SBT Small Biz Thoughts

Par Karl W. Palachuk

AMÉLIORER RAPIDEMENT LES OPÉRATIONS INFORMATIQUES, L'ASSISTANCE ET LA PRODUCTIVITÉ DES ÉQUIPES MSP

eBook réalisé à la demande d'**Acronis**

SOMMAIRE

AMÉLIORER RAPIDEMENT LES OPÉRATIONS INFORMATIQUES, L'ASSISTANCE ET LA PRODUCTIVITÉ DES ÉQUIPES MSP

Par Karl W. Palachuk

En décembre 2019, Boeing a procédé au lancement de sa capsule Starliner, direction la Station spatiale internationale (ISS). La mission était simple : lancer la capsule, l'amarrer à la station et la faire revenir sur Terre en un seul morceau.

55 minutes après le lancement, la NASA a indiqué que la capsule Starliner était en « off-nominal insertion ». Pour faire simple, elle s'était placée sur la mauvaise orbite.

La mission était un échec. Et pas qu'un peu ! Heureusement, aucun équipage n'était présent à bord.

Dans un secteur où la précision est reine, comment un tel raté a-t-il pu se produire ? La raison est simple : deux systèmes logiciels n'ont pas communiqué entre eux comme ils auraient dû le faire. Malgré toute la bonne volonté de l'équipe à mettre en place des communications ouvertes et sans faille, un bug est survenu : une horloge interne a été mal réglée et la capsule s'est retrouvée hors de la trajectoire prévue.

Prenons quelques instants pour y réfléchir : les trois partenaires (la NASA, SpaceX et Boeing) s'étaient engagés à travailler ensemble dans un état d'esprit de coopération et d'ouverture. Ils étaient donc tous bien intentionnés et concentrés sur les mêmes objectifs. Tout le monde regardait dans la même direction et souhaitait les mêmes résultats.

Boeing a dépensé 1,5 milliard de dollars pour que la mission soit réalisée dans les règles de l'art. Et pourtant, elle a échoué.

Cette histoire peut nous en apprendre beaucoup sur la relation entre la complexité, les interconnexions et l'utilisation efficace des logiciels. Même lorsque les différents partenaires se mettent d'accord sur des spécifications de conception et élaborent un projet sur des plates-formes complètement ouvertes et bien documentées, les choses peuvent mal tourner.

Imaginez maintenant un environnement dans lequel les développeurs ne sont plus des partenaires, mais des concurrents. Chacun publie des spécifications expliquant comment se connecter à l'API qu'il développe, mais il n'y a aucun échange entre eux.

Le résultat est exactement celui que vous attendez : un projet très compliqué et potentiellement source de problèmes.

LES API, AIMÉES ET DÉTESTÉES À LA FOIS

La technologie évolue à vitesse grand V. Si, dans la plupart des secteurs d'activité, de nouvelles façons de travailler apparaissent tous les 10 ans, dans l'informatique, c'est tous les 18 à 24 mois qu'émerge une nouvelle génération de technologies. Si vos opérations n'ont pas changé en cinq ans, il y a de fortes chances que votre entreprise ait pris du retard.

En ce début d'année 2021, nous sommes au cœur d'une ère dominée par les API. Ces interfaces de programmation sont apparues au début des années 2000 et permettent aux applications de fonctionner ensemble, d'échanger des informations et d'automatiser les processus.

À l'époque, les API étaient une véritable bénédiction pour de nombreux fournisseurs de services managés, car elles permettaient à des outils très variés de fonctionner ensemble. Bien entendu, plus vous achetiez de middlewares pour gérer vos API, plus cela vous coûtait cher. Certains middlewares étaient assez onéreux et, la plupart du temps, ne consistaient qu'en un programme créé à la-vite pour résoudre un problème urgent. Cela dit, ils tenaient leur promesse.

Au fil du temps, cette stratégie autrefois portée aux nues s'est peu à peu muée en une espèce de méthode de création d'un monstre de Frankenstein informatique.

Mais revenons au temps présent. Les API ont désormais atteint une maturité élevée, ce qui ne veut pas dire qu'il ne faut pas gérer les connexions entre elles, même dans les circonstances les plus favorables et avec une programmation à toute épreuve. En effet, lorsque vous connectez les logiciels de deux entreprises différentes, une modification de l'un ou de l'autre peut interrompre les fonctionnalités. Si les deux logiciels sont reliés par une connexion tierce, les choses se compliquent davantage encore.

Chaque connexion exige un minimum de gestion et représente une faille de sécurité potentielle qu'il convient de surveiller. Les ransomwares sont devenus un secteur très lucratif, et les cybercriminels ont découvert que les fournisseurs de services informatiques étaient des cibles de choix pour voler des données et propager du code. À l'instar des autres types d'attaques, les ransomwares choisissent un point d'entrée et l'assaillent. Par conséquent, vous devez défendre tout ce qui peut représenter une faille.

Le secret pas très avouable du développement logiciel est que la maintenance et le support finissent toujours par coûter plus cher que le logiciel lui-même. (Les fournisseurs de services informatiques, qui gagnent leur pain avec le support, le savent bien.) Sans oublier que chaque ensemble de connexions accroît le besoin de surveillance, de maintenance et de support.

LE VRAI COÛT DE L'ÉCLATEMENT DES OUTILS

En plus de vous obliger à payer différents fournisseurs, l'utilisation de nombreux outils disparates entraîne l'augmentation des coûts de formation, d'intégration et de maintenance. D'après une étude de Gartner, un système intégrant une multitude de composants entraîne des frais supplémentaires dans plusieurs domaines. Au bout du compte, bien que les API permettent de connecter différents logiciels, elles le font de façon inefficace. Chaque nouvelle connexion complique un peu plus l'environnement, requérant un surplus de documentation, de formation et de maintenance.

La maintenance d'un système interconnecté complexe implique un effort qui affecte directement la productivité globale : chaque heure passée sur cette tâche est une heure qui n'est pas consacrée à l'assistance aux utilisateurs finaux.

Selon une étude récente de Forrester Research, la dépendance à des outils d'ancienne génération représente un frein majeur à la modernisation et à la transformation numérique, sachant que 86 % des entreprises utilisent au moins un outil de ce genre et que seuls 12 % d'entre elles ont déployé des outils de surveillance modernes et entièrement intégrés.

Cette dépendance envers des outils disparates, obsolètes et mal connectés augmente les coûts de prise en charge de l'environnement, dégrade la qualité du service fourni et accroît les risques de sécurité (nous y reviendrons plus tard). Le manque d'intégration constitue un autre motif de frustration. Près de la moitié (46 %) des entreprises interrogées se plaignent de dépenser trop de temps et d'argent dans la maintenance et l'intégration des différents protocoles de sécurité.

Qui plus est, certains outils peuvent proposer des fonctionnalités similaires ou identiques, que vous payez donc deux ou trois fois. Dans tous les cas, il est certain qu'au moins un de vos outils n'exploite pas toutes ses fonctions intégrées, certaines étant supplantées par les fonctionnalités similaires d'autres composants. Ces chevauchements font que la plupart des outils sont sous-utilisés : l'environnement est trop complexe, les ressources ne sont pas suffisantes et l'administration des différents éléments implique une forte charge de travail.

> Pour résumer, la plupart des entreprises utilisent un éventail d'outils dont la conception ne prévoit pas des connexions fluides avec d'autres produits. Elles dépensent de l'argent pour des solutions intégrant des fonctionnalités en double, ce qui accroît les coûts de maintenance et les frais de licence initiaux. Enfin, à chaque fois qu'un composant est ajouté, il faut former les effectifs, renforcer la surveillance et mettre à jour la documentation.
>
> Heureusement, une alternative existe.

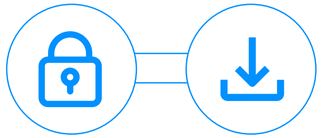
UN NOUVEAU MONDE, CELUI DES INTÉGRATIONS RÉUSSIES

Nous sommes loin des API poussives des débuts. Les équipes informatiques optent de plus en plus pour des solutions logicielles qui sont intégrées dès la conception, et non assemblées de bric et de broc après coup. La fin de l'informatique dominée par la traduction des commandes API approche.

En matière de développement, la complexité est un facteur important d'augmentation des coûts de maintenance, de sécurité et de support. Plus vous disposez de systèmes séparés pour la sauvegarde, la protection antimalware, le support à distance et la gestion, plus vous devez établir de connexions, qui représentent autant de points faibles et de vecteurs de menaces au sein de votre environnement. Je m'explique.

Exemple 1

Vous disposez de deux solutions logicielles et d'un connecteur fournis par deux ou trois partenaires qui doivent travailler ensemble. L'un d'eux peut très bien modifier son outil, risquant ainsi d'interrompre la connexion ou de créer une vulnérabilité exploitable.



Exemple 2

Vous disposez de trois solutions logicielles et de deux connecteurs fournis par deux, trois, quatre ou cinq partenaires qui doivent travailler ensemble. De nouveau, l'un d'eux peut très bien modifier son outil, risquant ainsi d'interrompre la connexion ou de créer une vulnérabilité exploitable.

Exemple 3

Examinons maintenant la même situation du point de vue des applications de sécurité intégrées, c'est-à-dire conçues pour fonctionner ensemble dès le début. La même équipe les a développées de façon à les rendre compatibles les unes avec les autres dès la conception.

Imaginons que vous souhaitiez connecter deux applications et leurs services, par exemple une solution de sauvegarde et un antivirus. Plusieurs scénarios sont possibles. Les applications sont-elles développées par la même société ? Sont-elles conçues dès le départ pour fonctionner ensemble ? S'il y a une connexion entre les deux systèmes, a-t-elle été écrite par l'une des deux entreprises principales ou par un tiers ?

En limitant la complexité logicielle, vous bénéficiez d'une plus grande efficacité, vous réduisez les tâches de maintenance, vous améliorez la productivité et vous renforcez la sécurité. Vous diminuez aussi vos coûts dès le début, car vous n'avez pas besoin de payer un middleware tiers pour faire fonctionner votre pile applicative ni de consacrer du temps à l'administration des applications ajoutées.

On constate un problème de plus en plus fréquent chez les fournisseurs de services informatiques : la lassitude, notamment de devoir payer des factures d'une multitude de sociétés juste pour pouvoir faire fonctionner un système correctement.

Une entreprise s'est attaquée de front à ce problème. Acronis a développé une pile de produits qui fonctionnent de façon harmonieuse les uns avec les autres. Basé sur l'intégration complète de ses différents composants, Acronis Cyber Protect optimise l'efficacité en simplifiant le fonctionnement et en diminuant le coût total de possession. Comme l'explique Lauren Beliveau, responsable marketing produit chez Acronis, « nous ne proposons pas un éventail de produits, nous proposons une pile de solutions ».

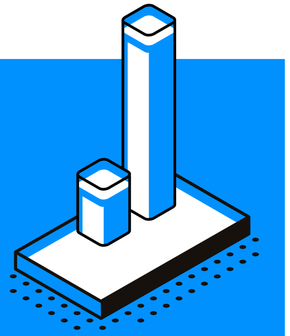
Mais le problème n'est pas seulement théorique. Dans le monde de la sécurité, le « patchwork » à l'ancienne d'outils hérités représente une sérieuse menace qui exige une surveillance renforcée. Chaque connexion constitue une vulnérabilité potentielle, de même que chaque correctif et mise à jour. Lorsque vous appliquez un correctif, vous devez surveiller que tout se passe bien et qu'aucun nouveau problème ne survient. Parfois, vous devez désinstaller un correctif, puis le réappliquer si des vulnérabilités apparaissent.

Malheureusement, une approche courante consiste à attendre un certain temps avant d'appliquer un correctif afin de vérifier qu'il ne va pas introduire d'autres problèmes, incompatibilités ou failles. Cette pratique laisse les applications vulnérables aux menaces connues pendant une période assez longue.

En outre, il est possible que des applications mal intégrées de différents fournisseurs ne soient pas capables de partager les données, alertes, fonctionnalités automatisées, documents, interfaces utilisateur, agents, etc. Ainsi, chaque point faible d'une connexion est une faille de sécurité et, aujourd'hui, le coût de ces points faibles est trop élevé pour être ignoré.

Avec Acronis Cyber Protect, l'antivirus détecte les sauvegardes et les analyse. Cette solution 100 % intégrée permet aux différents composants (sauvegarde, antivirus, etc.) de fonctionner plus efficacement ensemble. Les sauvegardes sont automatiquement analysées pour y détecter d'éventuelles menaces (virus, malwares, ransomwares, etc.) et vérifier que les données sont saines. Les correctifs sont appliqués aux sauvegardes comme aux systèmes en ligne. Le tout de façon réellement harmonieuse.

Des logiciels moins complexes sont gages d'une plus grande efficacité, d'une maintenance réduite, d'une productivité renforcée et d'une sécurité accrue



LA MATURITÉ DE L'ENTREPRISE, UN FACTEUR À NE PAS NÉGLIGER

La maturité de l'entreprise qui propose les outils est un facteur de complexité rarement pris en compte. Entre la phase de démarrage et la pleine maturité, une entreprise passe par différentes étapes. Au début, elle propose un produit immature qui n'effectue qu'une seule tâche (par exemple, la protection antivirus). Au fil du temps, le produit devient pleinement fonctionnel. À mesure que l'entreprise assoit sa position sur le marché, ses priorités changent et s'orientent davantage vers la rapidité de commercialisation de son produit et l'augmentation de son chiffre d'affaires.

Le principal objectif des entreprises établies est d'étendre leur connectivité et les fonctionnalités qu'elles proposent. C'est là qu'elles commencent à adopter les API, afin de pouvoir toucher le public le plus large possible. Cette phase est certainement la plus propice au bricolage. La plupart du temps, ce bricolage marche, sauf que les API ne sont pas matures et changent en permanence. Si les API sont efficaces, les utilisateurs vont demander d'autres fonctionnalités. L'entreprise passe alors à la phase suivante, qui consiste à élargir sa clientèle.

Une entreprise arrivée à cette étape est davantage orientée vers l'achat ou le développement de nouvelles fonctionnalités. Sa stratégie est de conquérir des clients en étoffant ses solutions et en collaborant avec un plus grand nombre de concurrents, le but final étant est de remporter des parts de marché en répondant à la demande des utilisateurs et en optimisant son ensemble d'outils. Cette phase d'essor coïncide avec des changements internes en profondeur et un gros effort de suivi de l'évolution des API, que ce soit en interne, entre les produits que l'entreprise achète et intègre, ou entre ses produits et ceux de ses concurrents.

L'étape suivante est l'expansion financière. La croissance d'une entreprise est nécessairement ponctuée de moments où elle a besoin de financements, que ce soit par le biais du capital-risque ou de toute autre source. Ce sont des phases où la réactivité des clients peut baisser. En effet, comme l'entreprise axe ses efforts sur la recherche de fonds, elle peut avoir tendance à faire passer le développement logiciel au second plan. L'importance de vendre prend alors le pas sur la résolution des problèmes ou l'ajout de fonctionnalités.

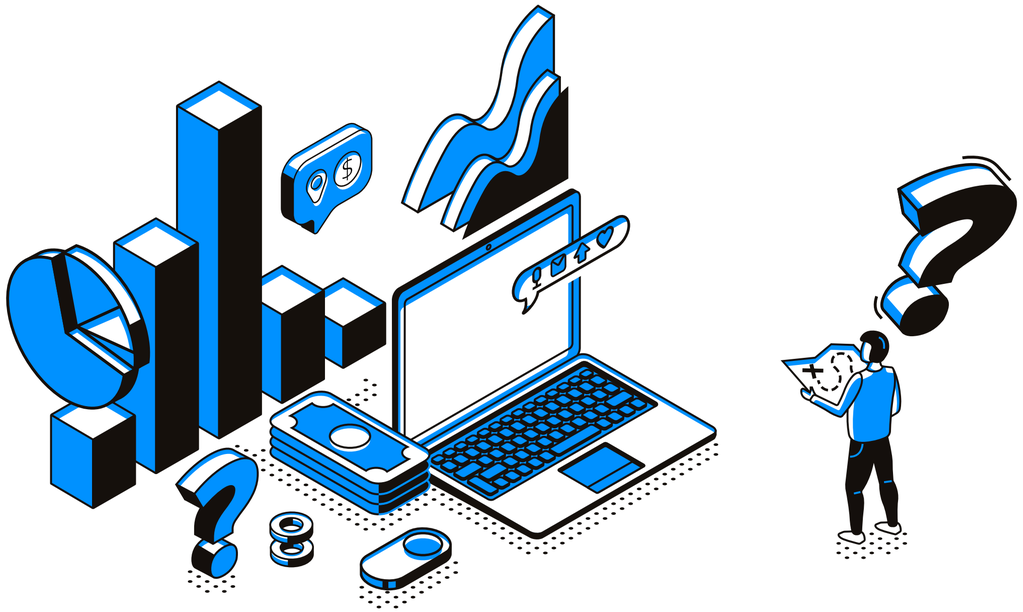
Si, dans votre parcours, vous avez vécu des fusions-acquisitions, vous avez peut-être constaté pendant ces périodes-là qu'un fournisseur habituellement ultraréactif cessait soudainement d'effectuer la maintenance nécessaire, et que la feuille de route du produit devenait très floue pour les professionnels utilisant le logiciel en question. À ce stade, les ventes constituent l'unique préoccupation de l'entreprise et les activités de développement (y compris de maintenance) sont réduites à peau de chagrin.

Les entreprises qui vivent assez longtemps pour parvenir à pleine maturité sont rares. Comment font-elles ? Elles développent des outils bien intégrés qui fonctionnent en parfaite harmonie les uns avec les autres ; les activités de programmation sont suffisamment soutenues pour permettre l'ajout de nouvelles fonctionnalités sans interruptions ni création de nouveaux problèmes. En plus d'avoir relevé les défis techniques, une entreprise mature est parvenue à mettre en place

un plan à long terme de financement du développement continu, des activités commerciales et du support client.

La technologie évolue chaque année un peu plus vite, faisant apparaître de nouveaux défis. Il est donc primordial de développer en permanence de nouvelles fonctionnalités. Ce principe s'applique à la cybersécurité plus qu'à tout autre domaine. Il y a dix ans, les virus provoquaient déjà des dégâts, mais aujourd'hui, ils peuvent obliger une entreprise à payer des millions de dollars de rançon, en plus de devoir subir le coût des temps d'arrêt.

Parlons maintenant de deux autres types d'entreprises : celles qui ne sont pas parvenues à un haut niveau de maturité et celles qui n'ont jamais été acquises et fusionnées avec d'autres. Ces entreprises continuent généralement à utiliser des produits d'ancienne génération. Très souvent, elles ne disposent ni du temps, ni du budget, ni des ressources internes nécessaires pour rester en phase avec les dernières exigences de sécurité.



Dans le meilleur des cas, elles travaillent avec des solutions obsolètes. Dans le pire des cas, leurs solutions ne s'intègrent pas aux outils les plus récents.

Comme je le disais précédemment, plus un ensemble d'outils est complexe, moins il est efficace. En plus de devoir affronter le problème de la multiplication des API, vous devez administrer une activité interne intense : faire fonctionner ensemble des logiciels qui n'ont pas le même niveau de maturité, veiller à ce que des fournisseurs disposant d'API disparates effectuent le support et mettre à jour en permanence la documentation.

Dans un tel contexte, votre but est de construire une pile performante. Cela peut impliquer de chercher les meilleures options, y compris auprès de plusieurs fournisseurs. Cela peut aussi signifier que vous achetez le plus de composants possible d'une même pile afin d'accroître l'efficacité, la sécurité et les bénéfices.

> Acronis Cyber Protect vous offre le meilleur des deux mondes. Fort de sa solide réputation de leader sur le marché de la protection et de la restauration des données, Acronis a mis au point toute une série de solutions de premier ordre pour protéger les données, les applications et les systèmes, et éliminer les middlewares devenus encombrants.
>
> Acronis Cyber Protect inclut des fonctionnalités que ses concurrents ne vont pas manquer de copier, comme l'application de correctifs aux images de sauvegarde afin d'éviter que les procédures de restauration fassent baisser le niveau de sécurité sur les ordinateurs des clients.

Entre les ransomwares, les risques de poursuites judiciaires à plusieurs millions de dollars et les réglementations gouvernementales, la décennie 2020 ne démarre pas sous les meilleurs auspices. Alors, évitez de vous lancer dans la création d'un environnement constitué d'outils de sécurité disparates en espérant qu'ils vont fonctionner de façon harmonieuse ! Optez pour une solution qui offre des fonctionnalités et une sécurité de pointe tout en simplifiant les opérations, en limitant la maintenance et en réduisant les coûts associés.

Passez à la seule pile de sécurité 100 % intégrée dès sa conception.

CONCLUSION

La sécurité ne peut plus être considérée comme une fonctionnalité complémentaire des autres services. Dans cette nouvelle décennie, les consultants en technologie doivent disposer de solutions complètes et solides, qui offrent une sécurité inégalée tout en permettant aux utilisateurs de faire ce qu'ils ont à faire.

La complexité diminue l'efficacité et la productivité tout en augmentant les coûts de maintenance, de documentation et de formation. Plus vous avez de composants, plus vous avez de connecteurs. Une pile complètement intégrée, dont les composants sont conçus pour fonctionner ensemble de façon harmonieuse, maximise la sécurité globale tout en simplifiant les opérations et en réduisant les coûts associés.

Nous ne sommes pas près de nous débarrasser des API. Heureusement, avec la pile entièrement intégrée d'Acronis, le leader de la cybersécurité et de la protection des données, vous pourrez maintenir un haut niveau de productivité même si vous gérez des systèmes complexes et interconnectés.

Les connexions, c'est bien. L'intégration dès la conception, c'est mieux.

RÉFÉRENCES

https://www.msn.com/en-us/news/technology/boeings-software-troubles-show-an-engineering-culture-clash/ar-BB16xEdq

https://www.forbes.com/sites/jonathanocallaghan/2019/12/20/boeing-starliner-spacecraft-launches-to-the-international-space-station-heralding-a-new-era-for-american-human-spaceflight/

If This Then That
https://ifttt.com/

Zapier
https://zapier.com/

ProgrammableWeb
https://www.programmableweb.com/

Salesforce.com
www.salesforce.com

Harvard Business Review, « The Strategic Value of APIs »
https://hbr.org/2015/01/the-strategic-value-of-apis

« Gartner Says Organizations Can Cut Software Costs by 30 Percent Using Three Best Practices »
https://www.gartner.com/en/newsroom/press-releases/2016-07-19-gartner-says-organizations-can-cut-software-costs-by-30-percent-using-three-best-practices

Forrester Research, « Prevalence Of Legacy Tools Paralyzes Enterprises' Ability To Innovate »
https://sciencelogic.com/wp-content/uploads/sciencelogic-os.pdf

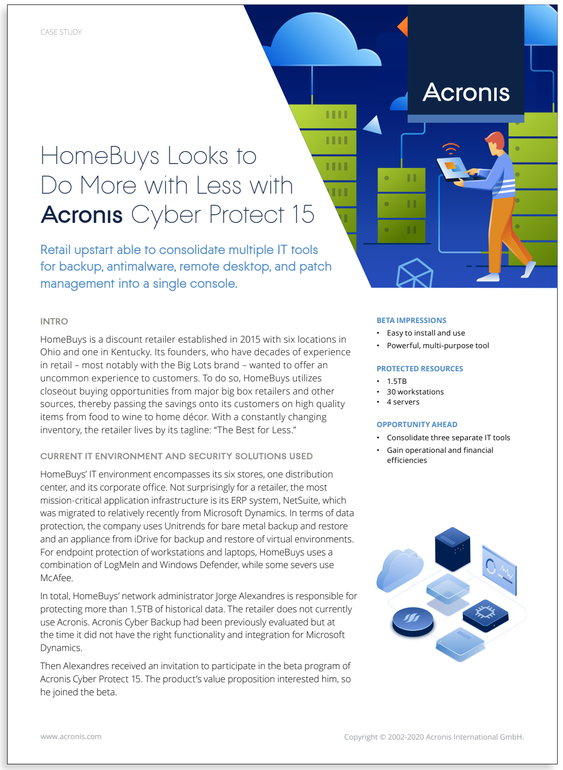
« Struggling With Toolchain Sprawl? You're Not Alone »
https://dzone.com/articles/toolchain-sprawl-youre-not-alone

À PROPOS DE L'AUTEUR

Karl W. Palachuk a créé puis revendu deux entreprises de services managés à Sacramento, en Californie. Fondateur et président de SMB IT Professionals, un groupe réunissant des professionnels de l'informatique orientés PME à Sacramento, il a également publié plusieurs ouvrages, dont « The Network Documentation Workbook » et « Managed Services in a Month ».

Depuis plus de 15 ans, Karl W. Palachuk est intervenant d'honneur lors de conférences et de séminaires dans le monde entier. Ce titulaire d'une licence de l'université Gonzaga et d'une maîtrise de l'université du Michigan possède la certification Microsoft Certified Systems Engineer. Il détient également le titre de Microsoft Small Business Specialist et figure parmi les membres originaux du groupe consultatif Small Business Specialist de Microsoft.

RESSOURCES SUPPLÉMENTAIRES


CASE STUDY

Acronis

HomeBuys Looks to Do More with Less with **Acronis** Cyber Protect 15

Retail upstart able to consolidate multiple IT tools for backup, antimalware, remote desktop, and patch management into a single console.

INTRO

HomeBuys is a discount retailer established in 2015 with six locations in Ohio and one in Kentucky. Its founders, who have decades of experience in retail – most notably with the Big Lots brand – wanted to offer an uncommon experience to customers. To do so, HomeBuys utilizes closeout buying opportunities from major big box retailers and other sources, thereby passing the savings onto its customers on high quality items from food to wine to home décor. With a constantly changing inventory, the retailer lives by its tagline: "The Best for Less."

CURRENT IT ENVIRONMENT AND SECURITY SOLUTIONS USED

HomeBuys' IT environment encompasses its six stores, one distribution center, and its corporate office. Not surprisingly for a retailer, the most mission-critical application infrastructure is its ERP system, NetSuite, which was migrated to relatively recently from Microsoft Dynamics. In terms of data protection, the company uses Unitrends for bare metal backup and restore and an appliance from iDrive for backup and restore of virtual environments. For endpoint protection of workstations and laptops, HomeBuys uses a combination of LogMeIn and Windows Defender, while some severs use McAfee.

In total, HomeBuys' network administrator Jorge Alexandres is responsible for protecting more than 1.5TB of historical data. The retailer does not currently use Acronis. Acronis Cyber Backup had been previously evaluated but at the time it did not have the right functionality and integration for Microsoft Dynamics.

Then Alexandres received an invitation to participate in the beta program of Acronis Cyber Protect 15. The product's value proposition interested him, so he joined the beta.

BETA IMPRESSIONS

- Easy to install and use
- Powerful, multi-purpose tool

PROTECTED RESOURCES

- 1.5TB
- 30 workstations
- 4 servers

OPPORTUNITY AHEAD

- Consolidate three separate IT tools
- Gain operational and financial efficiencies

www.acronis.com

Copyright © 2002-2020 Acronis International GmbH.

Blog Acronis : pour suivre l'actualité et obtenir les points de vue éclairés du leader mondial de la cyberprotection

Chaîne YouTube Acronis : pour visionner régulièrement des vidéos portant sur des cas d'utilisation, des démos, des analyses de cybermenaces et des nouveautés concernant la société

Centre de ressources Acronis : plate-forme incontournable rassemblant des livres blancs sur la cyberprotection, des eBooks, des articles détaillés, des tutoriels, des présentations graphiques, etc.

Événements Acronis : pour rester au courant des événements en cours, webinaires, interviews, etc., et s'y inscrire

À PROPOS D'ACRONIS

Acronis unifie la protection des données et la cybersécurité pour fournir une cyberprotection intégrée et automatisée. Son but ? Relever les défis du monde numérique d'aujourd'hui en matière de fiabilité, d'accessibilité, de confidentialité, d'authenticité et de sécurité (SAPAS). En proposant des modèles de déploiement qui répondent aux besoins des fournisseurs de services et des professionnels de l'informatique, Acronis offre une cyberprotection de premier plan pour vos données, applications et systèmes, via une large gamme de solutions innovantes : antivirus de nouvelle génération, sauvegarde, reprise d'activité après sinistre et gestion de la protection des terminaux. Ses technologies primées de protection contre les malwares pilotée par l'intelligence artificielle et d'authentification des données par blockchain permettent à Acronis de protéger tous les types d'environnements (Cloud, hybride, sur site) à un coût abordable et prévisible.

Fondée à Singapour en 2003 et incorporée en Suisse en 2008, la société Acronis compte aujourd'hui plus de 1 500 collaborateurs répartis dans plus de 33 sites et 18 pays. Ses solutions ont été adoptées par plus de 5,5 millions de particuliers, 500 000 entreprises (dont la totalité des sociétés du classement Fortune 1000) et des équipes de sport professionnelles de haut niveau. Les produits Acronis sont distribués par un réseau de 50 000 partenaires et fournisseurs de services, couvrant plus de 150 pays et plus de 40 langues.

SBT Small Biz Thoughts

Par Karl W. Palachuk

SmallBizThoughts.com

eBook réalisé à la demande d'**Acronis**

acronis.com