

Date de publication :

25 février 2025

Auteur(s) :

Hollie Hennessy, Analyste principale

On the Radar : les solutions de sauvegarde et de restauration Acronis assurent une cybersécurité plus résiliente des systèmes OT

Résumé

Introduction

L'offre d'Acronis pour les technologies opérationnelles (OT) se concentre sur le volet « restauration des données » d'une stratégie de cybersécurité. Elle fournit des fonctions de sauvegarde, de restauration et de sécurité des données pour les environnements OT, afin d'améliorer la résilience de la cybersécurité. Le large réseau des partenaires et des canaux de distribution d'Acronis renforce également sa réputation dans le domaine de la sécurité des systèmes OT.

Analyse Omdia

La sécurité des systèmes OT vise plusieurs objectifs, dont la reprise des activités en cas d'incident ou d'attaque. Dans les environnements opérationnels et ceux des infrastructures critiques, peut-être même plus que dans certains environnements informatiques, la continuité des activités est essentielle, compte tenu des exigences réglementaires imposées, ainsi que des conséquences financières souvent importantes ou des dommages potentiels causés par les interruptions d'activité.

Tout environnement doit donc disposer d'un plan de sauvegarde et de restauration efficace, testé et éprouvé. Même avec la meilleure protection, une attaque peut toujours se produire. Toute stratégie de cybersécurité doit donc impérativement prévoir ce qu'il convient de faire en cas d'incident et comment rétablir le bon fonctionnement des systèmes dans les plus brefs délais. Les sauvegardes régulières sont essentielles, tout comme un processus rapide et efficace de restauration des données exfiltrées.

L'offre de sauvegarde et de restauration d'Acronis s'adresse en priorité à des partenaires et distributeurs. Elle permet aux fournisseurs de services et éditeurs de solutions pour l'industrie d'intégrer des fonctions de sauvegarde et restauration dans leurs services et plates-formes. L'offre peut aussi être vendue en tant que telle à des entreprises dotées d'environnements OT.

Pourquoi vous intéresser à Acronis ?

Acronis a conclu des partenariats avec des équipementiers OEM et sa solution de sauvegarde et restauration est adoptée par un grand nombre de leaders de l'automatisation industrielle dans les secteurs de la fabrication, de la santé et de l'énergie. La solution aide à garantir la conformité aux exigences réglementaires (par exemple, la directive NIS2) et aux normes (comme ISA/IEC 62443). Elle peut aussi améliorer l'offre des fournisseurs de solutions d'automatisation industrielle qui pourront proposer un service plus robuste et fiable à leurs clients. Grâce à son expertise de la sauvegarde et de la restauration, Acronis a pu développer une solution qui répond aux besoins des environnements industriels, y compris ceux qui utilisent encore d'anciens systèmes.

Contexte du marché

Le marché de la sécurité des systèmes OT est dominé par la gestion des ressources, la surveillance, la détection et la réponse, aspects que les plus grands fournisseurs du secteur proposent intégralement ou partiellement. Toutefois, pour répondre aux exigences réglementaires et aux besoins des entreprises industrielles et des environnements OT, des fonctionnalités supplémentaires s'imposent.

La continuité des activités dans ces environnements (pour des raisons opérationnelles, financières ou de sécurité) est donc d'une importance capitale. Il faut impérativement pouvoir détecter les violations ou les attaques, et prévenir les menaces connues. Ainsi, de nouvelles fonctionnalités ont émergé pour répondre à ces besoins, qu'il s'agisse d'automatisation préventive ou d'approches plus proactives, telles que la gestion des risques et des vulnérabilités, la simulation des attaques et des violations, ou la gestion de la surface d'attaque.

Mais comme aucun système n'est infaillible, il est nécessaire de pouvoir restaurer les données après un incident. Ce segment du marché traite la résilience de la cybersécurité, avec des outils et des services d'intervention sur incidents, d'investigation numérique, et de restauration des données et des systèmes. À cet égard, les solutions Acronis sont particulièrement bien adaptées aux besoins des environnements OT.

Le cadre de cybersécurité NIST (CSF) 2.0 est une référence fiable quant aux exigences de cybersécurité de toutes les organisations, plus ou moins critiques. Initialement axé sur les infrastructures critiques, ce cadre est largement adopté et référencé, bien que son champ d'application se soit élargi. La version mise à jour du framework couvre de multiples fonctionnalités :

- Identifier
- Protéger

- Détecter
- Répondre
- Restaurer
- Et sa dernière fonction : Gouverner

Présentation de la solution/du service

Les fonctionnalités Acronis de protection des données couvrent largement deux domaines : la sauvegarde et la reprise après sinistre, via la plate-forme Acronis Cyber Protect. Les fonctionnalités suivantes sont proposées :

- Sauvegarde d'image complète d'un système en cours d'exécution, avec patching à sécurité intégrée qui crée une sauvegarde d'image avant l'application des correctifs
- Restauration en un clic en libre-service
- Universal Restore pour une restauration vers n'importe quel matériel ou hyperviseur
- Instant Restore permettant le démarrage et l'exécution en cours de reprise
- Sécurité renforcée grâce à des sauvegardes immuables
- Prise en charge de Windows, Linux et d'autres systèmes d'exploitation/applications, y compris d'anciennes versions comme Windows XP, toujours utilisées dans les environnements industriels.
- Scans anti-malware et mise à jour d'antivirus automatisés dans le cadre du processus de restauration
- Service de reprise d'activité après sinistre entièrement intégré

Conçu pour les environnements OT, Acronis Cyber Protect procède à l'installation et aux sauvegardes sans qu'il faille arrêter ni redémarrer les systèmes. De plus, l'offre Acronis propose la restauration sur un nouveau matériel si nécessaire. Ceci se fait par l'intermédiaire de l'agent Acronis Cyber Protect, qui peut être installé avec ou sans composant anti-malware, en fonction des contraintes et des exigences du client.

La fonction de restauration en un clic permet à des utilisateurs non spécialistes en informatique ou en sécurité de remettre les systèmes en service, sans qu'ils aient besoin de compétences techniques particulières. C'est d'autant plus important dans les environnements distants et distribués, tels que les plates-formes pétrolières en mer, où l'accessibilité sur site peut être difficile, ainsi que quand le temps est compté, pour relancer une chaîne de production par exemple. Il est également possible de restaurer en redémarrant à partir d'une sauvegarde de disque locale ou du cloud Acronis. De plus, les données sauvegardées sont automatiquement analysées à la recherche de malwares avec la dernière version de l'antivirus.

Les informations et les données de contrôle sont agrégées dans un tableau de bord centralisé appelé Centralized Acronis Monitoring Hub, aux fins d'analyse des métadonnées et d'intégration avec des logiciels tiers.

Informations sur l'entreprise

Contexte

Fondée à Singapour en 2003 et enregistrée en Suisse en 2008, Acronis compte à présent plus de 1 800 employés dans 45 pays. L'éditeur sert plus de 750 000 clients professionnels dans 150 pays.

La société a connu une croissance significative ces dernières années en s'appuyant sur son expertise de la protection des données pour proposer une large gamme de solutions de cybersécurité à ses partenaires et clients. Acronis est également précurseur du concept de fusion des deux domaines avec sa plate-forme Acronis Cyber Protect.

L'entreprise accorde une grande importance à la recherche et au développement, avec Acronis Labs, qui emploie plus de 500 ingénieurs, dont plus de 20 titulaires d'un doctorat. Plus de 200 brevets ont été déposés au cours de ses 17 années d'existence. L'unité Acronis Threat Research Unit (TRU) publie également régulièrement ses résultats d'analyses des cybermenaces, qu'elles soient déjà bien connues ou apparues récemment.

En août 2024, il a été annoncé qu'EQT, une société de capital-investissement européenne, allait acquérir une participation majoritaire dans Acronis, pour une valorisation estimée à 4 milliards de dollars. Cette transaction devrait être finalisée au premier ou au deuxième trimestre 2025. Auparavant, Acronis avait levé plus de 500 millions de dollars auprès d'investisseurs tels que CVC Capital Partenaires, BlackRock et Goldman Sachs.

Position actuelle

Acronis propose une gamme de technologies de cybersécurité au-delà de la sauvegarde et de la restauration des environnements OT, avec notamment sa nouvelle solution Extended Detection and Response (XDR) et son assistant d'intelligence artificielle (AI) générative. L'offre Acronis couvre largement les éléments suivants :

- Protection des données (voir ci-dessus)
- Cybersécurité (sécurité des terminaux, prévention des malwares, EDR/XDR, etc.)
- Gestion des terminaux (gestion des correctifs, gestion des vulnérabilités, accès distant, etc.)

Si une partie des activités d'Acronis porte sur la vente directe à l'utilisateur final, l'entreprise privilégie surtout les partenaires, à savoir les revendeurs, fournisseurs de services managés (MSP) et OEM. Dans le domaine de l'automatisation industrielle, on retrouve notamment ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation et Yokogawa.

Acronis propose une version freemium de sa plate-forme, les fonctionnalités plus avancées étant facturées à l'utilisation.

En projet

Bien qu'Acronis envisage de développer sa plate-forme d'intelligence artificielle pour proposer des fonctionnalités de cybersécurité supplémentaires, l'éditeur n'a pas prévu de couvrir l'IoT ni l'OT.

Données principales

Tableau 1 : Fiche solution : Acronis

Nom du produit	Acronis Cyber Protect	Classification des solutions	Protection des terminaux et sauvegarde/restauration
Numéro de version	v16	Date de publication	Février 2024
Secteurs couverts	Fabrication Santé Recherche en labo (ou biopharmaceutique) Pétrole/gaz Production d'énergie/Énergie Logistique Automobile Vente au détail Éducation/gouvernement Construction	Zones géographiques couvertes	Amérique du Nord Amérique latine et du Sud EMEA APAC
Taille des entreprises cibles	Entreprise, PME, TPE	Formules de licence	Licences perpétuelles ou abonnement
URL	www.acronis.com https://www.acronis.com/en-us/products/cyber-protect-enterprise/	Circuit(s) de distribution	Direct
Siège social	Schaffhausen, Suisse	Nombre de collaborateurs	+ ou - 2 000

Source : Omdia

Commentaire de l'analyste

Les nombreuses innovations d'Acronis et sa spécialisation dans le domaine de la protection et de la restauration des données donnent lieu à une offre très attractive pour les environnements industriels. De multiples options de déploiement, de sauvegarde et de restauration permettent de répondre aux besoins spécifiques de chaque client. Nombre de fournisseurs de solutions de sécurité OT avec lesquels les fournisseurs de services ou les éditeurs de solutions d'automatisation industrielle pourraient nouer un partenariat ne proposent pas de fonctionnalités de restauration de données, ce qui représente une opportunité de taille pour Acronis. Les concurrents d'Acronis dans le domaine de la restauration de données ont plutôt tendance à se concentrer sur la partie informatique. Ils ne peuvent pas non plus rivaliser avec la

spécialisation d'Acronis dans les environnements industriels, ni avec la réputation qu'Acronis a acquise grâce à son intégration étroite et ses partenariats avec les plus grands OEM industriels.

Ceci dit, l'offre d'Acronis pour ses partenaires est la plate-forme la plus étendue, qui ne répond pas aux exigences de sécurité OT au-delà de la fonction de restauration, sans perspectives futures en ce sens. Ses partenaires MSP/fournisseurs de services de sécurité managés (MSSP) privilégient la fourniture de services informatiques aux utilisateurs finaux. De plus, l'entrée dans l'espace IoT/OT avec une solution de sécurité des opérations nécessiterait probablement un développement important, étant donné les comportements des terminaux et les protocoles propriétaires. La plate-forme permettrait aux partenaires de proposer des fonctionnalités de sécurité informatique essentielles, mais il est probable qu'ils se tournent vers d'autres fournisseurs de sécurité OT pour les besoins de détection, de prévention et de visibilité de leurs clients industriels. Bien que les leaders de la sécurité OT ne se concentrent pas actuellement sur la protection et la restauration des données, l'occasion leur est donnée de combler ce manque et de créer un environnement plus concurrentiel.

Annexe

On the Radar

On the Radar est une série de notes de recherche consacrées aux fournisseurs qui apportent des idées neuves, des solutions innovantes ou des modèles économiques attractifs sur leur marché. Les fournisseurs On the Radar méritent d'être suivis pour leur impact potentiel sur les marchés, mais aussi pour leur approche, leurs récents développements ou leur stratégie pouvant s'avérer disruptifs et intéressants pour les acheteurs et utilisateurs de technologies.

Pour aller plus loin

[*Omdia Market Radar: OT Cybersecurity Platforms, 2025*](#) (Janvier 2025)

[*2025 Trends to Watch: IoT Cybersecurity*](#) (septembre 2024)

« [*Xage Sécurité annonce un nouveau partenariat avec Armis et Yokogawa Engineering Asia pour fournir un accès distant sécurisé*](#) » (septembre 2024)

[*Omdia Secure Industrial Networks Survey 2023: Overall Findings*](#) (décembre 2023)

Autrice

Hollie Hennessy, analyste principale, cybersécurité IoT

askananalyst@omdia.com

Droit de citation

Pour demander l'autorisation de citer et d'utiliser les recherches et les données Omdia, contactez Omdia à l'adresse citations@omdia.com.

Omdia Consulting

Nous espérons que cette analyse vous aidera à prendre des décisions stratégiques éclairées et inspirantes pour votre entreprise. Si vous avez d'autres besoins, l'équipe de consultants d'Omdia peut vous aider. Pour plus d'information à ce sujet, contactez-nous directement à l'adresse consulting@omdia.com.

Copyright et clause de non-responsabilité

Les recherches, données et informations d'Omdia mentionnées dans le présent document (les « Documents Omdia ») appartiennent à TechTarget, Inc., ses filiales ou sociétés affiliées (collectivement « Informa TechTarget ») ou ses fournisseurs de données tiers et sont protégées par le droit d'auteur. Les données, recherches, opinions ou points de vue publiés par Informa TechTarget ne doivent pas être interprétés comme des faits.

Les Documents Omdia reflètent les informations et les opinions à la date de leur publication initiale et non à la date du présent document. Les informations et opinions exprimées dans les Documents Omdia sont susceptibles d'être modifiées sans préavis, en conséquence de quoi Informa TechTarget décline toute obligation ou responsabilité de mettre à jour les Documents Omdia ou la présente publication.

Les Documents Omdia sont fournis en l'état et en fonction de leur disponibilité. Aucune déclaration ou garantie, expresse ou implicite, n'est formulée quant à l'équité, la précision, l'exhaustivité ou l'exactitude des informations, opinions et conclusions contenues dans les Documents Omdia.

Dans les limites prévues par la loi en vigueur, Informa TechTarget et ses sociétés affiliées, dirigeants, administrateurs, collaborateurs, agents et fournisseurs de données tiers déclinent toute responsabilité (y compris, sans limitation, toute responsabilité découlant d'une faute ou d'une négligence) quant à l'exactitude, l'exhaustivité ou l'utilisation des Documents Omdia. En aucun cas, Informa TechTarget ne pourra être tenu pour responsable des décisions commerciales, d'investissement ou autres prises ou fondées sur les Documents Omdia.

CONTACTEZ-NOUS

omdia.com

askananalyst@omdia.com