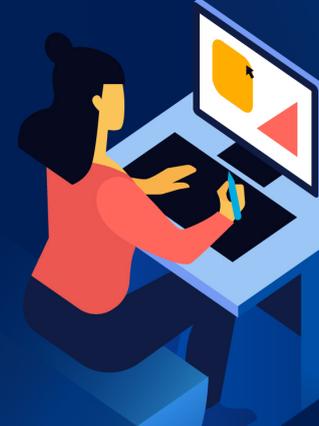




Acronis



LIVRE BLANC

# Les cinq niveaux d'intégration d'une plate-forme axée MSP

Comment permettre aux MSP d'intégrer efficacement des services de cyberprotection pour doper leurs revenus et développer leur activité grâce à la protection des systèmes, applications et données de leurs clients.



# Introduction

Pour rentabiliser et développer leur activité tout en réduisant le taux d'attrition, les MSP doivent surmonter de nombreux obstacles. De nombreux fournisseurs ont mis progressivement en place une offre multiservices, créant une infrastructure hétérogène, véritable mosaïque de services issus de divers éditeurs. L'absence d'intégration qui en résulte renforce la complexité tant au niveau métier que des opérations, entraînant une hausse des coûts et limitant le développement ultérieur des services.

**Les services de cybersécurité** constituent assurément l'une des pistes prometteuses à explorer par les MSP pour développer leur activité et doper leurs revenus. D'innombrables cyberattaques, telles que les ransomwares, menacent le monde entier. Les entreprises (et en particulier les PME) peinent à éviter les temps d'arrêt coûteux et les pertes de données qui en résultent. La tentation est grande pour un MSP d'ajouter quelques solutions de cybersécurité ponctuelles à sa gamme de services actuelle. Ce faisant, il ne fait qu'accroître le manque d'homogénéité de l'infrastructure, et chaque ajout de nouveau service érode les bénéfices et détériore l'efficacité.

**Il existe une manière plus rationnelle** de satisfaire aux besoins immédiats des PME en matière de cyberprotection tout en assurant une croissance stable et rentable de son activité. Pour ce faire, les MSP doivent relever cinq défis de taille en matière d'intégration et d'automatisation, au niveau opérationnel et technologique. Ce livre blanc analyse ces défis et donne des pistes aux MSP pour les relever.



*« La collaboration avec Acronis présente de nombreux avantages : la solution est facile à utiliser et permet d'assurer la continuité des activités dont CUT a besoin grâce à la restauration rapide des machines virtuelles ou physiques. »*

**Michael Edmunds,**  
**Directeur du marketing partenaires,**  
**Bastion Backups**

# Les statistiques le montrent, la cyberprotection et les opérations informatiques de base sont un casse-tête pour les entreprises.

Il suffit de prendre le temps d'écouter ses clients pour comprendre que l'implémentation et le maintien de la cybersécurité constituent l'une des difficultés majeures, en raison de la pénurie de personnel compétent.

## Voici quelques résultats d'une étude de marché indépendante :

- Délai moyen entre la disponibilité et l'installation d'un correctif : 102 jours (*Ponemon Institute : 2018 State of Endpoint Security*)
- Perte de productivité annuelle moyenne due aux pannes informatiques : 545 heures (*ERS IT Solutions, 2019*)
- Durée moyenne de reprise après une panne informatique : 200 minutes (*ERS IT Solutions, 2019*)
- Coût moyen par terminal d'une cyberattaque avérée : 470 \$ (entreprise) à 763 \$ (PME) (*Ponemon*)

Selon les projections de Cybersecurity Ventures, ces problèmes ne feront qu'empirer ; en effet, le nombre de postes vacants dans le domaine de la cybersécurité devrait atteindre les 3,5 millions d'ici 2021 au niveau mondial

## Cette situation représente un énorme potentiel d'activité pour les MSP. Il ne leur reste plus qu'à saisir cette opportunité en proposant une suite de services de cyberprotection, notamment :

- Effectuer des ventes croisées de services de cyberprotection aux clients existants
- Attirer de nouveaux clients grâce à des offres de base, puis développer ces comptes en ajoutant des services de cyberprotection
- Proposer d'abord une cyberprotection pour une application populaire (p. ex. Office 365), puis l'étendre à d'autres applications (p. ex. applications

de back-office de finance et de comptabilité) et à de nouvelles plates-formes (p. ex. terminaux mobiles, serveurs, stockage et sauvegarde dans le Cloud)

Pour pouvoir tirer le meilleur profit de cette stratégie et pérenniser la croissance de l'activité, il convient de mettre en place une approche plus judicieuse reposant sur cinq niveaux d'intégration de la plate-forme MSP. Pour conquérir de nouveaux clients, faire fructifier son portefeuille client et limiter le taux d'attrition, tout en réduisant les dépenses d'investissement et les frais d'exploitation afin d'augmenter les marges, il est nécessaire d'améliorer l'intégration à différents niveaux : environnement métier, produits, gestion, interface utilisateur et technologie. Passons en revue ces différents niveaux.

Selon les projections de Cybersecurity Ventures, les problèmes de cybersécurité auxquels doivent faire face les PME ne feront qu'empirer ; en effet, le nombre de postes vacants dans le domaine de la cybersécurité devrait atteindre les 3,5 millions d'ici 2021 au niveau mondial.



# Niveau 1 : Intégration métier

Les services de cyberprotection sont certes attractifs, mais ne peuvent être rentables que s'ils s'intègrent parfaitement à votre infrastructure existante, ainsi qu'à vos systèmes métier. Faire appel à un nouveau fournisseur pour chaque nouveau service proposé coûte cher à chaque étape de votre processus métier.

## LE DÉFI :

Le recours à différents fournisseurs pour élaborer une suite de services basée sur une infrastructure hétérogène augmente les coûts et la complexité de la gamme de services et des offres groupées, de l'intégration aux systèmes de facturation et de provisionnement, de l'élaboration et de l'exécution d'un programme marketing et de la négociation et de la gestion des contrats/SLA avec les fournisseurs.

## LA SOLUTION :

Une plate-forme intégrée commune pour la fourniture des services qui simplifie le regroupement, s'intègre de façon transparente aux systèmes de back-office, permet une communication marketing unifiée et réduit le nombre de fournisseurs à gérer.

## LES AVANTAGES :

Ventes et commercialisation plus simples et plus pratiques se traduisant par une concrétisation plus rapide des prospects, une marge plus élevée sur les services fournis et une baisse des coûts de gestion des fournisseurs.



## Niveau 2 : Intégration de l'interface utilisateur

Le défi de l'intégration de l'interface utilisateur est simple, mais fondamental : moins l'interface est centralisée et plus les coûts liés au centre de données (consommation d'énergie, refroidissement, immobilier) seront élevés, de même que les coûts de formation de vos techniciens. Gênés par la complexité de la gestion de l'infrastructure, ces derniers risquent de ne pas pouvoir repérer toutes les alertes critiques.

### LE DÉFI :

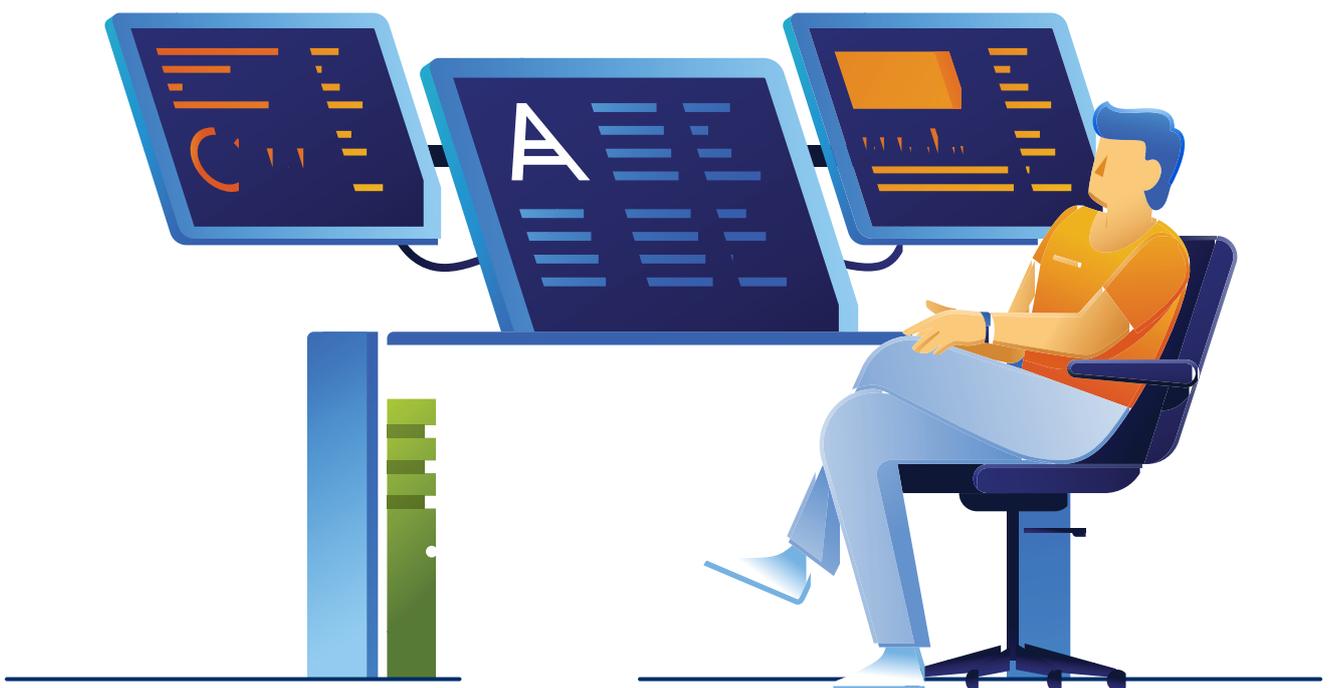
Pour gérer une multitude de produits issus de fournisseurs différents, il faut jongler avec plusieurs consoles et acquérir des compétences spécifiques à chaque technologie.

### LA SOLUTION :

Notre console de gestion intégrée, dotée d'une interface utilisateur uniforme, est optimisée pour les opérations informatiques et prend en charge le workflow métier dans l'ensemble de la suite de services.

### LES AVANTAGES :

Formation plus rapide et plus économique, opérations plus performantes et amélioration de l'épanouissement professionnel des techniciens en informatique grâce à l'utilisation d'outils conviviaux.



## Niveau 3 : Intégration de la gestion

Les nouveaux services ont besoin d'être intégrés à une infrastructure. Vous devez pouvoir les provisionner, les surveiller à distance et gérer leurs performances sur le site du client, collecter des informations à des fins de dépannage, appliquer des correctifs et des mises à niveau et enfin, facturer le client.

Idéalement, vous pouvez enrichir vos services de nouvelles fonctionnalités et capacités au niveau de l'API. Plus l'intégration avec vos systèmes de gestion existants est fluide et transparente, moins leur fonctionnement sera coûteux et plus vos marges seront élevées.

### LE DÉFI :

L'absence d'intégration entre différents systèmes (*RMM, PSA et solutions de cybersécurité tierces, p. ex.*) génère des opérations manuelles coûteuses et limite le développement du produit.

### LA SOLUTION :

Unification de la gestion des règles, des audits, des contrôles d'accès et de la confidentialité, étroitement liée à des systèmes de dépannage, d'alerte et de gestion et surveillance à distance. Adoption de systèmes avec API et points d'intégration simples à déployer et permettant d'utiliser des contrôles de sécurité d'accès personnalisés et autres règles de sécurité par groupe et individu.

### LES AVANTAGES :

Fourniture de services plus efficace et à marge plus élevée ; possibilité d'étendre les services de cyberprotection via l'intégration de l'API de la plate-forme.

« Les intégrations avec la plate-forme ConnectWise sont indispensables pour nos MSP. L'intégration entre Acronis Cyber Cloud et ConnectWise Control est la première du genre. Elle fonctionne très bien et nos MSP en apprécient la valeur. »

**Jeff Bishop,**  
Directeur produits, ConnectWise



# Niveau 4 : Intégration produit

Rien de commun entre une gamme de services basée sur de multiples produits disparates et une offre reposant sur une plate-forme permettant d'ajouter un nouveau service par une simple activation logicielle.

Pour remplir toutes les fonctions d'un smartphone, vous aviez autrefois besoin d'un téléphone à clapet, d'un dispositif GPS, d'une lampe de poche, d'un appareil photo et ainsi de suite. Vous disposez aujourd'hui d'un appareil compact, rentable, facile à sécuriser, à gérer, à utiliser et à mettre à jour avec de nouvelles applications. Les MSP ont besoin d'une approche produit intégrée similaire basée sur une plate-forme.

## LE DÉFI :

L'élaboration d'une suite de services à partir de produits multifournisseurs risque de générer des problèmes technologiques persistants, notamment en matière d'interopérabilité. L'ajout et le regroupement de nouveaux services augmentent les coûts et la complexité de la gestion, du provisionnement, de la facturation et des rapports. Votre équipe informatique aura de plus en plus de mal, techniquement et financièrement, à gérer l'ajout de ces nouveaux produits. De plus, elle manquera de temps pour s'occuper des nouveaux clients et faire face à la concurrence des nouveaux venus sur le marché.

## LA SOLUTION :

Une plate-forme qui permet de proposer un ensemble complet de services de cyberprotection : sauvegarde, reprise d'activité après sinistre, synchronisation et partage de fichiers, antivirus, antimalware, évaluations des vulnérabilités, gestion des correctifs et une large gamme de cibles de stockage.

## LES AVANTAGES :

Vous allez pouvoir proposer une gamme étendue et flexible de services de protection des données et de cybersécurité répondant à une multitude de cas d'utilisation métier, sans les coûts et la complexité d'une infrastructure hétérogène multifournisseurs. Vous bénéficierez en outre d'une intégration plus granulaire des produits et d'échange d'informations entre produits, p. ex., la capacité d'analyser les archives de sauvegarde stockées dans le Cloud pour vérifier l'absence de malware avant de les utiliser pour la restauration.

**Terminal ordinaire**

- 1 processeur
- 8 Go de RAM
- Windows 10
- 1 To de stockage en local
- Office 365
- Six applications supplémentaires

**FONCTIONS DE GESTION DE LA CYBERSÉCURITÉ/ OPÉRATIONS INFORMATIQUES**

**Système d'exploitation :** règles, correctifs, vulnérabilités, gestion de la configuration

Gestion et surveillance à distance, défenses comportementales antimalware, protection des données/sauvegardes, antivirus basé sur les signatures, données Cloud, gestion des réseaux

# Niveau 5 : Intégration technologique

Une intégration technologique avancée entre les composants d'une infrastructure de services permet de générer de nouvelles fonctionnalités et capacités, ce qui n'est pas possible avec des produits distincts issus de différents fournisseurs.

Une collaboration étroite entre les différents services d'une suite permet de générer de nouvelles fonctionnalités (p. ex. application de correctifs et analyse antimalware des sauvegardes avant toute opération de restauration) et de nouvelles capacités. Par exemple, l'emploi d'un agent de terminal unique permet de remédier aux problèmes posés par un environnement multiagents : baisse des performances, conflits d'interopérabilité et de ressources, absence d'intégration des alertes, des rapports et de l'utilisation de l'apprentissage automatique et de l'intelligence artificielle.

## LE DÉFI :

Les offres groupées multifournisseurs de services autonomes empêchent toute possibilité de créer de nouvelles fonctionnalités à forte valeur ajoutée (p. ex. l'inclusion d'investigations numériques dans les sauvegardes). La multiplication des agents de terminal pose des problèmes de performance et d'interopérabilité.

## LA SOLUTION :

Des produits étroitement liés procurent les mêmes avantages qu'une offre de services unique (p. ex. application de correctifs et recherche de malwares dans les sauvegardes avant toute opération de restauration) et optimisent les performances (p. ex. agent de terminal unique pour gérer l'ensemble des services).

## LES AVANTAGES :

Nouvelles fonctionnalités multiservices utiles, diminution de l'impact de l'agent sur la performance du terminal, renforcement de l'automatisation de la réponse aux événements et simplification de la gestion et de la maintenance.

*« Notre objectif était le regroupement en une seule technologie afin de bénéficier d'une gestion centralisée de l'ensemble de nos clients, avec la possibilité d'effectuer une surveillance et une gestion globales depuis une seule interface. Nous avons besoin de tout gérer depuis un seul emplacement. »*

**Borhan Zoufan,**  
**CTO, Caspian IT Group, expliquant son choix**  
**d'Acronis Cyber Cloud**



# Résumé

Le progrès technologique passe par la consolidation. Au siècle dernier, on utilisait des équipements de réseau coûteux et encombrants (routeur, commutateur, serveur d'accès à distance, modem numérique) ; aujourd'hui, il suffit d'un boîtier économique, compact et facile à gérer. Les anciens téléphones aux fonctionnalités limitées (appel et message) ont été remplacés par des appareils iOS ou Android contenant des dizaines d'applications.

La marche vers l'intégration est inévitable et sera bénéfique aux fournisseurs comme aux consommateurs. Cette même évolution concerne aujourd'hui le monde des MSP, sous la forme des **cinq niveaux d'intégration d'une plate-forme axée MSP** qui vous offrent les avantages suivants :



**Acquérir de nouveaux clients,** faire fructifier les comptes existants, réduire le taux d'attrition et augmenter les marges



**Réduire le risque métier de vos clients** grâce à une cybersécurité renforcée, à la protection contre les pertes de données et à la réduction des temps d'arrêt



**Réduire l'hétérogénéité de votre infrastructure d'offre de services,** minimiser vos problèmes d'intégration et limiter les coûts de gestion des fournisseurs et des technologies



**Tirer parti de l'intelligence artificielle,** du libre-service client et autres technologies d'automatisation pour développer votre activité et optimiser les opérations en limitant les coûts d'infrastructure et de personnel

## Pour plus d'informations,

**Découvrez comment tirer parti des cinq niveaux d'intégration d'une plate-forme axée MSP :**

Pour plus d'informations, consultez le [Centre de ressources Acronis](#)

CONSULTER

Obtenez une évaluation gratuite de 30 jours d'[Acronis Cyber Backup Cloud](#)

ESSAYEZ MAINTENANT

Contactez directement [Acronis](#)

DEMANDER UNE DÉMONSTRATION