arcserve®

LIVRE BLANC

La haute disponibilité n'est pas un luxe.

Élimination des interruptions de service des petites et moyennes entreprises.

L'informatique apporte d'énormes avantages aux petites et moyennes entreprises, mais représente également un énorme risque. Lorsque les marchés sont mondiaux et que l'entreprise fonctionne 24h/24, la moindre interruption de service peut rapidement engendrer une perte de chiffre d'affaires, une baisse de la productivité, une dégradation de l'image de marque et des problèmes juridiques. Les interruptions de service de longue durée peuvent même menacer la survie de votre entreprise.

Sachant cela, comment gérer ce type de menace potentielle ? La douloureuse réalité est que la plupart des entreprises ne la gèrent pas correctement.

La continuité d'activité, c'est-à-dire la planification, la préparation et la mise en oeuvre de systèmes d'information plus résilients en prévision des interruptions de service non planifiées, est souvent considérée comme un problème informatique qu'il incombe au département informatique de traiter. Cette perception engendre invariablement la mise en place d'un large éventail de solutions tactiques, sans stratégie générale fournissant des orientations. En réalité, comme l'indique son libellé en anglais (business continuity), la continuité d'activité est un problème d'entreprise qui doit être traité avec une stratégie d'entreprise.

Voici quelques hypothèses qui vous aideront à déterminer rapidement si votre plan de continuité d'activité actuel vous met en danger :

- **Si votre plan nécessite des interventions manuelles importantes, vous êtes en danger.**
- **Si votre plan accepte une perte de données au-delà de quelques secondes pour les systèmes critiques, vous êtes en danger.**
- **Si votre plan ne permet pas de rétablir l'accès aux systèmes critiques en quelques minutes, vous êtes en danger.**
- **Si votre plan dépend d'une technologie de sauvegarde et de restauration qui n'a pas su suivre les évolutions technologiques, vous êtes manifestement en danger.**

Les techniques de sauvegarde et de restauration sont utilisées depuis 30 ans pour protéger les systèmes informatiques, mais elles ont été mises au point à une époque beaucoup plus simple. La sauvegarde de données sur bande ou sur disque, ainsi que la création d'instantanés des donnéees, crée une image ponctuelle des données applicatives. La restauration à partir d'une copie ponctuelle ne vous permet de récupérer que les données de la sauvegarde la plus récente. Que la copie ait été effectuée il y a 15 minutes ou avant-hier, la restauration à partir d'une sauvegarde signifie que vous devez affronter les conséquences de la perte de données. Une perte de données peut être acceptable pour certains systèmes, mais pour la plupart de vos applications métiers les plus importantes, elle sera catastrophique.

Les techniques de sauvegarde et de restauration ont été mises au point pour des processus informatiques relativement simples, à une époque où l'on planifiait des périodes à intervalles réguliers pendant lesquelles personne n'utilisait le système. Les applications métiers dont vous avez besoin en permanence pour vos opérations quotidiennes nécessitent une technologie qui garantit la disponibilité continue des systèmes et élimine le risque de perte de données, sans reposer sur des fenêtres de sauvegarde.

La technologie de haute disponibilité actuelle, désignée ci-après par « la haute disponibilité », transfère en continu les modifications des applications et des données vers un environnement de secours. En cas de catastrophe ou d'incident (tremblement de terre, panne de courant, problème d'installation d'un logiciel, etc.), le basculement sur une copie à jour de votre système est automatique et instantané. La haute disponibilité élimine les interruptions de service et les pertes de données.

La haute disponibilité à la portée de tous

La haute disponibilité est la solution idéale pour protéger les systèmes contre les interruptions de service et les pertes de données. Cela dit, elle a été contestée pendant de nombreuses années. Cette technologie a été considérée comme trop complexe et trop coûteuse pour les petites et moyennes entreprises. Il était généralement estimé que seules les grandes entreprises riches et pourvues de ressources informatiques abondantes pouvaient déployer des solutions de haute disponibilité. Cette critique était légitime jusqu'à récemment.

La haute disponibilité utilise généralement des technologies de réplication et de surveillance des serveurs via signal heartbeat pour maintenir la synchronisation entre les systèmes informatiques distants et les applications du datacenter principal. Auparavant, cela nécessitait des réseaux dédiés à large bande passante entre deux sites et des copies redondantes du serveur, du système de stockage et du matériel réseau, avec des applications et des logiciels d'exploitation spécialisés. En raison du coût de cette redondance, la haute disponibilité a toujours été inaccessible pour les petites entreprises.

Aujourd'hui, les réseaux peu coûteux à large bande passante sont omniprésents. En outre, de nombreux fournisseurs de services permettent de déployer facilement des serveurs virtuels à la demande à moindre coût. Autrement dit, la haute disponibilité est désormais accessible à un coût beaucoup moins élevé, ce qui étend sa portée à un plus grand nombre d'entreprises.

Compte tenu de la baisse spectaculaire du coût d'une infrastructure de haute disponibilité, le plan de continuité d'activité de nombreuses entreprises se retrouve à un point d'inflexion. Les solutions de sauvegarde non coordonnées, qui se chevauchent souvent, abondent dans le datacenter. Si votre stratégie de continuité d'activité repose sur la sauvegarde et la restauration, vous constatez probablement que ces solutions en silos posent d'énormes problèmes de maintenance, qui réduisent fortement la productivité et, surtout, compliquent considérablement la reprise après sinistre. Les solutions actuelles de haute disponibilité proposent une approche universelle de la continuité d'activité qui réduit le coût de la protection des données, simplifie la reprise après sinistre et élimine les pertes de données et les interruptions de service.

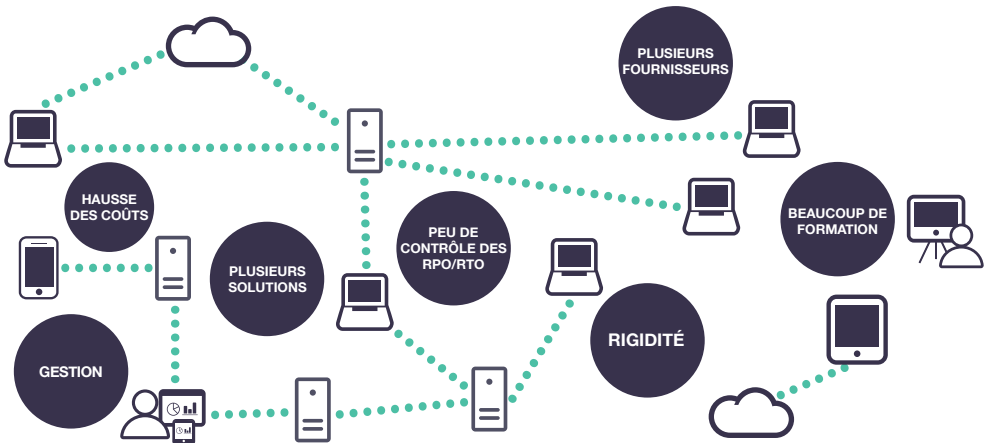

Figure 1 – Les risques cachés de la complexité des solutions de sauvegarde en silos

La haute disponibilité peut être appropriée pour votre entreprise, mais sans analyse détaillée de ses systèmes pour déterminer leurs besoins en matière de restauration, vous ne saurez pas quelles applications en bénéficieront. Ce qui est certain, c'est que les obstacles au déploiement d'une solution de haute disponibilité ont été levés et que vous pouvez désormais vous consacrer aux autres contraintes de la mise en oeuvre d'un plan de continuité d'activité.

Les 10 principaux écueils de la continuité d'activité

Tout le monde parle de la meilleure façon d'aborder la reprise après sinistre, mais il est tout aussi utile d'examiner les écueils qui vous attendent si vous ne l'abordez pas correctement. Voici les 10 principaux écueils de la planification de la reprise après sinistre et de la continuité d'activité.

1 C'est l'entreprise qui est en jeu, et non pas la technologie !

Reprise après sinistre, haute disponibilité, sauvegarde et restauration, continuité d'activité... appelez cela comme bon vous semble, le but est le même : maintenir le bon fonctionnement de l'entreprise, en toutes circonstances. Les entreprises se laissent trop souvent dominer par la technologie. Elles oublient ce qu'il est essentiel de garder à l'esprit : la reprise après sinistre vise à répondre à un besoin métier et doit être régie par les exigences de l'entreprise. Avant de réfléchir aux modalités de mise en oeuvre d'une solution de reprise après sinistre, vous devez réfléchir aux raisons de sa mise en oeuvre. Parlez-en aux responsables métiers pour identifier leurs priorités. Pour certains, il s'agira de l'e-mail, alors que pour d'autres, il s'agira du système de saisie des commandes en ligne ou de Microsoft SharePoint. Le fait est que si vous ne les interrogez pas, vous ne saurez pas quels sont les systèmes les plus importants. Une fois que vous connaîtrez les besoins de l'entreprise, vous pourrez définir les priorités qui dicteront vos choix technologiques pour la reprise après sinistre.

2 Un sinistre n'est pas nécessairement un cataclysme

Lorsque vous pensez à la reprise après sinistre, vous imaginez probablement des tempêtes, des inondations, des attaques terroristes et autres fléaux de cette nature, et non pas une mise à niveau logicielle qui s'est mal passée avec une procédure de retour arrière mal définie ou une erreur matérielle sur un élément essentiel de l'équipement réseau. Il est en fait très courant de prévoir le pire scénario et d'être assailli par de banales erreurs faisant partie du quotidien. Votre plan de reprise après sinistre doit prendre en compte toutes les éventualités, de l'événement courant au cataclysme.

3 Comment allouer un budget sans connaître le coût des interruptions de service ?

Les entreprises ont trop souvent tendance à allouer un budget à la reprise après sinistre avant de déterminer le risque financier des interruptions de service et des pertes de données. Si vous ne quantifiez pas ce que vous risquez de perdre en cas de panne de systèmes critiques, il vous sera difficile de déterminer le budget à allouer pour éviter ces pertes. Votre approche de la reprise après sinistre doit être alignée sur les besoins de l'entreprise. Cela implique d'évaluer le coût financier des interruptions de service avant d'allouer un budget. Dans le calcul du coût des interruptions de service, n'oubliez pas d'inclure le coût du non-respect des réglementations qui donne souvent lieu à des sanctions financières.

4 Évaluation des risques

Les événements considérés comme des sinistres varient d'une entreprise à une autre, voire d'un département à un autre. Certains événements (par exemple, les tremblements de terre) sont potentiellement si catastrophiques que toute entreprise doit s'en protéger. D'autres événements sont plus courants (par exemple, une panne matérielle sur un réseau), mais ont un impact financier hors normes. Lorsqu'on pense à la reprise après sinistre, il est essentiel de se poser la question suivante : contre quoi voulons-nous nous protéger ? Ne négligez pas la banalité. Les petites pertes découlant des problèmes courants s'accumulent rapidement.

5 Avez-vous un plan ?

Si votre plan de reprise après sinistre se résume à un Post-It collé sur les bandes de sauvegarde stockées dans la maison de campagne de votre administrateur système, vous êtes en difficulté. Aussi insensé que cela puisse paraître, un nombre surprenant d'entreprises n'ont pas de plan de reprise après sinistre. Vous devez absolument élaborer un document formel détaillant les applications, le matériel, les installations, les fournisseurs de services, le personnel et les priorités dans leur intégralité, puis obtenir l'adhésion de toutes les parties prenantes de l'entreprise à ce document. Votre plan doit représenter tous les domaines fonctionnels et indiquer clairement ce qui se passe avant, pendant et après un incident.

6 Nous avons un plan, mais nous ne l'avons pas testé

Un plan de reprise après sinistre n'est utile que s'il fonctionne. La seule façon de vous assurer que votre plan fonctionne est de le tester. Le test du plan dans des conditions de sinistre simulées est essentiel, mais cette opération peut aussi être problématique. La réalisation d'un test de reprise après sinistre est coûteuse et accapare du temps et des ressources au détriment des opérations quotidiennes. Cela dit, à moins que la reprise ne soit entièrement testée au niveau des applications, vous rencontrerez inévitablement des difficultés lors d'un sinistre réel. Recherchez des solutions de protection des données qui vous permettent de créer des environnements pour réaliser des tests sans perturbation de votre plan de reprise après sinistre.

7 Qui est responsable et de quoi ?

Un sinistre réel est chaotique et déroutant. Si les employés clés ne comprennent pas leurs responsabilités relatives à la reprise après sinistre, le processus de reprise est long et entravé par de nombreux problèmes. Votre plan de reprise après sinistre doit indiquer clairement le rôle et les responsabilités de chaque personne concernée, y compris ce qu'il faut faire si des personnes clés ne sont pas disponibles. Ces personnes doivent également être impliquées dans les tests de votre plan de reprise.

8 Point de restauration : quoi ? Temps de restauration : qui ?

Il est très important de savoir à quel point chaque domaine de votre entreprise est sensible aux interruptions de service et aux pertes de données. Ces informations éclairent le choix de la technologie de reprise après sinistre, fournissent la base du plan de reprise après sinistre et indiquent les conséquences de l'incapacité à restaurer chaque application métier. Deux indicateurs sont utilisés pour enregistrer la tolérance d'une application aux interruptions de service et pertes de données : l'objectif de point de restauration (RPO) et l'objectif de temps de restauration (RTO). Ces deux indicateurs sont exprimés en durée. Le RPO indique une durée avant l'incident et le RTO indique une durée après l'incident.

Le RPO est une mesure de la perte de données. Plus le RPO est long, plus la perte de données qu'une application peut tolérer avant qu'elle ne devienne un problème pour l'entreprise est importante. Considérez-le comme le point dans le temps jusqu'auquel vous pouvez restaurer des données avec succès. Toutes les données entre ce point et l'incident auront disparu.

Le RTO est une mesure de l'importance d'une application pour les opérations courantes de l'entreprise. Plus le RTO est court, plus vous devez travailler vite pour restaurer l'application en ligne avant que l'entreprise ne commence à subir des pertes importantes.

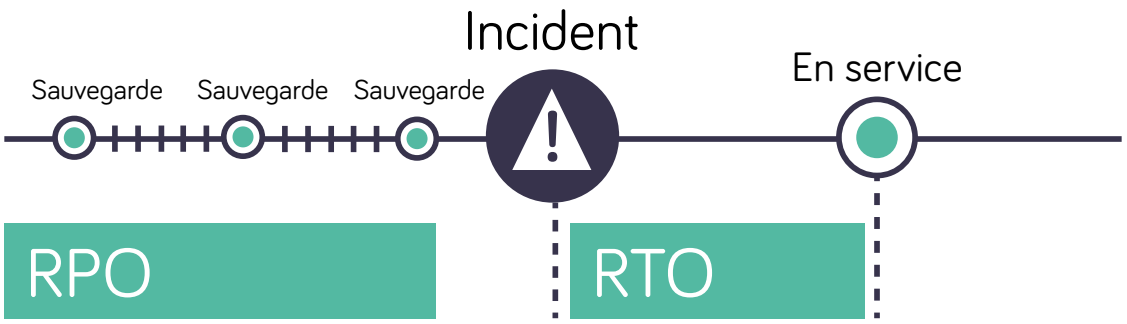

Figure 2 - La connaissance de la fréquence à laquelle vos différentes applications et sources de données doivent être sauvegardées (objectif de point de restauration, ou RPO) et de la vitesse à laquelle vous devez les récupérer (objectif de temps de restauration, ou RTO) est essentielle pour élaborer votre plan de continuité d'activité.

Si vous ne connaissez pas les RPO et RTO de chaque application, vous êtes dans le noir en ce qui concerne la reprise après sinistre. Tout ce que vous ferez pour assurer la reprise après sinistre ne sera qu'une conjecture. Les RPO et RTO vous permettent de définir les niveaux de service à atteindre.

Les technologies telles que la protection continue des données sont essentielles pour garantir la réalisation de ces objectifs.

9 La reprise sera plus longue que vous ne le pensez

Pour de nombreuses entreprises, la réflexion sur la reprise après sinistre s'arrête au moment où les bandes de sauvegarde quittent le datacenter. Il est pourtant essentiel de savoir combien de temps il faudra pour restaurer les systèmes clés de l'entreprise et combien de données critiques seront perdues après un incident. Même si vous pouvez accéder à des copies de sauvegarde hors site, vous n'avez aucune garantie quant à la restauration rapide des applications. Avez-vous accès à un équipement qui permet la lecture des données ? Pouvez-vous restaurer les données et reconstruire les systèmes applicatifs suffisamment rapidement pour satisfaire les utilisateurs ? Avez-vous la bande passante nécessaire pour restaurer des données stockées chez un fournisseur de services de Cloud computing ? Le fait de savoir combien de temps il vous faut pour restaurer des applications et quels sont les effets des interruptions de service sur votre entreprise peut vous amener à faire des choix technologiques différents.

10 Retour à la normale

Le retour à la normale après le basculement vers un site de reprise est souvent négligé dans les plans de reprise après sinistre. Il est facile de comprendre pourquoi. Lorsque nous pensons aux sinistres, notre esprit se concentre uniquement sur la protection des ressources précieuses. On se préoccupe peu de ce qu'il advient de ces ressources après un sinistre.

La capacité à effectuer un retour arrière vers les systèmes de production est tout aussi importante que la capacité à effectuer un basculement sur incident. Sans planification minutieuse, un datacenter de secours est peu susceptible d'avoir la même capacité ou les mêmes performances que celles du site de production.

Sans plan de retour arrière, vous pouvez réussir le basculement initial et voir ensuite les pertes s'accumuler au fil des semaines pendant lesquelles votre entreprise peine à fonctionner à partir d'un site de secours mal équipé.

Maîtrise des risques

À l'exception de l'e-mail, il est presque impossible de savoir quelles applications présentent le plus grand risque pour votre entreprise en cas d'interruption de service sans obtenir des informations à ce sujet de la part des utilisateurs des applications. Les RPO et RTO sont des indicateurs qui permettent de mesurer ce risque. Ils indiquent également les applications prioritaires dans le cadre de vos efforts en matière de reprise après sinistre.

Les RPO et RTO fonctionnent sur un continuum. Pensez à une ligne temporelle au centre de laquelle se trouve la panne. Le point RPO se situe avant la panne et indique la perte de données maximale tolérée par une application. Plus ce point est éloigné de la panne, plus la perte de données et le coût potentiel sont importants.

Le point RTO se situe après la panne, c'est-à-dire à l'opposé du RPO sur la ligne temporelle. Le RTO indique la durée d'interruption tolérée par une application avant que les pertes de l'entreprise ne commencent à s'accumuler, c'est-à-dire la vitesse à laquelle vous devez remettre l'application en service après une panne.

Si vous pouvez recréer les informations du système à partir d'autres sources, la perte de données en cas d'incident peut être problématique, mais dans une moindre mesure. Par exemple, les factures manquantes dans le système de la comptabilité fournisseurs peuvent être recréées en demandant aux fournisseurs de les renvoyer. En revanche, si vous ne pouvez pas régénérer facilement les données (par exemple, les commandes des clients en ligne), la perte de ces informations peut avoir un impact direct sur le chiffre d'affaires, la productivité des utilisateurs, la réputation de votre entreprise et la conformité réglementaire.

De même, l'interruption des systèmes d'entreprise non critiques (par exemple, les rapports mensuels d'une application d'analyse) n'a pas le même impact sur l'entreprise que celle des systèmes impliqués dans les opérations quotidiennes, tels qu'une application de point de vente. Le RTO mesure l'impact de l'interruption de service d'une application sur l'entreprise et vous permet de savoir quels outils de reprise après sinistre appliquer à cette application. Les sauvegardes périodiques peuvent être suffisantes pour une application d'analyse, mais pas pour un système de point de vente critique exigeant une solution de haute disponibilité.

La différence entre les valeurs des RPO et RTO et les résultats des tests réguliers de reprise après sinistre indique si vous avez un problème de disponibilité au niveau de l'application. Sachez qu'un écart ne signifie pas nécessairement que la stratégie de continuité d'activité appliquée est incorrecte. Les entreprises possèdent souvent un large éventail de technologies de reprise après sinistre provenant de différents fournisseurs, dont beaucoup se chevauchent, font double emploi et compliquent la reprise. Les tests permettent de déceler les problèmes et les incohérences dans les technologies de continuité d'activité existantes, ainsi que les domaines dans lesquels une consolidation sur une seule approche ou un seul fournisseur de solutions peut améliorer le RTO.

En quoi consiste la réussite en matière de haute disponibilité ?

Nous savons tous comment se traduit la réussite en matière de haute disponibilité : aucune interruption de service des applications, aucune perte de données applicatives. Cela dit, est-ce réaliste pour les petites et moyennes entreprises ?

La technologie de la haute disponibilité ne repose plus sur l'approche complexe et ésotérique de la continuité d'activité d'autrefois. Les grandes entreprises utilisent des techniques de haute disponibilité pour protéger leurs applications métiers les plus critiques depuis des années. Cette technologie a fait ses preuves. Elle est largement reconnue comme un outil standard de prévention des incidents. Elle est simple, reproductible, mesurable et automatisée. Les technologies telles que la protection continue des données, la réplication ainsi que le basculement et le retour arrière automatisés sont essentielles.

L'évolution des produits de haute disponibilité les a rendus financièrement accessibles aux petites et moyennes entreprises. Du fait de la réduction de leur coût et des frais d'infrastructure (large bande passante, virtualisation des serveurs, nombreux fournisseurs de services), associée à une amélioration considérable en termes de facilité d'utilisation, la haute disponibilité est bel et bien devenue une solution alternative de continuité d'activité viable pour les entreprises de toutes tailles.

Les interruptions de service et les pertes de données font partie de la vie des entreprises informatisées. La compensation de ce risque avec la technologie appropriée doit être examinée dès le début des cycles de développement des logiciels et de déploiement des produits. Le fait de savoir quel est le niveau de protection exigé par chaque application vous permet d'allouer les ressources appropriées. Avant la mise en service d'une application dans un environnement de production, ses RPO et RTO doivent être clairement identifiés et les solutions de continuité d'activité adéquates doivent être mises en place pour garantir la reprise de l'application en cas de panne.

Les solutions de continuité d'activité qui ne permettent pas d'éliminer les interruptions de service et les pertes de données ne sont pas des solutions de haute disponibilité. De nombreuses solutions disponibles promettent d'améliorer la reprise après sinistre, mais si elles n'éliminent pas votre exposition, ce ne sont pas des solutions de haute disponibilité.

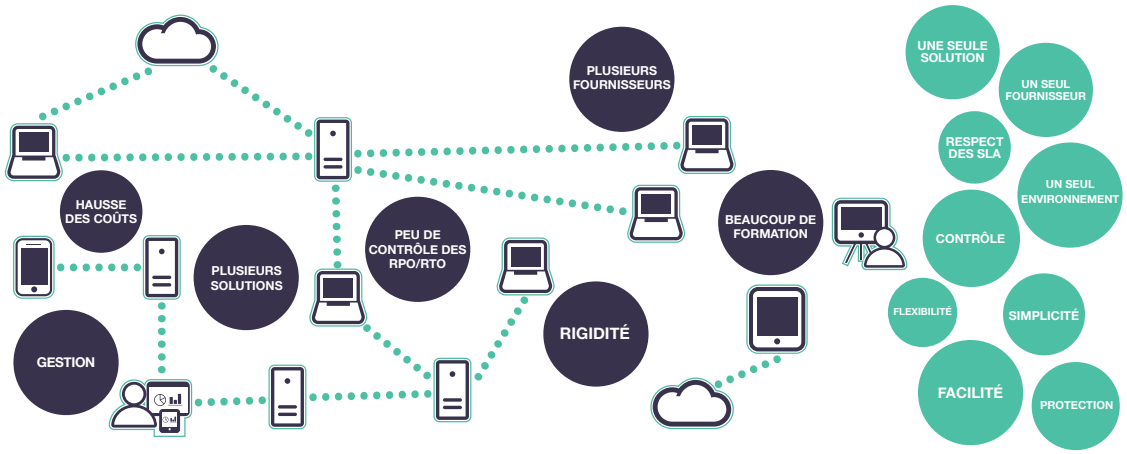

Figure 3 – Une solution unifiée de continuité d'activité

arcserve®

LIVRE BLANC

À propos d'Arcserve® Unified Data Protection

Arcserve fournit une protection sans interruption de service, sur laquelle s'appuient des entreprises du monde entier depuis plus de 20 ans. Aujourd'hui, Arcserve® Unified Data Protection (UDP) répond à tous vos besoins en matière de protection des données et de haute disponibilité. Avec un contrôle centralisé, Arcserve® UDP unifie la protection, y compris la sauvegarde, les clichés de vos systèmes, la réplication et la déduplication, de vos ressources applicatives virtuelles, physiques, sur site ou résidant dans une infrastructure de type Cloud. Arcserve® UDP Assured Recovery™ fournit un processus de test de reprise en temps réel pour la validation, sans perturbation, des plans de continuité d'activité. Pour en savoir plus sur la protection des données unifiée Arcserve® Unified Data Protection (UDP) et notre offre d'évaluation gratuite de 30 jours, rendez-vous sur : http://arcserve.com/availability.

Pour en savoir plus sur Arcserve UDP, **rendez-vous sur arcserve.com**