Acronis Cyber Protect para petróleo e gás, energia elétrica e energia

Resiliência cibernética desenvolvida especificamente para operações industriais críticas

Resumo executivo

As operações de petróleo e gás e de energia elétrica e energia dependem de sistemas de tecnologia operacional (OT) baseados em PC para gerar, transmitir, armazenar e distribuir energia com segurança. Esses ambientes enfrentam restrições únicas: sistemas herdados com longo ciclo de vida, locais com conectividade restrita e baixa tolerância ao tempo de inatividade. Ao mesmo tempo, o ransomware tem como alvo cada vez mais os ambientes de OT.

O Acronis Cyber Protect para OT foi projetado para oferecer backup seguro, recuperação rápida e resiliência operacional para sistemas de OT sem interromper a produção. Ele ajuda as organizações a restaurar estados do sistema validados, reduzir o tempo de recuperação e dar suporte aos requisitos de recuperação e auditoria comuns nos padrões industriais de cibersegurança.

Com a confiança dos fornecedores de automação

YOKOGAWA · Honeywell · GE VERNOVA · ABB · EMERSON

Por que a Acronis para energia elétrica e energia e petróleo e gás?

- Baixo impacto do agente
- Operação offline/ isolada da rede
- Velocidade de restauração bare metal
- Validação de backup/ verificação antimalware
- Recuperação com um só clique
- Suporte a SO herdado
- Restauração universal
- Armazenamento imutável + replicação + criptografia

O Acronis Cyber Protect para OT foi desenvolvido especificamente com base nas prioridades de OT: disponibilidade, conveniência, recuperação, prevenção, realidade herdada e ambientes mistos, além de fluxos de trabalho de recuperação conduzidos pelo operador para ambientes remotos e restritos.

Valor para o negócio

Valor operacional:

- Minimize o tempo médio de recuperação (MTTR) de sistemas de OT críticos.
- Mantenha a continuidade da produção.
- Reduza o risco restaurando estados do sistema validados.

Proteção de risco e da marca:

- Reduza a probabilidade de restaurações inseguras ou comprometidas.
- Demonstre resiliência cibernética e prontidão para recuperação à governança interna, parceiros e órgãos reguladores.

Impacto de custo total de propriedade (TCO):

- Reduza o OpEx minimizando o tempo de inatividade e simplificando a recuperação de sistemas de OT críticos.
- Otimize o CapEx estendendo o ciclo de vida dos ativos herdados e viabilizando a recuperação para hardware de substituição.

Valor para OEMs e parceiros:

- Incorpore resiliência aos sistemas fornecidos.
- Reduza a carga de suporte pós-implantação.
- Permita receita recorrente por meio de serviços de resiliência e suporte ao ciclo de vida.

Setores atendidos

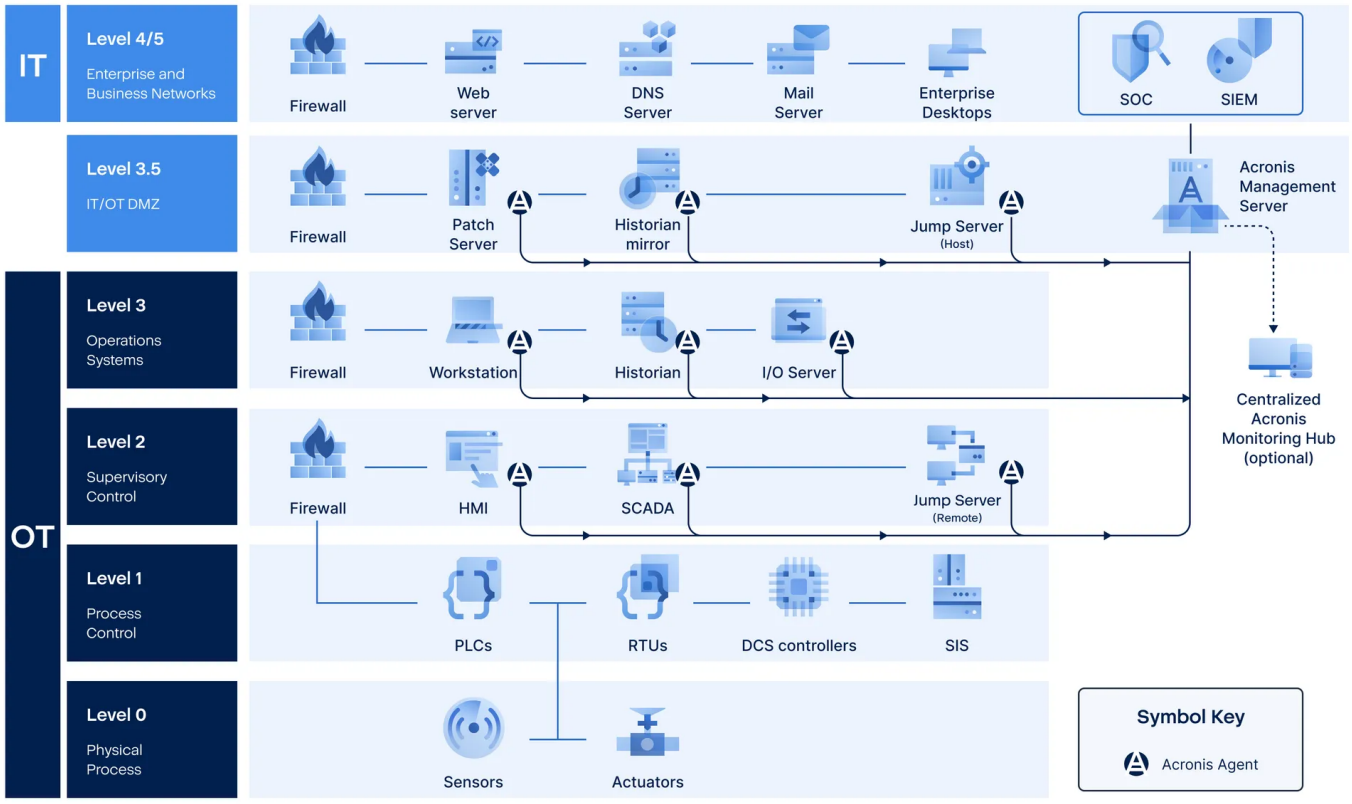
Energia elétrica:		
Geração de energia (térmica, nuclear, hidrelétrica, eólica, solar, biomassa e resíduos para energia).	Transmissão e distribuição (redes de transmissão, incluindo sistemas HVDC, subestações, redes de distribuição).	Borda da rede e energia distribuída (recursos energéticos distribuídos (DER), microrredes, BESS).
Petróleo e gás:		
Upstream (exploração, perfuração, produção offshore/onshore, produção de gás natural e processamento em campo).	Midstream (compressão e transmissão de gás, transporte por dutos, terminais de armazenamento, liquefação e transporte de GNL).	Downstream (refino, produção petroquímica e química, gás em líquidos (GTL), regaseificação de GNL).

Desafios operacionais em ambientes de OT de energia e de petróleo e gás

Desafio	Por que isso importa
Custo alto de tempo de inatividade	Interrupções podem causar riscos à segurança, perda de produção, interrupção de serviço e exposição regulatória. A recuperação rápida é crítica.
Desafios de cibersegurança	Ransomware e ciberataques direcionados ameaçam cada vez mais SCADA, HMI, historian, estações de trabalho de engenharia e outros sistemas de OT críticos.
Locais isolados da rede e com conectividade restrita	Locais remotos e distribuídos podem ter conectividade limitada. Produção contínua, redes segmentadas e sistemas herdados complicam a aplicação de patch, portanto backup e recuperação precisam funcionar localmente.
SOs herdados e hardware herdado	Muitos sistemas de OT executam builds Windows/Linux de longa duração ou imagens bloqueadas pelo fornecedor, nas quais fazer upgrade é arriscado ou proibido.
Sistemas frágeis e determinísticos	Operacionalmente sensíveis: ambientes de OT exigem controle rigoroso sobre reinicializações, atualizações de software, implantação de agente e mudanças de configuração. A proteção deve ter baixo impacto, ser previsível e operacionalmente segura.
Suporte de TI limitado no local	Locais distribuídos muitas vezes dependem de operadores ou engenheiros de OT. A recuperação deve ser simples e rápida, mesmo sem suporte de TI no local.
Pressão de conformidade e garantia	Os operadores enfrentam expectativas crescentes de prontidão para recuperação, evidências de auditoria e garantia de fornecedores alinhadas com estruturas de cibersegurança industrial.
Dependência de fornecedor	Software OEM proprietário, imagens licenciadas e configurações específicas de hardware podem limitar a flexibilidade, aumentar os custos e complicar a migração, a recuperação e as reconstruções.

Quais sistemas e dados o Acronis Cyber Protect protege

Área do ambiente de OT	Sistemas protegidos	Dados protegidos
OT principal e ICS	Servidores/clientes SCADA, estações de trabalho HMI, estações de operador DCS, estações de trabalho de engenharia, historiadores, servidores de aplicações OT.	Imagens do sistema operacional, pilhas de aplicativos, configurações SCADA/HMI, bancos de dados de historiador, lógica de alarmes, parâmetros operacionais.
Infraestrutura de energia	PCs de controle de subestação, servidores HVDC/FACTS, controladores DER/microgrid, controladores de site BESS, servidores de gerenciamento de recarga de veículos elétricos.	Software de controle do site, arquivos de configuração, conjuntos de dados operacionais, drivers de dispositivo, imagens de recuperação.
Operações de petróleo e gás	Servidores de monitoramento de dutos, sistemas de detecção de vazamento, sistemas DCS/SCADA de refinaria, PCs de controle de turbomáquinas, sistemas de transferência de custódia.	Configurações de processo, dados de monitoramento, arquivos de calibração/ajuste, registros operacionais.
Engenharia e digitalização	PCs de engenharia, estações de trabalho CAD/CAM, sistemas de simulação, servidores de gerenciamento de ativos, plataformas de gêmeo digital.	Arquivos de projeto de engenharia, desenhos, modelos, documentação, repositórios de configuração, dados de projeto confidenciais em termos de PI.
DMZ de OT e sistemas de suporte	Jump hosts, servidores de aquisição de dados, servidores de autenticação/ segurança, sistemas intermediários de OT/TI.	Configurações de gateway de acesso, logs, imagens do sistema, dados de política/ configuração.



*List of protected systems not exhaustive

Visibilidade de SIEM e SOC: a integração de SIEM on-premises da Acronis encaminha alertas e eventos que cobrem backup, segurança e RMM para SIEMs de terceiros via syslog ou exportar arquivo, ajudando as equipes de OT e segurança a centralizar o monitoramento e a detecção de incidentes em todos os ambientes protegidos.

Como a Acronis protege sistemas de OT

Backup otimizado para OT:
Backups de imagem completa e backup no nível do arquivo com baixa utilização de recursos, adequados para sistemas OT em operação, sem necessidade de tempo de inatividade planejado para muitas implantações.

Projetado para sites segmentados e com isolamento físico:
Suporta operação offline e armazenamento local (SAN/NAS/zonas de armazenamento dedicadas) e pode ser implantado em alinhamento com a segmentação de rede OT e a conectividade restrita.

Recuperação segura e verificada:
Validação de backup e verificações de integridade, além de verificação opcional de malware dos pontos de restauração, para reduzir o risco de restaurar sistemas comprometidos.

Recuperação rápida conduzida pelo operador:
Fluxos de trabalho de recuperação guiados e simplificados para sites com presença limitada de TI, permitindo que as equipes locais restaurem sistemas quando o acesso remoto não estiver disponível.

Restauração independente de hardware:
Restaure em hardware novo ou diferente (incluindo P2P, P2V e V2P)* para manter as operações em execução quando os PCs industriais originais estiverem obsoletos ou indisponíveis.

Suporte a sistemas OT críticos para a segurança e SIS:
Em operações de petróleo e gás e de energia, a prioridade é clara: segurança em primeiro lugar. Sistemas instrumentados de segurança (SIS), incluindo plataformas como Triconex, DeltaV SIS e Honeywell Safety Manager, dependem de estações de trabalho de engenharia baseadas em PC, repositórios de configuração, sistemas de manutenção, sistemas de documentação, interfaces de historiador e servidores de suporte para dar suporte a operações seguras.

O Acronis Cyber Protect para OT se concentra em proteger e recuperar esses sistemas de suporte baseados em PC. Ajudando a restaurá-los para um estado validado e confiável após falha de hardware, corrupção, ransomware ou interrupção operacional, a Acronis oferece suporte à resiliência cibernética em torno de ambientes OT críticos para a segurança, mantendo uma distinção clara entre resiliência cibernética e segurança funcional.

Proteja qualquer sistema OT baseado em PC, da era XP até o presente, com a Acronis

Acronis oferece suporte a sistemas operacionais de PC herdados que outros fornecedores abandonaram:

Windows

- Windows Server 2003 SP1, R2 e posterior, 2008/2008 R2, 2012/2012 R2, 2016, 2019, 2022 exceto 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 Professional SP1, SP2, SP3
- Windows 7, 8/8.1, 10 (exceto RT), 11 (todas as edições)

Linux

- Kernel 2.6.9 a 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 - 23.04
- Fedora 11 - 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 e V2P, o que significa que o sistema pode ser restaurado de ambientes físico-para-físico, físico-para-virtual ou virtual-para-físico, garantindo que a recuperação continue possível mesmo quando o PC industrial original ou seu hardware exato não estiver mais disponível.

Principais cenários operacionais abrangidos

Falha de sistema OT	Incidente de ransomware ou malware	Patch ou atualização do fornecedor com falha	Perda de estações de engenharia	Interrupção em local remoto ou offshore
Falha do disco ou da placa-mãe do PC industrial. Restaure o sistema completo rapidamente para retomar as operações sem reconstruí-lo do zero.	Isole os sistemas afetados e restaure backups limpos e validados para retornar a um estado operacional confiável, reduzindo o risco de reinfecção.	Reverter para o último estado operacional confiável após uma alteração causar instabilidade ou comportamento inseguro.	Restaure os PCs de engenharia e os repositórios de projeto para evitar semanas de reconfiguração e dar suporte ao controle seguro de mudanças.	Habilite a recuperação local sem dependência de internet ou VPN para subestações, estações de compressão, plataformas e locais remotos de produção.

Caminhos de restauração por modo de falha

O Acronis Cyber Protect para OT oferece várias opções de recuperação para que as equipes possam selecionar o caminho de restauração mais seguro e rápido com base no modo de falha, nas restrições do local e nas prioridades operacionais.

Modo de falha	Caminho de restauração recomendado	O que a Acronis permite	Pessoal típico
Exclusão acidental ou corrupção de um conjunto limitado de arquivos.	Restauração granular (restauração de arquivo/pasta).	Restaure apenas os arquivos necessários (por exemplo, artefatos de projeto, arquivos de configuração, relatórios) sem reconstruir o sistema inteiro. Minimiza o impacto operacional e evita mudanças desnecessárias na estação de trabalho ou no servidor de OT.	Engenheiro de controles/ automação ou engenheiro de OT/ICS.
Falha parcial da aplicação ou configuração incorreta (o sistema ainda é iniciado).	Reverter para o último estado operacional confiável (ponto de restauração).	Reverter o sistema para um ponto de restauração validado após um patch com falha, uma atualização do fornecedor ou um erro de configuração. Ajuda a retornar a pilha de aplicações de OT a um estado operacional previsível.	Engenheiro de controles/ automação ou engenheiro de OT/ICS.
O sistema não é iniciado (falha de disco, SO corrompido, impacto de ransomware).	Restauração bare metal (mídia de recuperação inicializável: Linux ou WinRE).	Inicie o dispositivo usando a mídia de recuperação da Acronis e restaure a imagem completa (SO, aplicações, drivers e dados) para retornar o sistema a um estado operacional confiável sem reinstalação manual.	Engenheiro de OT/ICS ou técnico local treinado.
Falha de hardware sem peça sobressalente idêntica disponível.	Restauração para hardware diferente (Restauração Universal).	Restaure a imagem do sistema em um hardware de substituição e injete os drivers de inicialização críticos necessários (por exemplo, controladores de armazenamento/chipsets) para colocar novamente em operação pilhas de OT herdadas e específicas de fornecedores quando os PCs industriais originais estiverem obsoletos ou indisponíveis.	Engenheiro de OT/ICS ou técnico local (TI opcional).
Interrupção em local remoto (acesso limitado/sem acesso de TI).	Recuperação conduzida pelo operador (recuperação com um clique).	Fluxos de trabalho de recuperação guiados e simplificados permitem que pessoal não técnico de TI restaure sistemas de OT localmente e com segurança, reduzindo o tempo de inatividade quando o tempo de deslocamento ou as restrições de acesso remoto atrasam a recuperação.	Operador/supervisor de turno ou técnico de campo/ subestação.
Incidente de ransomware ou malware (risco de reinfecção durante a restauração).	Recuperação mais segura (verificar/ validar pontos de restauração antes da recuperação).	Valide os backups e verifique os pontos de restauração em busca de malware antes da restauração para reduzir o risco de restaurar imagens comprometidas. Oferece suporte a um fluxo de trabalho de recuperação mais seguro ao retornar as operações de OT a um estado confiável.	Engenheiro de OT/ICS com cliente potencial de segurança de OT.

Modo de falha	Caminho de restauração recomendado	O que a Acronis permite	Pessoal típico
Cargas de trabalho de OT virtualizadas precisam do retorno mais rápido do serviço (onde a virtualização é permitida).	Recuperação rápida usando máquinas virtuais em espera.	Onde a virtualização for permitida, recupere as cargas de trabalho de OT como máquinas virtuais para reduzir o tempo de restauração do serviço e permitir que as etapas completas de validação sejam concluídas sem atrasar a disponibilidade operacional.	Engenheiro de plataforma de OT/virtualização (OT/TI compartilhado).
Auditoria, manutenção e garantia de resiliência exigem prova de capacidade de recuperação.	Capacidade de recuperação verificada (validação de backup e verificações de inicialização).	Valide que os backups podem ser recuperados executando verificações de integridade e verificação de inicialização. Fornece garantia operacional de que sistemas críticos de OT podem ser restaurados dentro dos objetivos de recuperação exigidos.	Engenheiro de OT/ICS com segurança/conformidade de OT.

Selecionando o caminho de restauração que corresponde ao modo de falha, as equipes de OT podem reduzir o tempo de inatividade, evitar mudanças desnecessárias no sistema e retomar as operações em um estado validado, em alinhamento com os procedimentos do local e as políticas de controle de mudanças.

Alinhamento de conformidade e garantia

O Acronis Cyber Protect para OT oferece suporte à prontidão de recuperação, às evidências de auditoria e às expectativas de garantia de fornecedores comumente usadas em programas de cibersegurança de energia e industriais, incluindo alinhamento com os princípios de prontidão de recuperação da IEC 62443 e regulamentações regionais, como a NIS 2, requisitos de resiliência de OT encontrados em regulamentações de infraestrutura crítica e planejamento e testes de recuperação com foco no setor, bem como expectativas de garantia de fornecedores e de desenvolvimento seguro cada vez mais relevantes para OEMs no âmbito da Lei de Resiliência Cibernética da UE (CRA).

GDPR NIS2 NIST IEC NERC CIP CRA

Facilitadores de conformidade da plataforma Acronis Cyber Protect

- Evidências de recuperação verificadas.
- Backups criptografados com controles de retenção.
- Processos de recuperação controlados.
- Práticas de SSDLC para oferecer suporte a avaliações de garantia de fornecedores.

IEC 62443-4-1 CERTIFIED

Certificado IEC 62443-4-1 da Acronis

A certificação IEC 62443-4-1 confirma que a Acronis aplica práticas de ciclo de vida de desenvolvimento seguro (SSDLC) em alinhamento com as expectativas industriais. Para organizações dos setores de petróleo e gás e de energia elétrica, isso fortalece a garantia de fornecedores, reduz o risco da cadeia de suprimentos e reforça a confiança em soluções de resiliência de OT.

Resumo

O Acronis Cyber Protect permite que organizações dos setores de petróleo e gás e de energia elétrica recuperem sistemas críticos de OT com segurança, previsibilidade e rapidez, sem interromper as operações, ao mesmo tempo em que oferece suporte às crescentes demandas de cibersegurança industrial e prontidão de recuperação.

Acronis

Saiba mais em
www.acronis.com