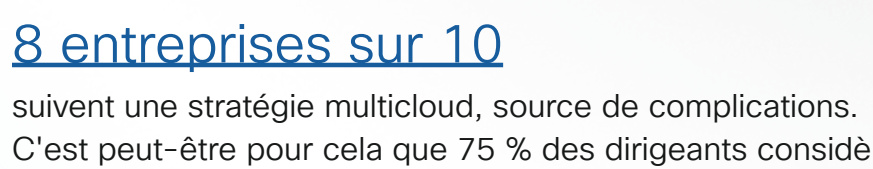


# Répondre aux besoins de travail hybride et multicloud des utilisateurs

Les méthodes de travail actuelles rendent la cybersécurité plus complexe. Découvrez comment instaurer une sécurité plus résiliente pour entrer de plain-pied dans le multicloud.

## Le monde du travail est en pleine mutation. Qu'en est-il de la sécurité ?



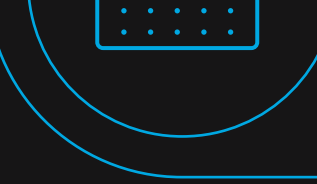
**8 entreprises sur 10**

suivent une stratégie multicloud, source de complications. C'est peut-être pour cela que 75 % des dirigeants considèrent que leur entreprise est **trop difficile à sécuriser**.

En attendant, le travail hybride n'est pas près de disparaître. **Plus de la moitié des collaborateurs** veulent en effet pouvoir se connecter à tout moment, où qu'ils se trouvent, sur n'importe quel appareil. Et 85 % des DSI souhaitent répondre à cette demande. Mais sont-ils équipés pour réussir ?

## Complexité et sécurité ne font pas bon ménage

La complexité est l'ennemi de la sécurité. Pourtant, les équipes IT utilisent en moyenne **entre 40 et 50 outils** pour se protéger, alors que la multiplication des plateformes cloud réduit la visibilité sur les menaces et les vulnérabilités.



**280 jours**

Délai moyen d'identification et de contrôle des failles

La complexité informatique est un défi en matière de sécurité.

- Sécurité et réseaux en silo
- Visibilité réduite
- Dépendance à un seul fournisseur cloud
- Impact sur l'expérience utilisateur

Les collaborateurs travaillant de manière hybride sont une cible rêvée pour les hackers.

**125 %** d'augmentation des cyberattaques en 2021

**4/5** failles au niveau des applications web sont dues à des identifiants volés

## Le chaos est difficile à ignorer.



## Les 4 piliers d'un environnement de sécurité simplifié et unifié

Il est impossible de relever les défis actuels avec des méthodes obsolètes. Pour résoudre les problèmes liés aux environnements de nouvelle génération, vous devez repenser votre stratégie en matière de réseaux et de sécurité.

- Cloud natif**  
Répondez aux besoins des utilisateurs en exploitant tout le potentiel de la sécurité cloud pour protéger les personnes, les réseaux, les applications et les données.
- Simplifié**  
Assurez une sécurité transparente et persistante qui ne se met jamais en travers de votre route.
- Unifié**  
La gestion unifiée des politiques, les consoles et les tableaux de bord produits optimisent la sécurité de bout en bout.
- Ouvert**  
Avec un large éventail d'API permettant une intégration étendue et un écosystème de développement robuste, votre environnement peut évoluer en fonction des besoins de votre entreprise.

## Cisco Security Cloud

La vision de Cisco pour la sécurité de bout en bout sur l'ensemble des environnements **multicloud a un nom** : Cisco Security Cloud, une plateforme ouverte et **unifiée qui permet de sécuriser tous les utilisateurs, réseaux et applications**, même dans les environnements les plus complexes.



### Les avantages économiques du cloud public, sans ses limites

Ne dépendez plus d'un seul fournisseur. Appuyez-vous sur l'intégration d'API ainsi que sur l'écosystème et le marché de développeurs de la plateforme Cisco Security Cloud pour fournir un modèle ouvert et étendu à vos équipes, réseaux, applications et données.

### Une visibilité totale sur les menaces et les vulnérabilités

Oubliez les silos afin de gagner en visibilité et d'exploiter vos données sur l'ensemble de vos réseaux, clouds, endpoints et applications.

### Une sécurité basée sur l'intention et IA

Vérifiez en continu l'identité des utilisateurs et des appareils, l'état des équipements, les vulnérabilités, et plus encore. Une plateforme unifiée permet aux utilisateurs de définir des politiques de manière centralisée et de les propager.

### La puissance de l'automatisation

Délai de gestion des violations de données réduit de **74 jours** par rapport aux processus manuels

### Une expérience simplifiée pour tous

Sécurité efficace et transparente grâce aux fonctionnalités d'**authentification unique (SSO)**, **architecture de microservices** facilement répliquable de sorte que toutes les connexions sont protégées, et plus encore.

### Plus d'efficacité et plus d'avantages

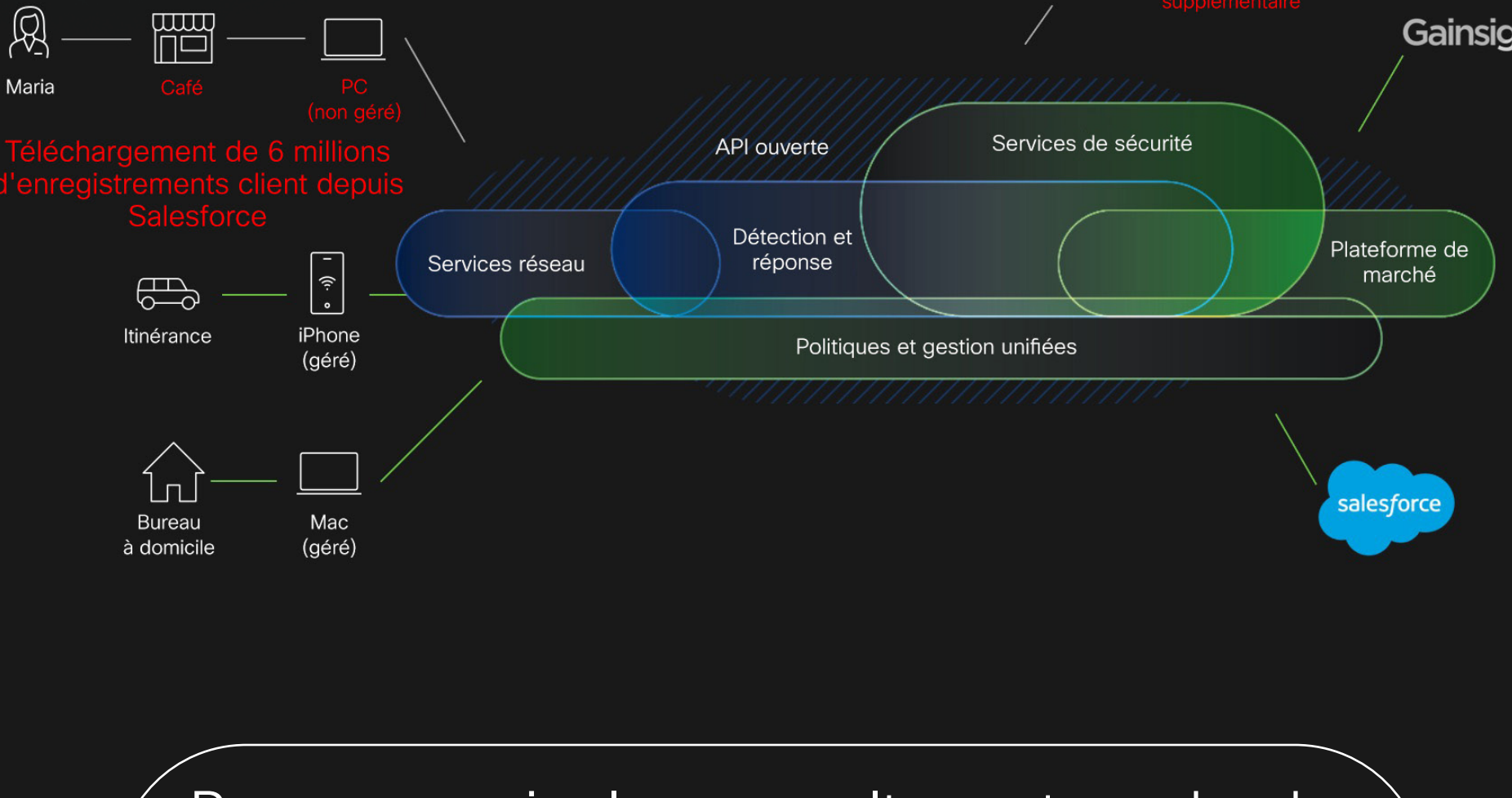
Pour vos équipes SecOps, NetOps, ITOps et DevOps

## Protégez tout, partout

- On-premise**  
Supervisez et protégez tous les composants de votre data center, les ordinateurs de bureau, les ordinateurs portables, mais aussi vos appareils mobiles à la maison.
- Dans le cloud**  
Assurez l'intégration avec les plateformes et les logiciels que vous utilisez pour vos activités, quels qu'ils soient et où qu'ils se trouvent.
- Hybride**  
Protégez tout, partout, grâce à une couverture de bout en bout.

## Sécurisez et connectez tout ce dont votre entreprise a besoin

Accès sécurisé en continu



Pour en savoir plus, consultez notre e-book : **Cisco Security Cloud**  
Préparez-vous pour un avenir placé sous le signe du travail hybride et du multicloud.