Acronis
Cyber Protect pour le secteur du pétrole, du gaz, de l'électricité et de l'énergie

Une cyberrésilience sur mesure pour les opérations industrielles critiques

Résumé

Les secteurs du pétrole et du gaz, de l'électricité et de l'énergie dépendent de systèmes de technologie opérationnelle (OT) basés sur PC pour produire, transporter, stocker et distribuer l'énergie en toute sécurité. Ces environnements sont soumis à des contraintes spécifiques : systèmes traditionnels à long cycle de vie, sites à connectivité restreinte et faible tolérance à l'interruption d'activité. Parallèlement, le ransomware cible de plus en plus l'OT.

Acronis Cyber Protect for OT offre d'emblée une sauvegarde sécurisée, une restauration rapide et une résilience opérationnelle des systèmes OT sans perturber la production. La solution aide les organisations à restaurer des états validés du système, à réduire le temps de restauration et à honorer les exigences courantes de restauration et d'audit des normes industrielles de cybersécurité.

Approuvé par les fournisseurs d'automatisation

YOKOGAWA · Honeywell · GE VERNOVA · ABB · EMERSON

Pourquoi choisir Acronis pour les secteurs de l'électricité et de l'énergie, ainsi que du pétrole et du gaz ?

- Faible encombrement de l'agent
- Fonctionnement hors ligne / isolé du réseau
- Rapidité de restauration sur système nu
- Validation de sauvegarde / analyse anti-malware
- Restauration en un clic
- Prise en charge des systèmes d'exploitation traditionnels
- Universal Restore
- Stockage immuable + réplication + chiffrement

Acronis Cyber Protect for OT a été spécifiquement pensé autour des priorités de l'OT : disponibilité, simplicité, restauration, prévention, réalité des environnements existants et mixtes, et workflows de restauration pilotés par les opérateurs pour des environnements distants et contraints.

Valeur pour l'entreprise

Valeur opérationnelle :

- Réduire le délai moyen de restauration (MTTR) des systèmes OT critiques.
- Maintenir la continuité de la production.
- Réduire les risques en restaurant des états validés du système.

Réduction des risques et protection de la marque :

- Réduire la probabilité de restaurations non sûres ou compromises.
- Démontrer la cyberrésilience et l'état de préparation à la restauration auprès de la gouvernance interne, des partenaires et des autorités de régulation.

Impact sur le coût total de possession (TCO) :

- Réduire les dépenses d'exploitation (OPEX) en minimisant les interruptions d'activité et en simplifiant la restauration des systèmes OT critiques.
- Optimiser les dépenses d'investissement (CAPEX) en prolongeant le cycle de vie des ressources existantes et en permettant la restauration sur du matériel de remplacement.

Valeur pour les OEM et les partenaires :

- Intégrer la résilience aux systèmes livrés.
- Réduire la charge de support post-déploiement.
- Permettre des revenus récurrents grâce à des services de résilience et d'accompagnement du cycle de vie.

Secteurs couverts

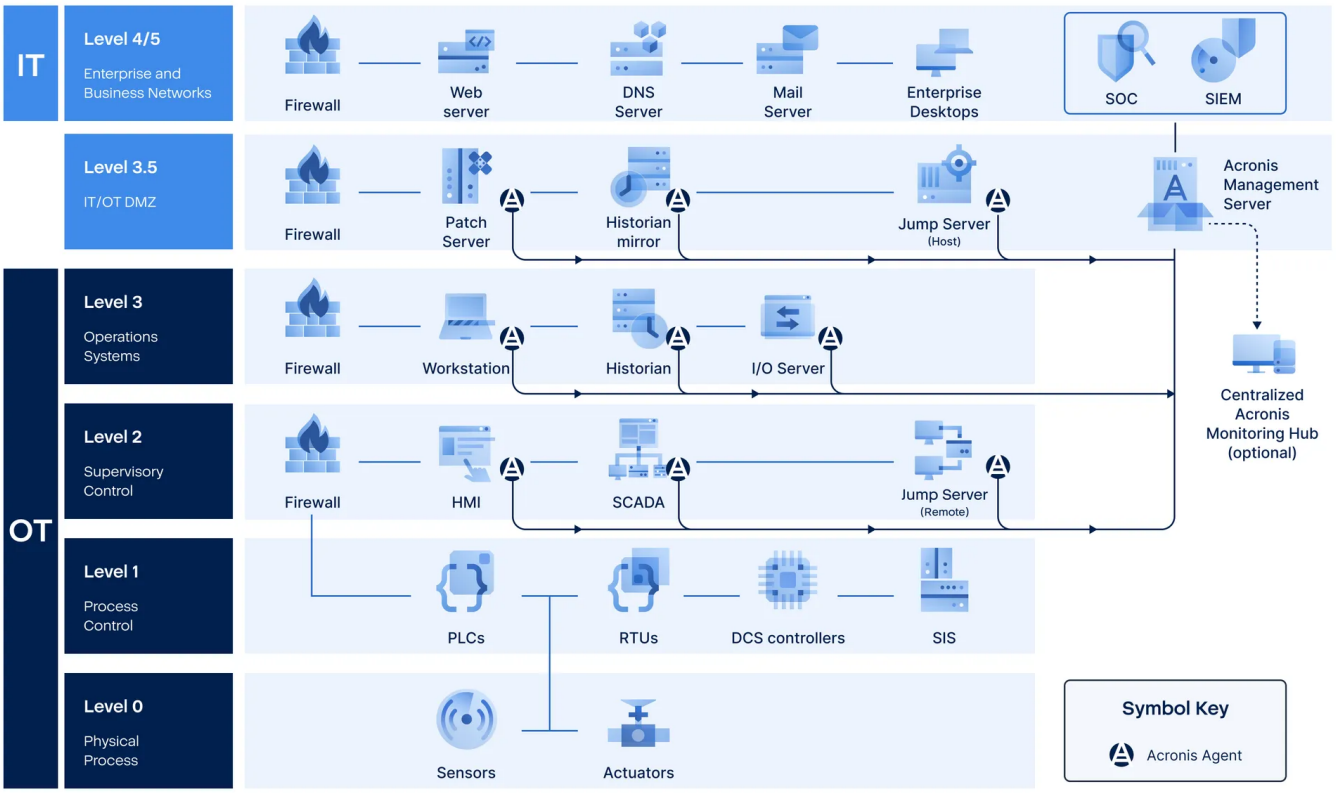
Électricité et énergie :		
Production d'électricité (thermique, nucléaire, hydroélectrique, éolienne, solaire, biomasse et valorisation énergétique des déchets).	Transport et distribution (réseaux de transport, y compris les systèmes HVDC, postes électriques, réseaux de distribution).	Périphérie du réseau et énergie distribuée (ressources énergétiques distribuées (DER), micro-réseaux, BESS).
Pétrole et gaz :		
Amont (exploration, forage, production offshore / onshore, production de gaz naturel et traitement sur site).	Intermédiaire (compression et transport du gaz, transport par pipeline, terminaux de stockage, liquéfaction et expédition de GNL).	Aval (raffinage, production pétrochimique et chimique, conversion du gaz naturel en carburant liquide GTL (gas-to-liquids), regazéification du GNL).

Défis opérationnels des environnements OT de l'énergie, du pétrole et du gaz

Difficultés	Pourquoi est-ce important ?
Coût élevé de l'interruption d'activité	Les pannes peuvent entraîner des risques pour la sécurité, des pertes de production, des perturbations de service et une exposition réglementaire. Une restauration rapide est critique.
Défis de cybersécurité	Les ransomwares et les cyberattaques ciblées menacent de plus en plus les systèmes SCADA, HMI, d'historisation, les postes de travail d'ingénierie et d'autres systèmes OT critiques.
Sites isolés du réseau et à connectivité restreinte	Les sites distants et distribués peuvent avoir une connectivité limitée. La production continue, les réseaux segmentés et les systèmes traditionnels compliquent l'application des correctifs ; la sauvegarde et la restauration doivent donc fonctionner localement.
Matériel et systèmes d'exploitation traditionnels	De nombreux systèmes OT exécutent des versions Windows / Linux à longue durée de vie ou des images verrouillées par le fournisseur, pour lesquelles les mises à niveau sont risquées ou interdites.
Systèmes fragiles et déterministes	Sensibles sur le plan opérationnel : les environnements OT exigent un contrôle strict des redémarrages, des mises à jour logicielles, du déploiement d'agent et des changements de configuration. La protection doit avoir un faible impact, être prévisible et sûre sur le plan opérationnel.
Support IT limité sur site	Les sites distribués dépendent souvent des opérateurs ou des ingénieurs OT. La restauration doit être simple et rapide, même sans support IT sur site.
Pression en matière de conformité et d'assurance	Les opérateurs font face à des attentes croissantes en matière de préparation à la restauration, de preuves d'audit et de garantie des fournisseurs, en alignement avec les cadres de cybersécurité industrielle.
Verrouillage fournisseur	Les logiciels OEM propriétaires, les images sous licence et les configurations spécifiques au matériel peuvent limiter la flexibilité, augmenter les coûts et compliquer la migration, la restauration et les reconstructions.

Quels systèmes et données Acronis Cyber Protect sécurise-t-il ?

Zone de l'environnement OT	Systèmes protégés	Données protégées
OT central et ICS	Serveurs / clients SCADA, postes de travail HMI, postes opérateur DCS, postes de travail d'ingénierie, historiques, serveurs d'applications OT.	Images de système d'exploitation, piles d'applications, configurations SCADA / HMI, historisation, logique d'alarme, paramètres de fonctionnement.
Infrastructure énergétique	PC de contrôle de sous-station, serveurs HVDC / FACTS, responsables du traitement DER / micro-réseaux, responsables du traitement de site BESS, serveurs de gestion de recharge des véhicules électriques.	Logiciel de contrôle de site, fichiers de configuration, jeux de données opérationnels, pilotes de terminal, images de restauration.
Opérations pétrolières et gazières	Serveurs de surveillance de pipeline, systèmes de détection de fuite, systèmes DCS / SCADA de raffinerie, PC de contrôle de turbomachines, systèmes de transfert de garde.	Configurations de processus, données de surveillance, fichiers d'étalonnage / de réglage, enregistrements opérationnels.
Ingénierie et numérisation	PC d'ingénierie, postes de travail CAD / CAM, systèmes de simulation, serveurs de gestion des ressources, plateformes de jumeau numérique.	Fichiers de projet d'ingénierie, dessins, modèles, documentation, référentiels de configuration, données de projet sensibles en matière de propriété intellectuelle.
DMZ OT et systèmes de support	Hôtes de rebond, serveurs d'acquisition de données, serveurs d'authentification / sécurité, systèmes OT / IT intermédiaires.	Configurations de passerelle d'accès, journaux, images système, données de stratégie / configuration.



*List of protected systems not exhaustive

Visibilité SIEM et SOC : l'intégration SIEM sur site par Acronis transmet les alertes et événements couvrant la sauvegarde, la sécurité et la gestion RMM vers des SIEM tiers via syslog ou l'exportation de fichier, aidant les équipes OT et de sécurité à centraliser la surveillance et la connaissance des incidents pour l'ensemble des environnements protégés.

Comment Acronis protège les systèmes OT

Sauvegarde optimisée pour l'OT : sauvegardes d'image et de fichier avec un faible encombrement, adaptées aux systèmes OT en production, sans interruption d'activité planifiée pour de nombreux déploiements.

Solution conçue pour les sites segmentés et isolés du réseau : prend en charge le fonctionnement hors ligne et le stockage local (SAN / NAS / zones de stockage dédiées) et peut être déployée selon la segmentation du réseau OT et la connectivité restreinte.

Restauration sûre et vérifiée : validation de sauvegarde et contrôles d'intégrité, avec analyse facultative des malwares au niveau des points de restauration afin de réduire le risque de restaurer des systèmes compromis.

Restauration rapide pilotée par l'opérateur : workflows de restauration guidés et simplifiés pour les sites à présence IT limitée, permettant aux équipes locales de restaurer les systèmes lorsque l'accès distant n'est pas disponible.

Restauration indépendante du matériel : sur du matériel neuf ou différent (y compris P2P, P2V et V2P)* pour maintenir la continuité des opérations lorsque les PC industriels d'origine sont obsolètes ou indisponibles.

Prise en charge des systèmes OT critiques en terme de sécurité et des SIS :
Dans les opérations pétrolières, gazières et électriques, la priorité est claire : la sécurité avant tout. Les systèmes de sécurité instrumentés (SIS), y compris les plateformes telles que Triconex, DeltaV SIS et Honeywell Safety Manager, dépendent de postes de travail d'ingénierie sur PC, de référentiels de configuration, de systèmes de maintenance, de systèmes de documentation, d'interfaces d'historisation et de serveurs de support pour garantir la fiabilité des opérations.

Acronis Cyber Protect for OT se concentre sur la protection et la restauration de ces systèmes sur PC de support. En aidant à les restaurer dans un état validé et fiable après une défaillance matérielle, une corruption, un ransomware ou une perturbation opérationnelle, Acronis soutient la cyberrésilience des environnements OT à la sécurité critique tout en maintenant une distinction claire entre la cyberrésilience et la sécurité fonctionnelle.

Protégez tout système OT sur PC, de l'ère XP à aujourd'hui, avec Acronis

Acronis prend en charge les systèmes d'exploitation PC hérités que la plupart des autres fournisseurs ont abandonnés :

Windows

- Windows Server 2003 SP1, R2 et versions ultérieures, 2008/2008 R2, 2012/2012 R2, 2016, 2019, 2022 (toutes options d'installation sauf Nano)
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010, 2011, 2012
- Windows Storage Server 2003, 2008/2008 R2, 2012/ 2012 R2, 2016
- Windows XP Professionnel SP1, SP2, SP3
- Windows 7, 8/8.1, 10 (sauf RT), 11 (toutes les éditions)

Linux

- Kernel 2.6.9 à 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 à 23.04
- Fedora 11 à 31
- SUSE Linux Enterprise Server 10, 11, 12, 15
- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4-7.7, 8.0-8.8, 8.11, 9.0- 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*
- Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* P2P, P2V et V2P signifient que le système peut être restauré depuis des environnements physique vers physique, physique vers virtuel ou virtuel vers physique, garantissant que la restauration reste possible même lorsque le PC industriel d'origine ou son matériel exact n'est plus disponible.

Principaux scénarios opérationnels couverts

Défaillance de système OT	Incident de ransomware ou de malware	Échec de correctif ou de mise à jour fournisseur	Perte des postes d'ingénierie	Panne sur site distant ou offshore
Défaillance du disque ou de la carte mère d'un PC industriel. Restaurer rapidement l'ensemble du système pour reprendre les opérations sans tout reconstruire depuis zéro.	Isoler les systèmes affectés et restaurer des sauvegardes propres et validées afin de revenir à un état de fonctionnement sain, tout en réduisant le risque de réinfection.	Restaurer au dernier état sain connu après qu'un changement a provoqué une instabilité ou un comportement non sûr.	Restaurer les PC d'ingénierie et les référentiels de projet afin d'éviter des semaines de reconfiguration et de favoriser une gestion sûre des changements.	Permettre une restauration locale sans dépendance à Internet ou au VPN pour les sous-stations, stations de compression, plateformes et sites de production distants.

Chemins de restauration par mode de défaillance

Acronis Cyber Protect for OT offre plusieurs options de restauration afin que les équipes puissent sélectionner le chemin de restauration le plus sûr et le plus rapide en fonction du mode de défaillance, des contraintes du site et des priorités opérationnelles.

Mode de défaillance	Chemin de restauration recommandé	Ce qu'Acronis permet	Personnel type
Suppression accidentelle ou corruption d'un ensemble limité de fichiers.	Restauration granulaire (de fichier / dossier).	Restaurer uniquement les fichiers requis (par ex. artefacts de projet, fichiers de configuration, rapports) sans reconstruire l'ensemble du système. Minimise l'impact opérationnel et évite des changements inutiles sur le poste de travail ou le serveur OT.	Ingénieur contrôle / automatisation ou ingénieur OT / ICS.
Défaillance partielle de l'application ou mauvaise configuration (le système démarre toujours).	Restaurer au dernier état sain connu (point de restauration).	Rétablir le système vers un point de restauration validé après l'échec d'un correctif, d'une mise à jour fournisseur ou erreur de configuration. Aide à ramener la pile d'applications OT à un état opérationnel prévisible.	Ingénieur contrôle / automatisation ou ingénieur OT / ICS.
Le système ne démarre pas (défaillance du disque, OS corrompu, impact du ransomware).	Restauration sur système nu (support de démarrage de secours : Linux ou WinRE).	Démarrer le périphérique à l'aide du support de secours Acronis et restaurer l'image complète (OS, applications, pilotes et données) pour ramener le système à un état sain connu, sans réinstallation manuelle.	Ingénieur OT / ICS ou technicien sur site formé.
Défaillance matérielle sans pièce de rechange identique disponible.	Restauration sur du matériel différent (Universal Restore).	Restaurer l'image système sur le matériel de remplacement et injecter les pilotes critiques requis pour le démarrage (par ex. responsables du traitement de stockage / chipsets) afin de remettre en ligne des piles OT traditionnelles et spécifiques aux fournisseurs lorsque les PC industriels d'origine sont obsolètes ou indisponibles.	Ingénieur OT / ICS ou technicien sur site (IT en option).
Panne sur site distant (accès IT limité / inexistant).	Restauration pilotée par l'opérateur (restauration en un clic).	Des workflows de restauration guidés et simplifiés permettent au personnel non informaticien de restaurer les systèmes OT localement et en toute sécurité, réduisant l'interruption d'activité lorsque le temps de déplacement ou les contraintes d'accès distant retardent la restauration.	Opérateur / superviseur d'équipe ou technicien de terrain / de sous-station.
Incident de ransomware ou de malware (risque de réinfection pendant la restauration).	Restauration plus sûre (analyser / valider les points de restauration avant la restauration).	Valider les sauvegardes et analyser les points de restauration à la recherche de malware avant la restauration afin de limiter le risque de restaurer des images compromises. Prend en charge un workflow de restauration plus sûr lors du retour des opérations OT à un état sain connu.	Ingénieur OT / ICS responsable de la sécurité OT.

Mode de défaillance	Chemin de restauration recommandé	Ce qu'Acronis permet	Personnel type
Les environnements OT virtualisés nécessitent le retour en service le plus rapide (lorsque la virtualisation est autorisée).	Restauration rapide à l'aide de machines virtuelles de secours.	Lorsque la virtualisation est autorisée, restaurez les environnements OT en tant que machines virtuelles afin de raccourcir la restauration du service et de permettre l'exécution complète des étapes de validation sans retarder le temps de fonctionnement opérationnel.	Ingénieur plateforme OT / virtualisation (partage OT / IT).
L'audit, la maintenance et l'assurance de résilience exigent une preuve de restaurabilité.	Restaurabilité vérifiée (validation de la sauvegarde et vérifications de la capacité de démarrage).	Assurez-vous que les sauvegardes peuvent être restaurées en effectuant des contrôles d'intégrité et en vérifiant la capacité de démarrage. Fournit une assurance opérationnelle que les systèmes OT critiques peuvent être restaurés dans le respect des objectifs de restauration requis.	Ingénieur OT / ICS avec spécialisation en sécurité OT / conformité.

En sélectionnant le chemin de restauration adapté au mode de défaillance, les équipes OT peuvent réduire l'interruption d'activité, éviter des modifications système inutiles et rétablir les opérations dans un état validé, conformément aux procédures du site et aux stratégies de contrôle des changements.

Alignement avec les exigences de conformité et d'assurance

Acronis Cyber Protect for OT prend en charge la préparation à la restauration, les preuves d'audit et les critères d'éligibilité aux assurances des fournisseurs couramment utilisés dans les programmes de cybersécurité de l'énergie et de l'industrie, y compris l'alignement avec les principes IEC 62443 de préparation à la restauration et les réglementations régionales, telles que NIS 2, les exigences de résilience OT figurant dans les réglementations relatives aux infrastructures critiques et la planification et les tests de restauration sectoriels, ainsi que les exigences d'assurance des fournisseurs et de développement sécurisé de plus en plus pertinentes pour les OEM dans le cadre du Règlement de Cyberrésilience de l'UE (EU CRA).

GDPR NIS2 NIST IEC NERC CIP CRA

Vecteurs de conformité de la plateforme Acronis Cyber Protect

Preuves de restauration vérifiées.

Sauvegardes chiffrées avec contrôles de rétention.

Processus de restauration contrôlés.

Pratiques SSDLC pour soutenir les évaluations d'assurance du fournisseur.

IEC 62443-4-1 CERTIFIED

Certificat Acronis CEI 62443-4-1

La certification CEI 62443-4-1 confirme qu'Acronis applique des pratiques de cycle de vie de développement sécurisé (SSDLC) alignées sur les attentes industrielles. Pour les organisations du pétrole et du gaz ainsi que de l'électricité et de l'énergie, cela renforce l'assurance du fournisseur, réduit le risque lié à la chaîne d'approvisionnement et soutient la confiance dans les solutions de résilience OT.

Résumé

Acronis Cyber Protect permet aux organisations du pétrole et du gaz ainsi que de l'électricité et de l'énergie de restaurer les systèmes OT critiques de manière sûre, prévisible et rapide, sans perturber les opérations, tout en répondant aux exigences croissantes de la cybersécurité industrielle et de la préparation à la restauration.

Acronis

Pour en savoir plus : acronis.com