Acronis

#CyberFit

Acronis Cyber Protect 15

Protégez vos données contre toutes les menaces grâce à une solution unique

Acronis

- **Bienvenue à toutes et à tous**
- **Ce webinaire est en cours d'enregistrement**
- **Veuillez soumettre vos questions via Q&R.**

#CyberFit

Maxime Clay

Senior Solution Engineer
Acronis

Acronis

Qui sommes nous?

© Acronis 2023

Acronis est un leader dans le domaine de la cyberprotection

Swiss

Depuis 2008, le siège social de l'entreprise est situé à Schaffhausen, en Suisse

Singaporean

Fondée en 2003 à Singapour, actuellement le siège international

Un double siège pour une double protection

Scale & Rapid Growth

$300M+ CA
50% de croissance
100%+ dans le cloud
Levée de fonds 500M
Valorisation à 3,5Mds

Global Reach

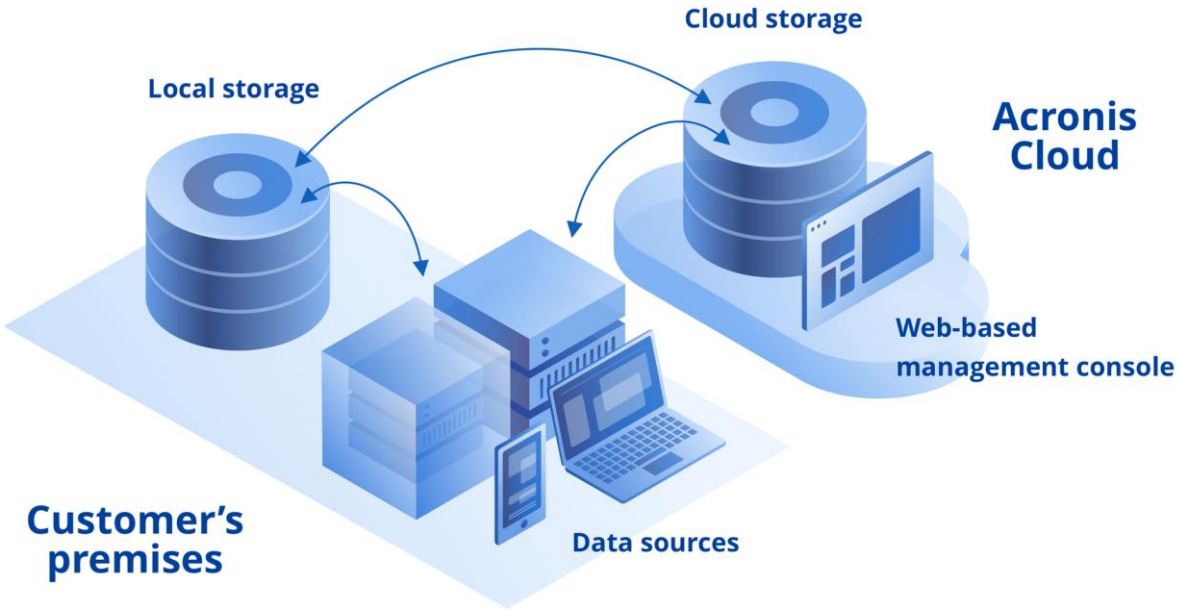
100% du Fortune 1000
16,000+ partenaires
750,000+ enterprise
5,500,000+ business

Global Presence

2000+ employés
34 bureaux
Solution disponible dans 150+ pays et 26+ langues

© Acronis 2023

Cloud, local, ou les deux !

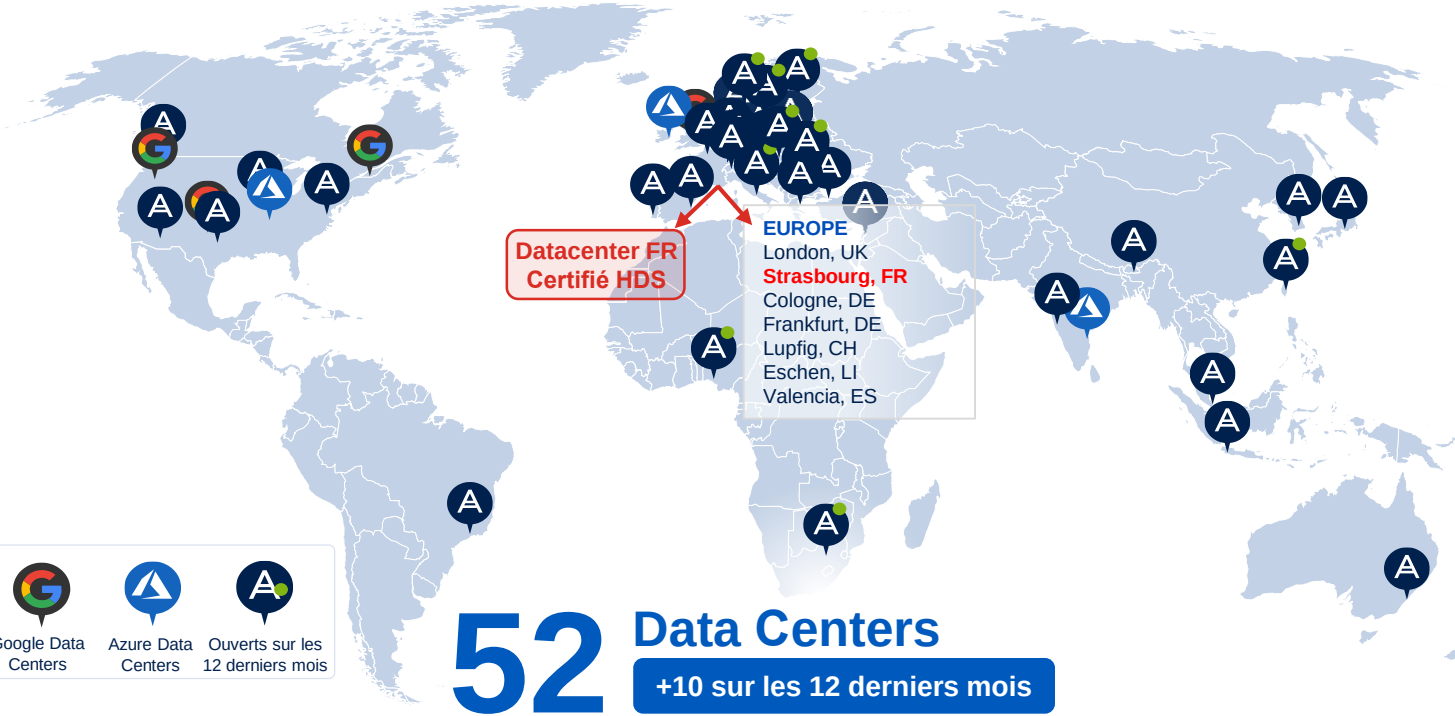


© Acronis 2023

Assurer la conformité et une présence locale

Choisissez parmi 52 DC dans le monde pour stocker des données - hébergés par Acronis, Google Cloud et Microsoft Azure

Australia
Austria
Bhutan
Brazil
Bulgaria
Canada
Czech
Denmark
Finland
France
Germany
Greece
Hungary
India
Indonesia
Ireland
Israel
Italy



Japan
Latvia
Liechtenstein
Nederland
New Zealand
Nigeria
Norway
Poland
Portugal
Romania
Singapore
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Turkey
United Kingdom
USA

Acronis Data Centers | Google Data Centers | Azure Data Centers | Ouverts sur les 12 derniers mois

52 Data Centers

+10 sur les 12 derniers mois

© Acronis 2023

Gardez le Contrôle de vos Données grâce à Cyber Protect 15

ANY MANAGEMENT

Management software deployed and controlled independently, enabling data protection control by customer, service provider, vendor, partner, or third-party from public/partner/private cloud or customer premises

Toute Protection

- Sauvegarde
- Stockage
- Reprise d'activité après sinistre (DR)
- Synchronisation & Partage
- Notary/ASign
- Protection anti rançongiciels

Tout Workload

- On-premises
- Private Cloud
- Cloud
- Mobile
- Applications
- Files
- Virtuel

Tout Stockage

- Disk, Tape
- NAS, SAN
- Partner Cloud
- Private Cloud
- Public Cloud
- Acronis Cloud

Tout Déploiement

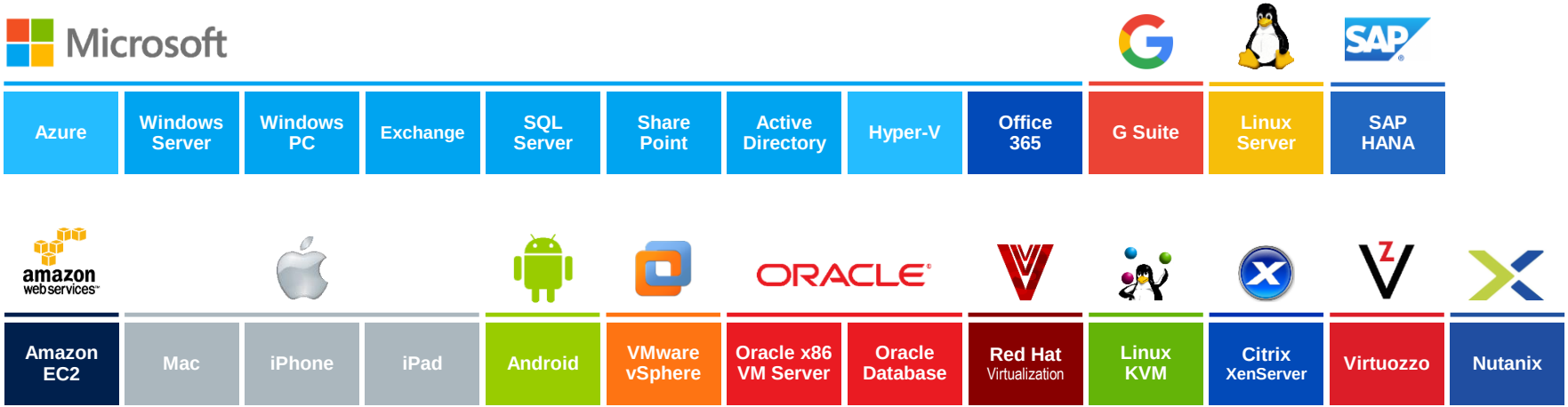
- Local
- Cloud privé
- Cloud partenaire
- Cloud Acronis
- Cloud public

Toutes Restaurations

- Physique
- Virtuelle
- Mobile
- Applications
- Fichiers
- Cloud

© Acronis 2023

Périmètre de protection très étendue, et en largeur et en profondeur



© Acronis 2023

Acronis

#CyberFit

Acronis Cyber Protect 15 au delà de la sauvegarde : la Cyberprotection

Terminaux et équipements en périphérie sous le feu des attaques

Les volumes de données augmentent rapidement, mais sans bénéficier du niveau de sécurité d'un centre de données d'entreprise

63 % affirment que la fréquence des attaques de terminaux a augmenté en 2018

Le délai moyen pour l'application de correctifs est de 102 jours

Les antivirus ratent 57 % des attaques

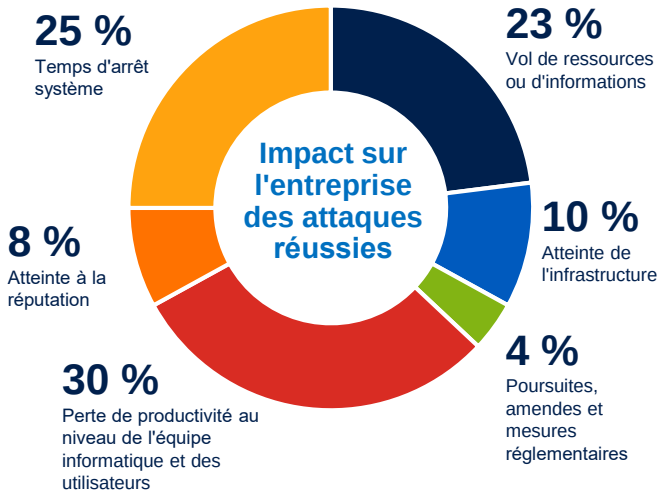
Les données ont une croissance 33 x plus rapide que le personnel informatique

50 % des disques durs tombent en panne dans les 5 ans

60 % des entreprises ont été ciblées par un ransomware

64 % ont été affectées par des attaques de terminaux en 2018 contre 54 % en 2017

- Bureaux distants
- Serveurs Cloud
- Serveurs hébergés
- Postes de travail
- Systèmes mobiles

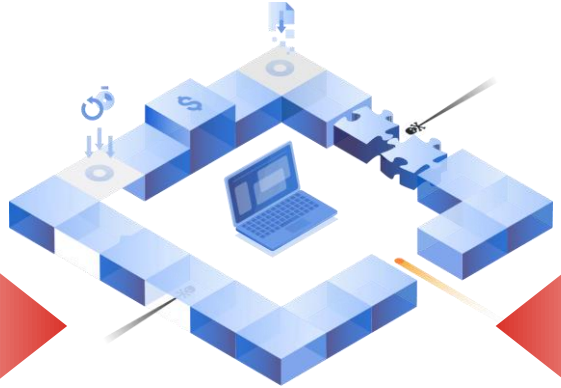


Chaque attaque aboutie coûte 7,1 millions de dollars pour une grande organisation, soit en moyenne 301 $ par employé ou 440 $ par terminal

Sources : « Trends in SaaS Data Protection », Spanning, 2016 ; « Understanding the Depth of the Global Ransomware Problem », Osterman Research, 2016 ; « Hosting and Cloud Study 2017 », 451 Research, 2017 ; « The 2018 State of Endpoint Security Risk », Ponemon Institute (à la demande d'Emerson Network Power) ; « CEO Survey » (United States), PwC, 2016

© Acronis 2023

Les outils proposés actuellement ne peuvent pas lutter contre les nouvelles menaces



Les antivirus traditionnels ne protègent pas les données

- Pas de restauration des données
- Attaques avancées et jour zéro
- Vulnérabilités connues

La multiplication des outils renforce la complexité

- Conflits entre agents
- Coûts de l'infrastructure et du personnel
- Pas de console unique

Les sauvegardes traditionnelles ne sont pas sécurisées

- Vulnérables aux attaques, compromissions et modifications
- Machines infectées ne pouvant pas être restaurées
- Aucune autoprotection, aucun soutien aux investigations

Complexes **Coûteux** **Peu fiables**

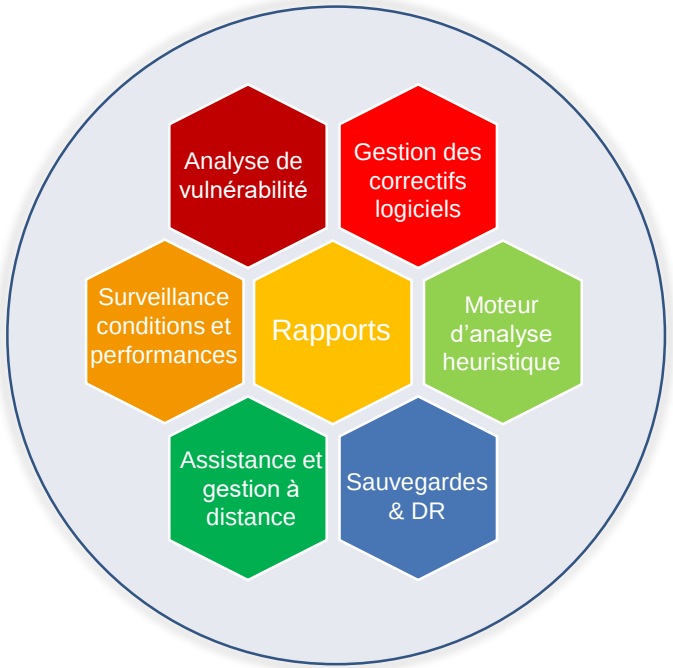
© Acronis 2023

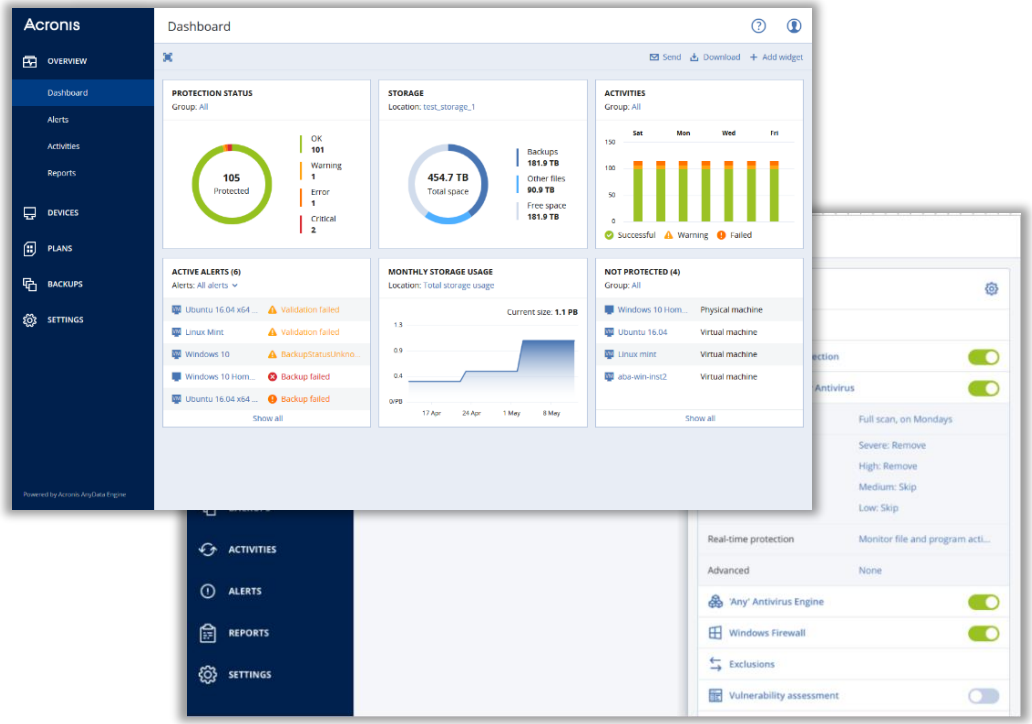
Acronis

#CyberFit

Mieux qu'une offre groupée de plus, une synergie de composants

Approche intégrée de la cyber-protection





© Acronis 2023

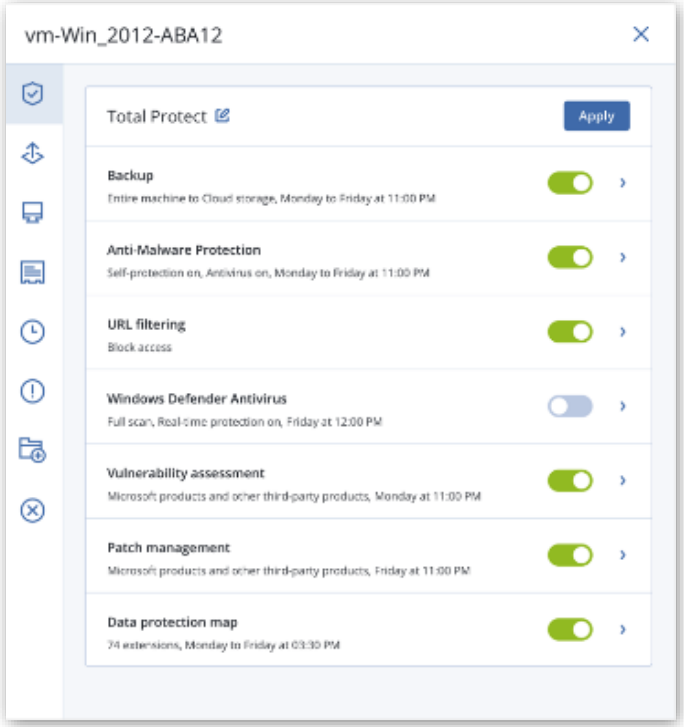
Cinq niveaux d'intégration

Fonctionnalités de cyberprotection exclusives intégrées

Une solution intégrée qui :

- élimine la complexité de l'empilement de solutions
- offre de nouvelles fonctionnalités de sécurité
- Limite et garde les coûts sous contrôle
- améliore la disponibilité

- **Une** formule de licence
- **Une** interface utilisateur
- **Une** console de gestion
- **Un** partage d'informations sur un système protégé
- **Une** source de données



© Acronis 2023

Acronis

#CyberFit

Une synergie de fonctionnalités au sein d’un seul agent

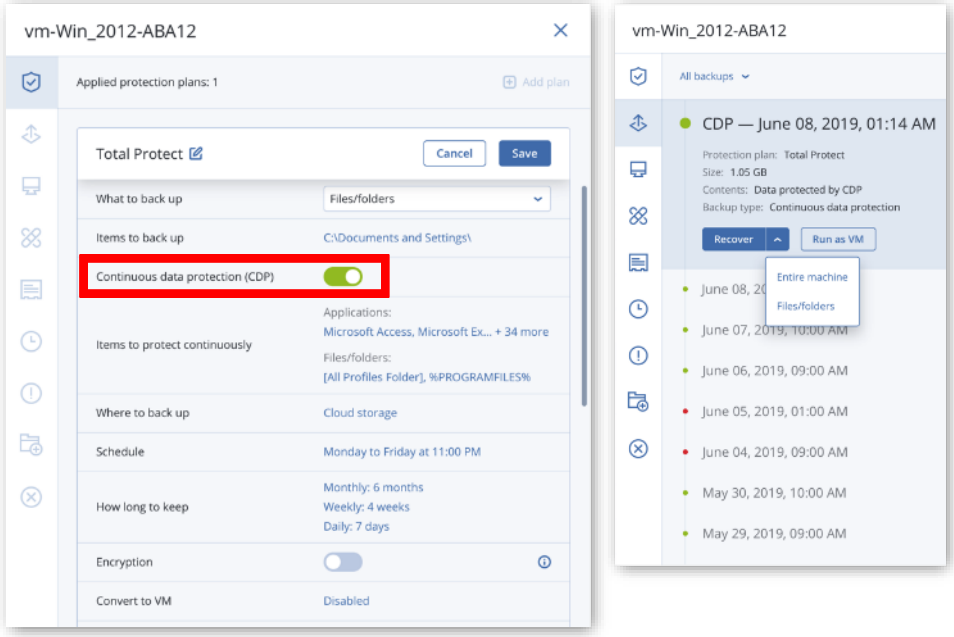
1. Protection continue des données (CDP)

Remédiation fiable et instantanée, sans perte de données, pour un investissement de départ très faible

Établissez, pour chaque équipement, la liste des applications critiques les plus utilisées par vos collaborateurs. L'agent Acronis surveille chaque modification apportée à la liste des applications.

En cas d'infection par malware, vous pourrez restaurer les données à partir de la dernière sauvegarde et appliquer les dernières modifications enregistrées ; vous ne perdrez aucune donnée.

- Permet d'éviter la perte d'un travail en cours.
- Les équipes informatiques contrôlent et sélectionnent les données sauvegardées en continu (documents Microsoft Office, documents financiers, journaux, PDF, etc.).



Pourquoi ? Pour une protection des données client, même entre les sauvegardes

© Acronis 2023

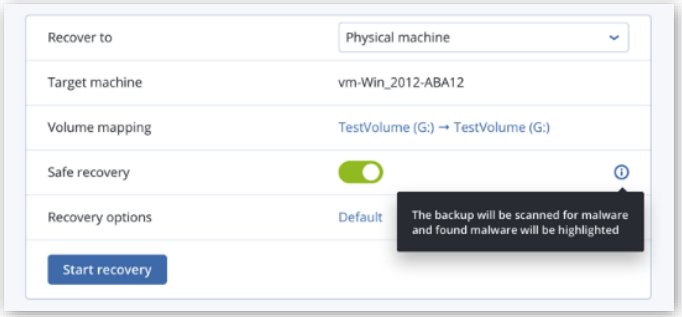
2. Prévention de la récurrence des infections

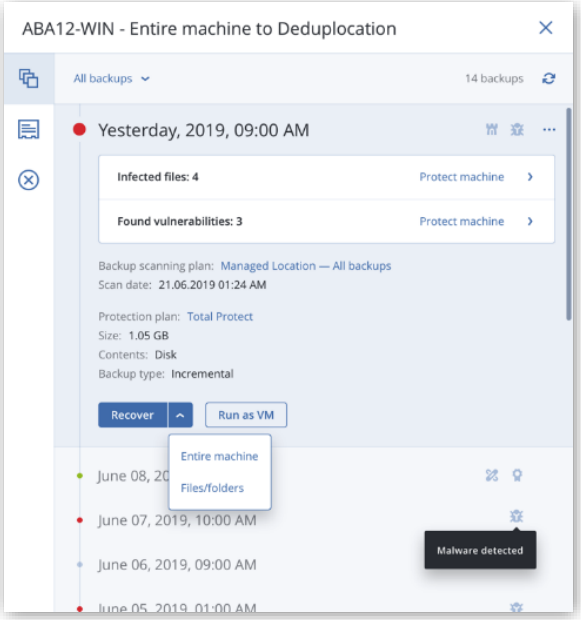
Intégration des mises à jour d'antivirus et de la gestion des correctifs dans le processus de restauration

L'image du système d'exploitation dans la sauvegarde peut présenter des vulnérabilités.

L'application de correctifs et des dernières définitions antimalware à la machine permet de restaurer l'image du système d'exploitation avec les correctifs les plus récents, ce qui réduit le risque de récurrence de l'infection.

- Met à jour la base de données antimalware.
- Installe les correctifs de sécurité les plus récents.





Pourquoi ? Gain de temps, moins d'efforts et protection des données : restauration rapide et aisée des images infectées/vulnérables

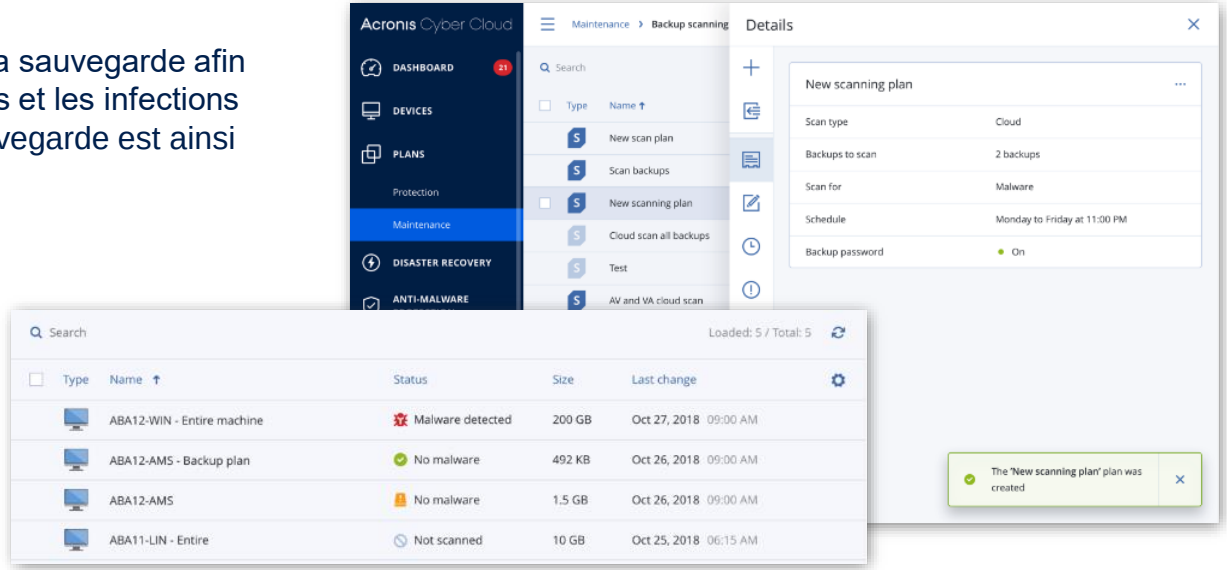
© Acronis 2023

3. Analyse centralisée des malwares

Analyse antimalware et évaluation des vulnérabilités dans les sauvegardes pour une sécurité renforcée

Analyse centralisée de l'ensemble de la sauvegarde afin d'identifier les vulnérabilités potentielles et les infections par malware ; la restauration de la sauvegarde est ainsi garantie sans malware.

- Renforce la capacité de détection des rootkits et des bootkits.
- Restaure uniquement les données saines.
- Réduit la charge sur les terminaux clients.



Pourquoi ? Protection renforcée économe en temps et en ressources : transfert de la charge des terminaux, analyses plus agressives

© Acronis 2023

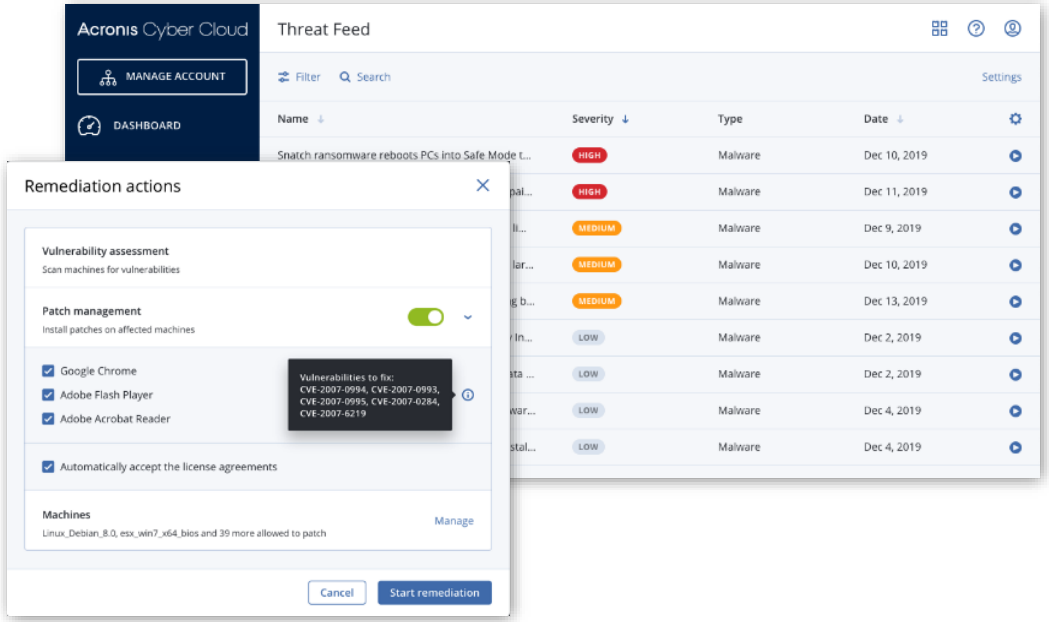
4. Plan de protection intelligent

Utilisation des alertes CPOC Acronis pour réduire le risque posé par les menaces actuelles et futures

Les centres d'opérations de cyberprotection Acronis (CPOC) surveillent le paysage des menaces et diffusent des alertes. Les solutions Acronis ajustent automatiquement les plans de protection en fonction de ces alertes de sécurité : sauvegardes plus fréquentes, analyses antivirus plus approfondies, installations de correctifs spécifiques, etc.

Les plans de protection sont restaurés lors du retour à la normale.

- Minimise les interruptions d'activité en cas de problème (épidémie de malware, catastrophes naturelles, etc.).
- Réduit le délai de réponse.
- Évite la perte de données.



Pourquoi ? Réaction plus rapide, prévention des interruptions et des pertes de données

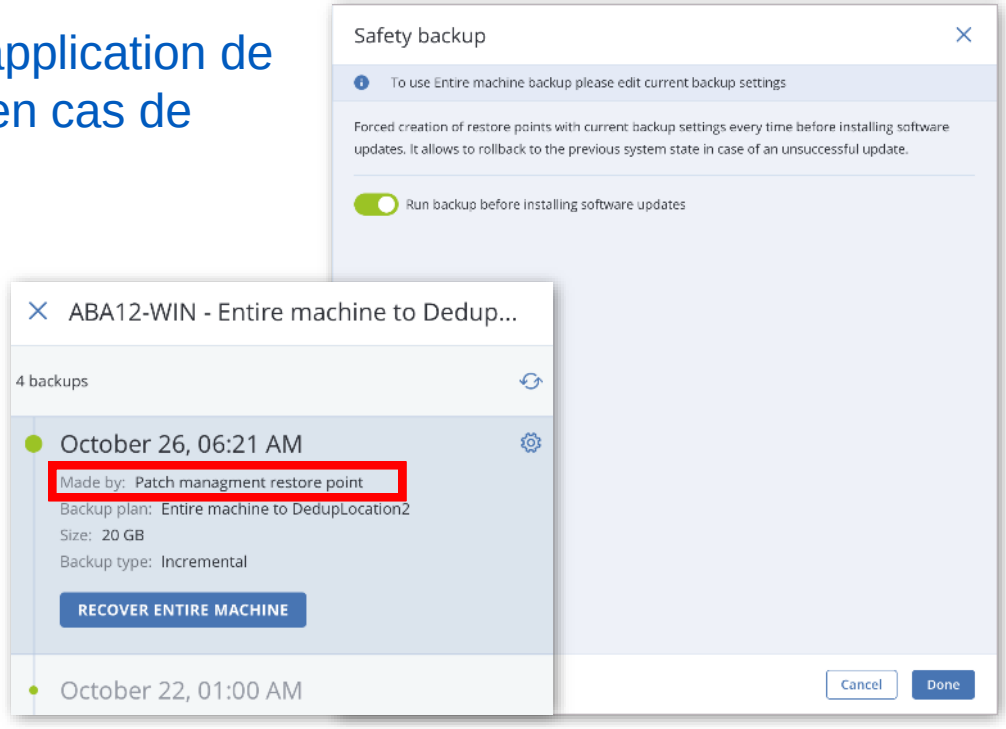
© Acronis 2023

5. Application de correctifs sans risques

Sauvegarde des terminaux avant l'application de correctifs pour assurer une reprise en cas de problème de mise à jour

L'application d'un correctif problématique peut rendre un système inutilisable. Les restaurations de correctifs présentent des limitations et peuvent être lentes. Créez une sauvegarde d'images de machines sélectionnées avant l'installation d'un correctif système ou applicatif.

- Les sauvegardes d'image complète sont le moyen le plus rapide et le plus simple pour revenir à un état utilisable.



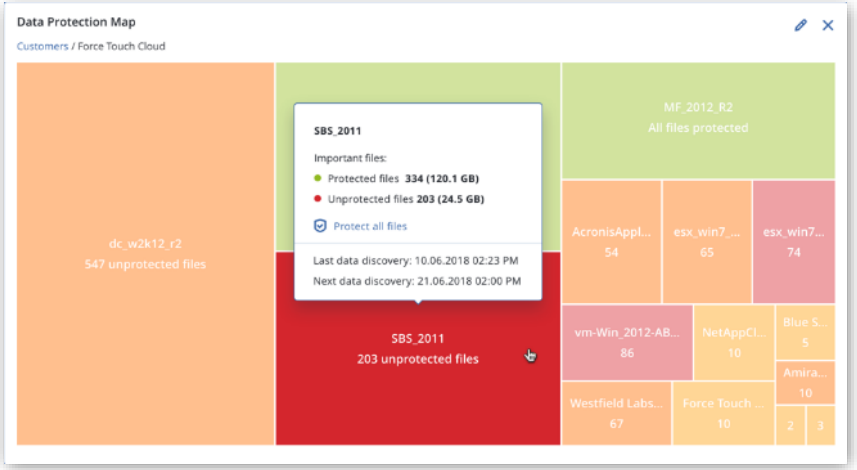
Pourquoi ? Économie de ressources, opérations plus rapides et plus fiables

© Acronis 2023

6. Carte de protection de données

Utilisez la classification automatique des données pour surveiller le statut de protection des fichiers importants. Une alerte indiquant si les fichiers sont ou non sauvegardés est envoyée aux équipes informatiques.

- Bonne visibilité sur la répartition des données entre les différents terminaux.
- Confirmation aisée de la protection de fichiers spécifiques et de l'inclusion dans des plans de sauvegarde.
- Exécution facile des mesures de réduction des risques.
- Génération de rapports de conformité à partir des données collectées.



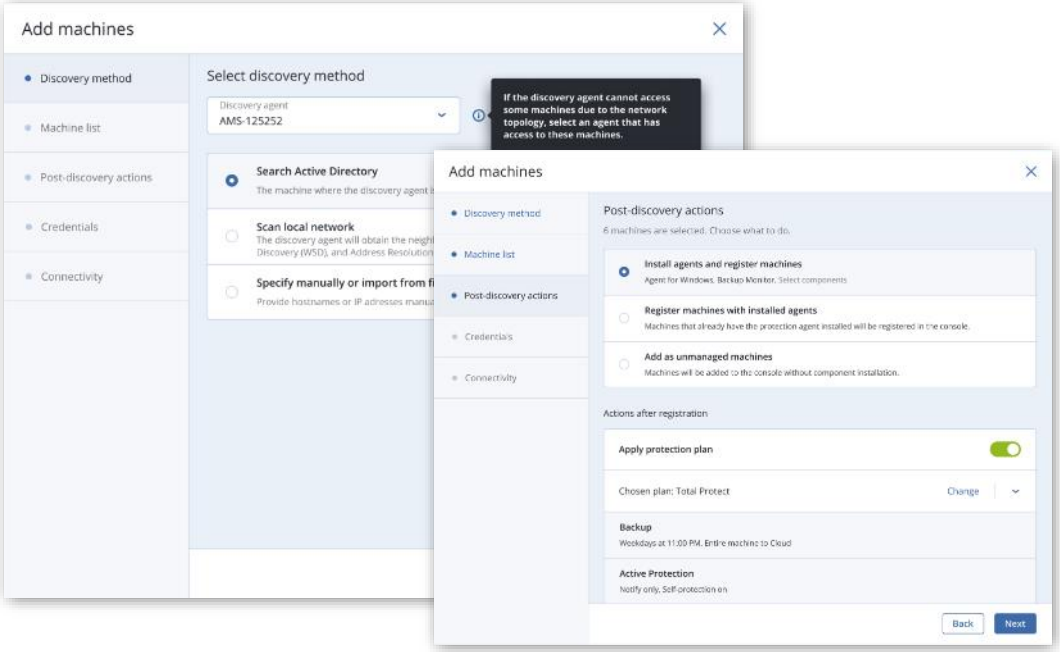
Pourquoi ? Protection complète de toutes les données sans exception, en toute simplicité

© Acronis 2023

7. Détection automatique des équipements et installation à distance des agents

Simplifiez le processus d'installation simultanée de plusieurs agents dans le Cloud et sur site.

- Détection basée sur le réseau
- Détection basée sur Active Directory
- Importation d'une liste d'ordinateurs à partir d'un fichier
- Application automatique du plan de protection
- Assistant permettant une installation d'agents à distance et par lots



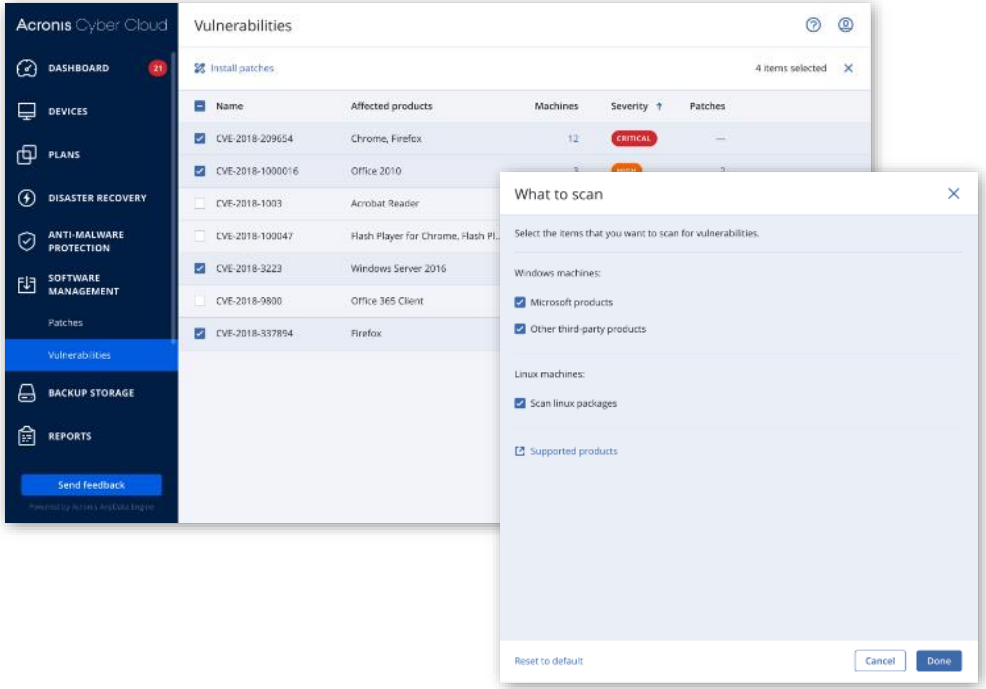
Pourquoi ? Intégration plus facile et rapide, diminution des ressources nécessaires, complétude de la protection

© Acronis 2023

8. Évaluation des vulnérabilités

Identifiez le problème
avant qu'il n'ait un impact.

- Mise à jour ininterrompue de votre base de données de gestion des vulnérabilités et des correctifs
- **Prise en charge :**
  - Microsoft :
    a) Postes de travail : Windows 7 et versions ultérieures
    b) Serveurs : Windows Server 2008 R2 et versions ultérieures
    c) Microsoft Office (2010 et versions ultérieures) et composants associés
    d) .NET Framework et applications serveur
  - Adobe, Oracle Java
  - Navigateurs et autres logiciels
  - Linux : CentOS & RedHat



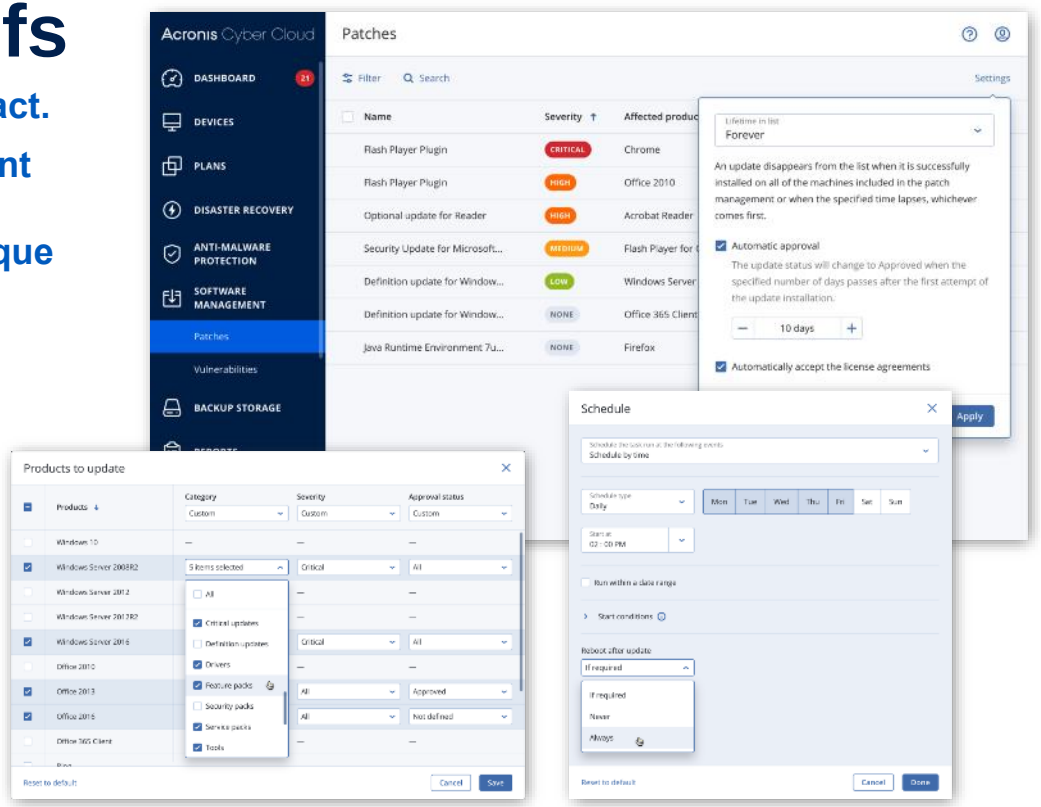
Pourquoi ? Atténuation des menaces potentielles, prévention des attaques

9. Gestion des correctifs

Résolvez le problème avant qu'il n'ait un impact.

La base de données des vulnérabilités contient 12 869 failles et vulnérabilités courantes et s'enrichit de 250 à 300 nouvelles entrées chaque semaine.

- **Approbation automatique** des correctifs
- Déploiement selon un **calendrier**
- Déploiement **manuel**
- Options **flexibles** de redémarrage et de périodes de maintenance
- Déploiement **par étapes**
- **Toutes les mises à jour Windows** y compris les applications Microsoft Office et Windows 10
- **+ 300 produits/applications et 1 437 versions de produits.** (liste des applications tierce ici)



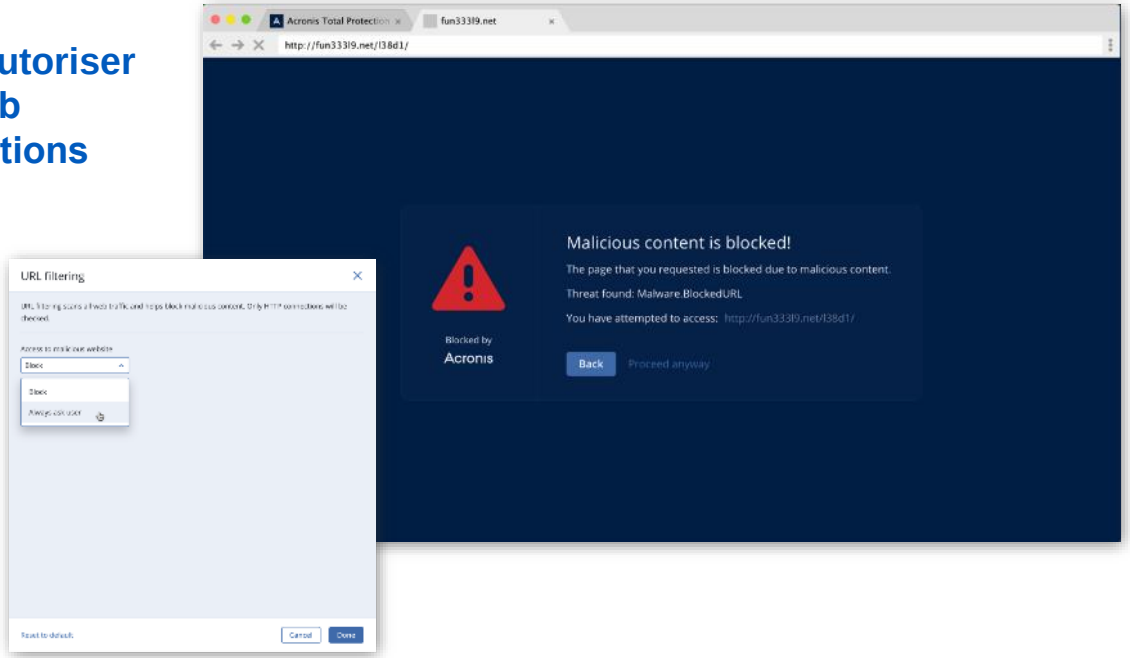
Pourquoi ? Automatisation de protection, atténuation des menaces potentielles, prévention des attaques. (Equifax & WannaCry)

© Acronis 2023

10. Filtrage des URL — Accès contrôlé aux URL malveillantes

Le filtrage des URL vous permet d'autoriser ou de refuser l'accès à des sites Web spécifiques en fonction des informations figurant dans une liste d'URL.

- Base de données tierce
- Intercepteur HTTP/HTTPS interne
- Liste noire/liste blanche d'URL
- Analyse de la charge active des URL malveillantes



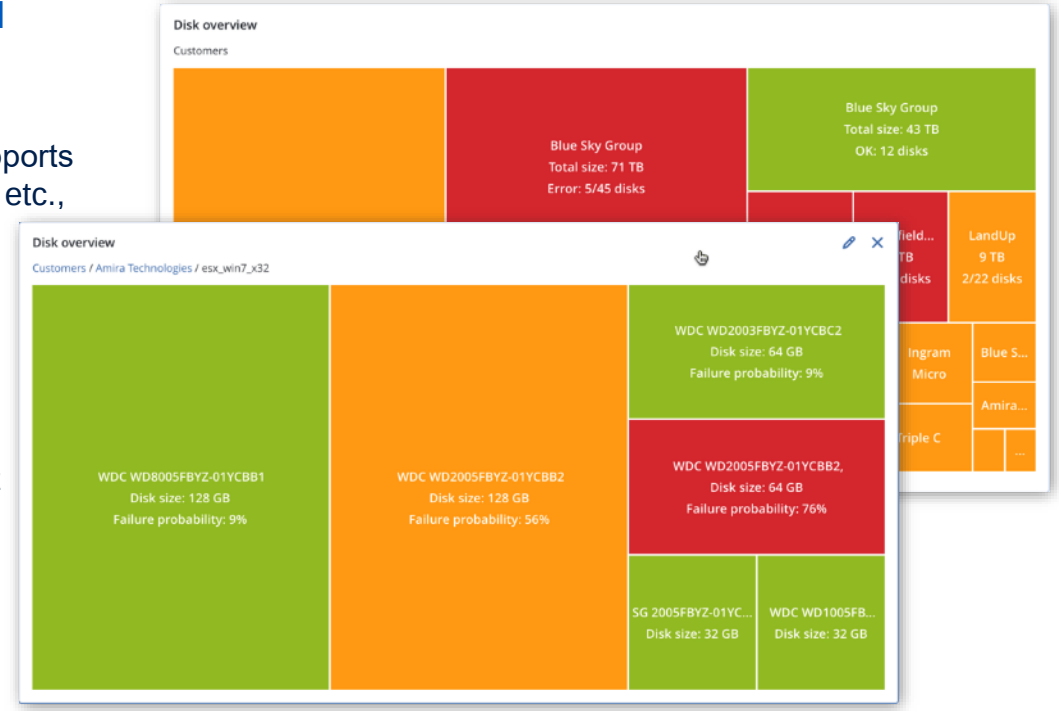
Pourquoi ? Prévention des attaques transmises par des sites Web malveillants/piratés, amélioration de la conformité et de la productivité

© Acronis 2023

11. Surveillance de l'intégrité des disques

Identifiez le problème de disque avant qu'il n'ait un impact.

- Combine modèle d'apprentissage automatique, rapports S.M.A.R.T., taille de disque, fournisseur de disque, etc., pour prédire les défaillances des disques durs.
- Modèle d'apprentissage automatique :
  - Permet de prédire plus de 80 % des défaillances.
  - Les défaillances sont avérées dans 98,5 % des cas (pourcentage en constante augmentation).
- En cas d'alerte concernant un disque, vous pouvez prendre les mesures nécessaires (sauvegarde des fichiers critiques depuis le disque défaillant, p. ex.).

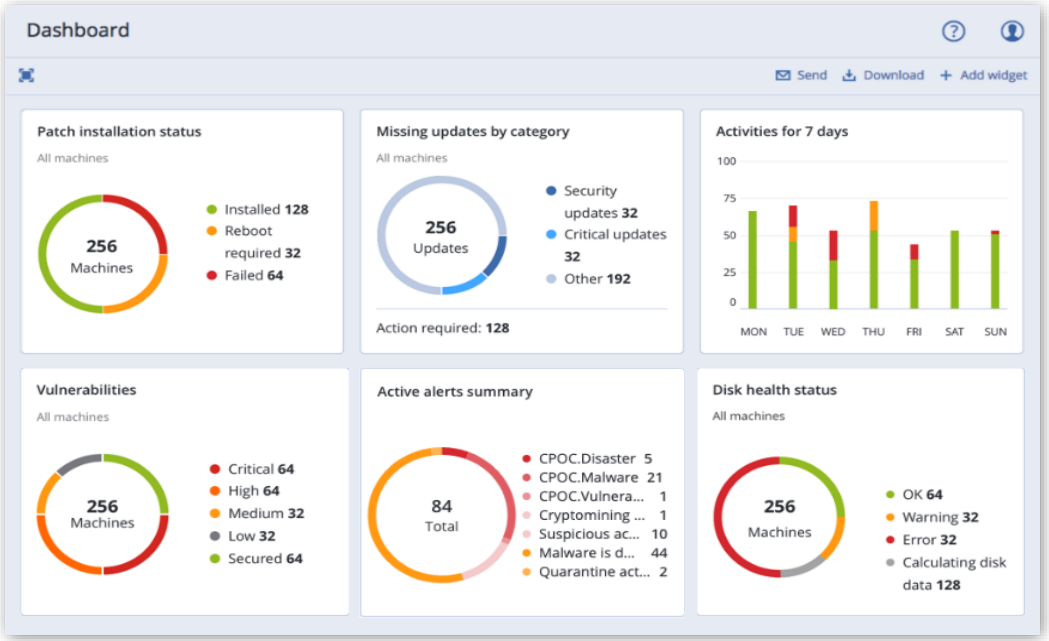


Pourquoi ? Limitation des pertes imprévisibles de données clients, amélioration proactive de la disponibilité, facteur de différenciation

© Acronis 2023

12. Flexibilité de la surveillance et de la production de rapports

- Surveillance de l'intégrité du matériel (disques durs, disques SSD)
- Contrôle actif par alertes
- Contrôle des mises à jour manquantes
- Widgets de tableaux de bord personnalisables
- Identification rapide des problèmes
- Accès rapide aux actions de gestion



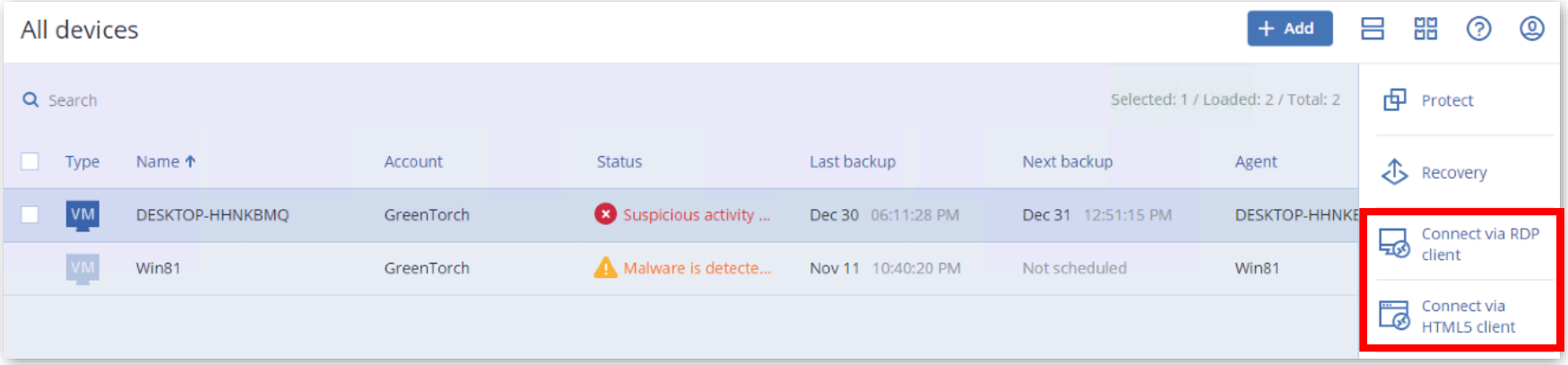
Pourquoi ? Console unique, opérations accélérées, démonstration de la valeur du fournisseur MSP et simplification des renouvellements

© Acronis 2023

13. Bureau à distance

Pilotez à distance n'importe quel terminal comme si vous étiez sur site.

- Permet de porter assistance un utilisateur distant et de gagner un temps considérable.
- Permet d'accéder à des systèmes se trouvant sur un réseau privé. Aucun changement de paramètres de pare-feu et aucune mise en place de tunnels VPN supplémentaires. Les connexions sortantes (port 443) sont utilisées.



Pourquoi ? Moins d'outils, connexion plus facile, meilleure réactivité

© Acronis 2023

PRA : Restauration locale et dans le cloud

Basculement hors site instantané vers le site de restauration cloud d'Acronis

En cas de panne du site tout entier, vous pouvez basculer les ressources de production vers les machines du centre de données cloud d'Acronis en quelques minutes, et ainsi permettre à votre entreprise de reprendre rapidement ses activités.

Restauration sur site avec Acronis Instant Restore

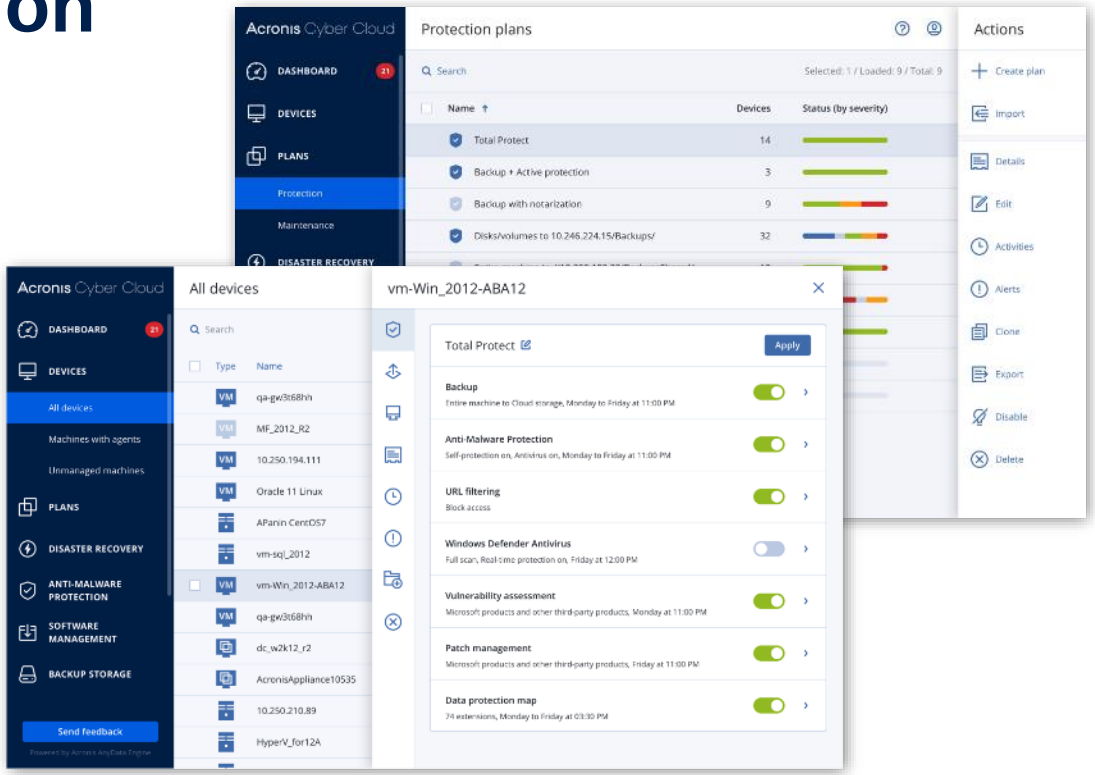
En cas de panne d'un serveur unique, vous pouvez restaurer la machine localement en exécutant les sauvegardes de systèmes Windows ou Linux, physiques ou virtuels, en tant que machines virtuelles VMware.

© Acronis 2023

Un plan de protection unique

Couvre tous les aspects de la cyberprotection :

- Sauvegarde
- Protection antimalware
- Filtrage des URL
- Gestion de l'antivirus Windows Defender
- Évaluation des vulnérabilités
- Gestion des correctifs
- Découverte des données (carte de protection de données)



Pourquoi ? Protection renforcée et plus efficace, automatisée

© Acronis 2023

Plus que du Backup ? Upgradez vers Acronis Cyber Protect

La protection la plus sûre, la plus facile et la plus fiable pour les entreprises

Proactive Protection

- **Evaluation des vulnérabilités** et **gestion des correctifs** pour éviter les temps d'arrêt et la maintenance
- Suppression des logiciels malveillants des sauvegardes
- **Prévention des infections récurrentes** (patch sur la restauration)

Active Protection

- Protection continue des données (**CDP**) pour éviter toute perte de données
- **Protection active contre les logiciels de rançon** et autres logiciels malveillants pour éviter les temps d'arrêt
- **Autodéfense de l'agent** et des stockages de sauvegarde

Reactive Protection

- Capacité de récupération intégrée en cas de catastrophe (**PRA**)
- **Récupération instantanée** : pas de perte de données, RTO et RPO proches de zéro
- **Stockage de métadonnées pour investigations** et les enquêtes sur incidents

Améliorations de la productivité

- Un nombre maximum de charges de travail protégées
- Gestion intégrée à distance pour un accès rapide
- Plans de protection préconfigurés pour les travailleurs à distance

© Acronis 2023

Acronis

#CyberFit

Reconnaissance de l'industrie de la sécurité

Participation aux groupes de lutte contre les malveillances informatique

Reconnaissance de l'industrie de la sécurité d'Acronis

MVI member	VIRUSTOTAL member	Cloud Security Alliance member
Anti-Malware Testing Standard Organization member	Anti-Phishing Working Group member	MRG-Effitas participant and test winner
Anti-Malware Test Lab participant and test winner	ICSA Labs certified	NioGuard Security Lab participant and test winner
AV-Comparatives approved business security product	VB100 certified	AV-Test participant and test winner

© Acronis 2023

Leader selon des tests indépendants

Décembre 2022 : AV-Comparatives nomme Acronis Cyber Protect Cloud **"produit de sécurité professionnel approuvé".** https://www.av-comparatives.org/tests/business-security-test-2022-august-november/#factsheet

Novembre 2022 : Acronis obtient **le badge VB100** dans les tests de Virus Bulletin
https://www.virusbulletin.com/uploads/vb100/test-reports/vb100-test-report-2022-11-21-acronis-cyber-protect.pdf

Décembre 2022: AV-TEST certifie Acronis Cyber Protect pour la **protection des points de terminaison sous MacOS** https://www.av-test.org/en/antivirus/business-macos/macos-monterey/september-2022/acronis-cyber-protect-15.0-226301/

Novembre 2022 : Acronis Cyber Protect Cloud **certifié comme solution anti-malware** par ICSA Labs https://www.icsalabs.com/sites/default/files/2022_11_testing_report.html

Juin 2022 : Acronis Cyber Protect Cloud advanced email security **certifié Enterprise et SMB Email security service** par SE Labs

Liens vers les différentes sources : https://www.acronis.com/en-us/blog/posts/acronis-earns-security-accolades-in-independent-evaluations/

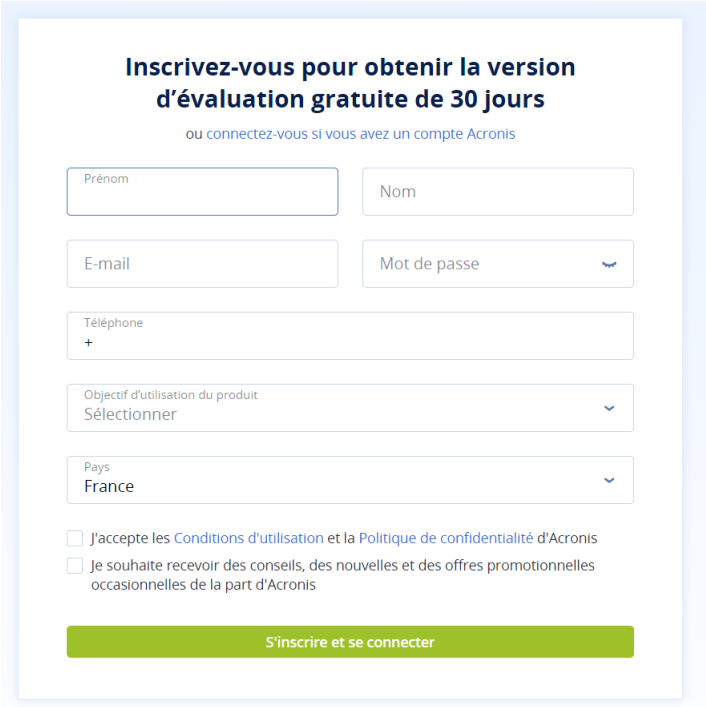
© Acronis 2023

Acronis Cyber Protect 15

Essayez gratuitement et sans limitations de fonctionnalités

Version d’évaluation 30 jours

https://www.acronis.com/fr-fr/business/cyber-protect/trial/#/registration



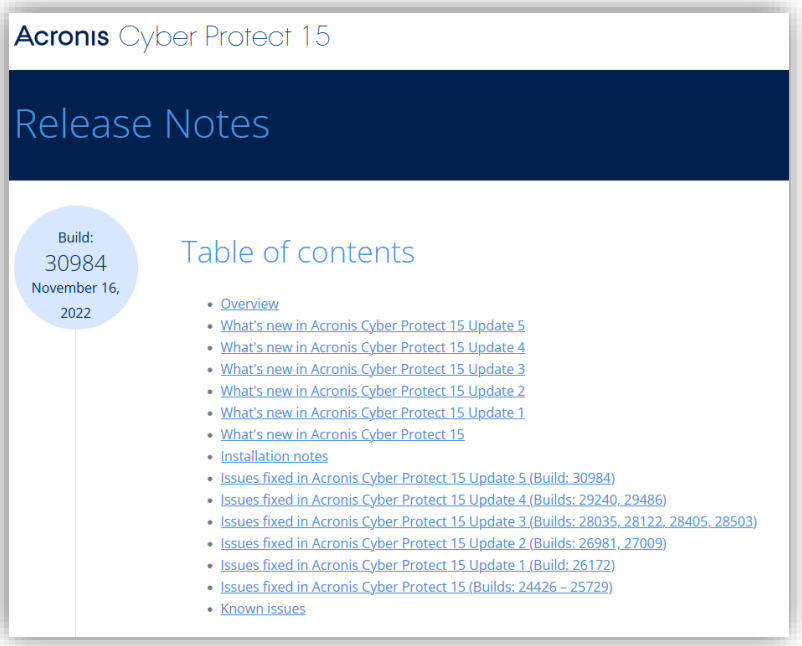
© Acronis 2023

Acronis Cyber Protect 15

Update 5 – What's new

What's new ?

https://dl.managed-protection.com/u/cyberprotect/rn/15/user/en-US/AcronisCyberProtect15_relnotes.htm



© Acronis 2023

Acronis

#CyberFit

Acronis

Questions ?

Maxime Clay

Senior Solution Engineer
Acronis

#CyberFit

Acronis

Merci de votre participation!

Maxime Clay

Senior Solution Engineer
Acronis

#CyberFit

Acronis

Cyber Foundation

Program

Transforming lives through education

Let’s work together to create new knowledge, putting our diverse experiences and strengths towards a brighter future!

Join us!