arcserve®

eBook

MUITO RESILIENTE OU MUITO EXPOSTA:

A disponibilidade contínua nos setores de alto risco

arcserve®

SEMPRE ATIVA. CONTÍNUA. TODA EMPRESA PRECISA QUE OS SEUS SISTEMAS E APLICATIVOS ESSENCIAIS ESTEJAM SEMPRE DISPONÍVEIS.

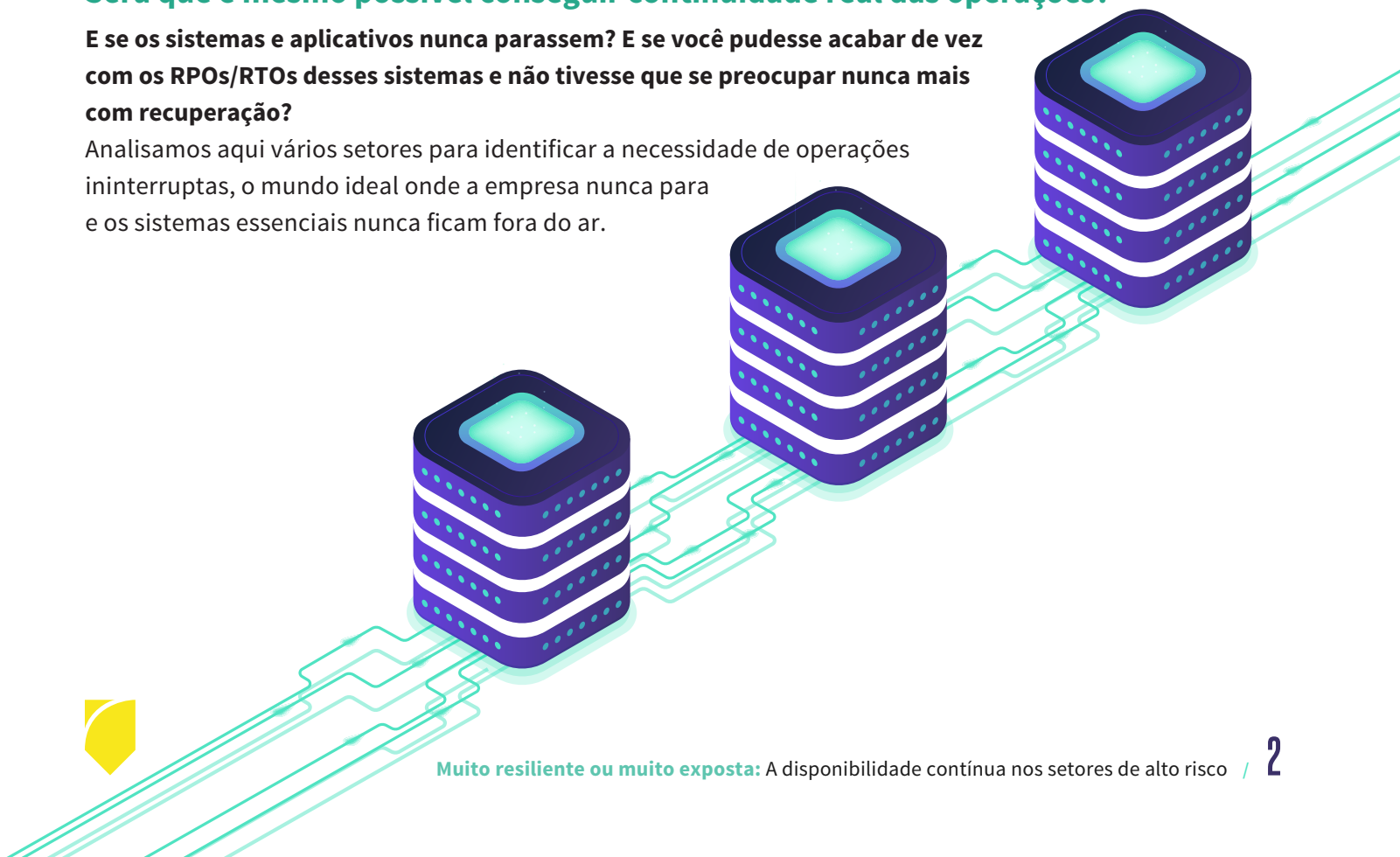
As empresas de hoje, globalizadas e com operação ininterrupta, não podem se dar ao luxo de ficar inativas. Elas trabalham com aplicativos e sistemas que armazenam IPs proprietários, mantêm sites de comércio eletrônico e sistemas em aeroportos funcionando, ferramentas de ERP e de logística operacionais e que viabilizam transações financeiras. Em todos esses casos, uma interrupção não planejada, mesmo que por poucos minutos, pode causar danos irreparáveis em termos de receita e produtividade. Ou seja, o backup e a recuperação já não são mais suficientes.

Para proteger esses sistemas e aplicativos, as empresas precisam mudar o foco do backup para a proteção contínua dos dados. Elas têm acabar com a preocupação com o tempo e objetivo de ponto de recuperação (RTOs/RPOs) e não se preocupar mais com recuperação.

Será que é mesmo possível conseguir continuidade real das operações?

E se os sistemas e aplicativos nunca parassem? E se você pudesse acabar de vez com os RPOs/RTOs desses sistemas e não tivesse que se preocupar nunca mais com recuperação?

Analisamos aqui vários setores para identificar a necessidade de operações ininterruptas, o mundo ideal onde a empresa nunca para e os sistemas essenciais nunca ficam fora do ar.



arcserve®

COMO PROTEGER TECNOLOGIAS IoT DE ATAQUES CIBERNÉTICOS NO SETOR DE MANUFATURA

As indústrias de manufatura raramente descansam. A maioria delas trabalha ininterruptamente, o que exige uma infraestrutura de TI altamente responsiva. Pensando em crescer e melhorar a eficiência operacional, várias delas estão adotando a Internet das Coisas (IoT, Internet of Things) para automatizar e gerenciar remotamente um número cada vez maior de ferramentas e sistemas. Mas os gastos crescentes com IoT e a mudança da adoção de projetos-piloto para a implementação em larga escala também trazem riscos.

No setor de manufatura, a automação das linhas de produção com IoT traz benefícios tangíveis, entre eles rendimento maior com custo menor. Entretanto, ela deixa essas linhas mais suscetíveis, criando vulnerabilidades que os criminosos cibernéticos se aproveitam. Nas indústrias, os ataques cibernéticos danificam infraestruturas e paralisam as operações, causando danos financeiros irreparáveis e queda na produtividade.

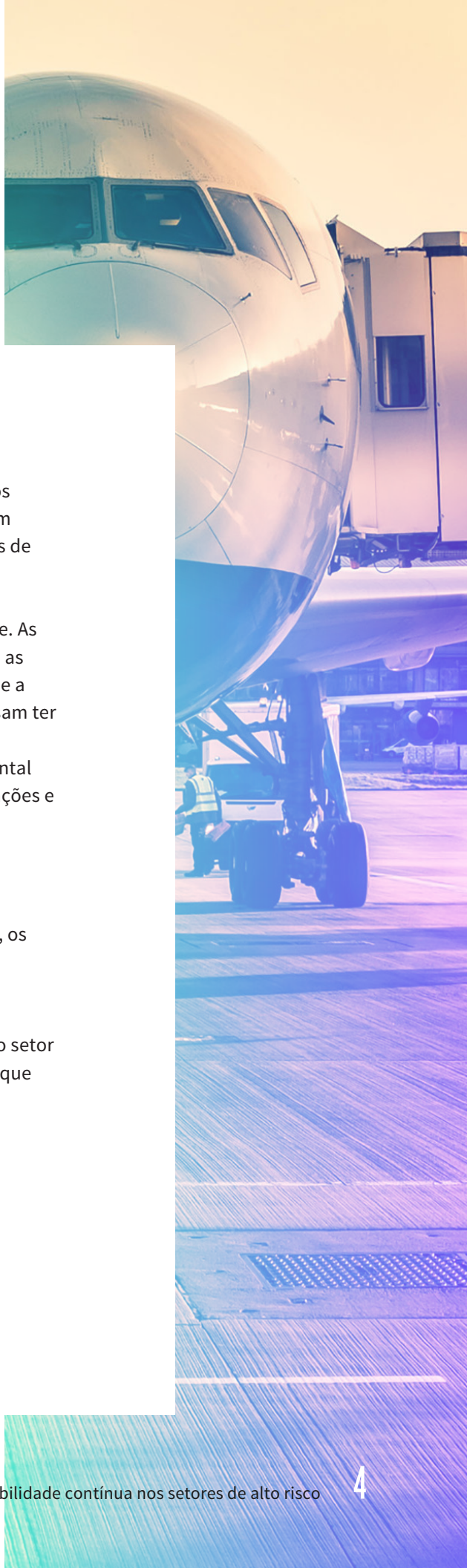
CASO ESPECÍFICO:

QUANDO A NORSK HYDRO, UM DOS MAIORES NOMES DO MUNDO EM PRODUÇÃO DE ALUMÍNIO, FOI ATACADA PELO RANSOMWARE LOCKERGOGA, A RECUPERAÇÃO DO ATAQUE CUSTOU US$ 41 MILHÕES, GRANDE PARTE DESSE VALOR RELACIONADO À PERDA DE PRODUÇÃO[1]. RESUMINDO, AS INDÚSTRIAS NÃO PODEM SE DAR AO LUXO DE TER SEUS SISTEMAS INOPERANTES POR UMA PARALISAÇÃO CAUSADA POR ATAQUES CIBERNÉTICOS, ERRO HUMANO OU DESASTRES NATURAIS.

Em um setor onde muitas empresas fabricam produtos ininterruptamente, a receita e o serviço delas dependem totalmente da disponibilidade dos seus sistemas essenciais. Nas complexas infraestruturas de TI atuais, a interconexão dos sistemas, mesmo que diferentes, significa que se um deles cai, o impacto é geral. Os executivos de TI das indústrias precisam se concentrar na entrega de operações confiáveis e em manter os sistemas e aplicativos operacionais, mesmo no caso de erro humano ou desastre natural. As soluções locais e/ou remotas de alta disponibilidade são fundamentais para preservar as operações e possibilitar o diferencial competitivo, deixando, para isso, os sistemas essenciais disponíveis ininterruptamente.

arcserve®

COMO MANTER A CONTINUIDADE DAS OPERAÇÕES NO SETOR DE VIAGENS E TRANSPORTE



Mais de 2,6 milhões de pessoas passam, por dia, pelos aeroportos dos Estados Unidos. São 3.480 aviões decolando por hora[2]. Qualquer contratempo em um sistema, seja de emissão de passagens, transporte de bagagens ou operações de voo, pode provocar um efeito dominó e interferir em todo o processo.

As empresas do setor de viagens e transporte geram dados ininterruptamente. As companhias aéreas precisam acompanhar cada movimento dos passageiros, as empresas ferroviárias precisam controlar os horários, o conteúdo das cargas e a manutenção dos trens e trilhos e no porto, e as autoridades portuárias precisam ter informações precisas sobre a carga transportada, os recursos e as pessoas envolvidas em todos os processos. Para os executivos desse setor é fundamental manter todos esses sistemas ativos ininterruptamente para garantir as operações e proteger os dados dos clientes e essenciais para a empresa.

A complexidade das empresas de viagens e transporte também traz outras vulnerabilidades para os planos de continuidade dos negócios. Por exemplo, quando acontece um desastre natural como um furacão, os horários mudam, os sistemas caem. A forma como empresa consegue retomar a atividade afeta significativamente a percepção dos clientes sobre ela.

Para manter os aviões no ar, os trens no horário e os navios de carga à tona, o setor de viagens e transporte não para, literalmente, e nem os sistemas essenciais que mantêm essas empresas em operação. Para elas, continuidade dos negócios significa atender às expectativas dos clientes em termos de disponibilidade, mantendo tudo operacional em cada ponto do caminho.

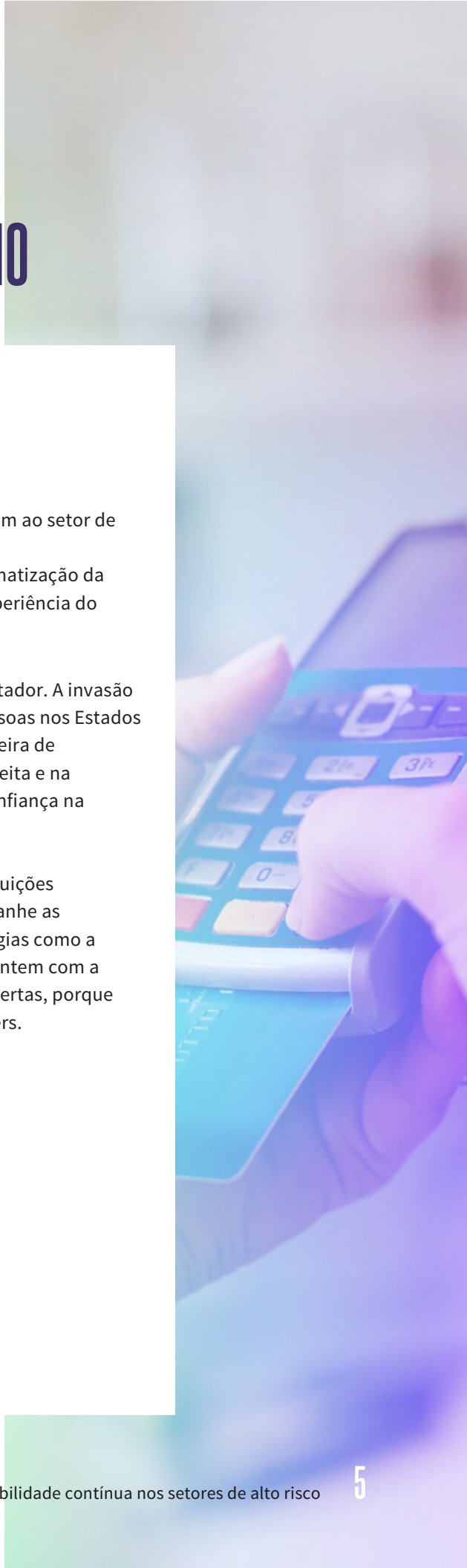
arcserve®

PROTEÇÃO CONTÍNUA DOS DADOS NO MERCADO FINANCEIRO ONDE AS TRANSAÇÕES NÃO PARAM NUNCA

Na atual economia global, "sempre ativo" é um termo que se aplica muito bem ao setor de bancos e serviços financeiros, que sofre essa mesma pressão todos os dias. A transformação digital no mercado financeiro exige a modernização e a automatização da infraestrutura de TI e também a garantia do nível mais alto em termos de experiência do cliente, com disponibilidade constante dos aplicativos bancários.

Assim como em todos os setores, o roubo de dados pode ter um efeito devastador. A invasão da Equifax, em 2017, comprometeu os dados pessoais de 145 milhões de pessoas nos Estados Unidos, expondo informações que incluíam desde data de nascimento a carteira de habilitação e seguro social[3]. Acontecimentos como esse têm impacto na receita e na reputação da empresa, deixando os clientes em choque porque perdem a confiança na capacidade da empresa de proteger seus dados.

Como parte da jornada de transformação digital, é fundamental que as instituições financeiras contem com um plano de continuidade dos negócios que acompanhe as inovações e atenda às expectativas do cliente. Com o surgimento de tecnologias como a criptomoeda e inteligência artificial (AI), é essencial que essas instituições contem com a proteção contínua dos dados e recursos aprimorados de monitoramento e alertas, porque essas inovações também trazem novas oportunidades de ação para os hackers.



arcserve®

MELHORANDO A EXPERIÊNCIA DOS USUÁRIOS DO APP COM ALTA DISPONIBILIDADE

Na atual economia da experiência, o cliente é o centro de tudo. Os clientes querem acessar o que precisam e quando precisam. A frustração só aumenta quando eles não conseguem fazer seus pedidos de comida ou compartilhar a última selfie com o filtro certo. E agora eles têm ainda mais voz. As mídias sociais são o canal perfeito para compartilhar todas as experiências, boas e principalmente más, no Twitter, Reddit e em comentários online.

O volume de dados do setor de tecnologia é impressionante. Pense nisto. Por dia, são enviados 6 mil tuítes por segundo[4], carregadas mais de 300 horas de vídeo por minuto no YouTube [5] e feitas 3,5 bilhões de buscas no Google [6]. Imagine se esses apps ficarem inativos. Os usuários ficarão desesperados.

A base da experiência do cliente, hoje, está mais na disponibilidade dos dados do que só em oferecer produtos de qualidade. Essas experiências, em grande parte viabilizadas pelas empresas de tecnologia e seus aplicativos, podem ser consideradas tão ou mais valiosas que produtos tangíveis. Por isso, é muito importante para a estratégia de TI de qualquer empresa de tecnologia contar com proteção contínua dos dados, para garantir que esteja sempre operacional e sem nenhum sistema inativo.

arcserve®

A SEGURANÇA DOS DADOS É A PRINCIPAL PREOCUPAÇÃO DOS PROFISSIONAIS DE TI DA ÁREA DA SAÚDE

Os dados são um bem de grande valor para qualquer instituição de assistência médica. As informações e o histórico dos pacientes podem determinar o curso do atendimento e oferecer elementos importantes para o diagnóstico. Segundo uma pesquisa feita pela Health Data Management (HDM), a segurança é a principal preocupação dos profissionais de TI da área da saúde porque permite reforçar a proteção das informações sobre os pacientes e defender dos ataques cibernéticos. Na mesma pesquisa, a HDM descobriu também que, para 93% dos entrevistados, proteger as informações relacionadas à saúde e à segurança dos dados é extremamente importante ou muito importante[7].

Com as regulamentações sobre privacidade e conformidade cada vez mais rígidas, proteger os dados dos pacientes não é mais uma questão de escolha, mas uma obrigação. A inovação na saúde moderna exige acompanhar as tecnologias não só na linha de frente do atendimento ao paciente, mas também nos bastidores, na proteção de seus dados.

Quando o assunto é garantir a continuidade das operações, os profissionais de TI da área da saúde dependem de soluções que mantenham o consultório médico, o pronto-socorro e todo o hospital operacionais o tempo todo. A queda de um sistema ou aplicativo de saúde pode se tornar realmente um caso de vida ou morte.

Os pacientes são a prioridade número um dos profissionais da saúde. Interromper um atendimento por causa de um erro humano ou desastre natural está fora de cogitação. Com tecnologia de alta disponibilidade, as instituições de saúde podem ter a certeza de que estarão "sempre ativas" e prontas para atender os pacientes, quando necessário.

arcserve®

CONSIGA CONTINUIDADE DOS NEGÓCIOS REAL COM AS SOLUÇÕES DE REPLICAÇÃO E ALTA DISPONIBILIDADE

Independentemente do setor de atuação, toda empresa tem sistemas e aplicativos que precisam ficar operacionais. Para proteger esses sistemas e aplicativos, as equipes de TI geralmente confiam em tecnologias criadas para reduzir o tempo de inatividade e a perda de dados no caso de uma pane inevitável.

O Arcserve Replication and High Availability (RHA) faz exatamente isso. Ele garante a continuidade dos negócios com tecnologias testadas e aprovadas e com uma única finalidade: manter a sua empresa ativa e operacional. Com tecnologia de replicação assíncrona, o Arcserve RHA é a única solução que combina alta disponibilidade com failover automático por heartbeat e proteção contínua dos dados para os aplicativos e sistemas on premises, remotos e na nuvem. Consiga disponibilidade real dos sistemas e aplicativos:

Replicação de dados em tempo real e mudança de tempo e objetivos de ponto de recuperação (RTOs e RPOs) para proteção contínua.

A tecnologia por journal replica qualquer mudança no arquivo, aplicativo e no sistema como um todo, por mínima que seja, para que você possa retroceder para um ponto no tempo e restaurar tudo como era antes do problema.

O failover automático acionado por tecnologia heartbeat elimina o tempo gasto da detecção à mitigação.

A compatibilidade com servidores físicos e virtuais e ambientes em nuvem, com criptografia e testes sem interferência no ambiente, melhora seu custo total de propriedade.

Quando acontece um período de inatividade, cada momento conta. Tenha operacionalidade constante e mais tranquilidade com o **Arcserve RHA**.

Referências

1. How to neutralize the impact of ransomware, **https://www.manufacturing.net/article/2019/05/how-neutralize-impact-ransomware**
2. Air traffic by the numbers, **https://www.faa.gov/air_traffic/by_the_numbers/**
3. Top Bank Tech Trends for 2018, **https://www.americanbanker.com/slideshow/top-bank-tech-trends-for-2018**
4. Internet Live Stats, **https://www.internetlivestats.com/twitter-statistics/**
5. YouTube by the Numbers: Stats, Demographics & Fun Facts, **https://www.omnicoreagency.com/youtube-statistics/**
6. Internet Live Stats, **https://www.internetlivestats.com/google-search-statistics/**
7. Providers and Progress: Baby Steps for Healthcare's Top Challenges, Health Data Management, accessed 5/13/2019.

Saiba mais em **www.arcserve.com/br**