Business

Cyberdefense

FORTINET

Cybersécurité à l'ère de la digitalisation

L'alliance stratégique d'Orange Business et Fortinet

L'évolution du marché et des modes de travail

Dans un contexte d’explosion de la cybercriminalité, les attaquants ciblent désormais tous types et toutes tailles d'entreprises. Cependant pour des raisons de compétitivité, celles-ci doivent continuer leur transformation vers le numérique. Les attaques prennent diverses formes telles que les rançongiciels ou le hameçonnage qui exploitent toutes les vulnérabilités technologiques et humaines. Elles évoluent très rapidement et les experts en cybersécurité soulignent notamment que l'émergence de l'intelligence artificielle complexifie davantage encore la lutte contre cette cybercriminalité.

69%* des entreprises françaises ont subi une cyberattaque en 2023, selon l'ANSSI, en augmentation continue depuis 5 ans.

*source : rapport ANSSI 2023

De nouveaux modes de travail avec une adoption massive du télétravail, des employés plus mobiles, une banalisation du Wi-Fi, ainsi que l’accès aux données professionnelles depuis une variété d'équipements parfois personnels, le tout associé à une adoption massive du Cloud, font que les réseaux d'entreprise sont devenus beaucoup plus complexes à maîtriser et à sécuriser.

75% Hameçonnage et hameçonnage ciblé

40% Rançongiciel

32% Exploitation de failles de sécurité

Types d'attaques les plus fréquents

source : rapport ANSSI 2023

« La cybersécurité n'est pas seulement une question de technologie, mais aussi de comportements humains. C'est dans l'alliance de la vigilance technologique et de la sensibilisation que réside notre meilleure défense. »

Barack Obama - 44e président des États-Unis

La transformation numérique est à l’origine d’une demande croissante pour des réseaux intelligents, flexibles et performants, à même d'absorber une utilisation massive du Cloud et d'Internet, d'offrir une grande mobilité aux utilisateurs, de supporter l'explosion des données tout en garantissant un environnement parfaitement sécurisé.

Pour toutes ces raisons les stratégies de sécurité se doivent d’évoluer pour assurer la protection des informations sensibles face à un environnement de travail hétérogène et évolutif.

Les challenges de gestion des réseaux et de sécurité

La généralisation du télétravail et l'évolution constante des menaces requièrent une vigilance accrue de toutes les entreprises, indépendamment de leur taille ou de leur secteur d'activité.

La cybersécurité est stratégique pour garantir la continuité d'activité des entreprises, protéger leurs données, leurs collaborateurs et clients tout en assurant productivité et accessibilité.

Les défis auxquels les entreprises font face :

- **la protection contre les attaques sophistiquées**
- **la gestion des équipements professionnels et personnels**
- **l'utilisation sécurisée des applications cloud**
- **la conformité réglementaire**

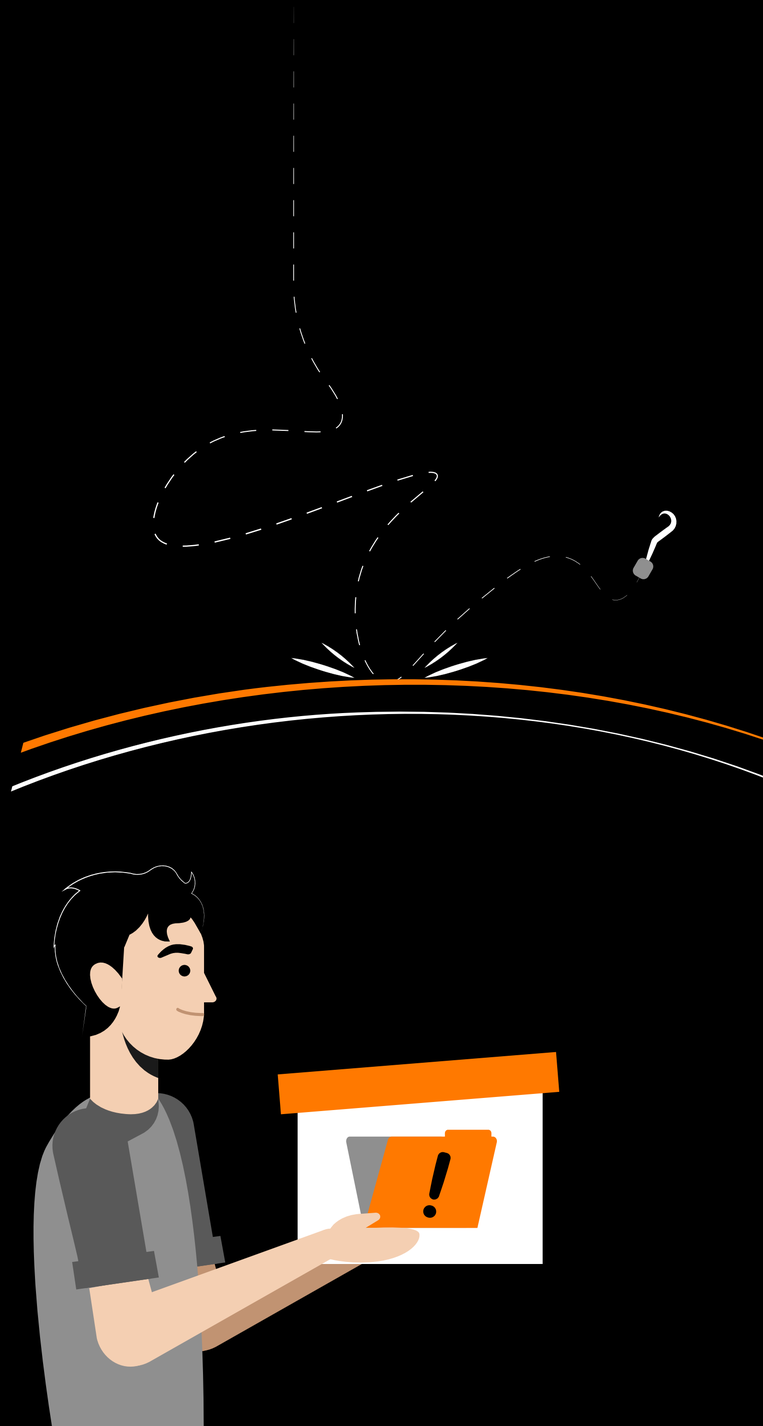
La nécessité de rechercher des solutions et de s'appuyer sur des partenaires compétents est incontournable pour maintenir une protection efficace.

> « Le niveau de cybersécurité en dit beaucoup sur l'avenir d'une entreprise. À l'image des enjeux de durabilité, les organisations de toutes tailles et notamment cotées intègrent dans leur rapport leur stratégie et objectifs cyber.
>
> Cet exercice de transparence, désormais imposé aux USA, est un indicateur précieux vis-à-vis des parties prenantes car il traduit : maîtrise de la transformation numérique, profitabilité et investissement à long terme, préservation des intérêts des clients et sous-traitants, capacité à attirer, retenir et engager des talents »

Laurent Celerier, Executive Vice-President "Central Europe & International Business", Orange Cyberdefense

Relever ces challenges exige une approche qui inclut systématiquement la sécurité dans les choix de connectivité du site à l'utilisateur lorsque ce dernier est à distance.

Les solutions technologiques avancées doivent être consolidées afin d'appliquer des politiques de sécurité unifiées et cohérentes sur l'ensemble des cas d'usages que couvre l'architecture réseau d'une entreprise.



Les stratégies à adopter pour allier meilleure connectivité et sécurité

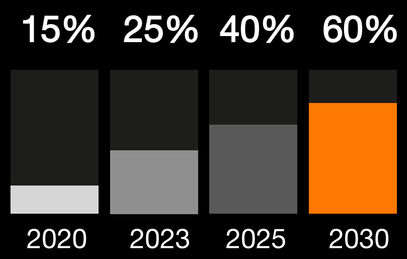
Orange Business propose une approche homogène afin de vous accompagner dans votre stratégie de sécurisation des infrastructures.

L'approche Secure SD-Branch de Fortinet répond aux défis de sécurité sur site comme aux cyberattaques. Cette solution contribue à mieux sécuriser l'utilisation du système d'information de l'entreprise avec l'intégration des fonctions de sécurité et de réseau. Grâce à une console unique, elle permet une gestion centralisée des fonctions SD-Branch telles que le pare-feu de nouvelle génération, la gestion des liens WAN, ou encore le pilotage des réseaux LAN et Wi-Fi, simplifiant ainsi la protection des utilisateurs, où qu'ils soient.

SD-Branch permet d'étendre les fonctionnalités du SD-WAN à l'ensemble du réseau de succursales par la consolidation des services et la convergence de la gestion.

Marché du SD-Branch en pleine croissance en France **

** : Source IDC SD-WAN & SASE : Panorama du marché 2023 et perspectives 2024



Les plus d'une approche SD-Branch

Une visibilité complète sur le réseau qui permet l'application de politiques de sécurité cohérentes, prévenant les intrusions et les logiciels malveillants, y compris les rançongiciels.

Une connexion sécurisée pour tous les employés accédant aux ressources de l'entreprise grâce aux avantages de l'architecture.

Les données sensibles restent protégées tout en offrant une expérience utilisateur optimale, avec des performances réseau améliorées.

La collaboration entre Orange et Fortinet offre aux entreprises une solution robuste et orchestrée pour naviguer dans un environnement en constante évolution.

Une expérience d’ultra connexion sécurisée quel que soit le terminal utilisé

Marc, commercial dans une entreprise avec de nombreux sites en France et à l’international

- **Besoins :** Déploiement rapide et agile de nouveaux sites ; ultra connexion permanente dans l'entreprise ou en mobilité ; multi-terminaux pour des usages privés et professionnels ; besoin de partage de grands volumes d'informations.

- **Menaces :** Les attaques d'hameçonnage ciblées, les logiciels malveillants, les risques de vol ou perte d’appareil, violations ou pertes de données voire d’exploitation.
Si un cybercriminel parvient à compromettre la sécurité des appareils de Marc, il pourrait accéder aux informations très confidentielles de l'entreprise ainsi qu'à des données personnelles sensibles.

- Avec l’approche SD-Branch pour la sécurisation de flux de données et d’accès de l’entreprise, Marc peut développer sereinement ses nouvelles succursales à l’international, notamment dans ses tous nouveaux locaux de Prague. Il y retrouve l'ensemble de son environnement de travail habituel grâce à une architecture de type SD-Branch composée de switchs et de points d’accès Wi-Fi + 5G pour étendre la sécurité au plus proche de l’utilisateur. Il empêche ainsi la propagation d’une menace à l’ensemble des autres utilisateurs et aux ressources stratégiques de l’entreprise et de ses partenaires.

- Grâce à la solution de convergence sécurisée d'accès et de partage de données au sein de l’entreprise, Marc peut partager un document très confidentiel. Dans un premier temps, Marc tente d’utiliser son compte personnel de stockage, ce qui est contraire aux règles de sécurité de l'entreprise. Heureusement, l’équipe informatique s’en rend compte immédiatement grâce à la visibilité dont elle dispose sur le réseau ; elle déclenche une action automatisée d’application des bonnes pratiques auprès de Marc en l’informant et en bloquant son action. Cette solution fonctionne pour le cloud et les datacenters privés. Pour l’’entreprise, c’est la garantie d’une politique de sécurité unifiée en temps réel et de la protection des utilisateurs, des données et des applications.

30% des organisations d'infrastructures critiques subiront une faille de sécurité d'ici 2025 ***

*** Source : Gartner "Predicts 30 of critical nifrastructure organisation"

L’avantage d'un écosystème unifié de réseaux et de sécurité

Les plus grands défis de la transformation digitale découlent de sa complexité intrinsèque. L'harmonisation des objectifs business avec la stratégie digitale, la gestion des interdépendances entre les solutions réseau, IT et cloud en garantissant la sécurité, représentent un véritable challenge pour les organisations.

Avec Evolution Platform, Orange regroupe les solutions de connectivité et de sécurité des réseaux les plus récentes de son écosystème de partenaires au travers d'une plateforme de services personnalisable et ajustable, en temps réel, aux besoins de votre entreprise. Pilotable depuis une console en self-service ou via des API, Evolution Platform combine une infrastructure numérique sécurisée et une gestion de services alignée avec les standards du cloud (instantanéité de déploiement et paiement à l'usage).

En s'appuyant sur la forte capillarité et l'étanchéité du réseau Orange, Evolution Platform promet des performances réseaux et sécurité accrues ainsi que des engagements de qualité de services assurés de bout en bout.

En gardant cela à l’esprit, Orange et Fortinet proposent des solutions et services complets de réseau, cloud et cybersécurité permettant :

1

Gestion simplifiée et contrôle automatique

La visibilité unifiée s'étend à l'ensemble de votre infrastructure, y compris les appareils intelligents, les objets connectés et les systèmes Operational Technology. Cette convergence de la sécurité et des réseaux garantit une protection optimale sur tous les périphériques, utilisateurs, appareils et données.

Pour une confidentialité accrue, vous pouvez sécuriser les ports et limiter l'accès à vos réseaux aux seuls utilisateurs et appareils approuvés. La segmentation et la micro-segmentation réseau permettent d'appliquer des politiques d'accès granulaires et de surveiller le trafic réseau en détail.

2

Sécurité avancée et enrichie avec l’IA

Vous pouvez renforcer la sécurité à travers vos environnements physiques, virtuels et cloud. Les FortiGuard Labs utilisent des capacités avancées d'Intelligence Artificielle et d’apprentissage automatique / Machine Learning (ML) pour générer une intelligence sur les menaces partagée en temps réel afin de maintenir toutes les parties de l'infrastructure de sécurité informées des dernières variantes d'attaques pour une détection et des réponses rapides.

3

Expérience utilisateur améliorée

Grâce à l’optimisation continue des performances réseau et applicatives, lors de l'accès et de l'utilisation de vos ressources et applications. Et ceci, quel que soit leur lieu d'hébergement et la localisation de vos utilisateurs.

4

Accompagnement

Accompagnement de bout en bout pour comprendre vos besoins d’aujourd’hui et de demain ainsi que les cas d’usages spécifiques à votre business.

- Consulting et audit
- Déploiement agile
- Suivi et vie de solution

Utilisateur de votre réseau : Qui, quand, quoi, comment et d’où ?

Utilisation ludique ou inappropriée du réseau,
Usurpation d’identité et élévation de privilèges par des pirates ou un collaborateur mécontent,
Vol ou perte de données et matériels,
Respect du cadre réglementaire et protection de la vie privée des utilisateurs…

...Les embûches sont nombreuses pour vos équipes réseau et sécurité !

Identification + Authentification + Autorisation des utilisateurs = Bon fonctionnement, traçabilité et intégrité de votre réseau

« Avec l’évolution des besoins et des usages, la numérisation des entreprises s’est accélérée et elles sont complètement dépendantes du numérique. La notion de confiance dans celui-ci devient indispensable. C’est pourquoi les organisations cherchent à avoir une connectivité agile, flexible et adaptable aux besoins des métiers actuels et futurs mais également sécurisée. Cette convergence réseau et sécurité est devenue indispensable à la pérennité des entreprises de toutes tailles. »

Christophe Auberger - Cyber Évangéliste Fortinet

A chaque usage, une expérience sécurisée et connectée

Sylvie travaille à l’international dans des lieux tels que les aéroports, hôtels ou cafés.

- **Besoins :** Accéder en toute sécurité aux ressources et aux applications de l'entreprise, et à des services cloud (Microsoft 365 ou Salesforce).
- **Menaces :** Les cyberattaques, les difficultés de connexion sécurisée en tous lieux aux applications métier.

- En déplacement, avec FortiSASE embarqué dans Evolution Platform, Sylvie bénéficie d’une connectivité sécurisée et optimisée. Elle se connecte à Internet depuis un tiers-lieu. Son trafic est automatiquement dirigé vers le point de présence Orange le plus proche. Là, il est inspecté et sécurisé grâce à des technologies de pointe telles que le pare-feu nouvelle génération, la prévention des intrusions et le filtrage du contenu. Cette solution SASE intègre la gestion des identités, des contrôles d'accès aux terminaux, aux réseaux et aux applications. FortiSASE associe l'expertise de Fortinet en matière de connectivité et de sécurité à la puissance du réseau Orange et à son savoir-faire en termes d'accompagnement (audit, design, build et run) et à l'expertise d'Orange Cyberdefense en termes de connaissance de la menace.

- Au bureau, sécurité et performances optimales avec Flexible SD-WAN permettent à Sylvie de toujours bénéficier d'une expérience fluide et sécurisée. En effet, le service Flexible SD-WAN de Fortinet intégré à Evolution Platform optimise le trafic en fonction du réseau, garantissant de meilleures performances. De plus, la sécurité des points de terminaison protège les terminaux de Sylvie contre les menaces, même sur les réseaux Wi-Fi publics non sécurisés.

SASE est une nouvelle approche de la sécurité des réseaux qui combine les fonctions de sécurité réseau et de réseau étendu (WAN) dans un seul service cloud.

82% des entreprises françaises déclarent que la sécurité est le principal facteur de décision lors du choix d'une solution SASE ****

**** source : IDC Survey: Security Is the Top Driver for SASE Adoption in France oct 2023

Orange et Fortinet, un partenariat axé sur la réussite

15 ans de partenariat

650 Experts Orange certifiés Fortinet

Partenariat stratégique

Orange et Fortinet s'associent pour proposer une solution complète, flexible, sécurisée et évolutive. Nous mettons nos savoir-faire en matière de connectivité, de cloud, de sécurité et d’intégration au service de votre projet de transformation digitale afin de vous apporter les bonnes réponses face à vos enjeux et besoins spécifiques. En choisissant Orange Business et Fortinet, vous bénéficiez d'une approche holistique, d'une expertise reconnue et d'une solution de sécurité complète pour soutenir votre projet de transformation numérique, et garantir la continuité de vos activités. Vous n’avez plus qu’à vous concentrer sur votre cœur de métier.

À propos d'Orange Business et Fortinet

Orange Business, l'entité d'Orange dédiée aux entreprises, est un intégrateur réseau et numérique de référence. Orange Business s'appuie sur son expertise en matière de connectivité nouvelle génération, de cloud et de cybersécurité, ses plateformes de services ainsi que sur son écosystème de partenaires pour offrir aux entreprises du monde entier des solutions numériques de confiance. Forts de 30 000 collaborateurs à travers 65 pays, Orange Business orchestre la transformation des entreprises de bout en bout en concentrant sa proposition de valeur sur les infrastructures digitales sécurisées, l'expérience clients, l'expérience salariés et l'expérience opérationnelle. Plus de 2 millions de professionnels, entreprises et collectivités en France et 3 000 multinationales font confiance à Orange Business.

Orange est l'un des principaux opérateurs de télécommunication dans le monde, avec un chiffre d'affaires de 43,5 milliards d'euros en 2022 et 296 millions de clients au 30 septembre 2023. Avec Evolution Platform, Orange couple l'expertise de son écosystème de fournisseurs à la puissance de son réseau via une intégration native des solutions de ses partenaires sur ce dernier pour permettre à vos utilisateurs de bénéficier des dernières mises à jour mais également de meilleures performances réseau et sécurité.

Fortinet (NASDAQ : FTNT) est un élément moteur de l'évolution de la cybersécurité ainsi que de la convergence des réseaux et de la sécurité. Notre mission est de protéger les utilisateurs, les dispositifs et les données, où qu'ils se trouvent. Aujourd'hui, nous déployons une cybersécurité sur le périmètre de votre choix, grâce à notre offre de plus de 50 produits professionnels. Plus d'un demi-million de clients font confiance aux solutions de Fortinet, des solutions déployées à grande échelle, bénéficiant de multiples brevets et reconnues par le marché. Le Fortinet Training Institute, l'un des programmes de formation les plus vastes et les plus étendus du secteur, se consacre à la formation à la cybersécurité et aux nouvelles opportunités de carrière disponibles pour tous. FortiGuard Labs, la division de Fortinet dédiée à la veille et aux études sur les menaces, conçoit et utilise des technologies IA et de machine Learning performantes pour apporter aux clients une protection optimale et une veille décisionnelle sur les menaces. Pour en savoir plus, consultez https://www.fortinet.com, le blog Fortinet et FortiGuard Labs.

En savoir plus :
www.orangebusiness.com
LinkedIn : Orange Business
Twitter : @OrangeBusiness

Sources :

* : rapport ANSSI 2023

** : IDC SD-WAN & SASE : Panorama du marché 2023 et perspectives 2024

*** : Gartner "Predicts 30 of critical nifrastructure organisation"

**** : IDC Survey: Security Is the Top Driver for SASE Adoption in France oct 2023

orange™ Business

FORTINET®