintes :** Budget, capacité | ▪ **Buts :** Simplicité de la gestion de projet<br>▪ **Contraintes :** Usine de câblage, rôles et responsabilités (SPC par rapport à SPAC) |

| Secteur | Ministères partenaires du GC |
|---|---|
| ▪ **Buts :** Profit, empreinte, visibilité dans l'approvisionnement, éducation<br>▪ **Contraintes :** PI, interopérabilité, normes sectorielles, accès à l'information | ▪ **Buts :** Atteindre les objectifs ministériels<br>▪ **Contraintes :** On n'en a relevé aucune pendant l'entrevue exploratoire. |

01 **Sommaire de gestion**

02 **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 **Analyse de cas d'approvisionnement**

05 **Annexe**




Gartner

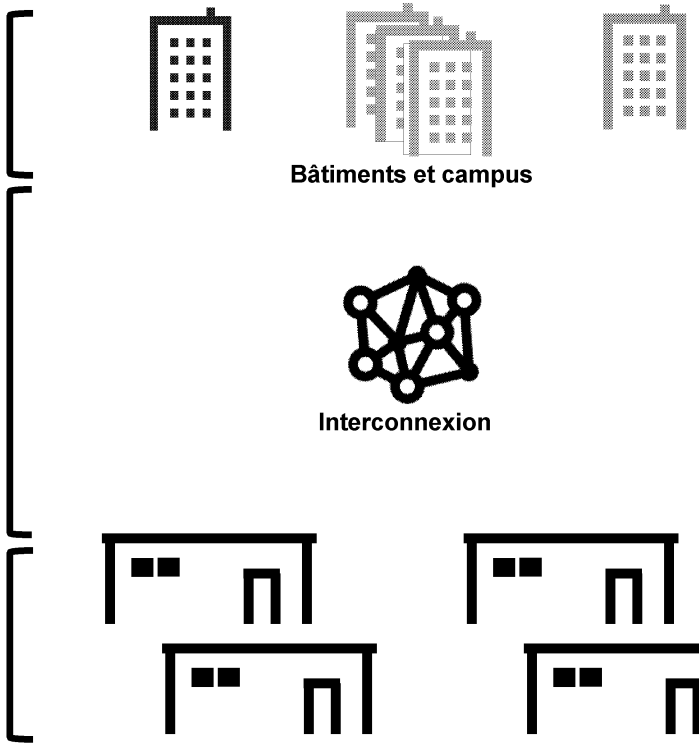
# La définition des trois réseaux de SPC aidera à clarifier les activités à venir en matière d'approvisionnement.

Pour répondre au mieux aux besoins de l'industrie, Gartner propose que l'on aborde le réseau de SPC et le traite comme étant composé de trois éléments distincts, tel qu'il est décrit ci-dessous, ce qui permettra l'établissement de **normes technologiques** comportant des paramètres et une portée clairement définis.

**RL** (réseau local)
- Réseau câblé intra-immeuble
- Réseautage sans fil (Wi-Fi)

**RÉ** (réseau étendu)
- Routeurs dorsaux
- Transport (optique, DWDM)
- Couche d'acheminement et de services en périphérie

**RCD** (Réseau de centres de données)
- Réseau sous-tendu/physique
- Réseau superposé/virtualisé

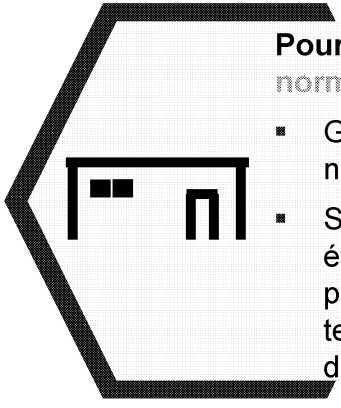


# Gartner a élaboré des considérations pour l'établissement de normes technologiques à l'échelle de SPC.

**Gartner recommande** d'établir des normes technologiques **pour chaque composante du réseau, soit le RL, le RÉ et le RCD (dans les limites définies)** dans le cadre de processus d'approvisionnements ouverts et concurrentiels.

La norme technologique doit demeurer en place pendant la durée de vie prévue de l'équipement dans chaque composante, et subir son renouvellement à son expiration :

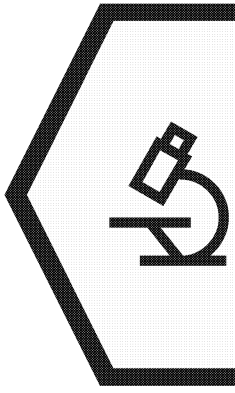
- Environ 10 ans pour le RL
- Environ 5 à 7 ans pour le RÉ et le RCD



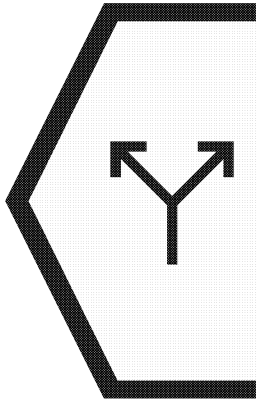
**Pour les réseaux de centres de données, Gartner recommande l'établissement** de normes technologiques pour deux composantes.

- Gartner recommande d'échelonner les dates de début et de fin des normes afin qu'elles n'expirent pas en même temps.
- SPC pourrait envisager un concours initial où la proposition retenue en première place établit la norme technologique pour le premier « RCD » pendant sept ans, et la proposition retenue en deuxième place établit la norme pour cinq ans. Les normes technologiques pour sept ans seraient établies dans le cadre d'autres processus d'approvisionnements.

# Gartner a fourni des balises de sécurité pour la sélection de fournisseurs sans normes technologiques établies.



L'approvisionnement effectué avant l'établissement d'une norme technologique, ou après l'expiration de la norme, doit faire l'objet d'un examen rigoureux afin de concilier les contraintes opérationnelles, techniques, de sécurité, juridiques, d'approvisionnement et sectorielles. De telles décisions doivent être prises en consultation avec les intervenants.



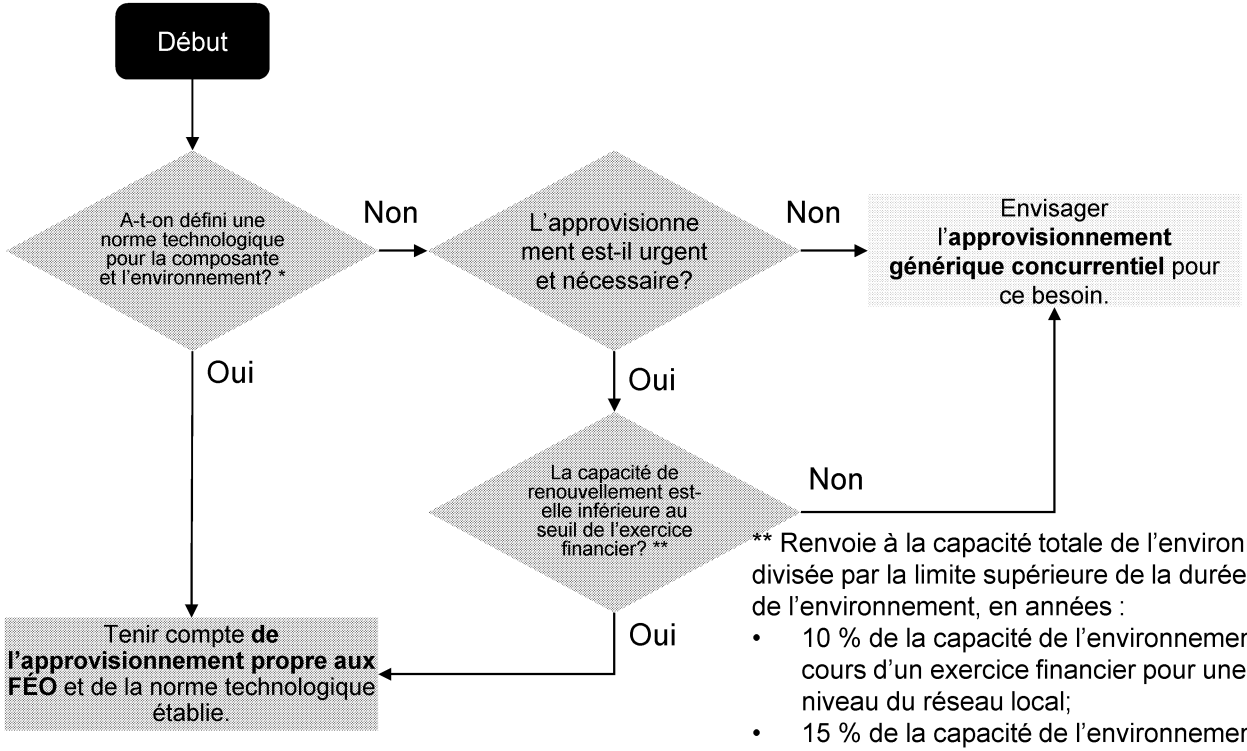
Pour les environnements existants comptant un fournisseur établi (norme de facto), mais ne suivant aucune norme technologique établie, Gartner recommande que les marchés à fournisseur unique soient approuvés lorsque la mise à niveau est urgente et nécessaire Cela se traduit par ce qui suit :

- Pour le RL, moins de 10 % de la capacité de l'environnement cible au cours d'un exercice financier.
- Pour le RÉ et le RCD, moins de 15 % de la capacité de l'environnement cible au cours d'un exercice financier.

# L’outil d’aide à la décision pour la sélection de fournisseurs de réseau pour les approvisionnements de SPC se résume dans cet arbre de décision.

* Désigne une norme technologique établie dans le cadre d’un approvisionnement ouvert pendant la durée de vie utile de l’équipement :
- 10 ans pour le RL,
- 5 à 7 ans pour le RÉ et le RCD.

Par composante, on entend le RL, le RÉ ou le RCD alors que par environnement, on entend l’équipement dans les paramètres d’une norme technologique.




** Renvoie à la capacité totale de l’environnement cible, divisée par la limite supérieure de la durée de vie utile de l’environnement, en années :
- 10 % de la capacité de l’environnement cible au cours d’un exercice financier pour une mise à niveau du réseau local;
- 15 % de la capacité de l’environnement cible au cours d’un exercice financier pour une mise à niveau du RÉ ou du RCD.

01 **Sommaire de gestion**

02 **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 **Analyse de cas d'approvisionnement**

05 **Annexe**




Gartner

# SPC doit mettre tout en œuvre pour inclure des chefs de file de l'industrie dans ses processus d'approvisionnement tout en tenant compte du contexte et des contraintes du GC.

- Gartner a fourni dans chaque composante du réseau une ventilation des **fournisseurs établis** que SPC doit s'évertuer à inclure dans ses efforts d'approvisionnement.
- **Pour être considéré comme a un chef de file** dans le Quadrant magique de Gartner, le fournisseur doit faire montre d'une attitude et de pratiques visionnaires dans son domaine et démontrer une exécution de haut niveau dans ses opérations, soit des attributs hautement souhaitables.
- Au besoin, on peut également inclure **les aspirants, les visionnaires et les spécialistes de créneau**.
- Bien que cela représente un point de vue du secteur, SPC doit également tenir compte des **contraintes** qui justifieraient **d'exclure certains fournisseurs particuliers** des processus d'approvisionnement ouverts. Ces contraintes comprennent, sans toutefois s'y limiter, celles qui s'associent aux éléments suivants : intégrité de la chaîne d'approvisionnement, sécurité, sanctions de gestion des fournisseurs, etc.

**Exemple du Quadrant magique de Gartner**

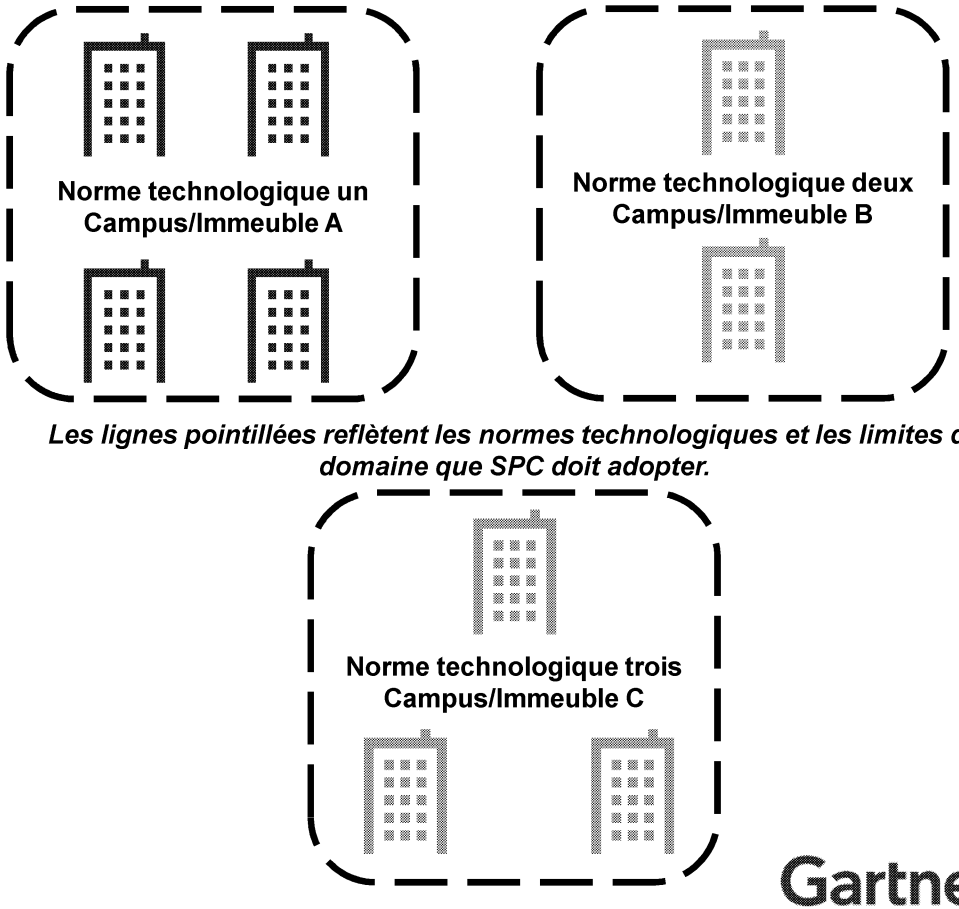
# RL




Gartner

# L’équipement de RL doit répondre à des normes technologiques ou limites associées à chaque immeuble ou campus de SPC.

- En tenant compte des **normes et des paramètres établis pour l’équipement de RL** (y compris le RL sans fil), SPC peut assurer l’efficacité opérationnelle tout en encourageant la concurrence.
- Les normes technologiques établies dans le cadre d’un **processus d’approvisionnement concurrentiel** se classent très haut sur les plans de la transparence, de l’équité et de la valeur, tout en réduisant au minimum les soucis d’interopérabilité technique.
- En normalisant les paramètres et les normes technologiques à l’échelle de l’immeuble ou du campus, SPC peut adopter une **approche d’approvisionnement multifournisseur** pour le matériel du RL.
- La durée de vie utile de l’équipement dans cette composante atteint environ 10 ans, ce qui devrait correspondre au cycle de vie des normes technologiques.

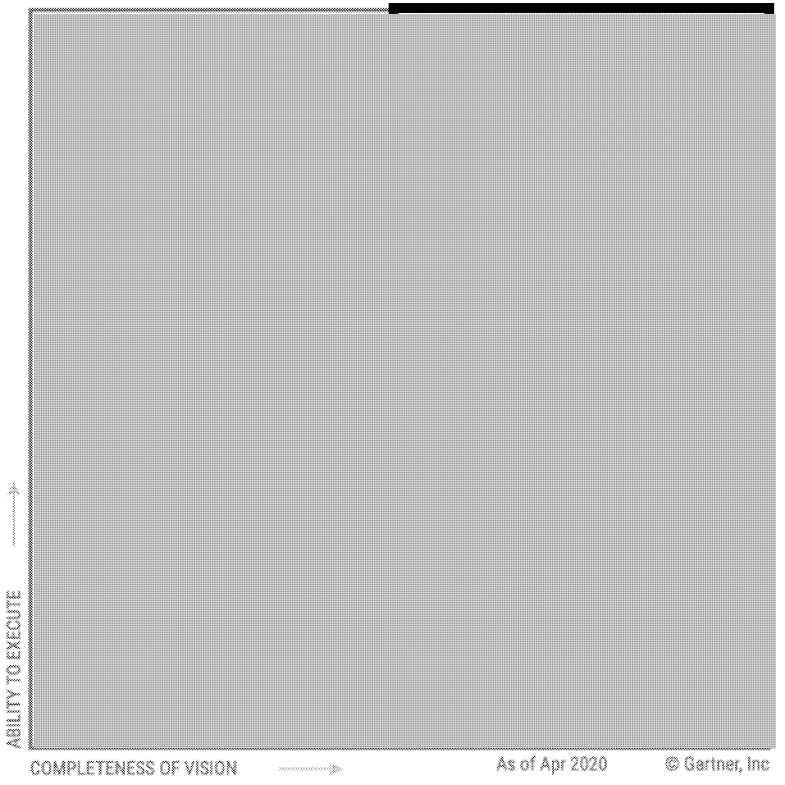



***Les lignes pointillées reflètent les normes technologiques et les limites de domaine que SPC doit adopter.***

# Ce Quadrant magique de Gartner Research présente les principaux fournisseurs d'infrastructure d'accès aux réseaux locaux câblés et sans fil.

- Le principal résultat opérationnel est une nouvelle **connectivité RL câblée et sans fil, actualisée ou élargie**. Habituellement, on la retrouve dans des environnements d'entreprise dont les planchers sont couverts de tapis, des immeubles de campus et des bureaux éloignés ou de directions générales, et **entre les appareils et applications des clients** ou d'autres actifs qui résident dans des centres de données ministériels, le nuage ou Internet. L'augmentation des points d'extrémité IdO ou des dispositifs OT servant à des applications comme l'automatisation de bâtiment nécessite une connectivité RL sans fil.
- Les **chefs de file** doivent avoir démontré leur capacité à entretenir de solides relations avec leurs **réseaux et leurs clients** et à n'avoir aucune lacune évidente dans leurs portefeuilles.
- **Gartner** prévoit qu'environ **1,7 milliard de nouveaux appareils par année** se connecteront au réseau d'entreprise d'ici 2023, mais non tous de la même façon ou selon la même architecture.

**Quadrant magique de Gartner Research des fournisseurs d'infrastructure d'accès aux réseaux locaux câblés et sans fil**




**Les profils d'entreprise de chacun de ces fournisseurs figurent dans les pages suivantes.**

# Profil d’entreprise de Juniper Networks

## *Aperçu de l’entreprise*

**Siège social :**
Sunnyvale, Californie
États-Unis

**Maturité :**
Fondation : 1996
Effectif : Environ 9 400 (2019)
Portée : Mondiale
Revenu : Environ 4,4 milliards $

## Contexte pertinent du réseau

Sa solution d’entreprise fondée sur l’IA propose un large éventail d’applications et de services de réseau en nuage et un ensemble complet de produits de commutation câblée et de RL sans fil. Ses activités sont géographiquement diversifiées et desservent des clients dans tous les marchés, des PME aux grandes entreprises. Grâce à son acquisition de Mist Systems, le fournisseur continue d’investir dans sa fondation d’IA, en misant sur la technologie d’IA de Marvis pour se démarquer tandis qu’il élargit ses applications d’assurance et d’analyse Mist dans l’ensemble du réseau campus. L’ajout des produits de commutation de la couche d’accès câblés de Juniper à l’architecture Mist a fait de la solution une offre complète de bout en bout.

## Forces

## Mises en garde

# Profil d'entreprise : HPE (Aruba)

## *Aperçu de l'entreprise*

**Siège social :**
Santa Clara, Californie
États-Unis

**Maturité : (Aruba)**
Fondation : 2002
Effectif : Environ 6 000 (2019)
Portée : Mondiale
Revenu : Environ 3 milliards $

### Contexte pertinent du réseau

Dans le cadre de la stratégie *Edge to Cloud* (« Périphérie au nuage ») de HPE, la plateforme de services en périphérie (*Edge Services Platform [ESP]*) Aruba offre un vaste portefeuille d'applications et de services de réseau gérés en nuage et sur place, conjointement avec ses produits de commutation d'accès câblé et de RL sans fil. Ses activités sont géographiquement diversifiées, et Aruba dessert ses clients dans tous les marchés, des PME aux grandes entreprises. Aruba jouit d'une forte présence en matière de sécurité dans le marché des réseaux campus, et continue de faire évoluer ses capacités d'automatisation des réseaux et de visibilité des applications.

## Forces

médias sociaux. Aruba continue d'influencer les tendances de la concurrence sur le marché

## Mises en garde

# Profil d’entreprise : Cisco

## *Aperçu de l’entreprise*

**Siège social :**
San José, Californie
États-Unis

**Maturité :**
Fondation : 1984
Effectif : Environ 75 000 (2019)
Portée : Mondiale
Revenu : Environ 59,1 milliards $

## Contexte pertinent du réseau

Ses produits Catalyst et Meraki offrent une vaste gamme de services de commutation câblée d’accès, de produits RL sans fil, d’applications et services de réseau. Ses activités sont géographiquement diversifiées, et Cisco dessert des clients dans tous les marchés, des petites et moyennes entreprises (PME) aux grandes entreprises. Cisco continue d’investir dans de nouvelles puces et l’élaboration de systèmes d’exploitation qu’il est possible de mettre à profit à l’échelle de son portefeuille.

## Forces

## Mises en garde

# Profil d'entreprise : Extreme Networks

## *Aperçu de l'entreprise*

**Siège social :**
San José, Californie
États-Unis

**Maturité :**

| | |
|---|---|
| Fondation | 1996 |
| Effectif (2019) | Environ 2 750 |
| Portée | Mondiale |
| Revenu (2018) | Environ 983,1 M$ |

## Contexte pertinent du réseau

Extreme propose une vaste gamme d'applications et de services de réseau sur place et gérés en nuage, conjointement avec ses produits de commutation câblée et de RL sans fil de bout en bout. Ses activités sont géographiquement diversifiées, et Extreme Networks dessert des clients dans tous les marchés, des PME aux grandes entreprises. Extreme continue d'investir dans son architecture de microservices conteneurisés – qui permet le déploiement sur n'importe quelle plateforme en nuage (Amazon Web Services [AWS], Google Cloud Platform [GCP] et Microsoft Azure) ou sur place – ainsi que dans ses solutions destinées aux marchés verticaux.

## Forces

## Mises en garde

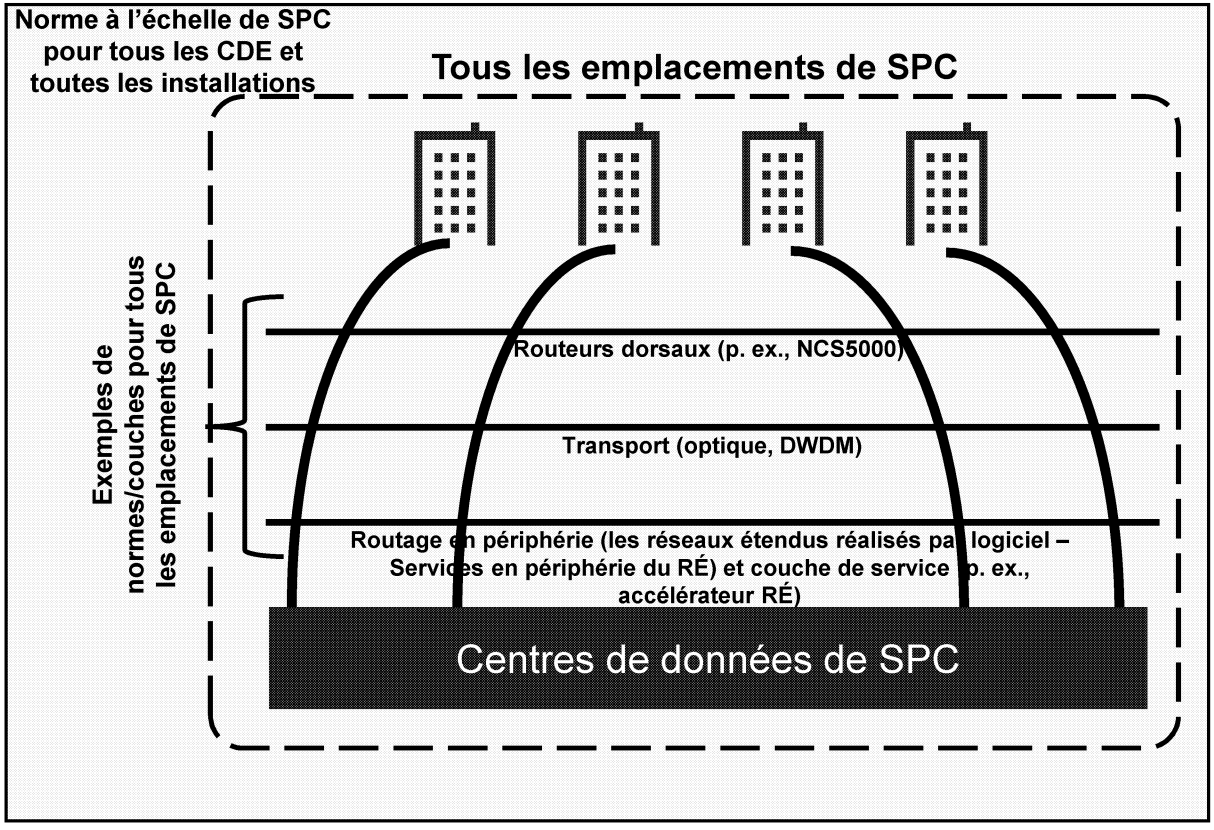
# RÉ




Gartner

# Création d'une norme technologique pour le réseau étendu (RÉ) pour tous les CDE et toutes les installations afin de soutenir la connectivité complète.

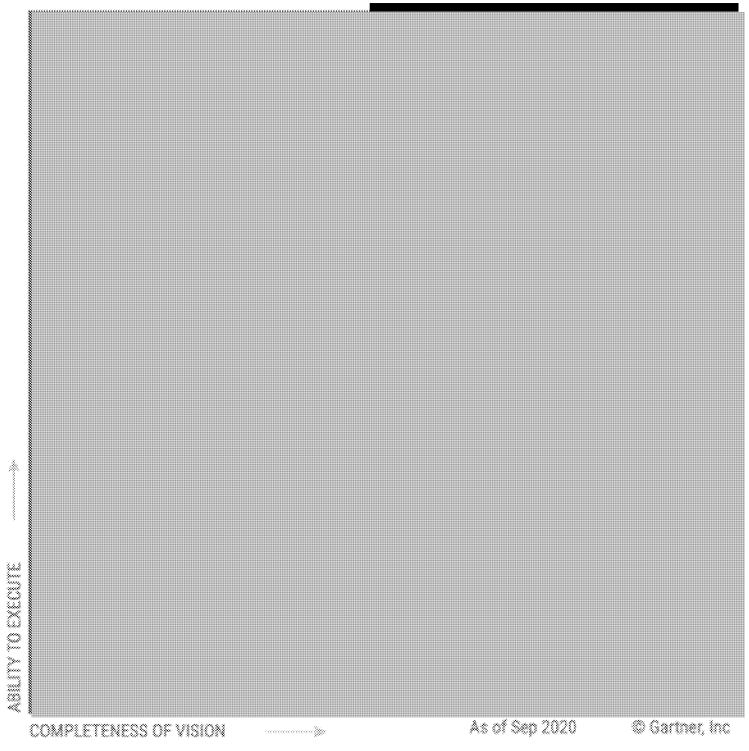
- Le RÉ s'étend sur tous les emplacements de SPC, et les **normes technologiques de RÉ doivent en tenir compte** afin de permettre une connectivité et une visibilité complètes au sein de SPC.
- Étant donné que le RÉ se compose de plusieurs couches (réseau principal, transport et périphérie/services), **on doit établir des normes technologiques à l'échelle de SPC pour chaque couche**.
- La durée de vie utile de l'équipement dans cette composante est d'**environ 5 à 7 ans**, ce qui devrait correspondre au cycle de vie des normes technologiques.



# Les principaux fournisseurs d'infrastructure en périphérie de RÉ figurent dans ce Quadrant magique de Gartner Research.

- Le résultat opérationnel fondamental est la **connectivité entre les utilisateurs, les applications et les services d'entreprise qui résident dans des emplacements répartis** (sur place et hors emplacement). Les emplacements comprennent l'administration centrale, les directions générales, les centres de données ministériels, les installations de colocation et d'hébergement, les fournisseurs de services SaaS et les fournisseurs de services infonuagiques. De plus en plus, les acheteurs exigent une capacité accrue en matière **d'agilité, d'automatisation**, d'orchestration, de souplesse et de contrôle des applications.
- Les **chefs de file** doivent démontrer une capacité soutenue à répondre aux **besoins changeants en matière** de périphérie de RÉ d'entreprise.
- **Gartner** considère les réseaux étendus réalisés par logiciel et SASE comme des technologies clés permettant d'aider les entreprises à rendre leurs réseaux agiles. **SASE répartit les fonctions** entre le lieu de travail et le nuage, et Gartner s'attend à voir plus de fonctions prises en charge dans le nuage.

**Quadrant magique Gartner Research des fournisseurs d'infrastructure en périphérie de RÉ**




**Les profils d'entreprise de chacun de ces fournisseurs figurent dans les pages suivantes.**

# Profil d’entreprise : VMware

vmware

## *Aperçu de l’entreprise*

**Siège social :**
Palo Alto, Californie
États-Unis

**Maturité :**
Fondation : 1998
Effectif : Environ 31 000 (2019)
Portée : Mondiale
Revenu : Environ 8,7 milliards $

## Contexte pertinent du réseau

Son produit porte la marque VMware les réseaux étendus réalisés par logiciel alimenté par VeloCloud, qui comprend principalement des appareils périphériques les réseaux étendus réalisés par logiciel (VCE), des passerelles (VCG) et un orchestrateur les réseaux étendus réalisés par logiciel (VCO). VMware est située en Californie, États-Unis, et Gartner estime qu’elle compte plus de 9 000 clients les réseaux étendus réalisés par logiciel. Nous nous attendons à ce que VMware investisse à l’avenir dans l’enrichissement de ses capacités de sécurité SASE, les voies d’accès multinuages, le calcul en périphérie et l’IA/AA pour améliorer l’analytique grâce à l’intégration de Nyansa.

## Forces

## Mises en garde




Gartner

# Profil d’entreprise : Fortinet

## *Aperçu de l’entreprise*

**Siège social :**
Sunnyvale, Californie
États-Unis

**Maturité :**
Fondation : 2000
Effectif : Environ 6 000 (2019)
Portée : Mondiale
Revenu : Environ 216 milliards $

## Contexte pertinent du réseau

Son offre de produit est Fortinet Secure les réseaux étendus réalisés par logiciel, qui comprend du matériel et des appareils virtuels Fortigate avec des logiciels de mise en réseau et de sécurité (FortiGuard) gérés par l’orchestrateur dans FortiManager. Nous nous attendons à ce que Fortinet investisse à l’avenir dans SASE, IA/AA pour le dépannage de SD-succursale/les réseaux étendus réalisés par logiciel, et l’orchestration en nuage/multinuage.

## Forces

## Mises en garde

# Profil d'entreprise : Versa Networks

## *Aperçu de l'entreprise*

**Siège social :**
San José, Californie
États-Unis

**Maturité :**

| | |
|---|---|
| Fondation | 2012 |
| Effectif (2019) | Environ 150 |
| Portée | Mondiale |
| Revenu | Environ 30 M$ |

### Contexte pertinent du réseau

Elle offre deux services, dont le principal est le VOS complet (anciennement FlexVNF), qu'elle peut livrer sur les passerelles de services infonuagiques Versa (CSG) ou le matériel de tierce partie, ainsi que Versa Director et Versa Analytics. La deuxième offre est Versa Titan, une solution infonuagique plus simple avec des caractéristiques natives limitées. Nous nous attendons à ce que Versa engage des investissements futurs dans SASE, le tissu multicouche et le RL réalisés par logiciel (SD-LAN) de campus.

## Forces

## Mises en garde

# Profil d’entreprise : Cisco

## *Aperçu de l’entreprise*

**Siège social :**
San José, Californie
États-Unis

**Maturité :**
Fondation : 1984
Effectif : Environ 75 000 (2019)
Portée : Mondiale
Revenu : Environ 59,1 milliards $

## Contexte pertinent du réseau

Elle dispose d’une offre de marque Cisco les réseaux étendus réalisés par logiciel alimenté par Viptela, qui comprend le logiciel Viptela OS ou IOS XE avec orchestration vManage. L’autre est Cisco les réseaux étendus réalisés par logiciel, alimenté par Meraki, qui comprend des appareils MX et des logiciels avec orchestration. On peut déployer facultativement Cisco Umbrella en vue de capacités de sécurité infonuagique enrichies. Nous nous attendons à ce que Cisco effectue des investissements futurs dans l’enrichissement des capacités de sécurité, l’augmentation de la visibilité du nuage, et l’utilisation de l’apprentissage automatique pour optimiser le rendement.

## Forces

## Mises en garde

# Profil d'entreprise : Palo Alto Networks

## *Aperçu de l'entreprise*

**Siège social :**
Santa Clara, Californie
États-Unis

**Maturité :**
Fondation : 2005
Effectif : Environ 7 000 (2019)
Portée : Mondiale
Revenu : Environ 3,4 milliards $

### Contexte pertinent du réseau

Son offre est le les réseaux étendus réalisés par logiciel CloudGenix avec dispositifs périphériques ION et Prisma Access en option pour une sécurité intégrée avancée. Palo Alto Networks a fait l'acquisition de CloudGenix au cours de la dernière année. Nous nous attendons à ce que Palo Alto Networks réalise des investissements futurs dans de nouveaux facteurs de forme, SD-succursale, SASE, l'automatisation et une visibilité accrue.

## Forces

## Mises en garde




Gartner

# Profil d'entreprise : Silver Peak Networks

## *Aperçu de l'entreprise*

**Siège social :**
Santa Clara, Californie
États-Unis

**Maturité :**
Fondation : 2004
Effectif : Environ 400 (2020)
Portée : Mondiale
Revenu : Environ 20,2 M$ pour le premier trimestre de 2019

## Contexte pertinent du réseau

Ses produits comprennent la plateforme les réseaux étendus réalisés par logiciel périphérique Unity EdgeConnect, composée de Unity Orchestrator, d'appareils EdgeConnect, et d'une fonction Unity Boost en option qui permet d'optimiser le réseau étendu. Nous nous attendons à ce que Silver Peak engage des investissements futurs dans le perfectionnement de l'analytique afin d'améliorer le dépannage, la visibilité et la sécurité, et orchestre des solutions de sécurité de tierces parties.

Nota : Le 13 juillet 2020, HPE a annoncé son intention d'acquérir Silver Peak. La présente recherche n'englobe pas les retentissements de cette acquisition, parce qu'elle s'est produite après la date limite de l'analyse. Cette entreprise fait maintenant partie de la filiale Aruba Networks de HPE depuis septembre 2020.

## Forces

## Mises en garde

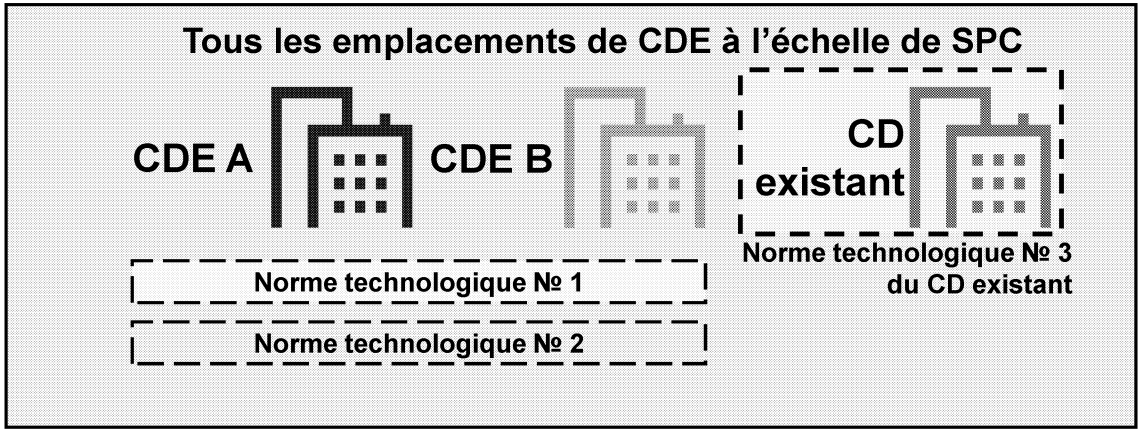
# Réseaux de centres de données (RCD)




Gartner

# SPC doit établir deux normes technologiques pour le RCD de ses CDE afin de promouvoir la concurrence et l'innovation.

- Étant donné que les **charges de travail des partenaires du GC sont réparties entre au moins deux CDE** et que, pour des impératifs liés aux opérations, à la sécurité et à la prise en charge, il est primordial que la charge de travail d'un partenaire donné soit gérée sur un RCD ayant une seule norme technologique, SPC doit établir des normes technologiques qui s'appliquent à tous les CDE.
- Une **stratégie reposant sur deux fournisseurs est toutefois souhaitable** pour encourager des prix concurrentiels et l'innovation. À cette fin, SPC doit envisager d'établir **deux RCD dans tous ses CDE**, chacun fondé sur une norme technologique **établie de façon concurrentielle**.
- Au fil du temps**,** les charges de travail des partenaires du GC seront réparties aussi uniformément que possible entre les deux RCD.

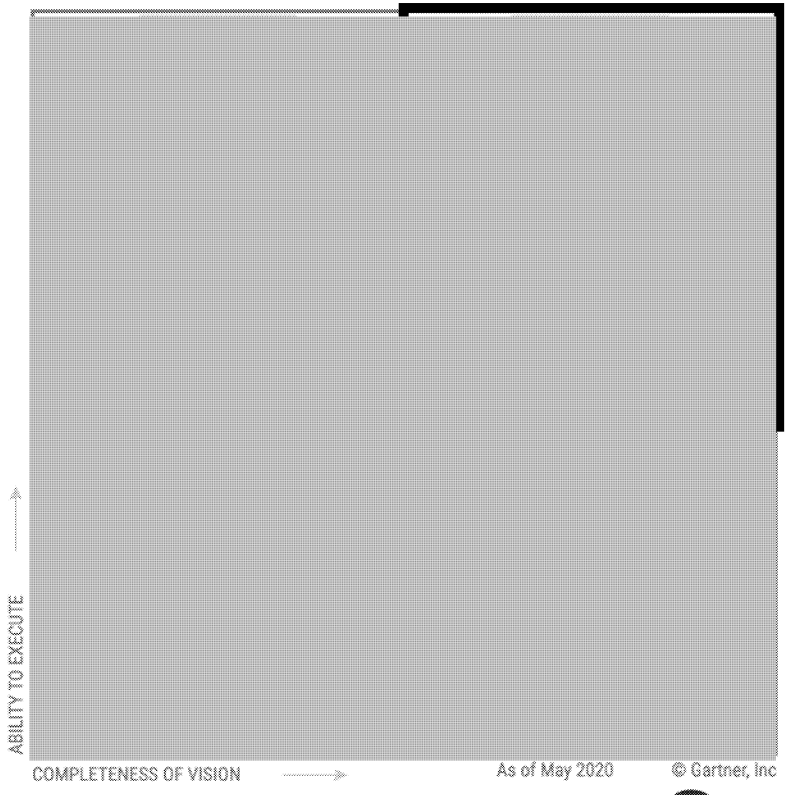



- Étant donné que les deux normes technologiques des RCD se concurrencent, SPC doit envisager des propositions de fournisseurs uniques, ainsi que des propositions conjointes qui pourraient comprendre des fournisseurs distincts superposés et sous-jacents.
- La norme technologique établie pour chaque **centre de données existant** aura ses propres paramètres, qui pourra s'appliquer à un centre de données secondaire où la charge de travail couvre plusieurs CD.
- La durée de vie utile de l'équipement dans cette composante est d'environ 5 à 7 ans, ce qui devrait s'harmoniser avec le cycle de vie des normes technologiques.

# Ce Quadrant magique de Gartner Research expose les principaux fournisseurs de réseaux de centres de données.

- Le principal résultat opérationnel de l'utilisation des services d'un fournisseur de réseaux est la **connectivité du réseau local au sein des centres de données d'entreprise** pour prendre en charge les **environnements infonuagiques et** assurés de manière automatisée avec la gestion centrale. Ces environnements sont hautement virtualisés (habituellement 80 %) et de plus en plus conteneurisés (souvent 10 % et en croissance).
- Les **chefs de file** doivent démontrer une capacité soutenue à répondre aux exigences changeantes du réseau pour les centres de données d'entreprise qui **sous-tendent les infrastructures infonuagiques et prêtes pour l'infonuagique, y compris un portefeuille de produits complet.**
- En ce qui a trait à l'**état souhaité**, les principaux aspects d'intérêt comprennent le soutien pour : l'automatisation, y compris l'harmonisation avec **DevOps** et l'infrastructure en qualité de principes de code (IaC), l'infrastructure hyperconvergente, Kubernetes et les conteneurs, et la **mise en réseau multinuagique**.

**Quadrant magique de Gartner Research des principaux fournisseurs de réseaux de centres de données**




**Les profils d'entreprise de chacun de ces fournisseurs figurent dans les pages suivantes.**

# Profil d'entreprise : Cisco

## *Aperçu de l'entreprise*

**Siège social :**
San José, Californie
États-Unis

**Maturité :**
Fondation : 1984
Effectif : Environ 75 000 (2019)
Portée : Mondiale
Revenu : Environ 59,1 milliards $

## Contexte pertinent du réseau

Son offre comprend la gestion du tissu par l'intermédiaire de l'*Application Policy Infrastructure Controller (APIC)* (« contrôleur de l'infrastructure des politiques en matière d'applications ») ou du *Data Center Network Manager (RCDM)* (« gestionnaire du réseau des centres de données »), des commutateurs Nexus et des outils associés, y compris le *Network Assurance Engine (NAE)* (« moteur d'assurance des réseaux ») et Network Insights. Nous nous attendons à ce que Cisco effectue des investissements continus pour étendre l'analytique et l'assurance, et enrichir les offres multinuagiques existantes.

## Forces

## Mises en garde

# Profil d'entreprise : Arista Networks

ARISTA

## *Aperçu de l'entreprise*

**Siège social :**
Santa Clara, Californie
États-Unis

**Maturité :**
Fondation : 2004
Effectif : Environ 2 300 (2019)
Portée : Mondiale
Revenu : Environ 2,41 milliards $

### Contexte pertinent du réseau

Son offre est le *Universal Cloud Network (UCN)*, qui comprend les commutateurs de série 7000, le système d'exploitation extensible (EOS) et la plateforme de gestion et de visibilité CloudVision. Nous nous attendons à ce qu'Arista continue d'investir dans la prestation de services infonuagiques et l'enrichissement de la sécurité.

## Forces

## Mises en garde




Gartner

# Profil d’entreprise : Juniper Networks

## *Aperçu de l’entreprise*

**Siège social :**
Sunnyvale, Californie
États-Unis

**Maturité :**
Fondation : 1996
Effectif : Environ 9 400 (2019)
Portée : Mondiale
Revenu : Environ 4,4 milliards $

### Contexte pertinent du réseau

Son offre principale dans ce marché comprend les commutateurs de séries QFX5000 et QFX10000, Junos OS et Contrail Enterprise Multicloud. Nous nous attendons à ce que Juniper engage des investissements continus qui amplifieront le rendement des appareils et composants Mist pour accroître l’autonomie du réseau, perfectionner la gestion en nuage et alimenter les améliorations de 400 Gb/sec.

## Forces

## Mises en garde

# Profil d'entreprise : VMware

vmware

## *Aperçu de l'entreprise*

**Siège social :**
Palo Alto, Californie
États-Unis

**Maturité :**
Fondation : 1998
Effectif : Environ 31 000 (2019)
Portée : Mondiale
Revenu : Environ 8,7 milliards $

## Contexte pertinent du réseau

Son offre vedette sur ce marché comprend NSX-T, un logiciel de superposition de réseau, et vRealize Network Insight (vRNI) pour la gestion et le dépannage. Nous nous attendons à ce que VMware continue d'investir dans les domaines de la gestion des superpositions et des calques sous-jacents, de la sécurité, et des capacités de prévision.

Nota : Gartner fait remarquer que Vmware se trouve en fait dans le quadrant visionnaire de son analyse du Quadrant magique, mais comme il est un chef de file en RÉ, on doit l'inclure dans cette analyse.

## Forces

## Mises en garde




Gartner

01 | **Sommaire de gestion**

02 | **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 | **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 | **Analyse de cas d'approvisionnement**

05 | **Annexe**




Gartner

# Gartner a analysé des cas d'approvisionnement pour mieux comprendre l'approche relative à la sélection des fournisseurs de réseau de SPC et formuler des recommandations pour améliorer le processus.

## Cas sélectionnés

**Gartner a examiné les cas d'approvisionnement suivants pour trouver des renseignements sur les activités actuelles relatives à la sélection de fournisseurs de RL, de RÉ et de RCD.**

**1)** [redacted] **–** Mise à niveau du RÉ et principale composante du RCD

**2) Centre de données CCM/CDSL** [redacted] **-** Migration de la charge de travail au CDE

**3) Lester B. Pearson –** RL de l'immeuble, phase 1

## Processus/Analyse

- Examen de la documentation
- Comprendre les solutions de rechange
- Utiliser l'arbre de décision pour la sélection de fournisseurs de réseau
- Validation avec Gartner Research
- Documentation des constats

## Résultat

Recommandations pour les cas d'approvisionnement et les futurs approvisionnements liés aux réseaux fondées sur l'arbre de décision pour la sélection des fournisseurs de réseau.

Documentation de la justification et de l'incidence quantitative prise en charge pour les situations où l'on ne suit pas l'arbre de décision pour la sélection de fournisseurs de réseau.




Gartner

# Sommaire des cas d'approvisionnement

| | Observations | Recommandations |
|---|---|---|
| **CDE** [redacted] Mise à niveau du RÉ et principale composante du RCD | ▪ Les composantes du RÉ requièrent une légère mise à niveau progressive (moins de 15 % de l'infrastructure du RÉ de SPC au cours d'un exercice financier et l'ajout de cartes de ligne dans les empreintes existantes).<br>▪ Les composantes du RCD font l'objet d'un processus d'approvisionnement pour la création d'une nouvelle principale composante de réseau net au CDE [redacted] où l'on n'a pas encore établi de norme technologique pour le RCD par voie de concurrence. | ▪ En se fondant sur la matrice de décision, Gartner recommande d'aller de l'avant avec l'acquisition d'équipement de RÉ propre au FÉO par l'intermédiaire du mécanisme de passation de marchés de la CASR. *<br>▪ En se fondant sur la matrice de décision, Gartner recommande d'aller de l'avant avec l'acquisition d'équipement de RCD propre au FÉO par l'intermédiaire du mécanisme de passation de marchés de la CASR. * |
| Migration de la charge de travail du **centre de données CCM/CDSL** [redacted] au CDE | ▪ Légère mise à niveau progressive du RÉ pour le système et SPC peut tirer parti de l'empreinte existante.<br>▪ Importants besoins en RCD et absence d'une norme technologique établie de manière concurrentielle. | ▪ En se fondant sur la matrice de décision, Gartner recommande d'aller de l'avant avec l'acquisition d'équipement de RÉ propre au FÉO par l'intermédiaire du mécanisme de passation de marchés de la CASR. * |
| **Réseau local de l'édifice Lester B. Pearson**, phase 1 | ▪ Ce cas d'approvisionnement concerne un processus d'approvisionnement qui a eu lieu en 2020, pour l'équipement lié à la composante du RL, tel que le définit la section Outil d'aide à la décision pour la sélection de fournisseurs de réseaux.<br>▪ Importante mise à jour de l'équipement d'un immeuble où l'on n'a établi aucune norme technologique durant les quelques dernières années. | ▪ En se fondant sur la matrice de décision, Gartner recommanderait un processus d'approvisionnement ouvert et concurrentiel pour les besoins en RCD. Toutefois, compte tenu des répercussions opérationnelles considérables associées à un processus d'approvisionnement ouvert et concurrentiel dans ce cas, on s'attend à ce que SPC procède plutôt à un approvisionnement propre au FÉO par l'entremise de la CASR, afin d'éviter ce qui suit :<br>  ▪ un revers financier estimé entre 31,5 M$ et 51 M$;<br>  ▪ des retards excessifs (de 12 à 24 mois) dans le cadre de ces projets cruciaux; et<br>  ▪ d'importantes répercussions potentielles sur ces organismes et leurs services.<br>▪ L'approche que suit SPC se conforme aux recommandations de Gartner qui se trouvent dans la section Outil d'aide à la décision pour la sélection de fournisseurs de réseaux et établit la norme technologique pour le RL dans cet immeuble/campus pour les 10 prochaines années. |

* Évaluer parmi les fournisseurs qualifiés dans le cadre de la CASR, qui était un appel d'offres ouvert et concurrentiel établissant un mécanisme d'approvisionnement pour l'équipement et les services de réseau.

# Évaluation des possibles répercussions si possibles si un appel d'offres concurrentiel était organisé plutôt qu'un processus d'approvisionnement fondé sur FÉO par l'entremise de la CASR pour le cas d'approvisionnement 2 : Migration de la charge de travail du centre de données CCM/CDSL ( au CDE

| Domaine | Répercussions quantifiées | Coûts estimatifs |
|---|---|---|
| **Équipe et compétences** | ▪ La difficulté de trouver des compétences spécialisées en TI dans cet environnement entraînera des problèmes pour SPC lorsqu'il s'agira de combler les postes requis afin d'assumer une charge de travail supplémentaire. Il faudrait doubler l'effectif de l'équipe actuelle pour les nouvelles technologies.<br>▪ Incidence sur l'équipe avec les problèmes associés à la COVID-19 et la charge de travail actuelle pour prendre en charge le travail supplémentaire requis en vue d'une DP concurrentielle. | ▪ Environ 2 M $ Employés à temps plein (ETP)<br>▪ Environ 2,5 M $ Services professionnels Opérations du RCD (x2 Sécurité) |
| **Technique et architecture** | ▪ Problèmes d'interopérabilité entre l'état actuel des données et le futur fournisseur<br>▪ Coûts irrécupérables – On a déjà acquis auprès du fournisseur actuel des unités de stockage, du matériel informatique et des logiciels, qui demeureraient inutilisés pendant 12 à 24 mois si une DP concurrentielle est requise. | ▪ Environ 20 M $ par année en coûts irrécupérables |
| **Présentation au CT** | ▪ La mise à jour complète de la présentation au CT nécessiterait jusqu'à un an pour achever le processus.<br>▪ Le pointage de l'ÉCRP augmenterait de 2 à 3, ce qui alourdirait les formalités et repousserait l'échéance d'achèvement de cette phase des travaux. | Prolongation du délai : 12 mois |
| **Mise à l'essai** | ▪ Le détournement des ressources pour la mise à l'essai du nouveau système causerait de multiples interruptions dans la mise en œuvre d'autres projets; plusieurs domaines, plusieurs gammes de services (ordinateur central, milieu de gamme, stockage, installations, réseau, sécurité/ATE).<br>▪ Incidence opérationnelle d'une période de changement restreinte de décembre à avril<br>▪ Délai de mise à l'essai prolongé d'au moins environ 8 mois pour vérifier l'intégration complète et réussie du réseau. | Prolongation du délai : 8 mois |
| **Coûts de possession pour les installations** | ▪ Coûts du CCM/CDSL engagés pour l'électricité, le soutien et l'entretien. Il est impossible de prolonger le bail du CDSL au-delà de mai 2024, à défaut de quoi SPC pourrait faire face à des poursuites judiciaires.<br>▪ est actuellement une salle de données vide en attente de nouvelles opérations; cette capacité resterait inutilisée durant 12 à 24 mois.<br>▪ Coût incrémentiel d'électricité et de refroidissement du CDE de deux fois plus élevé que celui de On estime la croissance de cette installation à environ 10 % par année. | ▪ CDSL : 4,5 M $ par année<br>▪ Barrie : 2,5 M $ par année |
| **Risques** | ▪ Cyberattaques à l'endroit des réseaux vieillissants<br>▪ Les contrats existants subiraient des répercussions en cascade, car on a dressé le plan d'approvisionnement au début du projet avec des composants conçus pour fonctionner ensemble.<br>▪ Incapacité de soutenir la croissance de la charge de travail axée sur les activités opérationnelles | Information non disponible |

Source : SPC

# Analyse détaillée des cas d’approvisionnement

# Cas d'approvisionnement 1 : CDE [redacted] – Mise à niveau du RÉ et principale composante du RCD (page 1 de 3)

| Description | Documents examinés |
|---|---|
| Achat d'équipement de réseau pour ajouter des cartes de ligne optique à ondes longues de 10 Go dans l'empreinte actuelle de Cisco NCS2000 DWDM, ainsi que les licences logicielles connexes, les licences de chiffrement de réseau, les panneaux de raccordement et les câbles à fibre optique.<br><br>La nomenclature comprend également des modules 100GE de 30 ports et 10GbE de 48 ports pour les commutateurs de centre de données Nexus 7700 de Cisco existants, ainsi que l'acquisition de nouveaux commutateurs de port Nexus 9300 48+6 de Cisco avec les SFP et émetteurs-récepteurs associés.<br><br>Cet équipement sera installé aux CDE de [redacted] afin d'assurer un connectivité chiffrée de CD à CD entre les deux centres de données, ainsi que la prise en charge de RCD de base pour le CDE de [redacted] | ▪ Bill Of Materials EDC [redacted] Annex_A_-_LoD_-_R000073858_-_FR.xlsx<br>▪ IPS_-_Technical_Justification_-_EDC [redacted] _Optical_73858.pdf |

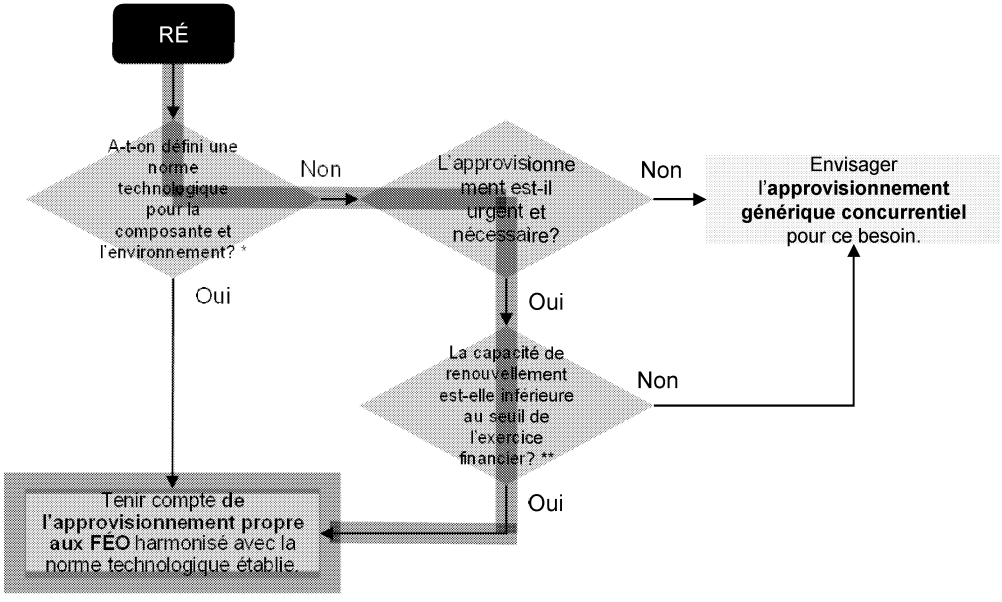
| Solution(s) de rechange |
|---|
| 1. Acquérir de l'équipement de RÉ au moyen d'un processus d'approvisionnement ouvert. Cela pourrait entraîner l'adoption d'une autre technologie utilisée par le fournisseur, ce qui nécessiterait une nouvelle empreinte de DWDM et ne permettrait pas d'utiliser la capacité restante de Cisco NCS2000 (tablettes vides). De plus, cela imposerait l'adoption de nouveaux outils et processus de soutien, et exigerait la prestation de formation et des essais.<br>2. Diviser les approvisionnements liés au RÉ (Cisco NCS2000) et au RCD (Cisco Nexus) de façon qu'on les acquière séparément, conformément aux normes établies en matière de RÉ et de RCD. |

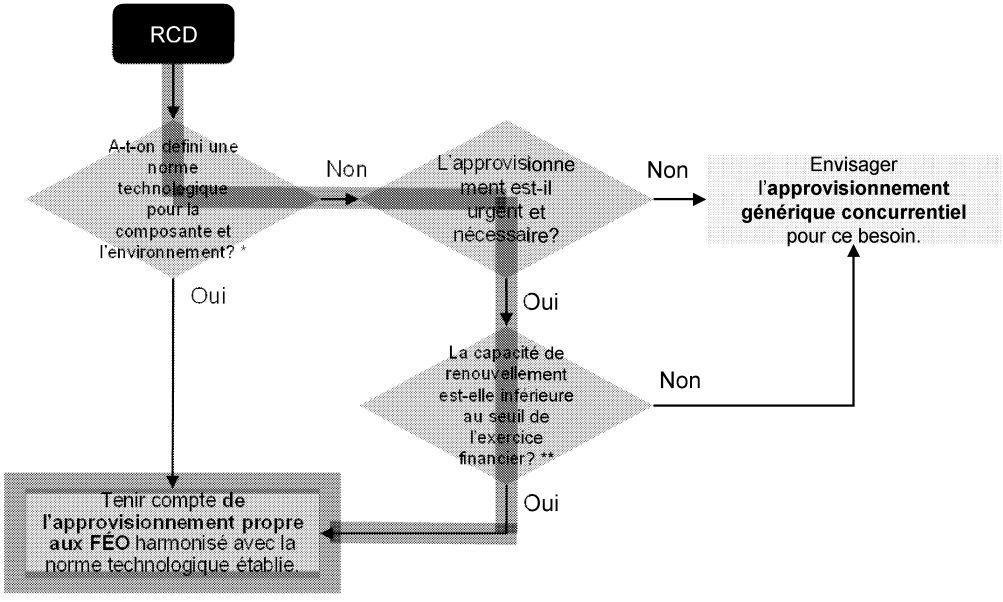
# Cas d'approvisionnement 1 : CDE [redacted] - Mise à niveau du RÉ et principale composante du RCD (page 2 de 3)

| Constats | Recommandations |
|---|---|
| Cet achat s'appuie surtout sur les cadres existants des CDE de [redacted] à l'exception des nouveaux Nexus 7000 et 9300. | Envisager un approvisionnement propre au FÉO tant pour les composants de RÉ de CD, selon la compatibilité existante, que pour les composants de RCD, d'après la compatibilité et l'intégration avec l'équipement de RCD existant du CDE de [redacted] |
| L'équipement de RÉ doit absolument être identique aux deux extrémités, ce qui oblige à prendre d'autres décisions d'approvisionnement auprès d'un fournisseur unique. | Envisager d'établir une norme de RÉ à l'échelle de SPC (tous les CDE et grandes installations) par voie d'un processus d'approvisionnement ouvert. |
| **Commentaires globaux** | |
| Utiliser une capacité inexploitée en remplissant des étagères ou des fentes vides avec de l'équipement existant constitue la manière la plus rentable et viable de répondre à ce besoin. Étant donné que les composants de RCD acquis dans le cadre de ce processus d'approvisionnement représentent une modeste mise à niveau (revenant à environ 5 % de la capacité en RCD établie avant l'exercice financier 2020-2021), un approvisionnement propre au FÉO se révèle un moyen efficient et efficace de répondre à ce besoin. | |

# Cas d'approvisionnement 1 : CDE [redacted] - Mise à niveau du RÉ et principale composante du RCD (page 3 de 3)

Figurent ci-dessous les cheminements et recommandations pour ce cas d'approvisionnement, fondés sur l'arbre de décision pour la sélection de fournisseurs de réseau.



# Cas d'approvisionnement 2 : Migration de la charge de travail du centre de données du CCM/CDSL [redacted] au CDE (page 1 de 3)

| Description | Documents examinés |
|---|---|
| SPC a commencé à consolider ses 800 centres de données en sept nouveaux centres de données d'entreprise (CDE). Dans le cadre de cet effort, la charge de travail de [redacted] actuellement hébergée dans l'ancien centre de données du CDSL subira sa migration aux centres de données d'entreprise (CDE) situés à [redacted] et à [redacted] À cette fin, il faut acquérir de nouvelles infrastructures aux CDE cible, y compris le RE (liens entre les centres de données et technologie d'optimisation des données) et l'équipement de réseautage des centres de données (RCD). SPC a déclaré que cette nouvelle infrastructure devra être compatible avec les solutions existantes déployées aux CDE de [redacted]<br><br>Les exigences comprennent l'approvisionnement en un seul point, le déploiement du micrologiciel central, l'automatisation de l'architecture multilocataire et de la virtualisation, le déploiement automatique du tissu, le contrôle d'accès détaillé en fonction des rôles (CAFR) et la compatibilité multiemplacement.<br><br>SPC a sélectionné des produits Cisco et Riverbed sur la base de leur compatibilité avec l'infrastructure existante. | ▪ Bill Of Materials WLM CCM [redacted] Riverbed_P2P 71968.xlsx<br>▪ Bill Of Materials WLM CCM [redacted] WAN CIsco_R000073361_-FR.xlsx<br>▪ WLM CCM (DCSL) Legacy DC Closure — RCD [redacted] _P2P 70268.xlsx<br>▪ IPS_-_Technical Justification_-_Encryption P2P 73361 WLM CCM [redacted] WAN Cisco.pdf<br>▪ technical-justification_for_Riverbed_Data_Centres WLM CCM [redacted] P2P 71968.pdf<br>▪ WLM CCM (DCSL) Legacy DC Closure [redacted] RCD Tech JUSTIFICATION P2P 70268.pdf |

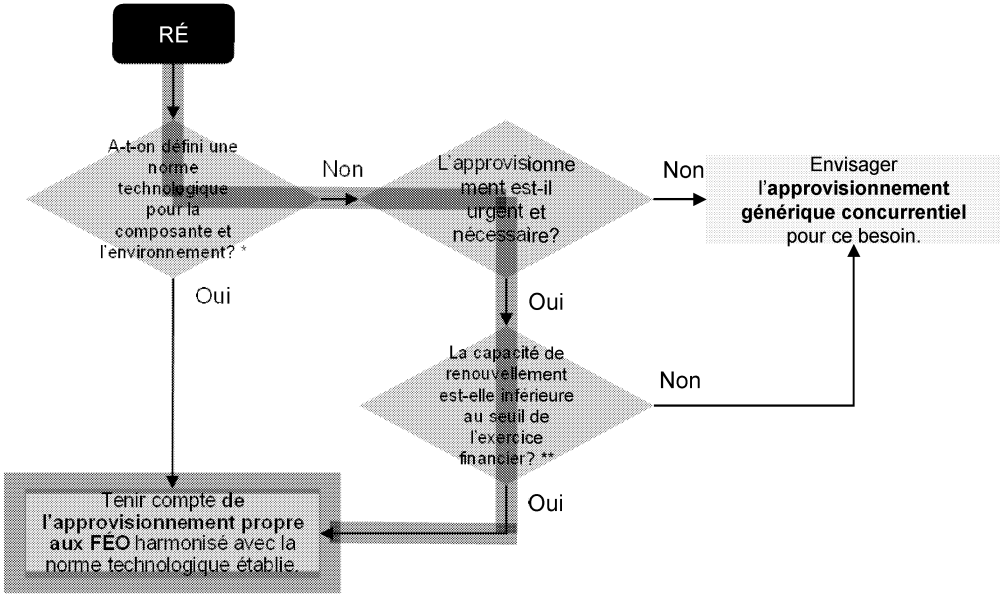
| Solution(s) de rechange |
|---|
| 1. Acquérir l'équipement par voie d'un processus d'approvisionnement ouvert pourrait entraîner le choix d'une autre solution. Choisir une solution de rechange entraînerait des coûts de formation, de mise à l'essai et d'exploitation supplémentaires et accroîtrait les risques opérationnels.<br>2. Fractionner les approvisionnements liés au RÉ (Cisco et Riverbed) et au RCD (Cisco Nexus) de façon qu'on les acquière séparément, conformément aux normes établies en matière de RÉ et de RCD. |

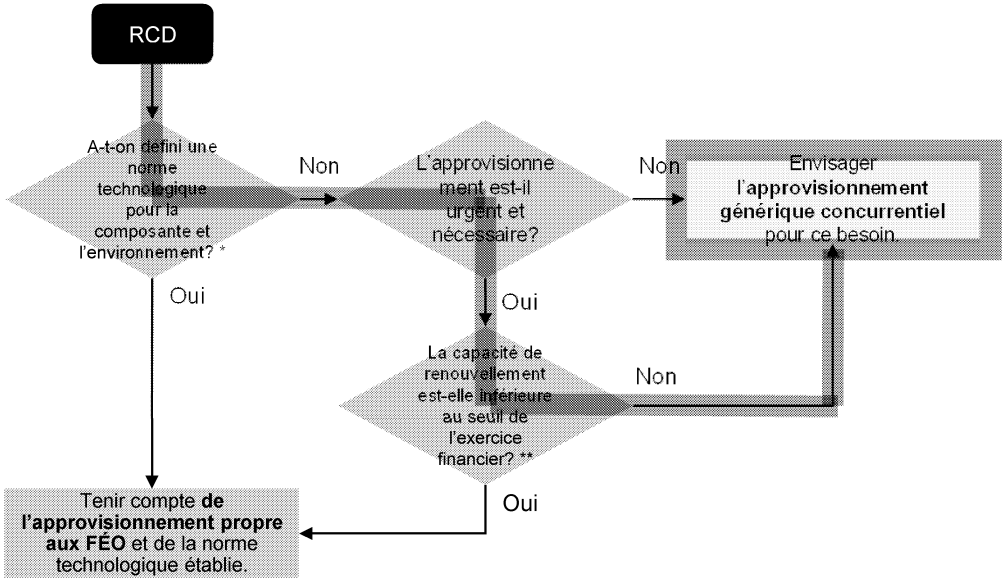
# Cas d'approvisionnement 2 : Migration de la charge de travail du centre de données du CCM/CDSL [redacted] au CDE (page 2 de 3)

| Constats | Recommandations |
|---|---|
| Les composants du RÉ, y compris les dispositifs Riverbed, doivent absolument s'intégrer à l'infrastructure existante du RÉ dans d'autres emplacements du GC. | • Envisager l'acquisition spécifique au FÉO des composants de RÉ d'après la compatibilité existante.<br>• Envisager la possibilité de lancer un appel d'offres pour les composants de RCD de la présente commande. |
| Dans cette vaste empreinte de RL de CD comportant au-delà de 50 commutateurs, plus de 90 % des connexions réseau sont internes et il n'y a qu'une connexion limitée à l'infrastructure existante externe. Vu l'ampleur de cette commande, SPC pourrait mettre sur pied une équipe distincte de soutien à la solution.<br><br>Un appel d'offres ouvert devrait reconnaître la valeur opérationnelle de continuer d'utiliser l'ancienne technologie de fournisseur, mais une solution de fournisseur unique peut ne pas être une exigence dure et difficile. | Établir une norme à l'échelle de SPC pour tous les CDE et toutes les grandes installations qui prescrit les règles pour les composants à fournisseur unique sur les bases du coût relatif d'entretien et de la nécessité d'intégration aux solutions existantes. |
| **Commentaires globaux** | |
| SPC doit définir un processus clair, transparent et détaillé pour justifier l'acquisition de solutions auprès d'un fournisseur unique, au-delà de cet approvisionnement. | |

# Cas d'approvisionnement 2 : Migration de la charge de travail du centre de données du CCM/CDSL ( ) au CDE (page 3 de 3)

Figurent ci-dessous les cheminements et recommandations pour ce cas d'approvisionnement, fondés sur l'arbre de décision pour la sélection de fournisseurs de réseau.



# Cas d'approvisionnement 3 : RL de l'édifice Lester B. Pearson, phase 1 (page 1 de 2)

| Description | Documents examinés |
|---|---|
| Le siège social d'Affaires mondiales Canada (AMC), situé au 125, promenade Sussex, à Ottawa, est connu sous le nom d'édifice Lester B. Pearson (LBP). Le bâtiment fait l'objet d'un projet de remise à neuf pluriannuel, qui a commencé avec la tour D en 2020. Services partagés Canada (SPC) mettra en œuvre une nouvelle infrastructure de RL dans le cadre de ce projet de modernisation.<br><br>SPC a présenté une demande de propositions fondée sur des exigences techniques sans parti pris particulier à l'égard de la technologie d'un fournisseur donné. | ▪ Annex A — SOW — Generic R000070124.docx<br>▪ ANNEX B GENERIC BOM — LoD — Generic R000070124.xlsx<br>▪ Annex C — SoR — Generic R000070124.xlsx<br>▪ Annex D — ITP — Generic R000070124.xlsx<br>▪ Annex E — Test Results — Generic R000070124.xlsx |

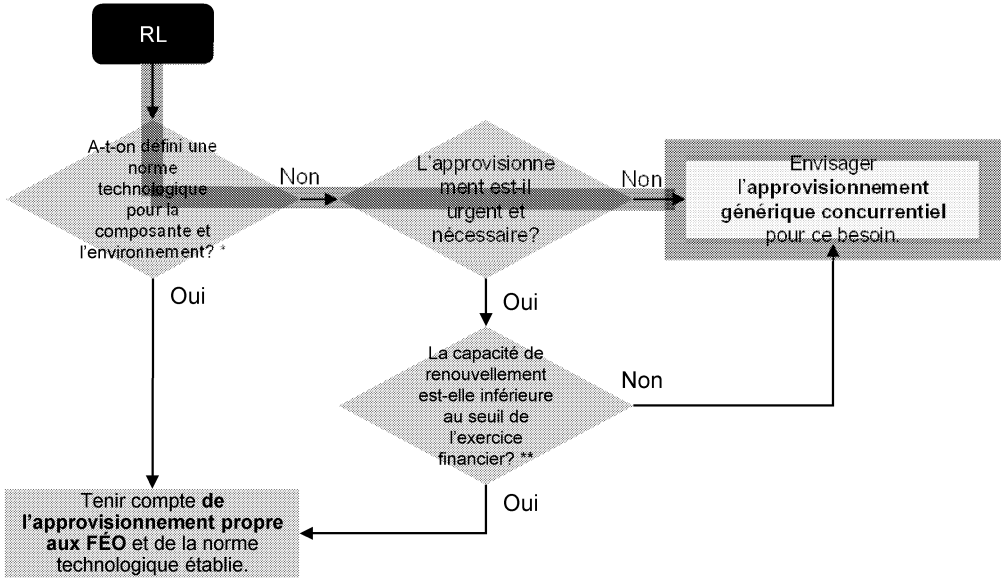
| Solution(s) de rechange |
|---|
| 1. SPC aurait pu définir l'équipement Cisco comme une exigence fondée sur la compatibilité avec d'autres emplacements semblables du GC. Toutefois, cette approche aurait limité la diversité des soumissionnaires, réduit la qualité des options. De plus, le nombre restreint de soumissionnaires aurait pu entraîner une augmentation du coût de la solution totale. |

| Constats | Recommandations |
|---|---|
| SPC a créé un processus d'appel d'offres concurrentiel qui permet la comparaison directe des solutions des fournisseurs, y compris l'utilisation d'équipement de FÉO. | Le processus utilisé pour l'édifice Lester B. Pearson doit s'appliquer à d'autres projets de RL de bâtiment autonomes. |

| Commentaires globaux |
|---|
| La mise en place d'un processus d'appel d'offres ouvert aide SPC à examiner les solutions concurrentielles et à choisir la meilleure solution au meilleur prix. Une norme technologique propre à chaque immeuble (ou campus) établie par voie d'un processus d'approvisionnement concurrentiel se classe très haut sur les plans de la transparence, de l'équité et de la valeur, tout en réduisant au minimum les soucis d'interopérabilité technique. |

# Cas d'approvisionnement 3 : RL de l'édifice Lester B. Pearson, phase 1 (page 2 de 2)

Voici les cheminements et recommandations pour ce cas d'approvisionnement, fondés sur l'arbre de décision pour la sélection de fournisseurs de réseau.



01 | **Sommaire de gestion**

02 | **Examen comparatif de la stratégie en matière de réseau et de sécurité de SPC**

- Contenu global
- Activités
- Concepts de communication
- Document de discussion

03 | **Outil d'aide à la décision pour la sélection de fournisseurs de réseaux**

- Point de vue des intervenants
- Définition du RL, du RÉ et du RCD
- Normes relatives à la technologie et fournisseurs

04 | **Analyse de cas d'approvisionnement**

05 | **Appendice 1**



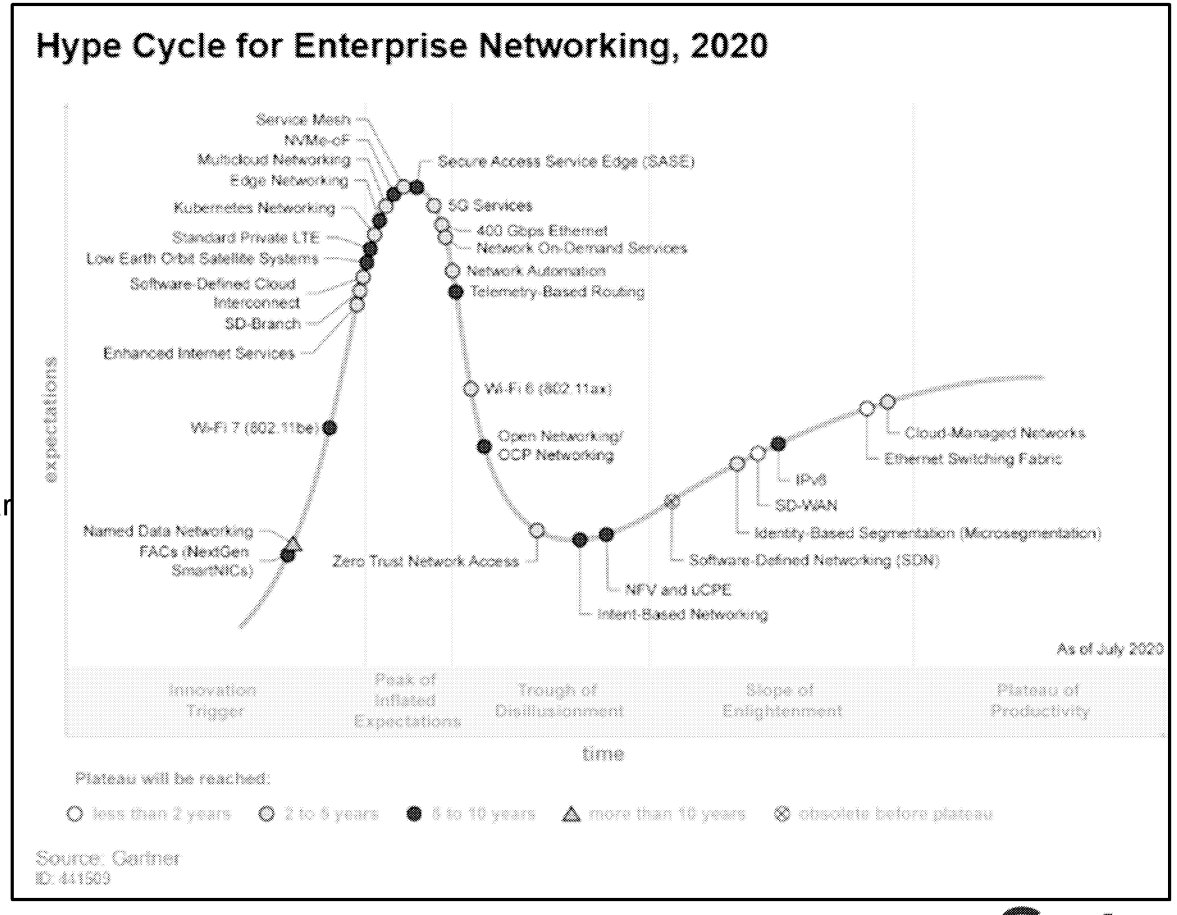

Gartner

# Gartner Research

# Perspectives sur les solutions émergentes

# Gartner Research—Cycle publicitaire (*Hype Cycle*) pour le réseautage en entreprise

- La stratégie en matière de réseau et de sécurité de SPC comprend les technologies abordées par Gartner;
  - SASE
  - Services 5G
  - Wi-Fi 6 (IEEE 802.11ax)
  - Accès au réseau moyennant vérification systématique (ARMVS) (confiance zéro)
  - Réseau défini par logiciel (les réseaux définis par des logiciels)
  - Segmentation fondée sur le justificatif
  - RÉ défini par logiciel (les réseaux étendus réalisés par logiciel)



# Stratégie en matière de réseau et de sécurité de SPC – Recherches sur les technologies par Gartner Research

| Solution | Gartner Research |
|---|---|
| SASE | ▪ D'ici 2024, au moins 40 % des entreprises posséderont des stratégies explicites pour adopter le SASE, contre moins de 1 % à la fin de 2018. |
| 5G | ▪ Déterminer les possibilités de mise à l'essai pilote des réseaux et services 5G pour offrir de l'innovation, sur la base des capacités actuelles en 5G. |
| Wi-Fi 6 | ▪ Le Wi-Fi 6 (802.11ax) représente une occasion d'améliorer substantiellement le rendement pour les cas d'approvisionnement spéciale. |
| Accès au réseau moyennant vérification systématique (ARMVS) (confiance zéro) | ▪ Les avantages de l'ARMVS sont immédiats. À l'instar d'un RPV traditionnel, les services fournis dans un environnement ARMVS sont invisibles dans Internet public et, donc, protégés des attaquants. |
| Réseau défini par logiciel (les réseaux définis par des logiciels) | ▪ Le marché n'a pas notablement adopté les véritables solutions les réseaux définis par des logiciels. Consultez les détails de la recommandation de Gartner à la diapositive X. |
| Réseau étendu défini par logiciel | ▪ Actualiser l'équipement de RÉ des directions générales en mettant en œuvre le réseau étendu réalisé par logiciel dans le cadre de la migration des applications vers le nuage public, en créant des RÉ hybrides; également lorsque l'équipement a atteint la fin de sa vie utile, ou lorsque les contrats de service réseau/MPLS gérés arrivent à renouvellement. |
| Segmentation fondée sur le justificatif | ▪ La segmentation fondée sur le justificatif est une forme de réseau fonctionnant par vérification systématique (confiance zéro) et sert à réduire l'étendu des dommages lorsqu'un pirate pénètre le réseau de l'entreprise, en réduisant la capacité de la menace à se propager latéralement. Il permet également aux entreprises de mettre à exécution des politiques de segmentation uniformes dans l'ensemble des charges de travail sur place et en nuage. |

# Gartner Research – SASE

- **Définition** *Secure Access Service Edge* (SASE, prononcé « sassy ») offre de multiples capacités telles que les réseaux étendus réalisés par logiciel, SWG, CASB, NGFW et l'accès au réseau moyennant vérification systématique (ARMVS) (confiance zéro).
  - SASE prend en charge l'accès aux travailleurs à distance et sur place des directions générales. SASE est fourni à titre de service, et se fonde sur le justificatif du dispositif ou de l'entité, combinée au contexte en temps réel et aux politiques de sécurité/conformité. Les identités peuvent s'associer à des personnes, des appareils, IdO ou des emplacements informatiques périphériques.
- **Justification du poste et de la vitesse d'adoption :** SASE est axée sur la transformation numérique des activités de l'entreprise, c'est-à-dire l'adoption de services infonuagiques par des effectifs répartis et mobiles, l'informatique en périphérie de réseau et des plans de poursuite des activités qui doivent absolument comprendre un accès à distance flexible, sécurisé, partout et en tout temps. Bien que le terme soit né en 2019, les premiers adhérents en ont déployé l'architecture dès 2017. **D'ici 2024, au moins 40 % des entreprises auront élaboré des stratégies explicites pour adopter la SASE,** contre moins de 1 % à la fin de 2018.
  - D'ici 2023, 20 % des entreprises auront adopté les fonctionnalités SWG, CASB, ARMVS et FWaaS du même fournisseur, en hausse par rapport à moins de 5 % en 2019. Cependant, de nos jours, la plupart des mises en œuvre font appel à deux fournisseurs (les réseaux étendus réalisés par logiciel + sécurité du réseau), bien que des solutions de fournisseur unique commencent à émerger. Les déploiements avec deux fournisseurs qui ont une profonde intégration entre les fournisseurs sont hautement fonctionnels et éliminent en grande partie le besoin de déployer quoi que ce soit de plus qu'un coupe-feu dynamique de niveau 4 dans les directions générales. Cela entraînera une nouvelle vague de consolidation, car les fournisseurs luttent pour investir afin d'être concurrentiels dans ce paysage hautement perturbateur et en évolution rapide.
  - SASE en est aux premières étapes du développement des marchés, mais la communauté des fournisseurs le commercialise et le développe activement. Bien que le terme soit relativement nouveau, l'approche architecturale (nuage si vous le pouvez, sur place si vous le devez) a connu son déploiement il y a au moins deux ans. L'inversion des modèles de mise en réseau et de sécurité de réseau à mesure que les utilisateurs, les dispositifs et les services quitteront le périmètre d'entreprise traditionnel transformera le paysage concurrentiel du réseau-service et de la sécurité de réseau-service au cours de la prochaine décennie, bien qu'on y prenne conscience que les gagnants et les perdants en seront évidents d'ici 2022. Les véritables services SASE sont infonuagiques personnalisés, dynamiquement évolutifs et accessibles à l'échelle mondiale, et se fondent généralement sur des microservices et une architecture multilocataire.

# Gartner Research – 5G

- **Définition** Les services 5G comprennent une connectivité de données cellulaires locales ou étendues fondée sur la version 15 ou plus récente du 3GPP, ce qui offre la prochaine génération de réseaux de communications cellulaires à suivre 4G LTE. Les fournisseurs fonderont les services, comme les applications nouvelles ou améliorées pour les utilisateurs finaux ou IdO, sur les exigences de rendement clés de la 5G, soit un débit de données mobiles allant jusqu'à plusieurs gigabits. Les services se fonderont également sur la transmission de données à faible latence et le soutien du déploiement massif de communications machine à machine prises en charge par les versions 16 et ultérieures.

- **Justification du poste et de la vitesse d'adoption :** 5G est le terme le plus souvent recherché parmi les technologies de réseautage envisagées pour les cycles publicitaires (*Gartner Hype Cycles*), d'après une mesure composite englobant la recherche (*Gartner Research*), l'interrogation (*Gartner Inquiry*) et les tendances de Google (*Google Trends*). Selon la *Global Mobile Suppliers Association (GSA)*, au 2$^{e}$ trimestre de 2020, plus de 70 fournisseurs de services avaient lancé des services sans fil commerciaux fixes ou mobiles à l'échelle mondiale au moyen de la technologie 5G conforme à la norme 3GPP. L'expansion de la disponibilité du réseau permettra aux services 5G de progresser rapidement dans l'état émergent. Toutefois, la couverture s'étendra lentement dans certaines régions, et les fournisseurs de services ont relevé peu de cas d'approvisionnement nécessitant des capacités de rendement 5G au lieu de solutions de rechange largement répandues comme Wi-Fi ou 4 G LTE. La ratification des deux prochaines prescriptions de la technologie 5G, soit les versions 16 et 17, prévues respectivement en 2020 et 2022, apportera des améliorations considérables du rendement au-delà du débit de données. Celles-ci soutiendront une latence ultra-faible et une énorme densité de couverture pour les points d'extrémité IdO à faible puissance et le découpage de réseau.

- **Conseils aux utilisateurs** : La technologie 5G continue d'éprouver des problèmes d'immaturité, de battage médiatique imposant et d'attentes irréalistes au sujet des caractéristiques et des ensembles de disponibilité, causés par la commercialisation des infrastructures et des fournisseurs de services. Les entreprises doivent intégrer des hypothèses de réseautage réalistes pour les plans d'activités en travaillant avec les chefs d'entreprise et les fournisseurs de services de réseau pour déterminer la disponibilité de la technologie 5G à des endroits précis. Un rendement optimal de la technologie 5G exigera l'utilisation de fréquences cellulaires de bandes basse et moyenne plus un spectre d'ondes millimétriques. Nous ne nous attendons pas à ce que la technologie 5G utilisant le spectre d'ondes millimétriques devienne facilement disponible hors des composantes urbaines denses. De plus, déterminer les endroits où les signaux d'ondes millimétriques disponibles pourront rencontrer des problèmes de propagation de signal en raison d'obstacles tels que les murs de bâtiment, les vitres de fenêtres et le feuillage épais.

  - **Relever les occasions de mettre à l'essai pilote des réseaux et des services 5G pour offrir de l'innovation, selon les capacités de 5G actuelles**, comme les données à haute vitesse. En même temps, mettre en lumière les applications où les technologies actuellement disponibles des fournisseurs de services (comme LTE-A) prendront en charge les scénarios d'utilisation nécessitant des vitesses de données pouvant atteindre 1 Gb/sec et une latence pouvant atteindre 30 millisecondes.

# Gartner Research – Wi-Fi 6 (IEEE 802.11ax)

- **Définition** Wi-Fi 6 (802.11ax) est la plus récente itération de la famille WLAN 802.11 de l'IEEE. Ses principales améliorations permettent au réseau de contrôler la connectivité des appareils pour la première fois et d'améliorer l'efficacité des fréquences existantes de 2,4 et 5 GHz, ce qui augmente le débit dans les régions densément peuplées. Son but consiste donc à prendre en charge un plus grand nombre de dispositifs, y compris IdO, correctement reliés au réseau.
- **Justification du poste et de la vitesse d'adoption** : L'IEEE, l'organisme de normalisation des technologies 802.11, a mis sur pied le groupe d'étude *High Efficiency WLAN* (*HEW* — "Haute efficacité de RL sans fil") à haut rendement en mai 2013 afin d'examiner les besoins les plus pressants pour la technologie Wi-Fi de prochaine génération. La ratification de la nouvelle norme Wi-Fi 6 (802.11ax) était prévue à la fin de 2019, mais accuse un retard jusqu'en 2020 et peut-être plus longtemps en raison de la COVID-19. La majorité des principaux fournisseurs ont déjà lancé sur le marché l'équipement de réseautage fondé sur des normes préliminaires. Les technologies Wi-Fi successives ont augmenté le débit par appareil à un rythme impressionnant au fil des ans (passant des 11 Mb/sec de 802,11 b à 10 Gb/sec, attendue selon la nouvelle norme).
  - Le nombre d'appareils IdO et la convergence de l'automatisation de bâtiment et des appareils de secteur d'activités sur l'infrastructure de communication de l'entreprise continuent de contribuer à la congestion. La norme 802.11ax permettra d'utiliser plus intelligemment les ressources réseau au lieu de laisser l'appareil prendre la décision relative à la connectivité comme l'ont permis les versions précédentes de la norme. Les progrès permettent à différents flux de communiquer simultanément avec plusieurs appareils et de réduire la latence d'une proportion pouvant atteindre 75 %.
- ***Conseils aux utilisateurs*** *:* Nous conseillons aux clients de ne pas payer un prix supérieur pour toute adoption du réseau Wi-Fi 6 (802.11ax), à moins que la solution sans fil existante ne fournisse pas le rendement et les fonctionnalités nécessaires pour répondre aux besoins définis des utilisateurs finaux.
  - Pour les chefs de file dans le domaine des TI, la technologie de réseau **Wi-Fi 6 (802.11ax) représente une occasion d'améliorer sensiblement leur rendement pour les cas d'approvisionnement spéciale** comme les déploiements d'appareils denses. On leur conseille de surveiller le calendrier de normalisation et la disponibilité des produits afin de trouver le bon point d'entrée pour les futures mises à niveau de l'infrastructure ainsi que la disponibilité des appareils client qui appuieront la nouvelle norme.
  - Nous informons les clients que la « certification Wi-Fi 6 » ne signifie pas actuellement la conformité avec la norme 802.11ax, puisque celle-ci n'a pas encore obtenu ratification. Toute organisation qui achète des produits prénormalisation doit pouvoir mettre à niveau ou mettre à jour ses produits sans frais pour qu'ils se conforment aux normes.

# Gartner Research – Accès au réseau moyennant vérification systématique (ARMVS) (confiance zéro) (1 de 2)

- **Définition** L'accès au réseau moyennant vérification systématique (ARMVS) (confiance zéro) crée une limite d'accès logique fondée sur le justificatif et le contexte autour d'une application ou d'un ensemble d'applications. Les applications sont cachées de la découverte, et l'accès se limite par l'entremise d'un courtier en confiance à un ensemble d'entités désignées. Le courtier vérifie le justificatif, le contexte et l'adhésion à la politique des participants spécifiés avant d'autoriser l'accès, et interdit les déplacements latéraux ailleurs dans le réseau. Cela empêche le public de voir les biens d'application et réduit considérablement la surface d'attaque.
- **Justification du poste et de la vitesse d'adoption :** L'ARMVS est une synthèse des concepts édictés par le projet de périmètres définis par logiciel de la *Cloud Security Alliance*, par la vision BeyondCorp de Google et dans le livre *Zero Trust Networks* d'O'Reilly. Les premiers produits sur le marché tendaient à se concentrer sur les cas d'approvisionnement nécessitant l'accès à des applications Web. Les produits plus récents et plus complets fonctionnent avec un plus large éventail d'applications et de protocoles.
- Tandis que de plus en plus d'organisations se retrouvent soudainement obligées de se tourner vers le télétravail, les RPV fondés sur le matériel présentent des limitations. L'ARMVS a éveillé l'intérêt de ceux qui recherchent une solution de rechange plus souple aux RPV et de ceux qui désirent un accès et un contrôle de session plus précis aux applications situées sur place et dans le nuage. Les fournisseurs d'ARMVS continuent d'attirer des fonds de capital de risque. Cela, à son tour, encourage les nouvelles entreprises en démarrage à pénétrer un marché de plus en plus bondé et à chercher des manières et moyens de se distinguer. Les activités de fusion et d'acquisition (F et A) dans ce marché battent leur plein, de plus grands fournisseurs de réseaux, de télécommunications et de sécurité ayant fait l'acquisition de plusieurs fournisseurs en démarrage.
- **Conseils aux utilisateurs :** Les organisations doivent évaluer l'ARMVS pour chacun de ces cas d'approvisionnement :
  - Ouvrir les applications et les services aux applications écosystémiques collaboratives, comme les canaux de distribution, les fournisseurs, les entrepreneurs ou les points de vente au détail, sans nécessiter l'emploi d'un RPV ou d'une composante démilitarisée (ZD).
  - Normaliser l'expérience utilisateur pour l'accès aux applications – l'ARMVS élimine la distinction entre se trouver à l'intérieur ou à l'extérieur du réseau d'entreprise.
  - Accès propre à l'application pour les entrepreneurs en TI et les employés mobiles ou à distance comme solution de rechange à l'accès par voie du RPV.
  - Étendre l'accès à une organisation acquise pendant les activités de fusion et acquisition, sans devoir configurer les règles du RPV et du pare-feu d'emplacement à emplacement. Les entreprises fusionnées peuvent partager rapidement et facilement des applications sans exiger l'intégration des réseaux ou des systèmes d'identité sous-jacents.

# Gartner Research – Accès au réseau moyennant vérification systématique (ARMVS) (confiance zéro) (2 de 2)

  - Faciliter l'emploi d'appareils personnels pour les utilisateurs – L'ARMVS peut améliorer la sécurité et simplifier les programmes « Apportez votre équipement personnel de communication » (AVEC) en atténuant les exigences de gestion complètes et en permettant un accès direct plus sécurisé aux applications.
  - Masquer les systèmes sur des réseaux hostiles, comme des systèmes sur l'internet public utilisés pour la collaboration.
  - Assurer le chiffrement jusqu'aux points d'extrémité lorsque vous ne faites pas confiance à l'entreprise de services de télécommunications ou au fournisseur d'infonuagique.
  - Permettre aux utilisateurs se trouvant dans des régions du monde potentiellement dangereuses d'interagir avec des applications et des données de façons qui atténueront ou élimineront les risques susceptibles de provenir de ces régions.
  - Sécurisation de l'accès aux enclaves de dispositifs IdO si le dispositif peut prendre en charge un le périmètre défini par logiciel léger ou un connecteur à appareil virtuel sur le segment réseau IdO pour la connexion.
- **Incidence sur les activités opérationnelles :** Les avantages de l'ARMVS sont immédiats. À l'instar d'un RPV traditionnel, les services fournis dans l'environnement ARMVS sont invisibles dans Internet public et, donc, protégés des attaquants. En outre, l'ARMVS offre des avantages appréciables en matière d'expérience utilisateur, d'agilité, d'adaptabilité, et de facilité de gestion des politiques. Pour les offres d'ARMVS en nuage, l'évolutivité et la facilité d'adoption présentent des avantages supplémentaires. L'ARMVS permet des scénarios de transformation numérique des activités opérationnelles qui s'adaptent mal aux approches d'accès habituelles. Grâce aux efforts de transformation numérique, la plupart des entreprises disposeront de plus d'applications, de services et de données à l'extérieur de leur entreprise qu'à l'intérieur. Les services ARMVS en nuage placent les contrôles de sécurité là où se trouvent les utilisateurs et les applications : dans le nuage. Certains des plus grands fournisseurs d'ARMVS ont investi dans des douzaines de points de présence dans le monde en vue d'un accès à faible latence.
- Évaluation des avantages : Modéré
- Pénétration du marché : 5 % à 20 % de l'auditoire cible
- Maturité : Adolescence
- Exemples de fournisseurs : Akamai; AppGate; Cato Networks; Cisco; Netskope; Perimeter 81; Proofpoint; Pulse Secure; SAIFE; Zscaler

# Gartner Research – Réseautage défini par logiciel (les réseaux définis par des logiciels) (1 de 2)

- **Définition :** Le réseautage défini par logiciel (les réseaux définis par des logiciels) est une approche architecturale de la conception, de la fabrication et de l'exploitation de réseaux qui promettait une agilité et une extensibilité accrues en abstrayant la topologie du réseau et le plan de contrôle. Cependant, les **entreprises n'ont jamais couramment adopté les produits les réseaux définis par des logiciels**. Plutôt, le les réseaux définis par des logiciels a engendré des innovations en automatisation, orchestration, segmentation et désagrégation du matériel et des logiciels de réseau.

- Justification du poste et de la vitesse d'adoption : Le les réseaux définis par des logiciels demeure un sujet de discussion d'importance dans de multiples marchés de réseaux et dans de nombreuses démarches de commercialisation des fournisseurs. Toutefois, les véritables technologies les réseaux définis par des logiciels n'ont pas réussi à s'attirer l'acceptation du marché des entreprises, et les organisations de réseautage d'entreprise ne devraient pas en tenir compte. L'espoir que les réseaux définis par des logiciels permettent le découplage du plan de contrôle du matériel de réseau et favorisent l'innovation logicielle indépendante ne s'est jamais concrétisé, et il n'existe effectivement aucune technologie des réseaux définis par des logiciels disponible sur le marché courant aujourd'hui.

  – Bien que les **véritables solutions les réseaux définis par des logiciels n'aient pas trouvé adoption appréciable sur le marché,** le développement de réseaux définis par des logiciels et la menace aux acteurs du marché établis ont eu une incidence profonde et positive sur l'évolution subséquente du marché. Le les réseaux définis par des logiciels a clairement influencé l'utilisation croissante des commutateurs de boîte blanche, le mouvement du matériel et des logiciels de source ouverte (pris en charge par le projet de calcul ouvert) et le développement de fournisseurs de logiciels de commutation de réseau indépendants. Plus important encore pour le marché des entreprises, il y a eu changement d'orientation de l'innovation des fournisseurs de réseaux traditionnels autour de l'exploitation et de la gestion. Cela a conduit à des améliorations de l'agilité et de l'automatisation, à une simplification des exigences opérationnelles, et à l'adoption générale d'une configuration à l'échelle fonctionnelle (c.-à-d. une gestion qui englobe les appareils dans un environnement de centre de données, de campus ou de RÉ). Sans la menace des réseaux définis par des logiciels, il est peu probable que les progrès opérationnels des fournisseurs traditionnels auraient vu le jour.

- **Conseils aux utilisateurs :** Bien que les réseaux définis par des logiciels soient manifestement désuets sur le marché des entreprises, de nombreuses organisations citent encore les réseaux définis par des logiciels comme une pierre angulaire de leur stratégie et leur architecture futures. Ce qui est crucial pour les entreprises, c'est de comprendre ce qu'elles essaient d'accomplir lorsqu'elles pensent « les réseaux définis par des logiciels ».

# Gartner Research – Réseautage défini par logiciel (les réseaux définis par des logiciels) (2 de 2)

- **Conseils aux utilisateurs (suite) :**
  - Ne vous laissez pas séduire et obnubiler par la publicité tapageuse et les affirmations du fournisseur selon lesquelles les produits commerciaux sont des réseaux définis par des logiciels, et ne participez à aucune discussion ou planification du déploiement des réseaux définis par des logiciels.
  - Concentrez-vous sur les résultats souhaités que vous essayez d'obtenir, comme l'automatisation accrue, la segmentation virtuelle, et l'orchestration externe.
  - Choisissez d'abord un cadre de travail opérationnel ou d'automatisation, puis décidez des fournisseurs et des produits de réseautage.
  - Évaluez les approches tant de l'infrastructure matérielle que de la superposition de logiciels.
  - Élaborez une collaboration interfonctionnelle et étudiez des méthodologies pour mieux intégrer les équipes de serveur, de virtualisation, de réseau, de sécurité et d'application.
- **Incidence sur les activités** : Il n'y a pas d'incidence commerciale directe des solutions les réseaux définis par des logiciels complètes. Cependant, l'innovation en aval peut accroître l'agilité du réseau, simplifier la gestion, rendre la sécurité plus robuste, et entraîner des diminutions des coûts opérationnels et en capital tout en favorisant la collaboration interfonctionnelle. Les nouvelles solutions de réseau doivent s'appliquer à amenuiser ou éliminer le problème des « intergiciels humains » qui afflige les solutions de réseau traditionnelles depuis deux décennies. En intégrant le fonctionnement des réseaux dans un processus opérationnel simplifié et automatisé conçu dans l'environnement de calcul virtuel, les organisations d'utilisateurs peuvent adapter le déploiement d'application à la rapidité croissante des activités. La technologie de superposition de réseau disponible peut créer de nouveaux environnements concurrentiels qui feront passer la préoccupation essentielle de l'infrastructure physique aux logiciels et aux fonctions opérationnelles.
- **Évaluation des avantages :** Faible
- **Pénétration du marché :** Moins de 1 % du public cible
- **Maturité :** Désuet
- **Exemples de fournisseurs :** NEC
- **Lecture recommandée** : **« État des réseaux définis par des logiciels : Si vous pensez que les réseaux définis par des logiciels sont la réponse, vous posez la mauvaise question »**

# Gartner – Segmentation fondée sur le justificatif (microsegmentation)

- **Définition** La segmentation fondée sur le justificatif (aussi connue sous les noms de microsegmentation, segmentation de réseau sans confiance, ou segmentation logique) utilise la protection pare-feu dirigée par les politiques, la charge de travail et le justificatif (habituellement articulé sur les logiciels) ou les communications réseau chiffrées de manière différentielle pour isoler les charges de travail, les applications et les processus dans les centres de données, les infrastructures-services (IaaS) du nuage public et les conteneurs. Cela comprend les charges de travail qui s'étendent sur de multiples fournisseurs d'IaaS sur place et en nuage public.
- **Justification du poste et de la vitesse d'adoption :** Comme de plus en plus de serveurs subissent la virtualisation ou passent à l'infrastructure-service, les pare-feu traditionnels, la prévention des intrusions et les antivirus suivent rarement le rythme rapide du déploiement de nouveaux actifs. L'entreprise en devient donc vulnérable aux attaquants, qui prennent pied, puis se déplacent latéralement dans les réseaux de l'entreprise. Cela a suscité un intérêt accru pour la visibilité, la segmentation plus évoluée, et les approches de réseautage moyennant vérification systématique (sans confiance) pour le trafic est-ouest entre les applications, les serveurs et les services dans les centres de données modernes. La nature de plus en plus dynamique des charges de travail des centres de données rend les stratégies traditionnelles de segmentation centrée sur le réseau complexes, voire impossibles, à appliquer. De plus, le passage à des architectures de conteneurs de microservices pour les applications a également intensifié le volume de trafic est-ouest et compliqué davantage la capacité des pare-feux centrés sur le réseau à fournir cette segmentation. **L'extension des centres de données dans le nuage public a aussi mis point de mire sur des approches logicielles de segmentation, dans de nombreux cas, à l'aide des capacités de segmentation intégrées des fournisseurs d'infonuagique.**
- **Conseils aux utilisateurs** : Les responsables de la sécurité et de la gestion des risques doivent se plier aux lignes directrices suivantes lorsqu'ils mettent en œuvre la segmentation fondée sur le justificatif :
  - Éviter de sursegmenter. La sursegmentation est la principale cause d'échec et une dépense inutile pour les projets de segmentation.
  - Éviter d'utiliser les adresses IP ou l'emplacement du réseau comme fondement des politiques de segmentation.
  - Commencer par un projet de cartographie de flux réseau pour comprendre les flux d'application et de données au serveur avant d'entreprendre le projet de segmentation.
  - Appliquer une segmentation adaptative continue. Commencer par de nouveaux actifs, puis combler les écarts et lacunes existants.
  - Adopter une approche fondée sur le risque et regarder au-delà des considérations techniques lors de la segmentation.
  - Concevoir en vue de politiques de segmentation uniformes pour l'ensemble des IaaS dans le nuage public et sur place.

# Gartner Research – RÉ défini par logiciel

- **Définition** Les produits de réseau étendu définis par logiciel (les réseaux étendus réalisés par logiciel) remplacent les routeurs traditionnels. Ils offrent plusieurs caractéristiques, notamment la sélection dynamique des chemins d'accès, sur la base de la politique opérationnelle ou de l'application; la politique centralisée et la gestion des dispositifs en périphérie de RÉ; et la configuration sans intervention. Les produits les réseaux étendus réalisés par logiciel sont indépendants des entreprises de télécommunications et des moyens d'acheminement, et peuvent créer des chemins sécurisés à l'échelle de plusieurs connexions de RÉ. Les produits les réseaux étendus réalisés par logiciel peuvent se fonder sur matériels ou logiciels; ils peuvent faire l'objet de gestion directe par des entreprises ou d'intégration dans une offre de services gérés.

- Justification du **poste et de la vitesse d'adoption** : **L'intérêt très répandu des clients pour les produits les réseaux étendus réalisés par logiciel se poursuit, et nous estimons que plus de 25 000 clients ont déployé des produits les réseaux étendus réalisés par logiciel dans des réseaux de production, ce qui représente plus de 600 000 emplacements. Nous nous attendons à une croissance rapide continue des déploiements des réseaux étendus réalisés par logiciel, et nous prévoyons que les revenus des fournisseurs augmenteront selon un taux de croissance annuel composé (TCAC) de plus de 23 % au cours des trois prochaines années**. Conjointement avec une topologie RÉ hybride, les réseaux étendus réalisés par logiciel améliorent la disponibilité, le coût et le rendement des RÉ d'entreprise. Les organisations qui passent à l'acheminement RÉ hybride ou par Internet seulement se tournent vers les produits les réseaux étendus réalisés par logiciel, en raison de leurs fonctionnalités et de leur gérabilité améliorées de sélection de parcours. Un grand nombre de fournisseurs (plusieurs douzaines) se concurrencent sur le marché, y compris les fournisseurs titulaires de réseaux et de sécurité, des fournisseurs en démarrage et des fournisseurs de moindre taille à vocation régionale ou verticale.

- **Conseils aux utilisateurs :** Les responsables du réseautage doivent renouveler leur matériel de RÉ de directions générales en mettant en œuvre les réseaux étendus réalisés par logiciel lorsqu'ils effectuent la migration d'applications vers le nuage public, lorsqu'ils réalisent des RÉ hybrides, lorsque l'équipement atteint la fin de sa vie utile, ou lorsque les contrats de service réseau/MPLS gérés arrivent à renouvellement. Suivre un processus complet de sélection des réseaux étendus réalisés par logiciel en évaluant un ensemble diversifié de fournisseurs et en réalisant un projet pilote. C'est particulièrement important maintenant, car les offres sur le marché ne sont pas toutes stables et évolutives. Faites participer les équipes de sécurité de réseau à la conception, à la planification et à la mise en œuvre, car les RÉ hybrides compatibles avec les réseaux étendus réalisés par logiciel ont une incidence directe sur le positionnement des contrôles de sécurité, comme les pare-feux et les passerelles Web sécurisées (SWG).

# Gartner Research – Chemin de solution pour l'adoption d'AIOps, 1er décembre 2020

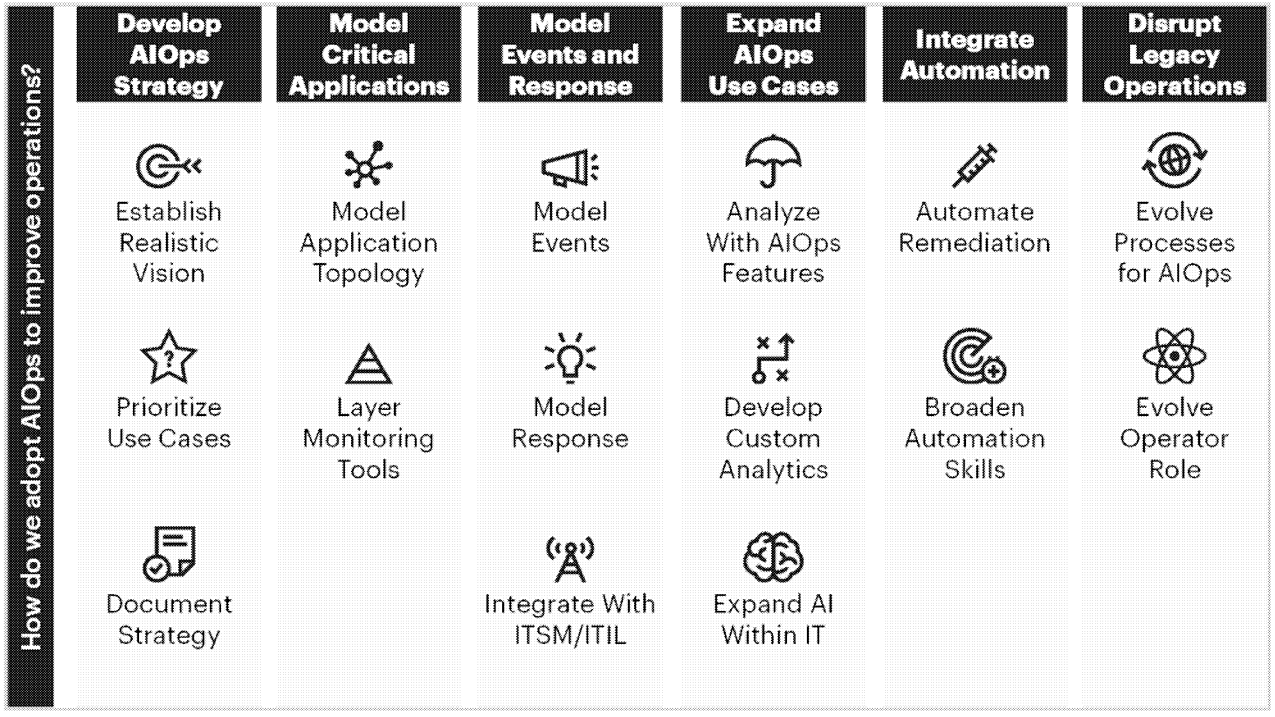
- L'IA promet de révolutionner le fonctionnement des TI, mais la plupart des équipes de TI éprouvent des difficultés à voir à travers le battage publicitaire les cas d'approvisionnement pragmatique et les bons outils. Les professionnels techniques des I et O doivent utiliser ce chemin de solution pour clarifier leur approche de l'adoption d'AIOps en superposant les outils, les plateformes et les caractéristiques d'AIOps.
- **Principaux constats**
  - L'ambiguïté et le battage publicitaire autour du terme « AIOps » constituent le principal obstacle à l'établissement d'une vision percutante et d'une stratégie réussie pour l'IA en exploitation de TI.
  - Les innombrables applications potentielles de l'IA en TI exigent d'établir des priorités et d'accorder une importance particulière à des cas d'approvisionnement de haute valeur.
  - La maximisation de l'incidence d'AIOps nécessitera de multiples outils et technologies, souvent en chevauchement. À l'heure actuelle, il n'existe pas de produit, de plateforme ou d'approche unificateur(trice) sur le marché, et il n'y en aura probablement jamais.
  - Les applications pratiques de l'« automatisation intelligente » sont beaucoup moins intelligentes que le terme sous-entend.
  - La majorité des pratiques d'AIOps s'articulent autour de l'exploitation traditionnelle. L'impact véritablement transformationnel de l'IA sur l'exploitation de TI est encore à venir.
- **Recommandations**
  - Les professionnels techniques qui cherchent à tirer le maximum de l'IA pour améliorer l'exploitation de TI doivent faire ce qui suit :
  - Élaborer une stratégie d'AIOps qui décrit et met en correspondance les cas d'approvisionnement prioritaires et l'ensemble d'outils à plusieurs couches qui résout les défis et problèmes individuels de chaque cas d'approvisionnement.
  - Intégrer la surveillance traditionnelle, l'observabilité moderne et l'analytique avancée pour établir un modèle opérationnel qui gère les applications et les services, plutôt que les composants et les ressources.
  - Étendre le portefeuille d'automatisation afin de créer plus d'intersections entre AIOps et l'automatisation.
  - Maximiser l'incidence d'AIOps en adaptant les processus et les opérations des TI qu'on ne peut automatiser.




Gartner

# Gartner Research – Chemin de solution pour l'adoption d'AIOps, 1er décembre 2020

**Solution Path for AIOps**




Source: Gartner
731459_C




Gartner

# Mesures et indicateurs de gestion des services – Exemples tirés d'une liste de plus de 100

## Référence : « *IT Performance Management Toolkit Tactics and Tools for Improving IT Metrics Maturity* » CEB, une entreprise Gartner

**Approvisionnement**

- **Nouveaux employés**
- **Nouveaux emplacements**
- **Nouveaux postes de travail**
- **Nouvelles applications**
  - Nouveaux services Saas
- **Mises en œuvre – Temps de mise en œuvre**
  - Circuits, commutateur, routeur, pare-feu
- **Livraison à temps (%)**

**Entretien**

- **Temps écoulé entre défaillances**
- **Visites d'emplacement**
- **Personnel d'entretien**
- **Temps écoulé entre défaillances**
- **Disponibilité du service (%)**

**Gestion de projets**

- **Livraison du projet à temps (%)**
- **Projets respectant le budget (%)**
- **Projets atteignant les objectifs (%)**

**Gestion du changement**

- **Nombre de changements CCC**
- **Changements dans le respect des délais et du budget**
- **Changements réussis (%)**

**Incident + Problème**

- **Incidents/Pannes**
  - Repérés par SPC (%)
- **Délai de réaction aux incidents**
- **Durée moyenne des réparations**
- **Problèmes – (p. ex., incidents récurrents)**
- **Analyse des causes fondamentales – Livraison à temps**

**Configuration**

- **Actifs dans la BDGC %**
- **Temps pour ajouter des actifs à la BDGC**

**Bureau de service**

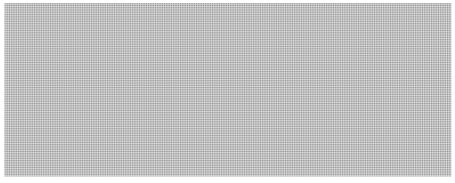
- **Délai moyen de réponse**
- **Résolution au premier appel**
- **Résolution en libre-service**

**Satisfaction de la clientèle**

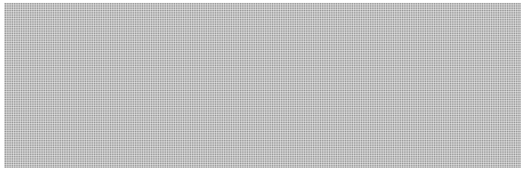
- **Pointage d'utilité moyen dans les FAQ du portail Web**
- **Pointage moyen de sentiment**

# Personnes-ressources

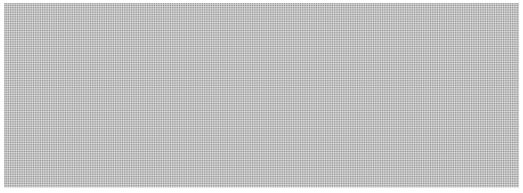
**Gartner**



**Gartner**



**Gartner**






Gartner