Preservando a disponibilidade em ambientes de tecnologia operacional (TO)

Os altos custos do tempo de inatividade do sistema de TO

Os sistemas de tecnologia operacional (TO) são um elo crítico na manutenção da disponibilidade de produção e da lucratividade da empresa. Quando falham, podem derrubar linhas de montagem, oleodutos, redes de utilidade pública e cadeias de suprimentos com eles. Os custos das interrupções resultantes podem variar de dezenas a centenas de milhares de dólares por hora. Uma pesquisa da ABB revelou que 69% das empresas sofreram interrupções de serviço pelo menos uma vez por mês nos últimos anos, e que essas interrupções custam às empresas US$ 150.000 por hora[1]. Outras consequências do tempo de inatividade de TO incluem:

- Custos de oportunidade de vendas devido a pedidos não atendidos e tempos de entrega mais longos.
- Aumento dos custos diretos de mão de obra por quantidade de bens produzidos.
- Danos ao relacionamento com o cliente final e à reputação de branding causados por entregas lentas ou não realizadas.
- A capitalização de mercado está diminuindo à medida que os investidores perdem confiança na capacidade da empresa de manter uma produção consistente.
- Penalidades financeiras por não cumprimento de acordos de nível de serviço e outras obrigações contratuais.
- Multas de conformidade e penalidades criminais por não atender aos requisitos regulatórios de resiliência cibernética.

Como resultado, as apostas são altas na defesa dos sistemas de TO contra ataques cibernéticos, desastres naturais, falhas de hardware, falhas de software e erros humanos, e em colocá-los de volta online rapidamente quando falham.

Muitas indústrias dependem fortemente da automação para processos de produção em tempo real, incluindo os setores automotivo, de energia, de energia elétrica, farmacêutico e de logística. Grande parte dessa tecnologia de automação é controlada, configurada e monitorada por PCs que rodam Windows ou Linux e que se enquadram na rubrica de tecnologia operacional (TO), sistemas de controle industrial (ICS) e infraestrutura ciberfísica. Aplicações comuns de TO incluem sistemas de supervisão e aquisição de dados (SCADA), sistemas de controle distribuído (DCS), interfaces homem-máquina (HMI) e sistemas de historiador operacional que capturam dados de processo em tempo real.

[1] ABB. "Valor da Confiabilidade: Relatório da Pesquisa ABB 2023."

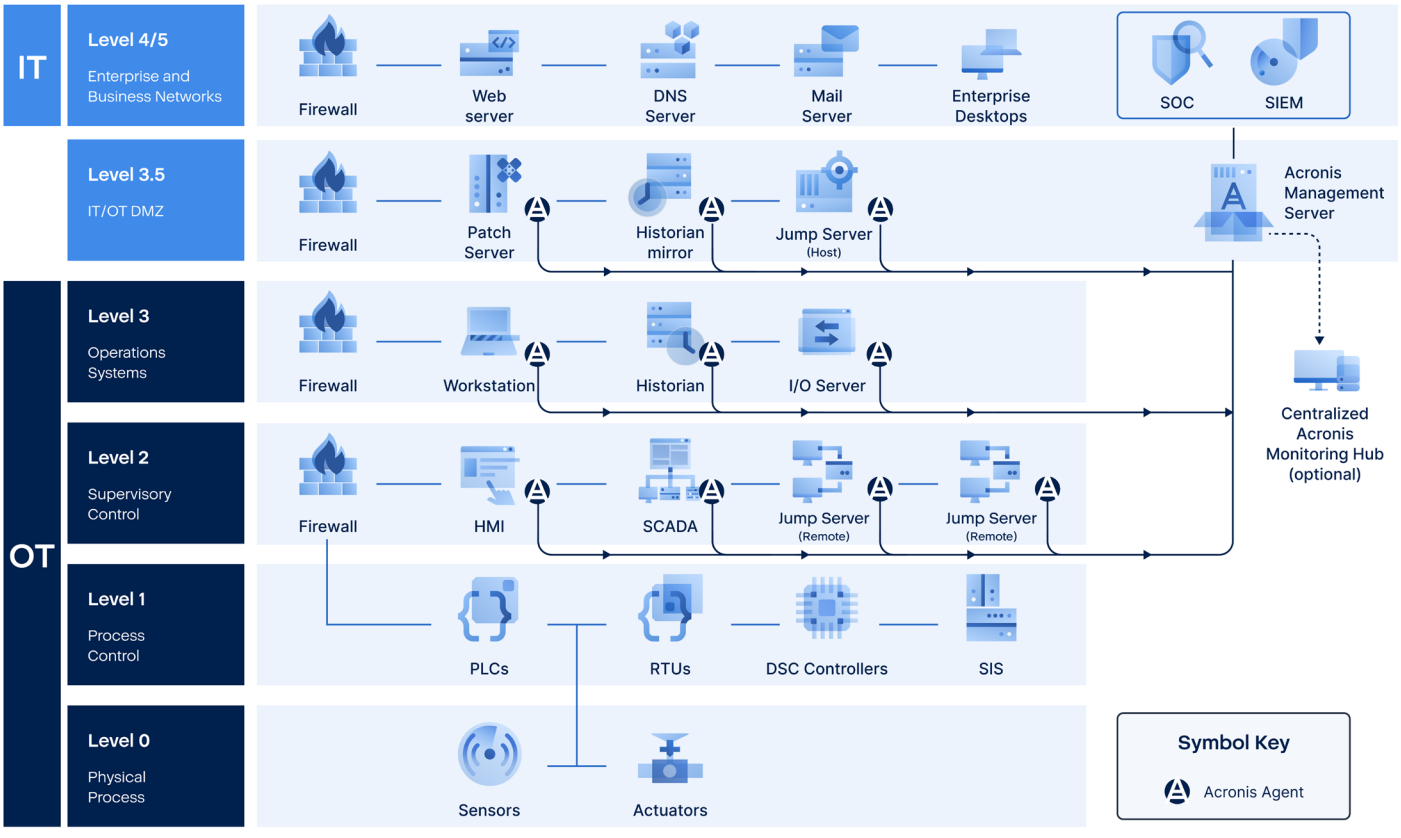
Os desafios de manter a disponibilidade do sistema de TO

A pressão para minimizar o tempo de inatividade do sistema de TO é amplificada pelo fato de que os ambientes de TO têm atributos únicos que os tornam mais difíceis de manter em funcionamento do que os sistemas de TI tradicionais de back-office e front-office:

- Muitos sistemas de TO operam em hardware e sistemas operacionais que têm muitos anos, alguns datando da era do Windows XP. Fazer upgrade para novo hardware e revisões de sistema operacional é arriscado, com o potencial de quebrar ou limitar a funcionalidade das aplicações de TO.
- A idade desses sistemas também torna difícil ou impossível equipá-los com medidas de cibersegurança atualizadas, como detecção e resposta de endpoint (EDR).
- Quando um fornecedor de sistema operacional anuncia a data de fim de suporte para uma versão específica do produto (por exemplo, como a Microsoft fez com o Windows XP em abril de 2014) os principais fornecedores de backup geralmente param de oferecer suporte dentro de cinco anos, e muitas vezes antes disso. Sem o suporte de um grande fornecedor de backup, os engenheiros de TO são forçados a depender de processos de backup manuais, lentos e propensos a erros, que exigem um tempo de inatividade agendado e caro para serem executados.
- As instalações onde os sistemas de TO estão localizados raramente têm suporte de TI local e muitas vezes estão distantes das equipes de TI centralizadas. Além disso, os ambientes de TO são frequentemente isolados para reduzir os riscos de segurança cibernética, o que impede a TI de usar ferramentas de monitoramento e gerenciamento remotas. Enviar pessoal de TI fisicamente para instalações de produção pode ser lento e caro, prolongando interrupções custosas.

A Acronis atende aos requisitos únicos de resiliência cibernética dos ambientes de TO

A plataforma Acronis Cyber Protect é amplamente utilizada na fabricação e na indústria para proteger uma variedade de sistemas de TO, incluindo (mas não se limitando a) os exemplos no Modelo Purdue mostrados na Figura 1.



*List of protected systems not exhaustive

Figura 1: Exemplos do Modelo Purdue de sistemas de TO com proteção da Acronis

O Acronis Cyber Protect oferece backup e recuperação para sistemas de TO com recursos que são essenciais em ambientes de produção que exigem uma disponibilidade extremamente alta, incluindo:

- A capacidade de instalar o agente do Acronis Cyber Protect e realizar backups sem nunca desligar ou reiniciar o sistema de TO.
- Execução de backup rápida, confiável e totalmente automatizada que alivia o processamento e o armazenamento de backup do sistema de TO.
- A capacidade de padronizar (ou personalizar) backups em sistemas e locais com planos de proteção de dados.
- Funções opcionais de segurança cibernética usando o mesmo agente Acronis, incluindo EDR, anti-malware e anti-ransomware.

A Acronis oferece proteção até mesmo para os sistemas de TO mais antigos

A Acronis reforça a estabilidade dos ambientes de TO protegendo todos os sistemas desde a era do XP até hoje (inclusive sistemas operacionais há muito abandonados por outros fornecedores) Isso garante uma recuperação rápida e confiável até mesmo dos sistemas legados mais antigos, com a opção de replicar um sistema em um novo hardware de PC através de um processo chamado recuperação bare metal, se necessário. Esse recurso instala automaticamente quaisquer novos drivers necessários para garantir que o sistema operacional e as aplicações de TO funcionem corretamente no novo hardware. A Figura 2 mostra a extensão do suporte da Acronis para sistemas operacionais e hipervisores desde a era do XP até o presente, destacando as versões do Windows e Linux mais comumente usadas em ambientes de TO:

A melhor cobertura do setor para diversos sistemas operacionais e hipervisores

Windows

- Windows Server 2003 SP1, R2 e posterior, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022, exceto Nano Server
- 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, 11 (todas as edições), 10, – todas as edições, exceto o Windows RT

Microsoft SQL Server
2022, 2019, 2017, 2016, 2014, 2012, 2008 R2, 2008, 2005

Microsoft Exchange Server
2019, 2016, 2013, 2010, 2007

Hipervisores

VMware vSphere
4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server
2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer/Citrix Hypervisor
8.2 - 4.1.5

Linux KVM
8 - 7.6

Scale Computing Hypercore
8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)
3.6-2.2

Red Hat Virtualization
4.0, 4.1, 4.2, 4.3, 4.4

Virtuozzo
7.0.14 - 6.0.10

Virtuozzo Infrastructure Platform
3.5

Hipervisor Nutanix Acrópole (AHV)
20160925.x até 20180425.x

MacOS

- **OS X** Mavericks 10.9, Yosemite 10.10, El Capitan 10.11
- **macOS** Sierra 10.12, High Sierra 10.13, Mojave 10.14, Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13, Sonoma 14

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

Figura 2: Suporte da Acronis para sistemas operacionais e hipervisores

A Acronis permite a restauração de sistema de TO sem a intervenção de TI

A Acronis oferece um recurso único chamado One-Click Recovery, que é crítico em ambientes de TO que não possuem equipe de TI no local e/ou são isolados, impedindo assim o uso de ferramentas de gerenciamento remoto por parte da equipe de TI centralizada. O Acronis One-Click Recovery permite que qualquer trabalhador local, independentemente do seu nível de habilidade em TI, recupere um sistema de TO com falha a partir de um backup local com apenas algumas teclas. Interrupções de produção caras devido a falhas no sistema de TO, que podem levar horas ou dias para serem resolvidas, incluindo o tempo necessário para que a equipe de TI seja enviada ao local, podem ser reduzidas para questão de minutos. O recurso oferece suporte à capacidade de recuperar sistemas de TO a partir de um backup local em disco ou da Acronis Nuvem, e de proteger os backups com criptografia Bitlocker e senhas de recuperação.

A proteção do sistema de TO da Acronis é utilizada pelos principais fornecedores de automação

Principais fornecedores de TO e ICS, incluindo ABB, Siemens, Honeywell e outros, utilizam o Acronis Cyber Protect como solução de backup para seus clientes finais como parte de uma solução white label ou co-branded. Nenhum outro fornecedor de proteção de dados desfruta de uma gama semelhante de parcerias e endossos pela indústria de automação.

A Acronis é reconhecida como líder em ciberresiliência para TO

Principais empresas de pesquisa em tecnologia, como Forrester Research, TAG Infosphere e Omdia, classificam a Acronis como líder em proteção de sistemas de TO.

Relatório do TAG Infosphere LER

Relatório Omdia LER

Conclusão

Acronis Cyber Protect é usado para proteger sistemas de TO em ambientes de fabricação e produção industrial ao redor do mundo. Sua combinação única de proteção de dados para sistemas operacionais desde a era do XP até o presente, One-Click Recovery para restauração de sistema de TO por trabalhadores não especializados em TI, e adoção por fornecedores líderes de automação, contribuíram para seu reconhecimento pela comunidade de analistas como um líder em resiliência cibernética da TO.

LEITURA ADICIONAL

Saiba mais sobre o Acronis Cyber Protect para TO

- Soluções de fabricação da Acronis
- Infográfico: Manutenção do tempo de disponibilidade de TO com One Click Recovery
- Estudo de caso: produtos Tata Steel Downstream
- Estudo de caso: ABB
- Estudo de caso: Johnson Electric
- Estudo de caso: BDR Pharma
- Obtenha uma avaliação gratuita de 30 dias do Acronis Cyber Protect
- Converse com um especialista em resiliência cibernética da TO

Acronis

Saiba mais em www.acronis.com