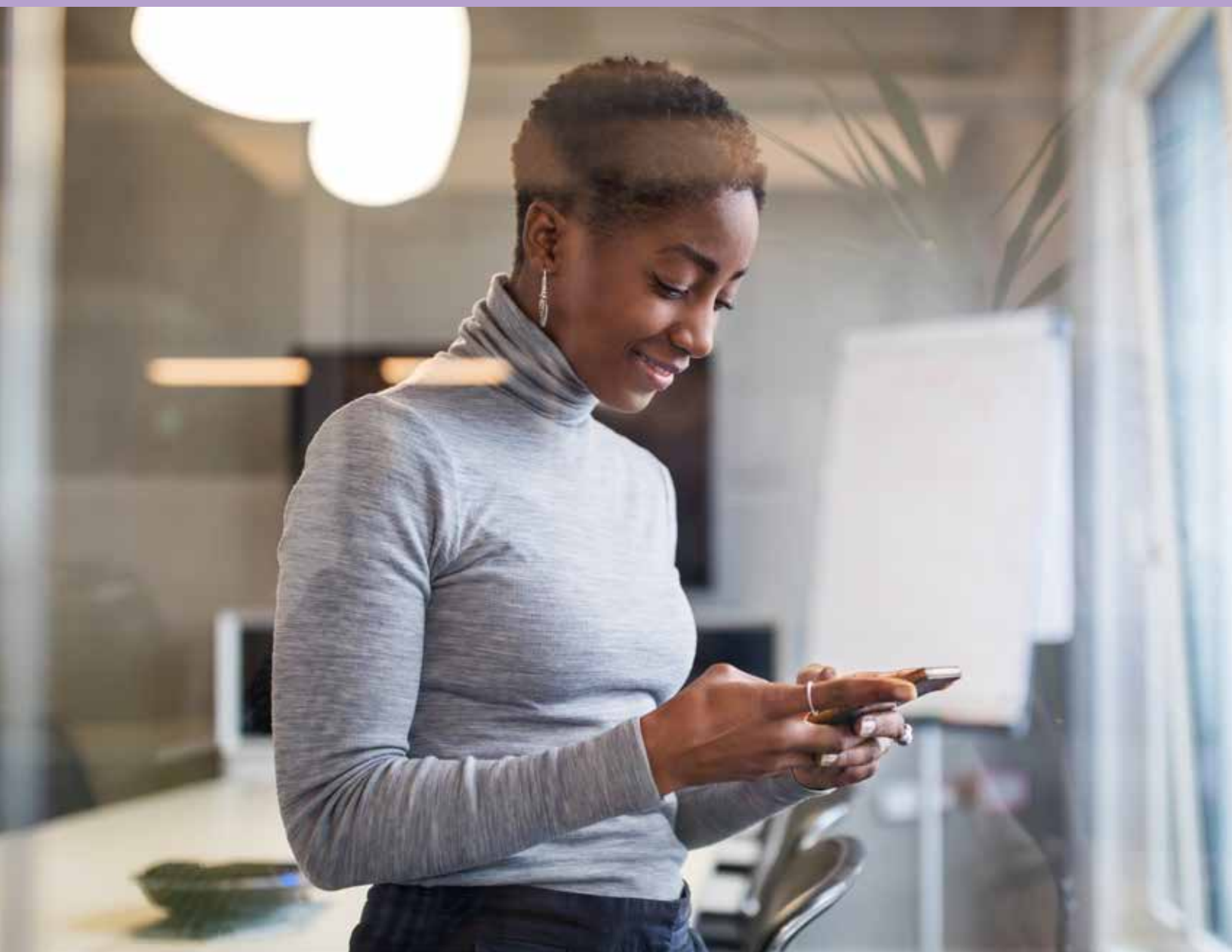
citrix

Livre blanc

Principes pour assurer la continuité d'activité

Protégez votre entreprise contre les disruptions et préservez partout la productivité de votre personnel



Ce livre blanc présente une stratégie complète pour maintenir la productivité des utilisateurs lors de disruptions prévues ou imprévues. Il propose des bonnes pratiques permettant la mise en place d'une stratégie complète de continuité d'activité et présente différentes technologies Citrix permettant de garantir l'accès sécurisé aux applications et données, sur tout appareil, via tout réseau et cloud. En garantissant des opérations fluides, quelles que soient les conditions, les solutions Citrix Workspace contribuent à protéger votre entreprise de nombreuses conséquences potentielles (pertes financières, dégradation d'image, affaiblissement des relations avec les clients et partenaires, perte de productivité, etc.).

Aucune entreprise n'est à l'abri d'une interruption mineure ou majeure, qu'il s'agisse d'un événement prévu comme une opération de maintenance IT, un déménagement de bureau, une situation d'urgence imminente (ouragan, tempête de neige, épidémie, etc.) ou d'un événement totalement imprévu frappant sans aucun préavis, comme un tremblement de terre, une tornade, un attentat terroriste ou un incendie. Même le plus petit incident, comme une coupure d'eau ou d'électricité, des retards dans les transports ou une épidémie de grippe saisonnière, peut avoir un impact majeur.

Le plan de continuité d'activité se focalise traditionnellement sur la planification du basculement et sur la haute disponibilité des systèmes métier stratégiques, mais ce n'est qu'un aspect du problème. Pour maintenir leur activité, les entreprises doivent adopter une approche plus complète, englobant à la fois des mesures organisationnelles et des nouvelles technologies, afin de réduire les interruptions, de préserver la sécurité et de garantir une productivité permanente aux utilisateurs et aux équipes. Les bonnes pratiques pour une stratégie de continuité d'activité complète doivent couvrir à la fois la structure de l'équipe en charge de la continuité d'activité, la planification de la continuité d'activité, des tests de reprise après sinistre et de continuité d'activité, une communication de crise et des programmes de sensibilisation et de sécurité des collaborateurs.

En fournissant aux utilisateurs l'expérience de qualité dont ils ont besoin, un Digital Workspace sécurisé garantit l'accès fluide aux applications et données métier hébergées localement ou dans un cloud public, sur tout appareil et via tout réseau. La prise en compte du contexte permet à l'entreprise d'établir un parfait équilibre entre sécurité et flexibilité pour sa situation actuelle, sans compromettre ses ressources. L'analytique et les insights aident les directions IT à garantir la sécurité, la conformité et la suppression des menaces, quels que soient l'endroit et la façon dont les gens travaillent.

L'importance de la continuité d'activité et les défis qu'elle génère

Prévues ou imprévues, les interruptions d'activité qui ne sont pas gérées efficacement coûtent cher. Les pertes de chiffre d'affaires, les opportunités de vente ratées et le non-respect des contrats de niveaux de service peuvent avoir un impact financier désastreux. La rupture de la chaîne d'approvisionnement et des relations avec les partenaires peut retarder le Time-to-market, faire échouer des initiatives importantes et affaiblir la position concurrentielle de l'entreprise. Une réponse inadaptée peut endommager l'image de l'entreprise auprès du public et ébranler la confiance de ses clients et de ses investisseurs. Suite à l'interruption, les utilisateurs peuvent éprouver des difficultés à retrouver leur pleine productivité du fait de pertes de données, de l'interruption d'une tâche en cours, de la perte de cohésion dans la collaboration avec les autres membres de l'équipe et la direction, sans compter l'impact personnel direct que la perturbation a pu avoir sur eux.

« La sécurité de nos étudiants, de notre personnel et des membres de notre communauté est essentielle. Pour permettre à nos collaborateurs de dispenser l'enseignement de grande qualité qui fait la réputation de l'Université de Sydney, nous devons pouvoir nous appuyer sur une technologie qui facilite le partage et la consommation du savoir, d'une façon totalement sécurisée. »

– **Jordan Catling, Directeur adjoint du département Client Technology ICT, Université de Sydney**

Pour les directions IT, la reprise d'activité suite à une disruption peut être un processus long et complexe, impliquant plusieurs tâches comme :

- Remettre les systèmes en ligne et restaurer les données perdues
- Remplacer les périphériques perdus ou inaccessibles et s'assurer que chaque nouveau poste peut exécuter les logiciels indispensables à l'utilisateur
- Assurer le provisioning et la configuration des applications
- Concevoir de nouvelles méthodes de travail et les communiquer aux utilisateurs (méthodes d'accès alternatives, nouvelles adresses pour les applications devenues inaccessibles, etc.)
- Exécuter ces différentes actions dans l'urgence

Un plan efficace de continuité d'activité simplifie et accélère considérablement ce processus, en aidant la direction IT à restaurer et à maintenir le service fourni à l'entreprise, tout en permettant aux utilisateurs de retourner aussi rapidement que possible au travail. Pour les événements connus à l'avance, comme un déménagement de bureau planifié ou un phénomène météo prévu, l'entreprise peut même prévenir de façon préventive toute interruption de l'activité.

Une approche globale pour votre stratégie de continuité d'activité

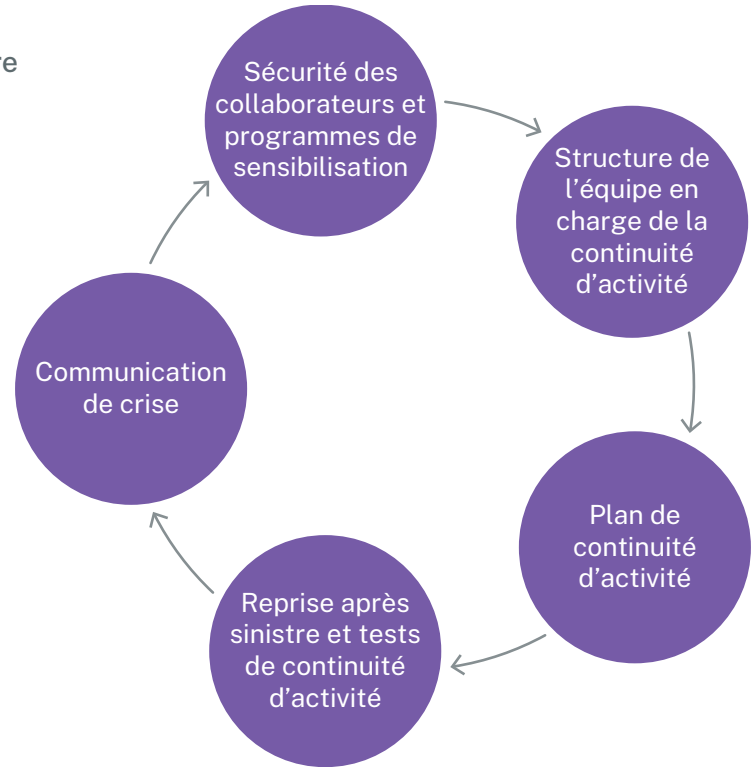
Bien que chaque situation d'urgence soit unique et que de nombreuses décisions doivent être prises à chaud, un plan de continuité d'activité offre un cadre et une orientation pour la prise de décisions, et définit clairement le responsable de ces décisions. Le succès d'un programme de continuité d'activité repose sur la participation active de l'ensemble de la direction dans le processus de développement de ce plan et sur l'adhésion du reste de l'encadrement de l'entreprise. Grâce à ce soutien, les équipes IT et en charge de la sécurité peuvent diriger l'élaboration d'une stratégie complète de continuité d'activité qui englobe l'ensemble des éléments essentiels suivants.

Structure de l'équipe

L'un des éléments majeurs à prendre en compte pour un plan de continuité d'activité est la définition d'une hiérarchie claire en matière de prise de décision. En situation d'urgence, les utilisateurs ne doivent pas avoir à se demander quelle autorité ou quelle personne a la responsabilité de chaque décision importante.

L'entreprise doit être capable d'effectuer toutes les tâches liées à la continuité d'activité dans chacun des sites qu'elle exploite, à la fois pour réagir aux événements locaux et

Standard Citrix en matière de continuité d'activité



coordonner la réaction à l'échelle de l'entreprise lorsqu'une situation d'urgence survient au niveau local ou à plus grande échelle. Les membres clés de l'équipe de continuité d'activité doivent demeurer impliqués dans les processus de planification et de test tout au long de l'année, afin de garantir l'efficacité et l'actualité du plan et de développer le niveau de familiarité et d'entraînement indispensable pour pouvoir agir sous pression en situation d'urgence réelle.

Chez Citrix, une équipe en charge de la continuité d'activité comprend dans chaque région des cadres, des informaticiens, des responsables de site et des locaux, de la sécurité physique, de la communication, des ressources humaines, des finances et d'autres services. Des équipes spécialisées sont dédiées aux tâches suivantes :

- **Intervention d'urgence** : dirige les efforts de planification de la continuité d'activité ; adresse les recommandations finales au comité de direction ; fournit une orientation générale pour la préparation, la réaction et la reprise
- **Communications** : assure la communication au profit de toutes les parties, notamment des employés, des fournisseurs, des services publics et des clients
- **Réponse sur site** : prépare les installations et les équipements en vue de la catastrophe imminente ; effectue une évaluation a posteriori des dommages et de leur impact sur la poursuite des opérations ; fournit une aide pour les déclarations de sinistre à adresser aux assurances ; sécurise les bâtiments et les terrains
- **Réactivité de l'entreprise** : sert de liaison entre les différentes Business Units ; prend les dispositions nécessaires pour mettre en œuvre les opérations de secours conformément au plan de chaque service de l'entreprise ; fournit une intervention tactique et une orientation métier

Chacune de ces équipes rend compte de son activité au Comité de Direction de Citrix.

Planification de la continuité d'activité

Tout plan de continuité d'activité doit identifier à un haut niveau les disruptions potentielles pouvant affecter n'importe quel site de l'entreprise (coupure d'électricité, épidémie, incendie) ou certains sites en particulier (tremblement de terre ou raz de marée dans les régions à fort risque sismique, troubles dans les régions politiquement instables, etc.).
La planification doit également s'étendre à l'ensemble de la chaîne d'approvisionnement, en intégrant la vérification des stratégies de continuité d'activité des principaux fournisseurs, en identifiant les risques potentiels liés aux interruptions d'activité et en évaluant des alternatives. Afin de disposer d'un nombre de situations gérable, concevez votre plan en fonction des pires cas de figure, plutôt que d'en établir plusieurs en fonction du degré de gravité de l'accident.

Il ne sera pas toujours possible de maintenir des opérations normales en situation d'urgence. Afin de limiter l'impact d'une réduction des capacités, votre équipe devra identifier ses opérations les plus vitales, les collaborateurs qui en ont la charge et la façon de repenser ces opérations si nécessaire.

Chez Citrix, cette tâche est confiée à une équipe de directeurs de division, qui dispose d'un analyste en continuité d'activité. Ce groupe travaille en étroite collaboration pour évaluer la criticalité de différents processus d'entreprise en termes de chiffre d'affaires, d'image, de conformité réglementaire ou autre. Il rapproche ensuite cette criticalité avec les dépendances des différents processus en termes d'applications, de personnel, de sites et d'équipements requis pour leur soutien. Une fois cette analyse effectuée, le groupe peut commencer à identifier les stratégies de restauration (et leurs coûts) pour chaque processus. Ces données fourniront à l'IT les moyens de définir un cadre qui garantit la disponibilité des applications critiques dans un délai (durée maximale d'interruption admissible) et à un niveau (perte de données maximale admissible) préétablis.

Les tests

Un plan de continuité d'activité n'est efficace que s'il est mis à jour. Sans un effort continu de préparation aux situations d'urgence, l'entreprise peut très bien découvrir le moment venu que son plan n'est plus adapté à son activité et éprouver d'autant plus de difficultés à réagir qu'elle éprouvait un certain sentiment de sécurité.

Les bonnes pratiques en la matière conseillent une mise à jour annuelle du plan de continuité d'activité afin de prendre en compte les changements en termes de sensibilité et de dépendance des applications, de priorités, de gestion des risques, de sites, d'activités et d'autres facteurs. Chez Citrix, le personnel en charge de la continuité d'activité assure le suivi de ces évolutions et les note tout au long de l'année afin de préparer cette revue annuelle. De même, il faut dans l'idéal organiser au moins une fois par an une simulation à grande échelle d'une situation d'urgence.

Ces pratiques, de même que la revue annuelle de tous les plans et la simulation des communications en situation de crise, constituent le strict minimum. Citrix effectue trimestriellement des tests de restauration et de continuité d'activité sur toutes ses applications stratégiques.

Les exercices introduisent régulièrement de nouveaux paramètres afin de garantir la flexibilité des plans en place et de donner la plus grande expérience possible aux membres de l'équipe qui devront un jour savoir réagir à l'inattendu.

Communication de crise

La mise en place d'un programme formalisé de communication de crise peut faire toute la différence entre la panique totale et une intervention d'urgence réussie. Ce plan doit identifier l'ensemble des parties prenantes à la communication d'urgence, y compris les employés, les sous-traitants, les clients, les fournisseurs, les médias et la direction. La communication de l'entreprise doit s'appuyer sur des ressources internes et externes : moyens de télécommunication, messagerie électronique, annonce publique, intranet, messagerie instantanée, SMS, site Web de l'entreprise, etc. L'équipe en charge de cette communication doit veiller à relayer au nom de l'entreprise un message cohérent via des canaux externes de type communiqués de presse, mises à jour de réseaux sociaux ou interviews de porte-parole. Des modèles de messages d'urgence peuvent être écrits à l'avance, personnalisés en fonction de publics spécifiques et du mode de communication choisi. Ces modèles peuvent être rapidement mis à jour en situation d'urgence réelle afin de refléter les conditions réelles rencontrées.

La sécurité des employés

La mise en sécurité des personnes doit demeurer la première priorité de toute intervention d'urgence. Il existe de nombreuses façons de concevoir un programme de mise en sécurité des collaborateurs. Les organismes comme la Croix-Rouge, les sapeurs-pompiers, la police ou les équipes CERT (Community Emergency Response Team) mises en place par des organisations publiques comme la FEMA aux États-Unis, peuvent jouer un rôle de formation, d'entraînement et de conseil utile à votre programme. Les simulations peuvent vous aider à définir et affiner les procédures qui conviendront le mieux à votre personnel, à vos installations et à votre situation géographique.

Check-list : la planification de la continuité d'activité	
Structure de l'équipe en charge de la continuité d'activité	• S'assurer l'adhésion des cadres • Former des équipes stratégiques de continuité d'activité
Planification de la continuité d'activité	• Créer des équipes d'analyse de l'activité • Concevoir des scénarios de catastrophe • Définir les priorités décisionnelles • Hiérarchiser la reprise en fonction des priorités métier • Mettre en rapport les objectifs de reprise avec les dépendances • Développer une stratégie de continuité de datacenter • Développer une stratégie de continuité du personnel • Prévoir des opérations de Scale-up/out en fonction de la gravité de la situation
Tests de continuité d'activité/reprise après sinistre	• Mettre à jour les plans régulièrement • Tester la restauration des applications stratégiques • Organiser des simulations et des exercices sur site
Communication de crise	• Établir un programme formalisé de communication de crise • Identifier l'ensemble des parties prenantes à la communication d'urgence • Identifier les canaux de communication internes stratégiques • Concevoir des modèles de messages
Sécurité des collaborateurs et programmes de sensibilisation	• Concevoir des programmes intégrant des exercices de simulation et une formation à l'intervention d'urgence dispensée par des organismes spécialisés • Prévoir la présentation du programme et une sensibilisation à la sécurité pour tout nouvel employé • Réviser et tester les procédures d'évacuation d'urgence

Une fois votre programme en place, il est indispensable de prévoir une présentation de ce programme à chaque nouveau collaborateur et une révision régulière avec l'ensemble des salariés. Les procédures d'évacuation doivent être revues et testées fréquemment et les collaborateurs doivent savoir où trouver la documentation relative à la continuité d'activité. Durant une situation d'urgence, accordez toute votre attention au niveau de stress de votre personnel et assurez-vous qu'il dispose d'un temps suffisant pour dormir, se restaurer et se détendre.

Continuité du personnel : garantir un accès ininterrompu aux ressources métier

La haute disponibilité infrastructurelle des ressources locales et cloud permet de garantir le maintien des opérations IT. Mais à quoi cela sert-il si les utilisateurs ont été déplacés ou ont perdu l'accès à leurs appareils ou systèmes habituels ? Un programme complet et efficace de continuité d'activité doit englober non seulement le datacenter, mais également le personnel. En clair, si les collaborateurs ne peuvent pas travailler, l'entreprise ne peut pas fonctionner.

Si la continuité d'activité s'est longtemps traditionnellement articulée autour de sites de secours prédéfinis ou d'unités spécifiques de reprise après sinistre, les entreprises privilégient aujourd'hui davantage les outils de mobilité d'entreprise permettant aux individus de travailler partout où cela s'avère pratique et efficace. Les personnes qui doivent en théorie travailler sur le site de secours même (membres de l'équipe de continuité d'activité, personnes en charge de la gestion des situations d'urgence, employés travaillant à des tâches stratégiques, experts en sinistres, etc.) peuvent désormais être hébergées dans n'importe quelle structure ou unité mobile disponible, sans aucun besoin en infrastructure ou liaison spéciale.

Chez Citrix, la même technologie de Digital Workspace sécurisé permet aux collaborateurs de se connecter à leurs applications et données aussi bien pour leurs opérations quotidiennes qu'en situation d'urgence, sur tout appareil, réseau et cloud. Cette approche leur permet de faire ce que dictent les priorités, qu'il s'agisse de continuer à travailler normalement, d'effectuer de nouvelles tâches rendues nécessaires par les événements ou bien de se focaliser en priorité sur leurs besoins propres et ceux de leur famille pour ensuite reprendre le travail lorsque les circonstances le permettront. Plutôt que d'acheter une multitude de PC répondant à des spécifications précises, de les configurer, puis de garantir leur accès aux applications, il suffit de fermer un site, de transférer les collaborateurs dans un autre endroit et de les laisser rapidement retourner au travail, dans l'environnement qui leur est familier. Ils bénéficient ainsi exactement de la même expérience qu'auparavant. Pour l'IT, finies les créations d'images pour des dizaines ou des centaines de machines différentes, puis la communication d'une longue liste de processus modifiés à tous les utilisateurs.

Cette approche génère de nombreux avantages importants :

Efficacité et économies : faire de la mobilité et de l'accès distant un composant majeur au cœur de votre programme de continuité d'activité vous permet d'accroître la valeur de ces investissements tout en supprimant bon nombre de dépenses et de processus associés à la continuité.

Une expérience fluide pour l'utilisateur : aucune procédure alternative n'est à apprendre ou à retenir, puisque les utilisateurs accèdent à leurs ressources et les utilisent exactement comme auparavant, avec la même expérience de Digital Workspace sécurisé pour tout scénario.

Sécurité et conformité : durant la gestion d'une disruption, les données et les applications sont délivrées en s'appuyant exactement sur la même infrastructure que celle utilisée durant les opérations quotidiennes, avec la même sécurité intégrée. Toutes les applications Windows demeurent sous le contrôle de l'IT, dans l'infrastructure cloud hybride, où la gestion centralisée et l'automatisation permettent l'application des stratégies, des mesures de protection antivirus et de maintien de la conformité réglementaire. De même, les utilisateurs accèdent partout et de façon sécurisée aux données et applications métier sensibles, depuis tout appareil, tout en permettant à l'IT de conserver une capacité complète de contrôle, de suivi, de publication de comptes-rendus et d'audits pour faciliter la sécurité et la conformité. Les données délivrées sur les appareils mobiles sont sécurisées et contrôlées grâce à la gestion des appareils mobiles (MDM), les applications l'étant quant à elles grâce à la gestion des applications mobiles (MAM). Le chiffrement de bout en bout fournit une couche supplémentaire de protection, les utilisateurs accédant aux applications et données d'entreprise en tout lieu et via tout réseau.

Une exécution plus pratique et à moindre risque : les entreprises peuvent mettre en œuvre leur plan de continuité d'activité en générant moins de désagréments pour les utilisateurs et pour l'activité. De ce fait, les entreprises décident plus facilement l'application du plan de façon proactive (déplacer par avance les collaborateurs dans l'attente de l'arrivée d'un ouragan ou d'une tempête de neige, maintenir à domicile des employés dès le début d'une épidémie ou même les évacuer vers une autre

ville en cas d'imminence de catastrophe à grande échelle) et seront moins tentées d'attendre en espérant que la catastrophe passera sans impacter leur activité. Le plan devient bien plus efficace lorsqu'il est perçu comme un ajustement acceptable à des circonstances exceptionnelles et non comme une solution de derniers recours appliquée en situation désespérée ou décidée au dernier moment.

Avec son siège implanté à Fort Lauderdale, en Floride, Citrix bénéficie d'une longue expérience pratique en matière de gestion de situations d'urgence. Citrix a transféré des personnes dans des salles de conférence d'hôtel, déplacé des charges de travail dans le monde entier suite à la fermeture de sites et augmenté rapidement ses capacités dans d'autres zones en prévision de catastrophes potentielles. Citrix l'a fait à de nombreuses reprises, tout particulièrement durant la saison des ouragans en Floride. Grâce à la flexibilité du personnel permise par les technologies Citrix, les services fournis en interne (aux membres de l'équipe Citrix) comme en externe (aux clients de Citrix) n'ont jamais été affectés.

Assurer la continuité du personnel grâce aux technologies Citrix

Grâce à un Digital Workspace sécurisé, Citrix aide les entreprises à garantir la continuité des opérations durant les interruptions. Leaders du marché, les solutions Citrix Workspace permettent aux directions IT de mettre à disposition de façon sécurisée toutes les applications (Windows, Web, SaaS et mobiles), toutes les données et tous les services, sur tout appareil, via tout réseau ou cloud. Citrix favorise la continuité du personnel grâce à des technologies complètes permettant de simplifier les opérations de sécurité et de réduire les risques dans les domaines clés suivants.

Accès contextuel

Au lieu d'avoir à se préoccuper de mettre en place des méthodes d'accès particulières, l'IT peut autoriser les personnes à accéder à leur Digital Workspace sécurisé comme d'habitude, sur toute connexion disponible. Les utilisateurs se connectent via une liaison LAN ou WAN d'entreprise, haut débit, satellite, publique ou mobile, en bénéficiant d'une sécurité complète, d'un contrôle d'accès et du suivi de la conformité. Citrix Gateway fournit aux directions informatiques un cadre de gestion unifié permettant de sécuriser, contrôler et optimiser l'accès aux applications et données sur tout appareil, via tout réseau ou cloud.

Les utilisateurs ayant perdu l'accès à leur appareil de travail habituel peuvent accéder à leur Digital Workspace sécurisé intégrant toutes leurs applications métier habituelles depuis tout appareil disponible. Il leur suffit de télécharger l'application Citrix Workspace sur un vieil appareil personnel ou même sur un appareil tout nouvellement acquis, y compris sur les ordinateurs de bureau et portables Windows et Mac, les produits mobiles iOS, Android et Windows, ou encore les périphériques mobiles Google Chromebook. Dans Citrix Workspace, les utilisateurs accèdent d'un seul clic aux applications métier mobiles, Web, SaaS, personnalisées et Windows, y compris aux applications de partage de fichiers et de productivité.

Sécurité des applications

La virtualisation de postes et d'applications Windows fournie par Citrix Virtual Apps and Desktop permet à l'IT de transformer des applications et des postes de travail complets en services à la demande délivrés partout, sur tout appareil et de façon sécurisée au sein de Digital Workspaces. Les applications et les données étant gérées au sein du datacenter ou du cloud, les directions informatiques peuvent assurer la protection des données, la conformité, le contrôle d'accès et l'administration des utilisateurs de façon centralisée, aussi facilement sur des périphériques personnels que sur des périphériques d'entreprise, empruntés ou neufs, le tout dans un environnement unifié.

Les appareils mobiles peuvent jouer un rôle de tout premier plan en maintenant la connexion des utilisateurs durant une disruption. Citrix Endpoint Management permet le provisioning et le contrôle des applications, des données et des appareils basés sur l'identité, le déprovisionnement de

« Nous voulons que nos collaborateurs comprennent qu'ils peuvent accéder à tout ce dont ils ont besoin via Citrix. »

– **Kyle Edgeworth, DSI adjoint, Municipalité de Corona**

compte automatique et la suppression à distance des données et applications sur tout appareil ayant été temporairement utilisé pendant une période de continuité d'activité. Les applications et les données métier, qu'elles soient développées par l'IT ou un tiers, y compris les applications de productivité mobile d'entreprise, résident dans un conteneur, isolées des applications et données personnelles sur l'appareil.

Sécurité des données

Citrix Content Collaboration permet aux utilisateurs, aux équipes et aux clients de synchroniser et de partager de façon sécurisée leurs fichiers, partout et depuis tout appareil. L'IT accorde facilement l'accès à des annuaires de données d'entreprise existants sans compromettre la sécurité. Les processus de routine (chaînes d'approbation, par exemple) peuvent être automatisés afin de faciliter le fonctionnement transparent des différents processus métier, même dans des circonstances inhabituelles. Les options de stockage flexibles, le contrôle basé sur des stratégies, la création de rapports, le chiffrement des données, la suppression à distance, la gestion des droits d'accès aux informations (information rights management, IRM) et l'intégration de la prévention des pertes de données (data loss prevention, DLP) permettent de sécuriser le contenu de l'entreprise en cas d'interruption.

L'association de ces différentes technologies Citrix aide les équipes en charge de la continuité d'activité à répondre à deux questions essentielles des utilisateurs :

- Puis-je encore accéder à mes applications, données et fichiers et collaborer efficacement avec les autres, à l'intérieur comme à l'extérieur de l'entreprise ?
- Tout fonctionne-t-il de la même façon que d'habitude, ou dois-je m'habituer à un périphérique, une méthode d'accès au réseau et un ensemble d'outils totalement nouveaux pour moi ?

Continuité du datacenter : maintenir la permanence des opérations informatiques

La plupart des grandes entreprises exploitent déjà un modèle cloud hybride et disposent de plusieurs datacenters, tout en tirant profit du cloud à des fins de mise à l'échelle et de redondance. Si l'un des datacenters ou cloud devient indisponible pour une quelconque raison, prévue ou imprévue, les utilisateurs doivent pouvoir accéder à leurs ressources via un autre datacenter ou cloud, qu'il soit également actif ou purement de secours, jusqu'à ce que le premier datacenter ou cloud redevienne opérationnel. Il est primordial de s'assurer que l'infrastructure associée est bien capable de prendre en charge cette réponse (basculement rapide et automatique, répartition de charge, capacité du réseau, etc.).

Les entreprises essentiellement tournées vers les PC de bureau traditionnels pour l'accès principal à leurs données et ressources sont souvent fortement désavantagées lorsqu'un événement inattendu survient. Grâce à l'accès distant Citrix Remote PC, les clients Citrix Virtual Apps and Desktops peuvent rapidement autoriser l'accès à chaque machine de leur environnement de travail physique. En cas d'imprévu, les administrateurs mettent rapidement un pack MSI à disposition des utilisateurs et leur garantissent partout l'accès sécurisé à ces appareils.

Continuité des utilisateurs

Dans l'idéal, votre direction informatique a déployé une solution qui garantit la même expérience utilisateur final quelle que soit la localisation physique. Citrix Workspace avec fonctionnalités intelligentes renforce la capacité de l'utilisateur à être productif en tout lieu. Bénéficier d'un flux intelligent d'actions sur tout appareil permet aux collaborateurs de continuer à avancer, même en période de troubles.

Sécurité des réseaux

Citrix ADC et Citrix SD-WAN rendent les reprises de datacenter totalement transparentes pour les utilisateurs. Si le datacenter principal connaît une défaillance, Citrix ADC redirige automatiquement et de façon transparente les utilisateurs vers le site secondaire, tout en continuant à assurer la répartition de charges et la répartition de charges mondiale (GSLB). Citrix ADC permet également aux entreprises utilisant un cloud public de sauvegarde de gérer cette infrastructure externalisée de la même façon que leur propre datacenter de sauvegarde. Citrix SD-WAN permet aux directions IT d'assurer l'accès aux applications et de les accélérer, d'optimiser l'utilisation de bande passante sur les cloud publics tiers et les réseaux privés et de renforcer la visibilité sur les performances applicatives dans le but d'optimiser l'expérience utilisateur quel que soit le scénario.

Automatisation et Reprise

Les solutions Citrix aident les directions informatiques à garantir la disponibilité permanente des ressources de datacenter. Citrix Hypervisor, la principale plateforme open source du marché pour la virtualisation rentable des infrastructures cloud, de serveurs et de postes, fournit des outils de gestion de l'ensemble de la reprise après sinistre à l'échelle du site. Cette reprise s'appuie sur la migration instantanée pour transférer les charges d'un serveur physique à un autre, et sur la haute disponibilité automatisée qui transfère les machines

virtuelles de l'hôte défaillant vers d'autres hôtes physiques automatiquement redémarrés, afin de protéger efficacement les charges critiques contre tout événement localisé.

Les services cloud Citrix favorisent la résilience en proposant un tableau de bord unique permettant à l'IT de gérer les ressources au sein d'une multitude de datacenters d'entreprise, de clouds publics et privés. Elles peuvent facilement réaffecter les utilisateurs à des sites de secours au gré des besoins, afin de réduire la charge pesant sur les ressources victimes de perturbations et de garantir une disponibilité et des performances optimales. Les services cloud Citrix s'exécutent sur une plateforme distribuée mondialement et hautement disponible, spécialement conçue pour assurer la continuité des opérations malgré les disruptions locales.

Analytique et informations

Un scénario de continuité d'activité peut modifier significativement la répartition des utilisateurs et des charges au sein de l'infrastructure réseau. C'est pourquoi il est tout particulièrement important de surveiller les performances afin de garantir une expérience de qualité à chaque utilisateur. En parallèle, les directions IT doivent demeurer vigilantes et à l'affut des menaces, afin qu'une interruption durant un peu trop longtemps ne crée pas d'opportunités d'attaques. Les solutions Citrix, notamment Citrix ADC, Citrix Application Delivery Management et Citrix Virtual Apps and Desktops, fournissent une visibilité complète sur votre infrastructure informatique, avec analytique en temps réel permettant de détecter les menaces, les mauvaises configurations et les problèmes de performance.

Citrix Analytics for Performance et Citrix Analytics for Security fournissent en temps réel des insights actionnables et en temps réel qui garantissent à votre environnement un fonctionnement aussi fluide que possible. Disposer d'informations détaillées sur l'expérience réelle de chaque utilisateur permet à l'IT d'allouer plus de ressources à ceux dont l'expérience n'est pas optimale.

Conclusion

Citrix propose une approche plus fluide et plus globale, qui permet aux utilisateurs de travailler exactement de la même façon durant leurs activités quotidiennes ou une période de perturbations. Des technologies complètes d'accès contextuel sécurisé au réseau, aux applications et aux données permettent aux utilisateurs de devenir totalement productifs sur tout appareil, via tout réseau ou cloud et en tout lieu, tout en aidant les directions IT à garantir une sécurité et un contrôle ininterrompus. En arrière-plan, l'automatisation et la reprise préservent la disponibilité des ressources informatiques, tandis que le suivi, la détection et l'analytique en temps réel aident l'IT à garantir une expérience de qualité, à maintenir la conformité et à prévenir les violations. En s'appuyant sur l'infrastructure utilisée au quotidien, cette approche rend également inutile le recours à des appareils et outils d'accès de secours, réduisant de ce fait les coûts et la complexité du plan de continuité d'activité.

Les Digital Workspaces sécurisés transforment radicalement la façon dont les directions IT du monde entier travaillent, autonomisent leurs utilisateurs et facilitent l'activité de l'entreprise. En intégrant des solutions Citrix à votre stratégie de continuité d'activité, vous protègerez votre entreprise bien plus efficacement contre les risques induits par les interruptions prévues ou imprévues.

Pour en savoir plus, consultez citrix.fr/virtual-apps.

citrix

Ventes aux entreprises
Amérique du Nord | 800-424-8749
International | +1 408-790-8000

Sites
Siège social | 851 Cypress Creek Road Fort Lauderdale, FL 33309, États-Unis
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, États-Unis