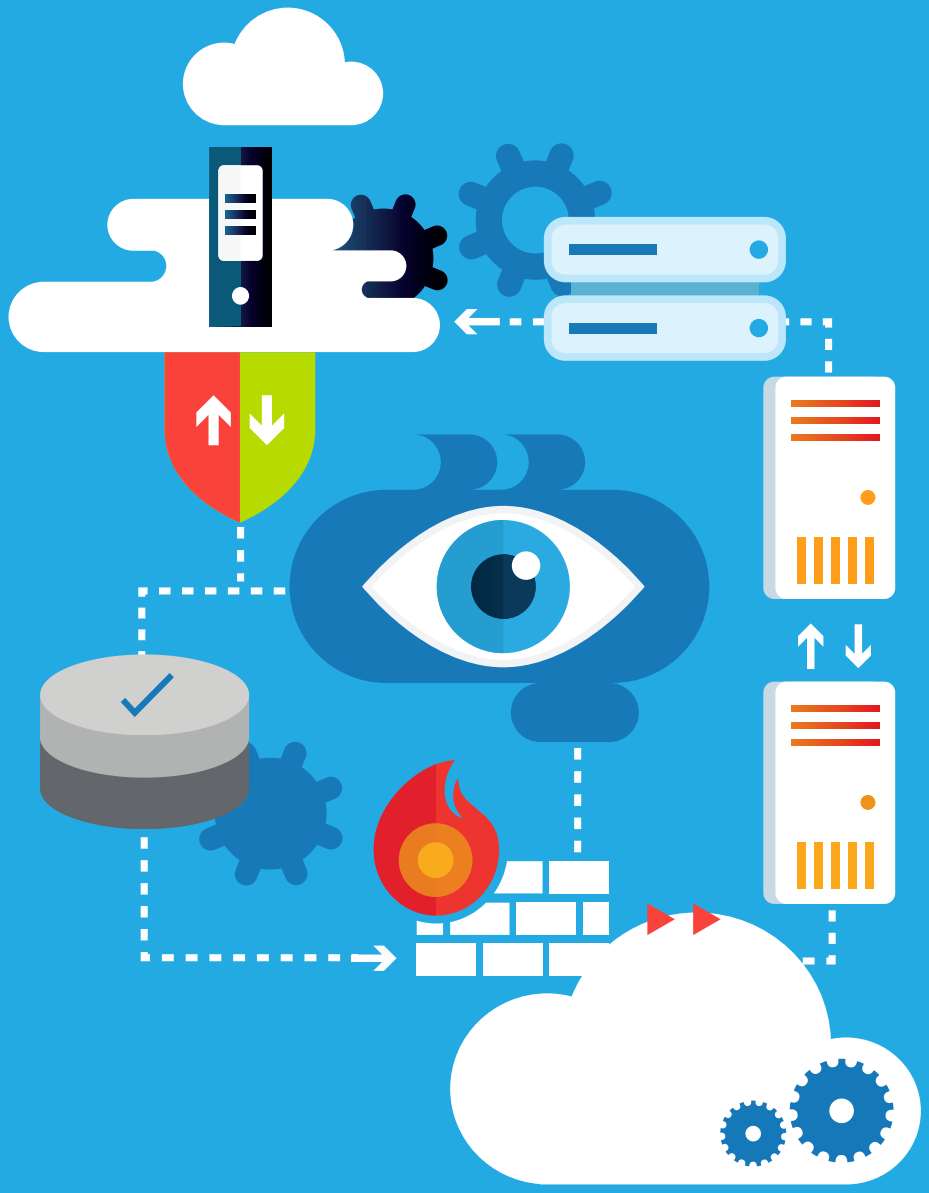
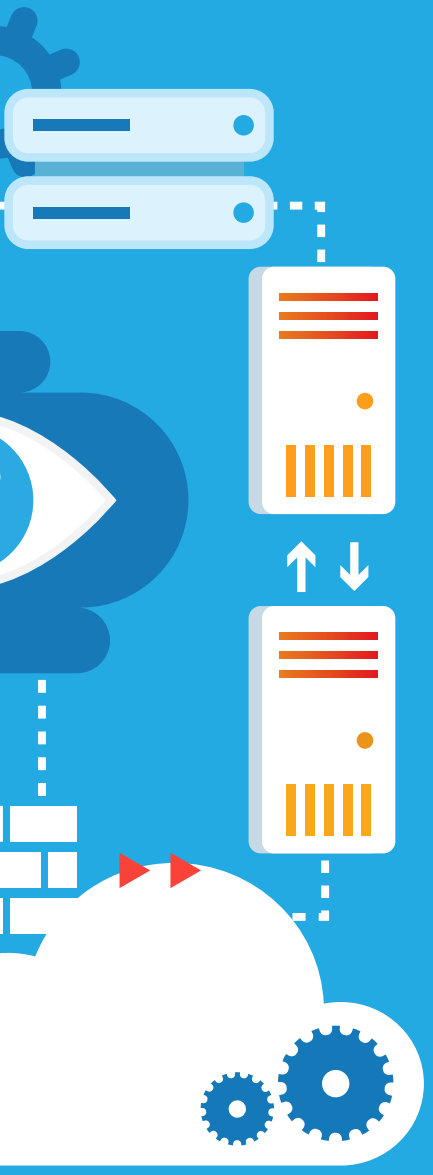
CITRIX®

Construisez une approche stratégique de la sécurité de votre réseau et de vos applications

Comment sécuriser l'intégralité de votre écosystème digital.





Sommaire

Les attaques sophistiquées contre les applications, telles que WannaCry et NetPetya, ont beaucoup retenu l'attention des médias, avec raison. Elles évoluent, sont répétées et leur fréquence augmente rapidement.

Mais les attaques contre les applications ne sont pas les seules menaces auxquelles vous devez porter attention. Les menaces en tout genre sont omniprésentes. Du réseau jusqu'aux applications, les attaques continuent de frapper les entreprises à chaque niveau de l'infrastructure. Historiquement, la solution consistait à rajouter un autre produit individuel, mais cette approche laisse des failles dans la sécurité. Seule une solution globale, de bout en bout peut protéger entièrement vos données, où qu'elles se trouvent.

Trouver l'équilibre entre sécurité et utilisabilité

Les utilisateurs veulent pouvoir choisir leurs applications et leurs appareils et avoir la flexibilité de travailler où et quand ils le souhaitent. Mais ces exigences entraînent une grande complexité, des risques pour la sécurité et la prolifération des systèmes que doivent gérer les équipes IT. Si elles adoptent la bonne solution, les entreprises n'ont pas à donner la priorité à l'un de ces problèmes plutôt qu'à l'autre, elles peuvent tout avoir.

Où que se trouvent les données, votre entreprise peut donner à ses collaborateurs les outils qu'ils désirent tout en garantissant aux équipes IT de disposer de la visibilité et du contrôle nécessaires pour surveiller activement l'intégralité de votre écosystème depuis une console unifiée.

← P. 3 | P. 5 →

Retour au sommaire

Les menaces se métamorphosent pour déjouer la sécurité

Les attaques ne cessent d'évoluer pour mettre en échec la sécurité.
Elles sont désormais omniprésentes à tous les niveaux de votre infrastructure informatique.
Voici un résumé de la manière dont les attaques évoluent.

Attaques réseau courantes :
Historiquement, les réseaux ont été la cible principale des attaques. Les formes de défense les plus efficaces comprennent les pare-feu, la correction et la formation, qui n'ont jamais été des options extraordinaires mais, tant que les données étaient dissimulées derrière un pare-feu, les entreprises pouvaient en général garder le contrôle. Ceci jusqu'à ce que les menaces progressent le long de la chaîne vers la pile et en dehors du datacenter.

Attaques contre le réseau

- Force brute
- Attaques de ver
- DNS
- Scan de ports
- Autres

Attaques courantes contre le web et les applications :
Avec la prolifération des données en dehors du datacenter et sur les différents clouds, web, appareils et applications, il est devenu de plus en plus difficile d'assurer la sécurité. Des attaques sophistiquées sont apparues, suivant les données tout au long des couches de la pile et en dehors du pare-feu, vers les couches cloud, web et applicative.

Attaques contre le web et les applications

- Navigation
- Attaques par interprétation des URL
- Attaques par injection SQL
- Attaques par usurpation d'identité
- Attaques par saturation
- DDoS (déni de service distribué)

← P. 4 | P. 6 →

Retour au sommaire

Les méthodes traditionnelles ne fonctionnent plus

Dans le but de déjouer les menaces émergentes, de nombreuses entreprises ont ajouté des solutions ponctuelles individuelles pour répondre à des besoins de sécurité spécifiques. Une pour la protection des terminaux, une autre pour les applications et une encore pour le réseau. Ces systèmes disparates ne fonctionnent pas car ils :

- **ajoutent de la complexité.** Avec le déplacement des données du datacenter vers le cloud, voire vers les terminaux situés au-delà du pare-feu, les équipes IT se sont retrouvées avec différents systèmes pour gérer et sécuriser toutes les données.

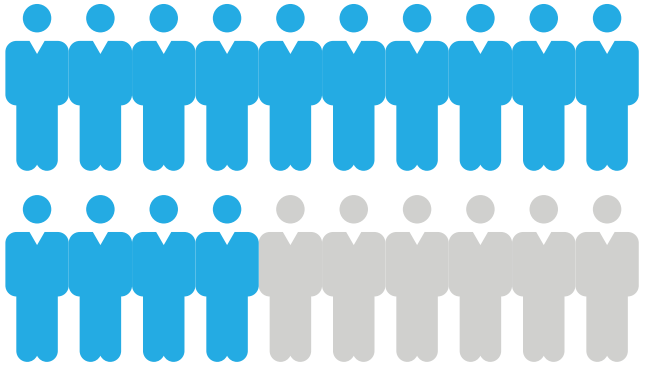
- **laissent des trous.** Ces différents systèmes n'ont pas été conçus pour une couverture de bout en bout et laissent des trous par lesquels des logiciels malveillants peuvent s'infiltrer.

- **ne se parlent pas entre eux.** Des solutions ponctuelles par silos ne peuvent pas détecter des anomalies ou des altérations et ne sont donc pas capables d'empêcher proactivement les menaces d'attaquer votre réseau.

- **ne peuvent pas identifier des attaques inconnues :** De nombreux systèmes de sécurité disparates sont confrontés au problème important des menaces qu'ils ne peuvent pas voir. Connues également sous le nom d'attaques de type « day zero », elles peuvent passer inaperçues pendant de longues périodes, permettant aux hackers d'accéder à des données sensibles aussi longtemps qu'ils ne sont pas découverts.

- **n'empêchent pas les menaces internes.** La majorité des solutions de sécurité visent à empêcher les méchants d'entrer mais ne sont pas conçues pour prévenir les fuites venant de l'intérieur. Les solutions ponctuelles ne sont pas conçues pour reconnaître et arrêter des comportements inhabituels. Par conséquent, elles sont incapables d'empêcher la fuite d'informations sensibles vers l'extérieur du réseau.

- **ne peuvent pas segmenter l'accès en se basant sur les besoins de l'utilisateur :** La gestion des comportements des utilisateurs sur les différents terminaux (notamment sur les appareils BYOD) est beaucoup plus difficile avec des solutions ponctuelles individuelles et ajoute au fardeau des équipes IT déjà surchargées.



Plus de

70 %

des cadres disent que le principal coupable à l'origine des risques de cybersécurité est la prolifération des applications et appareils BYO que les collaborateurs emmènent sur le lieu de travail.[1]

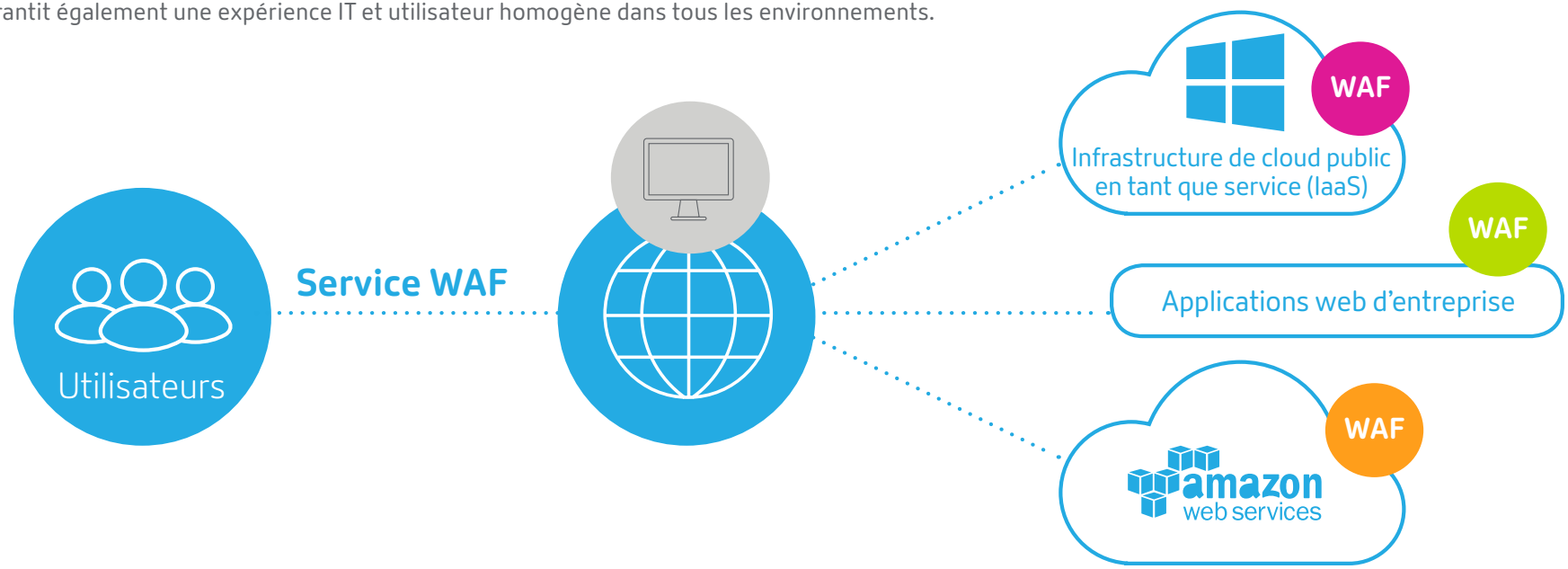
← P. 5 | P. 7 →

Retour au sommaire

Pourquoi une nouvelle approche de la sécurité est primordiale

Avec la prolifération des services cloud que nous constatons aujourd'hui, il est fort probable que votre entreprise rencontre de nouveaux types de menaces. Vous avez donc besoin d'une plateforme qui puisse sécuriser vos données partout, que ce soit au niveau de la couche réseau, web ou applicative.

Une approche de bout en bout, qui comprend un pare-feu d'application web (WAF) entièrement intégré, vous permet de gérer des menaces sur tous les clouds, réseaux, appareils et utilisateurs. Elle garantit également une expérience IT et utilisateur homogène dans tous les environnements.



← P. 6 | P. 8 →
Retour au sommaire

74 %

des entreprises reconnaissent qu'un nouveau cadre de sécurité IT est nécessaire pour améliorer la posture de sécurité et réduire les risques.[1]

← P. 7 | P. 9 →

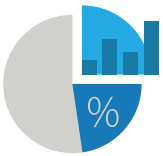
Retour au sommaire

L’approche idéale de la sécurité est holistique

Une méthode unifiée, contextuelle et sécurisée fournit des systèmes fiables et disponibles tout en veillant à ce que les données restent confidentielles et protégées grâce à :

Une visibilité à 360 degrés

Vous avez besoin d’une vue complète sur le trafic et les transactions qui traversent votre écosystème afin de pouvoir détecter les menaces ou activités inhabituelles, telles qu’un signe indiquant que des identifiants sont utilisés à une heure atypique depuis un emplacement improbable.



La fourniture d’insights actionnables provenant de l’analytique

La télémétrie avancée vous permet de collecter des données depuis n’importe quelle source (journaux d’appareils, de serveurs, d’applications, compteurs, emails, produits SIEM tiers, etc.). Vous pouvez alors suivre, analyser et détecter les anomalies sur vos réseaux, clouds, applications, trafic web et utilisateurs, et alerter proactivement les équipes IT sur les problèmes potentiels avant que ceux-ci n’infectent vos systèmes.

Un accès simplifié

Que ce soit pour un appareil BYOD, un poste de travail dédié ou un appareil partagé, le SSO (Single Sign-On) simplifie le processus d’accès pour les utilisateurs tout en réduisant la charge que représente pour les équipes IT la résolution de problèmes de mots de passe ou d’expiration de privilèges d’accès.

La capacité à gérer, renouveler, définir et appliquer des stratégies

Assurez-vous que votre entreprise peut contrôler les niveaux d’accès afin que seules les personnes autorisées aient connaissance des données sensibles.

Envoyez des mises à jour et des correctifs au niveau mondial

La correction et la mise à jour de la multitude d’appareils utilisés sont presque impossibles. En gérant les systèmes depuis un emplacement centralisé, les équipes sont capables de déployer des correctifs et des mises à jour en quelques minutes au lieu de plusieurs heures.

Protégez-vous des attaques ciblées contre la couche applicative

Appliquer un ensemble de règles pour protéger les pare-feu d’application web (WAF) des serveurs vous aide à vous protéger contre les attaques courantes, notamment le cross-site scripting (XSS) et les injections SQL.

Fournissez un chiffrement de bout en bout

Gérez le trafic et les certificats pour apporter de la résilience à votre datacenter et vous protéger sur des environnements hybrides et multi-cloud.

← P. 8 | P. 10 →

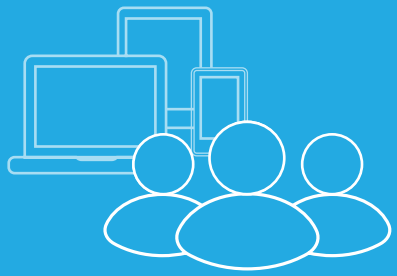
Retour au sommaire

Une sécurité complète avec un espace de travail digital sécurisé

Unification

Les équipes IT peuvent configurer, superviser et gérer l'ensemble de votre infrastructure informatique grâce à une vue unifiée afin d'offrir une expérience utilisateur unifiée.

Sécurisation



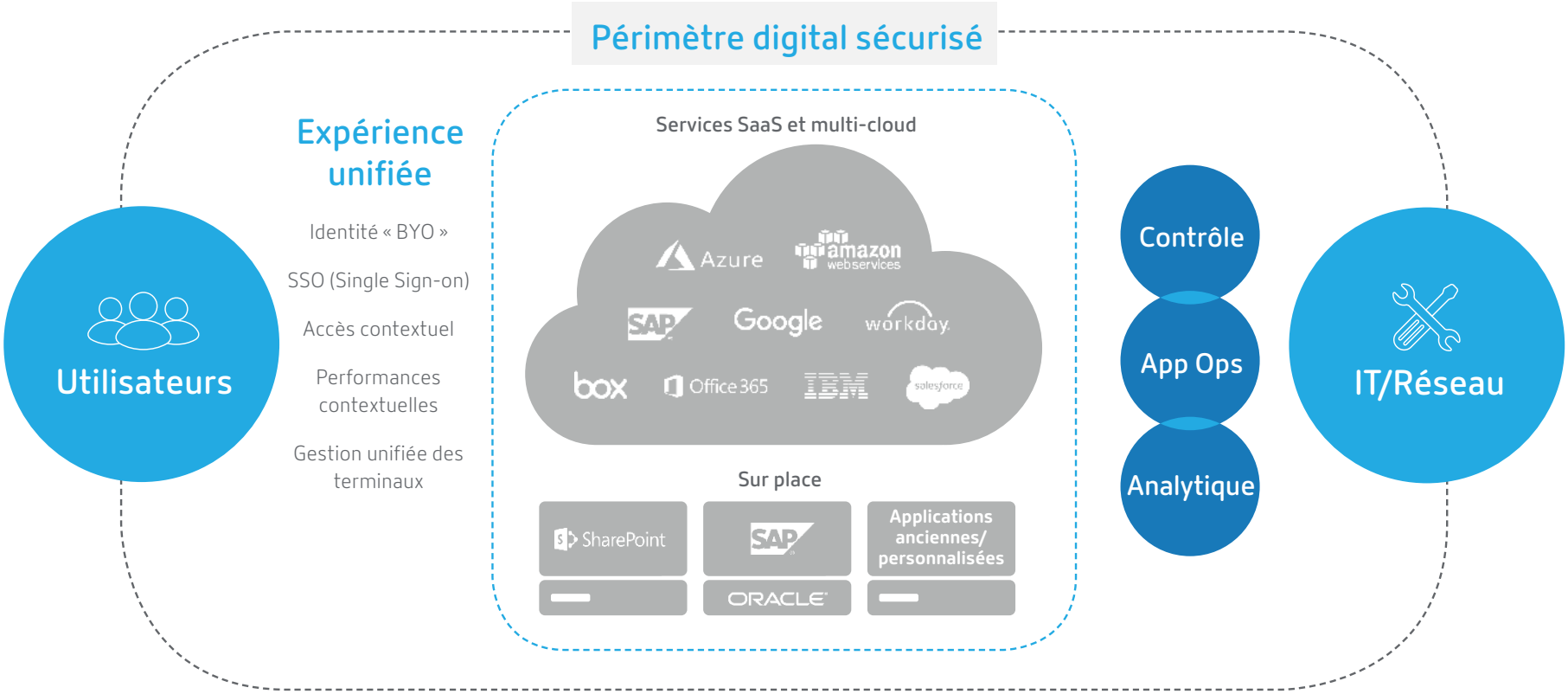
Une stratégie de sécurité centrée sur les utilisateurs place l'utilisateur au centre de votre infrastructure de sécurité et synthétise l'ensemble des connaissances relatives à l'utilisateur et à son comportement pour fournir un accès contextuel, des contrôles de sécurité et des analyses prédictives afin d'offrir une visibilité complète sur le réseau et l'écosystème des utilisateurs.

Contextualisation

Les Digital Workspaces utilisent le Machine learning pour s'adapter aux schémas et particularités de chaque utilisateur afin qu'il puisse mener à bien ses activités en toute sécurité et rester productif, où qu'il se trouve.

Offrez la bonne expérience au bon utilisateur au bon moment

L'augmentation incessante de la complexité du réseau et du nombre d'applications fonctionnant sur une grande variété de clouds est complexe à gérer et augmente vos risques de sécurité. Citrix Workspace permet aux équipes IT de prendre le contrôle des menaces de sécurité et de les gérer proactivement dans les environnements distribués, hybrides, multi-cloud et multi-appareils d'aujourd'hui. Au lieu de gérer plusieurs produits individuels qui ne s'intègrent pas et qui peuvent donc entraîner des failles dans la sécurité de bout en bout, Citrix est le seul fournisseur qui permette une approche complète de la sécurité des applications et du réseau à de multiples niveaux. L'offre de sécurité de Citrix Analytics vous fournit un unique tableau de bord pour surveiller, gérer et résoudre les risques de sécurité.



← P. 10 | P. 12 →

Retour au sommaire

Avantages métier supplémentaires de notre approche de la sécurité

Collaboration sécurisée avec protection de la propriété intellectuelle :
Conçu spécifiquement pour fournir une sécurité adaptée aux entreprises, Citrix permet à vos utilisateurs d'échanger et de collaborer sur des documents facilement, professionnellement et de façon sécurisée tout en respectant les standards de chiffrement AES 256 pour toutes les métadonnées et tous les contenus.

Conformité, risques et gouvernance (GRC) :
En intégrant la solution GRC dans le champ d'application de l'approche de la sécurité Citrix et en la prenant en charge à l'aide de nos fonctionnalités d'analytique complètes, nous sommes capables de fournir une approche beaucoup plus synchronisée répondant à tous vos besoins en matière de sécurité et de conformité.

← P. 11 | P. 13 →

Retour au sommaire

Notre direction cherchait à obtenir un mode de travail efficace et flexible mais nous devions nous assurer qu'il était fiable. Avec Citrix Workspace, nous savons que notre sécurité est optimale, ce qui est essentiel lorsque l'on manipule, comme Stater, des informations financières aussi sensibles.

— Frank Veldink, architecte Infrastructures de communication et d'information chez Stater

CITRIX®

Découvrez comment une approche intelligente et intégrée de la sécurité peut vous aider à fournir l'accès, le contrôle et la sécurité dont vous avez besoin sur **citrix.fr/secure**.

Sources :
*La nécessité d'une nouvelle architecture de sécurité informatique, Ponemon Institute LLC, parrainé par Citrix, 2017

Retour au sommaire