



> O que você precisa
saber **agora** sobre a arquitetura de
proteção de dados de próxima geração

Não é preciso que ninguém explique a importância de uma proteção de dados eficiente e eficaz. Você já sabe que a capacidade de não apenas proteger, mas também de recuperar dados depois de interrupções no sistema e perda de dados **e com rapidez** são componentes essenciais para sua empresa.

Ainda assim, sua arquitetura de proteção de dados pode possuir um **grande** calcanhar de Aquiles.

Pode ser o hardware e a infraestrutura de computação e rede vulneráveis, que representam uma base não muito sólida. Talvez sejam os silos inflexíveis de proteção de dados, que representam o fim da eficiência e da eficácia do seu plano. Também pode ser a exposição da infraestrutura a eventos pequenos e grandes de perda de dados.

É sua tarefa identificar tudo o que pode dar errado, e se proteger de cada eventualidade.

A boa notícia é que estamos vivendo um momento empolgante no mundo das arquiteturas de proteção de dados. A tecnologia está evoluindo exponencialmente, ajudando você a aumentar a eficiência operacional, atender melhor às necessidades dos usuários finais e oferecer uma proteção de dados, uma desduplicação e uma capacidade de recuperação mais robustas.

Diante disso, o que você precisa saber a respeito do futuro do setor?

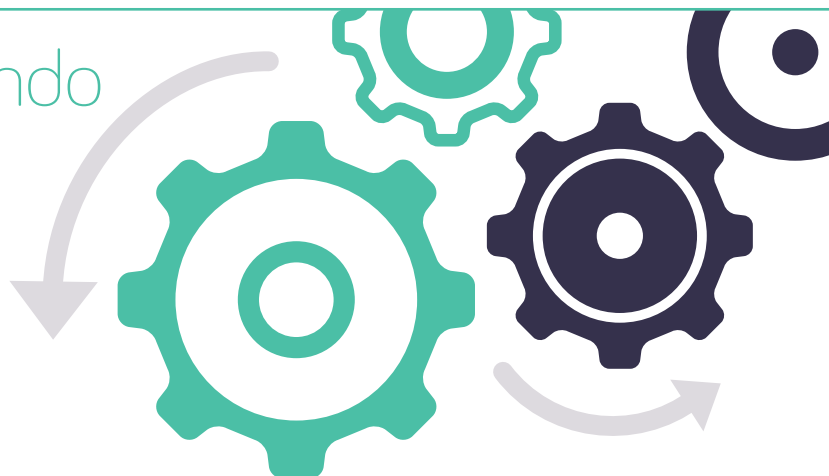
Vamos mostrar as forças que estão por trás da evolução rápida das arquiteturas de proteção de dados, as tendências em que você deve ficar de olho, o que todos devemos exigir das arquiteturas de próxima geração e o panorama atual do mercado.

Não se preocupe. O setor está bastante movimentado atualmente, mas vamos explicar tudo para você.

Sumário

- Capítulo 1: [O que está provocando a mudança das arquiteturas atuais?](#)
- Capítulo 2: [Tendência importante: appliances de proteção de dados de uso específico](#)
- Capítulo 3: [Tendência importante: appliances de failover e gateway para a nuvem](#)
- Capítulo 4: [Tendência importante: tecnologia unificada de proteção de dados](#)
- Capítulo 5: [Tendência importante: licenças com tudo incluído](#)
- Capítulo 6: [Requisitos da arquitetura de próxima geração](#)
- Capítulo 7: [O panorama atual do mercado](#)
- Capítulo 8: [Como encontrar a solução certa de próxima geração](#)
- Capítulo 9: [Arcserve UDP](#)

O que está provocando a mudança das arquiteturas atuais?



Para prosperar atualmente, os fabricantes de soluções de proteção de dados como a Arcserve não podem parar de inovar para ajudar os clientes a gerenciar um grau de complexidade cada vez maior.

Quais são as pressões sobre o mercado?

Até pouco tempo atrás, não havia uma solução única para proteção de dados, desduplicação e recuperação. Os departamentos de TI eram obrigados a usar diversas soluções pontuais, de vários fabricantes, o que criava ambientes que eram por natureza mais complexos e exigiam mais esforço para gerenciar.

Sem dúvida, essas situações também resultavam em uma proteção de dados inconsistente.

Agora, pense na ampla adoção de virtualização e de aplicativos de negócios com várias camadas, cada um com o próprio esquema complexo de proteção de dados. É o suficiente para fazer você ficar um pouco tonto.

Quer mais? E a opinião pública, cada vez mais preocupada com a perda de dados?

Nesse cenário, [perdas de dados amplamente divulgadas](#) têm um impacto enorme na lucratividade dos negócios e na confiança do consumidor. Com isso, os departamentos de TI são obrigados a demonstrar uma conformidade rigorosa e uma organização de dados à diretoria, a comitês e a investidores, mesmo sem ter uma previsibilidade de recuperação consistente nem a capacidade de medir os principais indicadores de desempenho que devem relatar.

Como se não bastasse, os departamentos de TI agora também precisam lidar com a consumerização da TI, trabalhando com recursos limitados.

Isso tudo pode parecer um desafio impossível de superar.

Mas não é.

Uma mudança está chegando. Já era hora.



No que se refere à entrega de serviços, a TI de hoje é interdependente em termos de sistemas e aplicativos.

Os fabricantes que identificaram essa oportunidade de balançar o mercado estão revendo suas práticas de proteção de dados e fazendo as mudanças fundamentais necessárias para alinhar seus produtos a elas. Além disso, seus produtos de próxima geração vão oferecer aos clientes mais capacidade de medição, maior usabilidade e recursos de recuperação aprimorados.

Em quais tendências atuais e futuras você deve ficar de olho?

Tendência importante: appliances de proteção de dados de uso específico



Os dias em que era preciso comprar, instalar e configurar softwares de backup em seus servidores estão cedendo lugar a uma nova tendência, que promete apresentar um caminho mais simples e direto para a proteção de dados.

Essa tendência são appliances físicos de uso específico, que foram pré-configurados com softwares de proteção e recuperação de dados.

Esses appliances estão em alta atualmente.

📖 Não somente 64% das empresas usa um appliance de backup de uso específico em seus ambientes hoje, como outros 29% ou 'planeja' ou 'tem interesse em fazê-lo no futuro próximo'. 📖

– Jason Buffington, analista sênior, Enterprise Strategy Group

O que está aumentando a demanda por appliances físicos?

A resposta é **simplicidade**.

Essas soluções simplificadas facilitam a definição de preços, a compra, a configuração e a implantação da arquitetura de proteção de dados. Isso significa que as pequenas e médias empresas são capazes de usar recursos de proteção de dados avançados sem precisar de departamentos de TI com orçamentos enormes. As soluções podem ser colocadas em operação rapidamente. Esse fato aumentou bastante

a velocidade de aquisição e implantação de infraestruturas de proteção de dados. Na verdade, de acordo com dados [publicados pela IDC*](#), as empresas gastaram US\$ 3,26 bilhões em appliances de backup de uso específico em 2014.

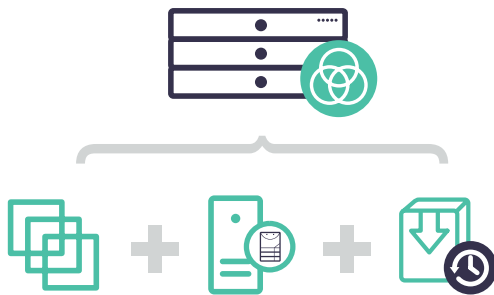
* International Data Corporation (20 de março de 2015). Worldwide Purpose-Built Backup Appliance (PBBA) Market Revenue Breaks the \$1 Billion Mark in the Fourth Quarter, According to IDC [Press release]. Consultado neste [link](#).

A evolução dos appliances físicos de proteção de dados

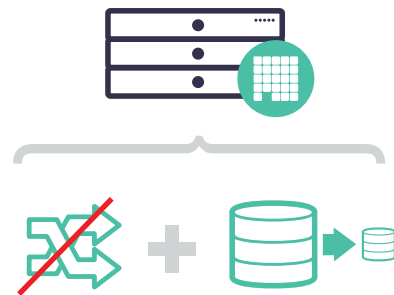
Até pouco tempo atrás, se você comprasse um appliance de backup de uso específico (PBBA, purpose-built backup appliance) tradicional, você receberia um pacote com softwares e hardwares adaptados, nada mais que uma solução posterior sem um design elegante, eficiência e facilidade de uso.

Agora, o mercado está evoluindo para soluções que foram projetadas levando em consideração os appliances físicos desde o início.

Entre esses appliances estão:



Appliances de backup integrados que têm compatibilidade nativa com vários aplicativos e vêm tanto com software de backup quanto com um servidor.

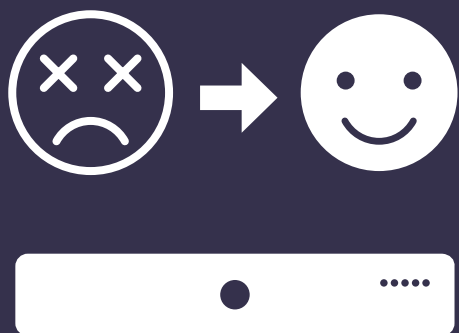


Appliances de deduplicação no destino ou na origem (os mais eficientes), que eliminam os dados duplicados e compactam os restantes, reduzindo o volume total de dados que precisa ser protegido.

Geralmente, os appliances de deduplicação são usados em conjunto com appliances de backup para reduzir os dados de forma impressionante. Contudo, estão sendo lançadas no mercado novas opções que trazem recursos integrados de backup e deduplicação em um só appliance.

Entre os appliances físicos de proteção de dados também estão os de failover e de gateway para a nuvem, embora essas duas opções de nuvem possam ser vistas como uma tendência separada. Por isso, vamos abordá-las com mais detalhes no próximo capítulo.

Tendência importante: appliances de failover e gateway para a nuvem



Quando os profissionais do setor de TI falam sobre appliances de proteção de dados de uso específico, eles geralmente se referem a appliances tradicionais de backup. É assim que o mercado tem se comportado há algum tempo.

No entanto, com o crescimento explosivo dos dados, a expansão dos recursos de nuvem e a expectativa dos usuários corporativos por acesso aos dados a qualquer momento e em qualquer lugar, duas novas categorias relacionadas à nuvem entraram em cena, e representam a direção na qual o mercado está apontando.

Essas categorias são os appliances de failover de backup/recuperação de desastres e os appliances de gateway para a nuvem.

Que valor essas novas categorias agregam à sua infraestrutura de proteção de dados?

	Tradicional	Ofertas novas
Solução simplificada	Appliances de backup	Appliances de failover de BC/DR Agilidade
Alimentado por outros softwares	Appliances de armazenamento com deduplicação Extensível para a nuvem	Appliances de gateway para a nuvem Eficiência Nativo na nuvem

Fonte: "Data Protection Appliances are better than PBBAs", Jason Buffington, Enterprise Strategy Group, 2014

Appliances de failover de backup/recuperação de desastres

Se o seu trabalho é andar na corda bamba da recuperação de dados, pense nos appliances de failover de backup/recuperação de desastres como sua rede de segurança.

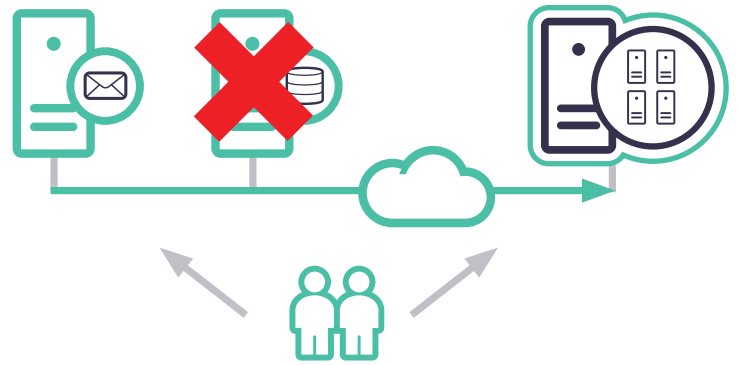
Esses novos appliances de failover integram software e hardware feitos especialmente para oferecer alta disponibilidade.

Eles geralmente são implantados localmente na empresa e em locais secundários, para que, no caso de um evento de perda de dados ou de falha nos sistemas, seja possível levantar uma máquina virtual ou um serviço no appliance, reduzindo tanto o tempo de inatividade quanto a perda dos dados.

Além disso, o backup e a recuperação dos seus aplicativos e dados mais importantes são feitos de forma tão transparente que os usuários finais nem saberão que foram redirecionados a um local de recuperação de desastres.

Esses appliances de failover oferecem um alto grau de automação do processo de recuperação de dados, o que é bem-vindo, além de geralmente trazer mais recursos para administradores de TI e provedores de serviços gerenciados que trabalham com acordos de nível de serviço (SLAs).

Em suma, se seu objetivo de tempo de recuperação é de alguns segundos, esse tipo de ambiente de recuperação de desastres é essencial.



Appliances de gateway para a nuvem

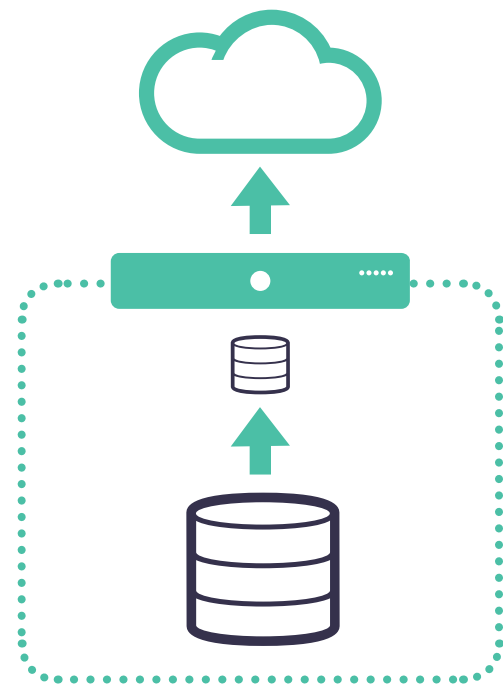
Os appliances de gateway para a nuvem são muito mais do que uma via de dados para seu MSP ou serviço de nuvem, seja ele público ou privado. Eles são feitos e otimizados para replicar seus dados para a nuvem.

Mas qual é o benefício?

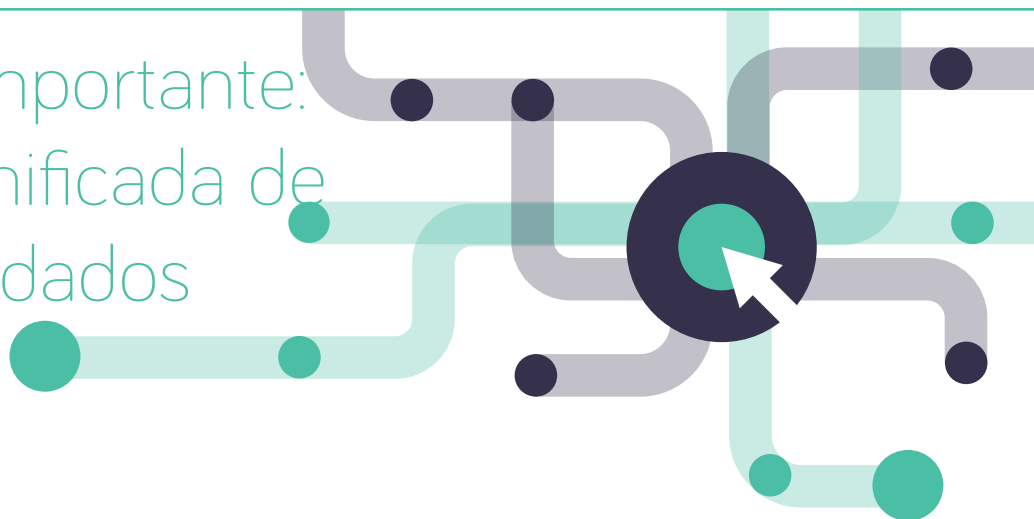
Embora haja diferenças entre os gateways para a nuvem, eles podem oferecer alguns ou todos os recursos a seguir:

- Criptografia integrada, garantindo a segurança dos dados
- Armazenamento local (mesmo que limitado), oferecendo acesso imediato a backups recentes guardados em cache no appliance
- Desduplicação, reduzindo o volume de largura de banda necessário para replicar os dados para o serviço de nuvem e proporcionando grande economia de custo

Não há dúvida: à medida que mais empresas levam seus dados para a nuvem, esses appliances são cada vez mais requisitados.



Tendência importante: tecnologia unificada de proteção de dados



A Marinha dos EUA acertou em cheio quando elaborou seu princípio de design “Keep it simple, stupid” (“Não complique, imbecil”).

Infelizmente, as tecnologias de proteção de dados não aderiam a esse princípio até há pouco tempo. Mas o que queremos dizer exatamente com proteção de dados **unificada**?

Estamos falando basicamente de uma solução única e leve, que não apenas ofereça toda a funcionalidade de que você precisa para ambientes físicos e virtuais, mas que também tenha sido projetada desde o início levando em consideração esse objetivo.

O que está gerando a demanda pela tecnologia unificada de proteção de dados?

Até pouco tempo atrás, a proteção de dados exigia um arsenal de produtos de nicho para gerenciar o crescimento explosivo dos dados e a consumerização da TI, com produtos que não interagiam entre si e resultavam em silos inflexíveis de dados.

Apesar de essa combinação de soluções poder atender às necessidades de uma empresa por um tempo, à medida que outras soluções de nicho fossem acrescentadas à mistura, com a mudança das necessidades e aumento dos níveis de serviço, veríamos o surgimento de um monstro de Frankenstein.

Isso também representava um desafio especial para as pequenas e médias empresas.

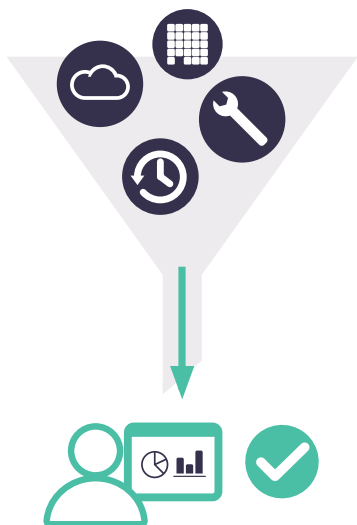
As grandes corporações contam com um pool de talentos de TI, que podem usar ao buscar conhecimento especializado a respeito de tarefas e tecnologias específicas de proteção de dados. Contudo, as pequenas e médias empresas não têm o luxo de usufruir de departamentos e orçamentos enormes de TI.



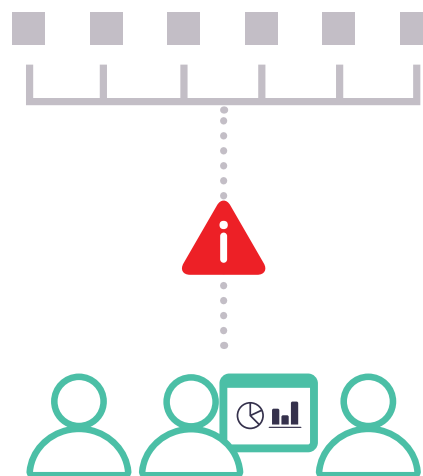
Elas precisam de funcionários generalistas de TI que, agora, graças à facilidade de uso das tecnologias unificadas de proteção de dados e de um único painel de gerenciamento, são capazes de implementar recursos avançados de proteção de dados, sem precisar de especialização.

Abordagens de fabricantes em relação às tecnologias unificadas de proteção de dados

Se você pesquisar um pouco, verá que os fabricantes geralmente adotaram uma de duas abordagens principais para o “estilo” da sua tecnologia de proteção de dados:



Alguns aproveitam elementos de suas tecnologias fundamentais de backup, deduplicação, gateway para a nuvem e recuperação, e os reescrevem para criar uma nova solução que seja unificada tanto no front end quanto no back end. O resultado é um produto leve e integrado, que faz tudo o que você precisa em um só lugar e apresenta uma experiência simplificada de gerenciamento.



Outros juntam pacotes de produtos complementares de backup e recuperação já conhecidos, sendo acessados por um único portal de gerenciamento. Embora com essa abordagem os usuários possam escolher entre um número maior de aplicativos e acessá-los em um só local, o resultado é um sistema inchado, que nem sempre permite uma integração perfeita e a automação de funcionalidades, além de exigir mais recursos para gerenciar.

É importante lembrar que essa tendência ainda está no início e que o grau de integração da tecnologia e de maturidade das interfaces de gerenciamento está em vários estágios de desenvolvimento, portanto você deve ter bastante atenção na sua pesquisa.

Tendência importante: licenças com tudo incluído



Licenças com tudo incluído:
mito ou realidade?

Esta tendência pode estar sendo exagerada. Na verdade, apenas um número pequeno de soluções realmente trazem licenças com tudo incluído, embora o mercado esteja começando a mudar nessa direção.

Por quê?

Basicamente, porque os preços são confusos. Com o desejo dos fabricantes de reduzir a confusão dos clientes e de oferecer uma experiência mais positiva, eles estão fazendo a mudança.

Quais opções de licenças de software com tudo incluído você pode encontrar?

Onde essas licenças estão disponíveis, elas podem usar como base:

- O número de servidores ou soquetes
- Terabytes de dados protegidos

Além disso, quando as licenças dependerem da capacidade, essa capacidade ainda pode ser detalhada como os dados protegidos antes ou depois da desduplicação, o que pode influenciar diretamente o custo.

Ainda assim, essas estruturas de preços ajudam a eliminar a ambiguidade e a fornecer rapidamente uma noção do que você precisará pagar pela solução de que precisa.

E as licenças sem restrições?

Elas ainda existem, mas são raras. Além disso, o fabricante talvez não seja capaz de fornecer a capacidade que você deseja com a estrutura de preços de que precisa, portanto é importante ficar atento para não cair em uma economia falsa.

O que você encontrará com mais frequência no mercado?

Os fabricantes costumam oferecer licenças de pacotes dos seus recursos mais populares, acrescentando outras funcionalidades como complementos. É um custo que muitas vezes é alto e passa despercebido. Nessa situação é muito mais difícil determinar o preço final.

Está avaliando appliances de backup com desduplicação?

Em alguns casos, você pode ter que pagar taxas extras por recursos como criptografia, replicação e aceleração do backup. E, em alguns casos específicos, até o algoritmo ou software de desduplicação é um complemento pago. Não é o que você esperaria de um pacote com "tudo incluído".

Está pesquisando appliances de backup integrados que vêm com licenças de software?

Muita atenção. [De acordo com o DCIG*](#), apenas pouco mais de 20% dos appliances integrados vêm com todos os recursos e funcionalidades de que você precisa. É verdade, eles vêm com um software de desduplicação e um console, mas você precisa examinar a fundo para descobrir se sua licença também inclui replicação, criptografia e softwares de agentes de sistemas operacionais, ou se esses recursos representarão custos extras.

Faça uma pesquisa

Independentemente do tipo de licença oferecido (limitada ou com tudo incluído), examine com cuidado e mantenha a mente aberta, pois a melhor opção de licença para sua empresa pode não ser a que você achava à primeira vista.

Falando em examinar com cuidado, você não pode deixar de ler **todos** os detalhes dos contratos.

* Arcserve (17 de dezembro de 2014). Trends in Data Protection with DCIG [Webinar]. Consultado neste link

Requisitos da arquitetura de próxima geração

A proteção de dados está cada vez mais complexa, e algumas soluções no mercado se tornaram obsoletas. Como você pode ter certeza de que não vai comprar gato por lebre?

As arquiteturas de proteção de dados de próxima geração são um ótimo lugar para começar. Quando cumprem suas promessas, elas facilitam seu trabalho e impressionam a todos. Elas também devem ser acessíveis e oferecer uma alta capacidade de dimensionamento e abrangência de recursos.

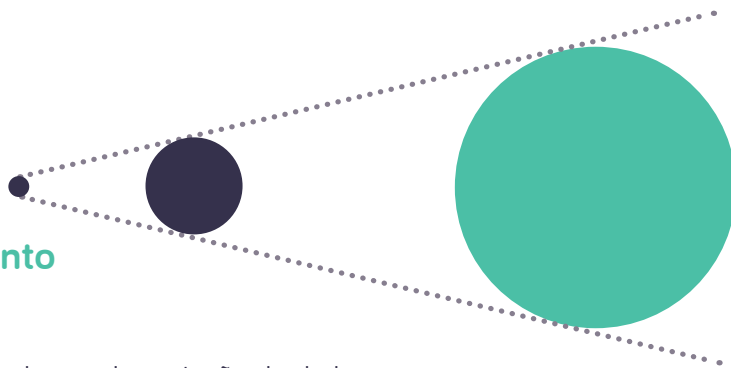
O que você deve esperar da evolução dessas soluções?

Abrangência da solução

As arquiteturas de próxima geração fornecem todas as tecnologias básicas de proteção de dados de que você precisa em uma só solução, como:



Atualmente, são poucos os fabricantes capazes de oferecer soluções robustas assim.



Capacidade de dimensionamento da solução

Esperamos muito mais das arquiteturas modernas de proteção de dados.

Elas devem não apenas se adaptar para atender a volumes maiores de dados, mas também devem manter acordos de nível de serviço de desempenho de janelas de backup, objetivos de ponto de recuperação (RPO) e objetivos de tempo de recuperação (RTO). Além disso, também devem ser flexíveis o suficiente para funcionar com diversas plataformas, seja disco ou fita, na empresa ou fora dela, no appliance ou na nuvem.

As empresas crescem, se fundem e são compradas, e suas arquiteturas de proteção de dados devem ser modulares e flexíveis o suficiente para permitir uma expansão, sem deixar a desejar no desempenho.

O que isso significa em termos leigos?

Você pode começar com um software de proteção de dados que você mesmo instalou, comprar um appliance depois que sua empresa crescer e, por fim, transferir alguns de seus dados para a nuvem, com a evolução da empresa.

Com uma solução com alta capacidade de dimensionamento você será capaz de fazer tudo isso, quando e onde precisar.

Facilidade de uso da solução

As arquiteturas modernas de proteção de dados devem não apenas ser simples de implementar, como também devem ser fáceis de usar. As soluções que não conseguirem oferecer um grau de simplicidade adequado serão ultrapassadas por produtos concorrentes que consigam.

Procure soluções que:

- Permitam a unificação de várias tecnologias de uma maneira fácil de configurar
- Possibilitem a criação de planos com base nos indicadores chave dos seus RPOs e RTOs, de forma simplificada
- Deixem tarefas e fluxos de trabalho complexos ocorrer sem precisar de intervenção
- Ofereçam a capacidade de ajustar detalhes dos recursos

Preço da solução

Houve uma época em que apenas as corporações eram capazes de bancar esse nível de proteção de dados e de capacidade de recuperação. Na verdade, há apenas dois anos, os consoles de gerenciamento unificado e a deduplicação eram recursos exclusivos das grandes empresas.

Isso mudou.

Hoje, as tecnologias de proteção de dados são flexíveis o suficiente para ser implantadas de diversas formas, otimizando a eficiência operacional e o custo, com licenças acessíveis.



O panorama atual do mercado

Avaliamos o panorama atual do mercado e concluímos que ele está carente.

A proteção de dados pode ter começado com software, mas evoluiu e agora possui infraestruturas híbridas com grande demanda de appliances e o surgimento da nuvem como destino.

Essa evolução teve como resultado a obsolescência de alguns produtos. Alguns com licenças caras, outros incapazes de medir ineficiências em processos. Há ainda os que não conseguem ser ampliados ou deixam a desejar na usabilidade. E outros que são soluções de nicho que devem ser combinadas com outras para oferecer a proteção de dados e a capacidade de recuperação robustas de que você precisa, embora aumentem o grau de complexidade com que você tem que lidar.

Em cada caso, essas soluções limitam sua capacidade de oferecer um serviço de TI consistente e de alta qualidade aos usuários finais.

Como um fabricante pode oferecer uma solução que seja verdadeiramente de próxima geração?

Para começar, isso significa deixar de lado o software legado e a adaptação de soluções anteriores.

Os fabricantes interessados no futuro estão analisando o panorama atual da proteção de dados como um todo e criando novas tecnologias integradas que são flexíveis e podem ser adaptadas e configuradas.

O que o mercado oferece hoje?

Se estiver pronto para procurar uma solução, esteja avisado: é um campo vasto, e nem todos os fabricantes começaram a alinhar suas soluções às novas e importantes demandas.

Hoje:



22

fabricantes oferecem 26 soluções de software de backup de servidores virtuais



10

fabricantes oferecem 47 appliances de backup com desduplicação



14

fabricantes oferecem 72 appliances de backup integrados

E esses números nem levam em consideração os appliances de backup integrados e com desduplicação que também estão disponíveis como appliances virtuais.

Embora existam muitos fabricantes, há alguns líderes claros no setor.

Eles são:

- Arcserve® UDP
- CommVault® Simpana®
- Dell® AppAssure
- Symantec Backup Exec™
- UniTrends™
- Veeam®

Com tantos fabricantes oferecendo soluções no mercado, pode ser difícil encontrar a solução perfeita para você.

Ainda assim, é algo que vale a pena tentar.

Quando você encontrar uma arquitetura de próxima geração que seja abrangente, e ofereça capacidade de dimensionamento e facilidade de uso, você estará mais que equipado para atender a seus desafios relacionados a dados e aumentar a eficiência.

Como encontrar a solução certa de próxima geração

Quando você leva em conta a variedade de opções disponíveis no mercado e avalia os recursos e a funcionalidade de cada uma, fazer uma comparação se torna uma tarefa penosa.

Essa tarefa fica ainda mais complicada quando os fabricantes não são muito claros sobre quais recursos estão incluídos ou não no preço anunciado.

Com isso, o que você deve levar em consideração ao avaliar suas opções?



Ignore as avaliações exageradas e determine com quais recursos você pode contar.

? Pergunte:

- A solução está disponível como appliance físico ou virtual? Ou ambos?
- A solução oferece um console de gerenciamento unificado?
 - Se oferecer, em que etapa do processo de desenvolvimento o fabricante se encontra?
 - Como é a integração do console com os diversos appliances que você terá que gerenciar?
 - Antes de assinar um contrato, faça um teste de integração ou veja uma demonstração para assegurar que a solução cumpra as promessas do fabricante.
- A solução oferece um appliance de gateway para a nuvem, permitindo backup, armazenamento e recuperação de dados na nuvem?
- Se a solução possuir desduplicação, ela acontece no destino ou na origem? Ou em ambos?
- A solução oferece appliances de failover de backup/recuperação de desastres e restauração imediata?

Quando se trata de licenças, é fundamental ler todos os detalhes com muita atenção.

? Faça perguntas como:

- A licença tem tudo incluído? Se tiver, o fabricante pode cumprir o que promete?
- A licença do fabricante corresponde a um conjunto de recursos mais limitado? Nesse caso, qual o preço final depois de acrescentadas todas as funcionalidades especializadas de que você precisa?



O que você deve levar em consideração?

Você deve dar atenção especial aos fatores que as arquiteturas de proteção de dados de próxima geração devem oferecer.

Eles são:

- **Abrangência da plataforma:** uma solução que traz tudo o que você precisa em termos de proteção de dados
- **Tecnologias unificadas:** integração perfeita, eliminando silos de dados impenetráveis
- **Virtualização:** máquinas virtuais que podem ter vários sistemas operacionais e aplicativos em um só servidor físico
- **Facilidade de uso:** design focado no usuário, capaz de permitir que um funcionário de TI sem especialização possa implantar e gerenciar a solução
- **Failover/recuperação a partir do zero imediatos:** alta disponibilidade e recuperação de desastres que asseguram a continuidade dos negócios
- **Replicação:** maior tolerância a falhas através de uma replicação de dados automatizada
- **Fita/arquivamento:** compatível com replicação para fita, para maior confiabilidade
- **Redução de dados:** deduplicação no destino ou na origem (mais eficiente), que reduz o volume total de dados a serem protegidos
- **Serviço de nuvem:** capacidade aprimorada de transferir dados para a nuvem e gerenciá-los

Quer saber como os pesos pesados se saem?

	Arcserve UDP7000	CommVault	Dell	Symantec Backup Exec 2014	Unitrends	Veeam
ABRANGÊNCIA DA PLATAFORMA						
Unificada						
Virtualização						
Facilidade de uso						
Failover/recuperação a partir do zero imediatos						
Replicação						
Fita/arquivamento						
Redução de dados						
Serviço de nuvem						

Nenhum
 Básico
 Médio
 Avançado
 Ótimo

Fonte: Arcserve

Claro que nenhuma solução é perfeita para todas as empresas, portanto tenha em mãos os requisitos da sua arquitetura e investigue com calma e cuidado para encontrar a solução certa para você.

Arcserve UDP

É a sua reputação que está em jogo. Você quer deixá-la à mercê do acaso?

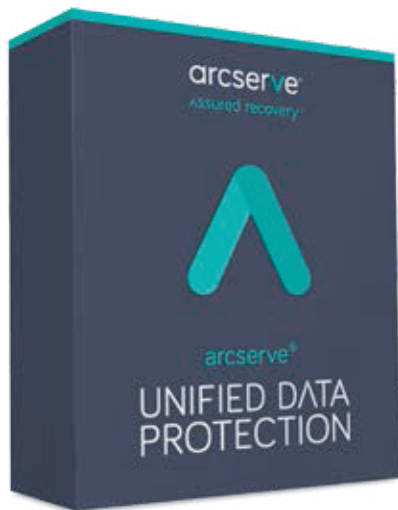
O Arcserve UDP é o primeiro appliance de proteção de dados completo do setor, com o recurso Assured Recovery™ e compatibilidade nativa com a nuvem.

📖 Como parte de um provedor de serviços gerenciados que lida com recuperação de desastres, eu fico mais tranquilo sabendo que as empresas dos meus clientes contam com a proteção de dados do appliance UDP. 📖

– Ian Richardson, CEO, Doberman Technologies

Quais as vantagens para você?

O Arcserve UDP alivia algumas das pressões do seu trabalho com benefícios como:



- ✓ **Uma arquitetura simplificada de proteção de dados e recuperação e um console de gerenciamento unificado e simplificado**
- ✓ **Melhora drástica da proteção dos dados e sistemas e das operações de recuperação, se compararmos com as soluções pontuais legadas**
- ✓ **Eficiência operacional amplamente melhorada e redução do custo**



O que o Arcserve UDP oferece?

O Arcserve UDP já vem com uma arquitetura simplificada de software e appliance de proteção e recuperação de dados, com backup, replicação e deduplicação global verdadeira. Além disso, é a solução de proteção de dados com imagens mais integrada do mercado.

O Arcserve UDP também oferece:

- ✓ Um appliance de failover de backup/recuperação de desastres de alta disponibilidade, com capacidade para três máquinas virtuais em standby
- ✓ Recursos nativos de software e appliances para nuvem que permitem a replicação de dados para serviços de nuvem públicos e privados, e também MSPs
- ✓ Proteção de servidores virtuais e físicos, **sendo a única solução unificada de software e appliance no mercado que oferece essa funcionalidade**
- ✓ Um console avançado de gerenciamento unificado de softwares e appliances
- ✓ Software que possibilita o teste automatizado da recuperação de sistemas, aplicativos e dados críticos, tudo isso sem nenhuma paralisação na empresa nem impacto nos sistemas de produção
- ✓ Licenças de software com tudo incluído, de acordo com soquetes de CPU (físicos ou virtuais) ou com terabytes de dados protegidos
- ✓ Uma arquitetura dimensionável, capaz de crescer quando você trabalha com o appliance e o software juntos

Como se não bastasse, a solução também é fácil de usar e implantar. Ela é tão simples que você pode tirar o appliance da caixa e implantá-la em 15 minutos.

 Como um cliente Arcserve de longa data, estou realmente impressionado com esta nova geração de appliance. Não sou da TI e consegui configurar o appliance Arcserve UDP sozinho. É fácil de implantar e possui vários recursos, como a deduplicação, que é muito eficiente. 

– Gary Hirschfield, diretor de administração, Sunrise Capital

A verdade é que seu trabalho está longe de ser simples, mas agora você pode ficar mais tranquilo. Por quê? Porque o Arcserve UDP é exatamente isso. Simples. Aproveite essa simplicidade para relaxar um pouco e sair da frente do monitor. Parabéns pela liberdade que você acabou de ganhar.