

Cisco Digital Network Architecture (DNA)

Q. Cisco® Digital Network Architecture, qu'est-ce que c'est ?

A. C'est une architecture logicielle de réseau ouverte et évolutive, conçue pour fournir rapidement des services permettant aux équipes IT d'accélérer l'innovation, de diminuer les coûts et la complexité, de réduire les risques, tout en se conformant aux exigences réglementaires.

Q. Motivations du marché : pourquoi les entreprises doivent-elles se doter de l'architecture Cisco DNA ?

A. La numérisation est encouragée par des tendances technologiques importantes: la mobilité, l'Internet des objets (IoT), le cloud et l'analytique. Le réseau est indispensable pour réunir tous ces éléments et permettre aux entreprises d'exploiter pleinement leur potentiel. Les clients qui souhaitent passer au numérique doivent évoluer vers un réseau fonctionnant à la vitesse du numérique afin de pouvoir :

- Exploiter des données de l'entreprise pour fournir à la fois des informations en temps réel et un historique, qui permettent de prendre de meilleures décisions ou de créer des modèles économiques inédits.
- Simplifier l'architecture réseau grâce à l'automatisation, pour s'adapter plus rapidement aux nouveaux besoins de l'entreprise tout en préservant la qualité de service.
- Des fonctions de sécurité accélérées : une détection plus rapide des menaces grâce à une visibilité complète sur l'ensemble du réseau en temps réel et à une capacité d'isoler rapidement les menaces, tout en répondant de façon durable aux exigences réglementaires.

Q. De quelle façon l'architecture Cisco DNA accélère-t-elle la transformation numérique ?

A. Cisco a réinventé le réseau, désormais **ouvert, évolutif et piloté par logiciels**, grâce à la programmabilité, à l'évolutivité des services et à la virtualisation. Cela permet aux équipes informatiques de s'adapter aux besoins changeants de l'entreprise en présentant des services innovants :

- **Informations et actions** : les informations obtenues via les API ouvertes permettent de contribuer aux innovations commerciales grâce à une visibilité en profondeur sur les données des utilisateurs, des applications et des appareils de l'ensemble du réseau. Par exemple, la solution de mobilité connectée Cisco CMX fournit des informations sur les clients et propose des interactions personnalisées.
- **Automatisation et assurance qualité** : nous avons intégralement reconstruit nos systèmes d'exploitation, qui proposent désormais des API riches, basées sur des modèles et programmables, ainsi que des fonctions de gestion basées sur des contrôleurs, d'hébergement des applications et de virtualisation pour permettre aux équipes IT de provisionner, d'orchestrer, d'adapter et de gérer l'infrastructure de façon simple et évolutive. Avec le module Cisco APIC-EM (Application Policy Infrastructure Controller Enterprise Module) et des applications telles que Cisco Plug and Play, nous proposons une automatisation dès la mise en service qui peut entraîner une réduction de 79 % des coûts. La virtualisation des fonctions de réseau (NFV) renforce l'agilité des succursales en leur permettant d'exécuter des services réseau sur toutes les plates-formes.
- **Sécurité et conformité** : nous avons intégré des fonctions de sécurité sur tout le réseau (routeurs, commutateurs, connexions sans-fil et cloud) pour aider les équipes IT à détecter et à isoler les menaces en continu grâce à Cisco ISE (Identity Services Engine), à la segmentation logicielle TrustSec® et au système StealthWatch pour l'analyse des données NetFlow.

Q. Quels sont les principes clés de cette architecture ?

A. Voici les piliers fondamentaux de cette architecture, conçue pour aider les entreprises à accélérer l'innovation ainsi qu'à réduire les coûts, la complexité et les risques :

- **Virtualisation** : nous virtualisons 30 années d'innovations réseau en séparant le logiciel du matériel et en offrant à nos clients la liberté d'accéder à nos services ou aux services tiers depuis tous les types de plates-formes, ainsi que la possibilité d'exécuter des applications sur le réseau.
- **Automatisation** : grâce à des contrôleurs et à des API ouvertes, Cisco simplifie la gestion du réseau par un processus d'abstraction et d'application centralisée des politiques. Cela permet aux équipes IT de se concentrer sur les objectifs de l'entreprise et d'appliquer des configurations de façon systématique afin d'améliorer les services et de garantir une sécurisation homogène des opérations, depuis le cœur jusqu'à la périphérie du réseau.
- **Analytique** : en révélant les données du réseau, Cisco donne accès à des informations contextuelles et approfondies sur les utilisateurs, les applications, les appareils et les menaces. Cela aide l'entreprise et le département IT à prendre de meilleures décisions.
- **Cloud** : pour permettre aux équipes informatiques de bénéficier d'une évolutivité à la demande des services réseau et d'un meilleur délai de rentabilité, nos solutions sont conçues en prenant en compte le cloud. Nous allons continuer à adopter un nombre croissant de modèles cloud pour simplifier les tâches de gestion, fournir des services cloud à la périphérie du réseau pour les déploiements sur les clouds publics ou hybrides, et, lorsque cela est possible, proposer des logiciels sous forme de service (SaaS) dans le cloud pour faciliter l'utilisation.

Q. Quels sont les avantages de Cisco Digital Network Architecture pour les clients ?

A. **Agilité de l'infrastructure IT et évolutivité** : grâce à l'automatisation basée sur des politiques, les équipes informatiques peuvent déployer et gérer des services sur des centaines d'appareils et de sites en répondant systématiquement aux besoins de l'entreprise. Par exemple, l'application de WAN intelligent (IWAN) de Cisco réduit les efforts requis pour effectuer des modifications de workflow à 10 clics, soit une réduction de 85 % des délais de provisionnement des services réseau. De plus, le service informatique peut s'appuyer sur des services virtualisés pour créer un réseau plus dynamique capable de provisionner, d'étendre et de réaffecter rapidement des services entre différentes plates-formes matérielles sans intervention.

- **Réduction des coûts informatiques** : grâce à l'automatisation des services, notamment le provisionnement Plug and Play dans le cloud dès la mise en service des produits, les clients voient leurs coûts d'installation diminuer de 79 %.
- **Réduction des risques** : d'après un rapport sur Cisco ASR (Aggregation Service Router), l'intégration de fonctions de sécurité sur tout le réseau, associées aux meilleurs systèmes de protection existants, permet aux équipes IT de détecter et d'isoler des menaces plus de 1 000 fois plus rapidement que la moyenne du secteur. Le délai moyen de détection des menaces est de 200 jours, tandis que le nôtre est de 17,5 jours.
- **Expérience améliorée pour l'utilisateur** : les équipes informatiques peuvent fournir des expériences entièrement différenciées grâce à EasyQoS, qui met à jour le réseau de manière dynamique pour optimiser les performances des applications sur tous les segments du réseau.
- **Optimisation des ressources** : le traitement analytique du Big Data et les informations contextuelles permettent aux équipes IT et aux dirigeants de mieux comprendre les tendances du réseau en tenant compte des utilisateurs, des applications et des objets. Par exemple, les équipes informatiques peuvent aider les dirigeants à prendre des décisions concernant le personnel, la pertinence de certaines promotions, l'efficacité au travail, les tendances détectées chez les clients, etc.

- **Protection des investissements** : la portabilité des licences du logiciel Cisco ONE permettra aux clients de transférer leur logiciel sur les prochaines générations de plates-formes compatibles. Par rapport au modèle classique d'achat de fonctionnalités séparées, le client rentabilise bien plus son achat du logiciel Cisco ONE grâce à notre gamme de suites logicielles associées. Il peut ainsi commencer sa transformation numérique dès aujourd'hui tout en étant prêt à bénéficier des futures innovations que lui réserve Cisco DNA.

Q. Quels sont les points clés, les nouveautés de la gamme de produits Cisco ?

A. Nouveau logiciel Cisco IOS® XE : Cisco modernise son système d'exploitation pour les entreprises afin de favoriser la programmabilité, l'automatisation basée sur des contrôleurs et un fonctionnement fiable sur tous les routeurs et commutateurs d'entreprise à partir d'une base de code unique. Le nouveau logiciel Cisco IOS XE sera progressivement pris en charge dans l'essentiel de l'infrastructure réseau d'entreprise Cisco dans les deux ans qui viennent. Le nouveau système d'exploitation comprend une plate-forme ouverte incluant des API basées sur des modèles, des fonctions de gestion programmables, l'hébergement d'applications via des conteneurs, des fonctionnalités de fog computing et de cloud computing ainsi que la virtualisation des fonctions de réseau pour les entreprises (NFV).

La virtualisation des fonctions de réseau (NFV) pour les entreprises : dans le cadre de la modernisation du logiciel Cisco IOS XE, Cisco NFV sépare le matériel et les logiciels et propose une suite complète de services logiciels. Cela permet aux clients d'utiliser des services Cisco ou tiers sur nos équipements spécialisés, sur les serveurs Cisco UCS® des gammes E ou C, ou encore sur des serveurs x86. La suite logicielle d'entreprise Cisco NFV comprend une couche de virtualisation ainsi que des fonctions de réseau virtuel et d'orchestration.

En outre, Cisco annonce de nouveaux services liés aux réseaux numériques et à la sécurité.

Nouveau service	Description	Valeur pour le client	Disponibilité
Informations et actions			
Informations sur le client et interactions via la Solution de mobilité connectée Cisco CMX Cloud	Fonctionnalités d'analyse des données de présence et services connectés Cisco CMX fournis selon un modèle de consommation dans le cloud.	Services de géolocalisation à coût réduit pour les déploiements de petite à moyenne envergure, diminuant le risque lié à investissement pour garantir la valeur du service.	Déjà disponible
Automatisation et assurance			
Automatisation dès la mise en service via Cisco Plug and Play	Simplifie et accélère le provisionnement dès la mise en service du produit et de façon sécurisée sans aucune intervention du service informatique.	Réduction spectaculaire des OpEx: les données de nos clients indiquent jusqu'à 79 % de réduction sur les coûts d'installation des appareils.	Déjà disponible
Hiérarchisation dynamique des applications via EasyQoS	Met à jour la qualité de service (QoS) instantanément et en temps réel sur tout le réseau, selon les besoins des applications.	Expérience améliorée pour l'utilisateur via la garantie de la qualité de service sur tous les segments du réseau. Les études démontrent une diminution de l'instabilité de 300 % et une amélioration de la qualité vidéo de 50 %.	Déjà disponible
Agilité des sites distants via la virtualisation des fonctions de réseau et l'automatisation des services Cisco pour l'entreprise	Permet aux équipes IT d'exécuter les opérations des succursales sur les serveurs Cisco UCS de gammes C et E, et prochainement sur les serveurs x86.	Permet aux équipes IT de gérer et de faire évoluer plus facilement l'infrastructure, pour une utilisation des ressources accrue et une prestation de services plus rapide et à moindre coût.	Déjà disponible
Sécurité et conformité			
Le réseau devient capteur et exécuteur grâce à Cisco Identity Services Engine et StealthWatch	L'infrastructure prête à accueillir l'architecture de réseau numérique transforme le réseau en capteur et exécuteur pour l'ensemble de l'infrastructure pour détecter et bloquer les menaces les plus sophistiquées.	Le réseau détecte et bloque les menaces plus rapidement sur tous les segments afin de mieux protéger les ressources de l'entreprise.	Déjà disponible

Q. Comment les clients utilisent-ils cette architecture?

A. Les services Cisco DNA (Digital Network Architecture) seront provisionnés avec Cisco ONE. Ce logiciel offre des solutions simples à forte valeur ajoutée grâce à la portabilité et à la flexibilité des licences. Les clients peuvent dès à présent construire leur architecture numérique avec notre gamme actuelle de produits, tout en bénéficiant des innovations qui surviendront au cours des mois et des années à venir grâce aux possibilités offertes par l'architecture logicielle.

Q. Comment s'intègrent les solutions Cisco Meraki® dans l'architecture Cisco DNA ?

A. L'offre de solutions gérées dans le cloud Meraki illustre la facilité d'utilisation et de déploiement appelée à devenir la marque de fabrique de toute la gamme de produits d'entreprise de Cisco. En matière d'architecture, les objectifs viseront à garantir une orchestration fiable à tous les niveaux, notamment pour les réseaux basés sur les solutions Meraki.

Q. En quoi l'approche de la sécurité de Cisco DNA est-elle différente de celles des systèmes de sécurité classiques, centrés sur la protection du périmètre du réseau ?

A. Par le passé, les solutions assuraient généralement la protection d'un périmètre de sécurité à l'aide de technologies de pare-feu, de détecteurs d'intrusion, de VPN et de contrôles d'accès. La multiplication et la diversification des points d'accès ont augmenté les menaces. Ce modèle est donc plus difficile à suivre, à moins de disposer de fonctions de sécurité avancées sur chaque port du réseau pour voir et contrôler simultanément toutes les activités. La nouvelle approche offre une meilleure visibilité sur l'ensemble des communications du réseau et du cloud. StealthWatch et Cisco ISE analysent les données NetFlow générées par les appareils du réseau pour détecter et identifier les menaces.

Cette approche permet également aux équipes informatiques de prendre des mesures instantanées, puisqu'elles peuvent ordonner à TrustSec d'isoler une menace directement depuis la console de gestion de StealthWatch. Il s'agit donc d'une solution intégrée offrant visibilité et contrôle pour pratiquement chaque communication du réseau, ce que ne permettrait pas une approche classique dédiée à la protection d'un périmètre de sécurité.

Q. Quelle est la différence entre un réseau SDN et l'architecture Cisco DNA ? Comment fonctionnent-ils ensemble ?

A. Selon l'Open Networking Foundation (ONF), le SDN est « une nouvelle architecture dynamique, gérable, économique et évolutive, ce qui la rend parfaitement adaptée à la nature dynamique et à haute bande passante des applications actuelles. Ce type d'architecture découple les fonctions de contrôle et de transfert du réseau, de façon à permettre de programmer directement le contrôle du réseau et d'abstraire l'infrastructure sous-jacente en faveur des applications et des services réseau. »

L'architecture Cisco DNA n'est pas un simple regroupement de technologies réseau à l'image du SDN. Il s'agit plutôt de rassembler les technologies dans une architecture globale conçue spécifiquement pour atteindre les objectifs de l'entreprise. L'architecture Cisco DNA permet de donner un rôle actif aux services réseau et de faciliter leur utilisation dans le cadre de la transformation numérique de l'entreprise. C'est une suite architecturale qui comprend des applications prêtes à l'emploi ainsi que des API faciles à utiliser. Cisco s'engage à aider ses clients à passer au SDN tout en optimisant la protection de leurs investissements.

Q. Par où commencer?

A. Les services avancés Cisco et nos partenaires agréés peuvent vous aider à commencer votre transition en vous proposant des conseils, des analyses, des évaluations du niveau de préparation de votre réseau ou encore des services de planification, de conception et de migration.

Q. Où trouver des informations complémentaires?

A. www.cisco.fr/dna.



Siège social aux États-Unis
Cisco Systems, Inc.
San José. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pte. Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site web de Cisco, à l'adresse : www.cisco.com/go/offices.



Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, visitez le site : www.cisco.com/go/trademarks. Les autres marques mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat commercial entre Cisco et d'autres entreprises. (1110R)