Apresentação da Solução

O Portfolio Spectrum Data Protection da IBM é 'imperdível'

Data: Outubro de 2017 **Autores:** Jason Buffington, Analista principal e Monya Keane, Analista de pesquisa sênior

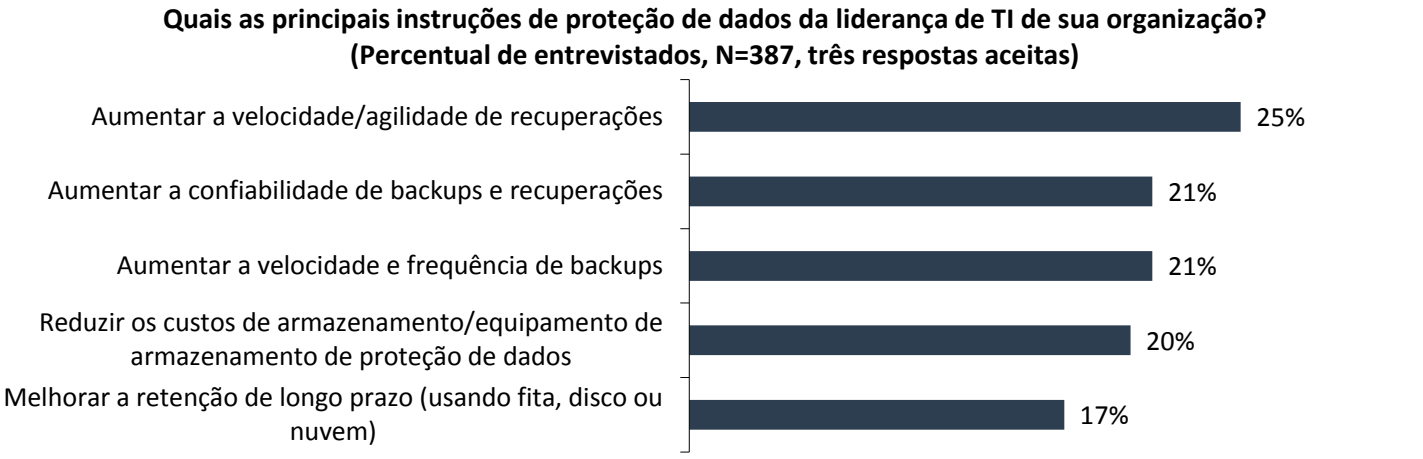
Resumo: As ofertas Spectrum Protect da IBM têm mais de 20 anos de conquistas na proteção e recuperação dos principais sistemas de TI.

Assim, é fácil supor que as novas ofertas de software Spectrum Protect Plus e Spectrum Copy Data Management simplesmente representassem o "Spectrum Protect com recursos extras". Essa suposição seria incorreta. Porém são independentes, abordagens reinventadas que visam resolver um desafio intimidador de TI –a proteção/recuperação da virtualização esperando alcançar um resultado de TI muito desejado, o gerenciamento e habilitação de dados eficaz (DM&E), muito conhecido também como "gerenciamento de cópia de dados" (CDM).

Introdução

Pesquisas do ESG demonstram que líderes seniores de TI estão dando instruções em suas organizações para simplesmente "*melhorar*" suas iniciativas de proteção de dados (ver Figura 1).[1]

Figura 1. Cinco principais instruções da liderança de TI para proteção de dados

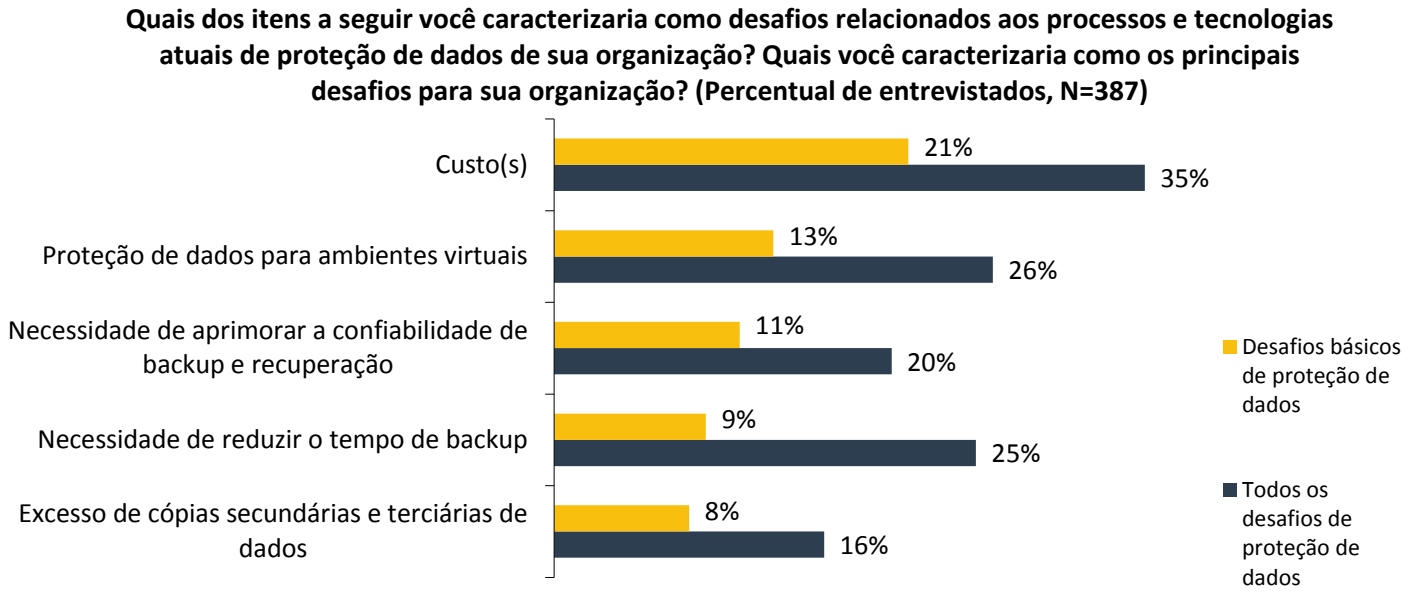


Fonte: Enterprise Strategy Group

[1] Fonte: ESG Research Survey, *2017 Trends in Data Protection Modernization*, dezembro de 2016.

Notadamente, os profissionais de TI encarregados da proteção de dados estão voltados para ações similares relacionadas à melhoria/redução, tentando ao mesmo tempo gerenciar os custos e desafios relativos à proteção e recuperação de ambientes virtualizados (ver Figura 2).[2]

Figura 2. Cinco principais desafios atuais relacionados a processos e tecnologias de proteção de dados



Fonte: Enterprise Strategy Group

Desafios modernos exigem soluções modernas

Em 2017, muitas organizações citaram o aumento do uso de virtualização de servidor e a melhoria do backup e recuperação de dados como áreas com investimento significativo para a modernização de data centers.[3]

Mas como mostram os dados citados na Figura 2, a virtualização cria desafios relacionados à proteção. Do mesmo modo, as muitas cópias de dados criadas no curso da busca de iniciativas de proteção e de não proteção também apresentam desafios.

Com tamanha pressão para reduzir custos de armazenamento e ao mesmo tempo aumentar a flexibilidade e agilidade de recuperação, seria fácil presumir erradamente, que as duas iniciativas estão sempre em conflito. É realmente possível atingir mais flexibilidade de recuperação e, ao mesmo tempo, reduzir os custos (ou aumentar o valor do negócio reconhecido a partir desses custos), o que é exatamente o que as organizações devem buscar agora:

- Mais capacidade de recuperação e confiança na virtualização.
- Gestão e habilitação de dados mais eficiente e mais econômica.

[2] ibid.
[3] Fonte: ESG Research Report, *2017 IT Spending Intentions Survey*, março de 2017.

Mais capacidade de recuperação e confiança na virtualização

Em 2017, não será mais uma simples questão de *se* você pode fazer um backup adequado de uma máquina virtual ou um conjunto de VMs hospedado em um host. Embora essa iniciativa tenha anteriormente sido considerada desafiadora, APIs de proteção de dados de hoje da VMware, Microsoft, e outros fornecedores de hipervisor fornecem agora mecanismos confiáveis para backup de qualquer VM.

O que permanece como uma verdadeira área de diferenciação é a capacidade de recuperar e alcançar *ampla* proteção em ambientes virtuais, um objetivo que normalmente ainda atormenta as organizações (ver Figura 3).[4]

Figura 3. Os dez principais desafios na proteção de um ambiente de servidor virtualizado

Fonte: Enterprise Strategy Group

Como mostra a Figura 3, o principal desafio para a proteção de dados específico da virtualização, segundo os entrevistados, permanece sendo a capacidade de recuperação dos dados (o que, na verdade, não deveria ser o caso, mas é). Também devem ser destacados os outros desafios citados com frequência: Como indicam as palavras destacadas na Figura 3, todos estão relacionadas de algum modo à *visibilidade*. Muitos desses desafios relacionados à visibilidade ainda existem porque algumas soluções de proteção de dados não têm simplesmente "experiência de virtualização". Em outras palavras, falta a elas instrumentação e conscientização contextual para serem capazes de demonstrar aos administradores de virtualização, administradores de operações de TI e outros stakeholders, a proteção e recuperação verdadeiras de seu ambiente virtual.

[4]Fonte: ESG Brief, *Reliable Virtualization Protection Continues to Elude Many Organizations*, outubro de 2017.

No futuro, as organizações apenas aumentarão seu nível de virtualização ainda mais. Assim, esses profissionais de TI afetados precisam buscar soluções modernas de proteção de dados, equipadas com instrumentação adequada e projetadas tendo em mente a agilidade de um ambiente altamente virtualizado.

Gestão e habilitação de dados eficiente e econômica (DM&E)

A chave para uma entrega efetiva do grande número de resultados de recuperação que as organizações exigem é desbloquear o valor comercial dos dados secundários. Quando a organização de TI desbloqueia esse valor, ela também pode justificar melhor os mecanismos de proteção em uso. Como mostram os dados apresentados na Figura 2, o custo, especialmente o de ter muitas cópias de dados, é um dos principais desafios enfrentados atualmente pelos profissionais de proteção de dados. Do mesmo modo, a redução dos custos relacionados a armazenamento é uma exigência básica da liderança de TI (ver Figura 1). A realidade conflitante para os profissionais de TI é que o nível de recuperação e agilidade que os stakeholders nas unidades de negócios exigem nem sempre pode ser atendido somente por backups.

Por essa razão, os administradores de proteção de dados, para atender os SLAs de suas organizações, se veem criando *mais* cópias (na verdade, uma gama mais ampla de *tipos* de cópias) via snapshots; réplicas e backups completos, incrementais e diferenciais. Na verdade, a natureza parcial e temporária dos snapshots combinada com a flexibilidade de replicação podem reduzir o armazenamento quando estes são gerenciados holisticamente e suportados por uma arquitetura de armazenamento moderna. Mas, sem essas integrações e uma estratégia complementar, a proteção do armazenamento pode aumentar como resposta a essas metas de recuperação, mesmo quando a administração executiva exige reduções de custo de armazenamento. Para agravar o problema, outras equipes de TI (isto é, desenvolvedores de aplicativos e pessoal de operação de TI) estão gerando ainda mais cópias para suportar seu próprio desenvolvimento e esforços no gerenciamento de correções.

Ao habilitar "cenários de não proteção" (como DevOps, relatórios ou análises) e, ao mesmo tempo, de forma cuidadosa o armazenamento é excluído, comprimido ou otimizado *e* utiliza-se mecanismos de proteção de dados mais inteligentes, uma organização pode realmente:

- Alcançar os resultados de recuperação e agilidade nos negócios.
- Estabelecer uma abordagem holística de longo prazo no gerenciamento e reutilização dos dados.
- Ser bem-sucedida sendo responsável e atendo-se ao orçamento de TI disponível.

Desse modo, qualquer organização empenhada em uma proteção de dados moderna deve buscar soluções que ofereçam uma gama abrangente de capacidades de recuperação e, ao mesmo tempo, desbloqueiem o valor comercial incremental habilitando casos de uso de não proteção.

Proteção abrangente com o portfólio de armazenamento definido por software da IBM

IBM e seu software Spectrum Protect (anteriormente conhecido como Tivoli Storage Manager ou TSM) têm sido inovadores líderes na proteção de dados empresariais por muitas décadas. Entretanto, poderia ser considerado um equívoco presumir que a oferta se tornou obsoleta como aconteceu com algumas soluções de backup antigas. O produto básico Spectrum Protect continuou a evoluir para atender às necessidades das empresas modernas e a IBM acaba de expandir seu portfólio de armazenamento com o IBM Spectrum Copy Data Management (Spectrum CDM) e o IBM Spectrum Protect Plus (SPP).

IBM Spectrum Copy Data Management

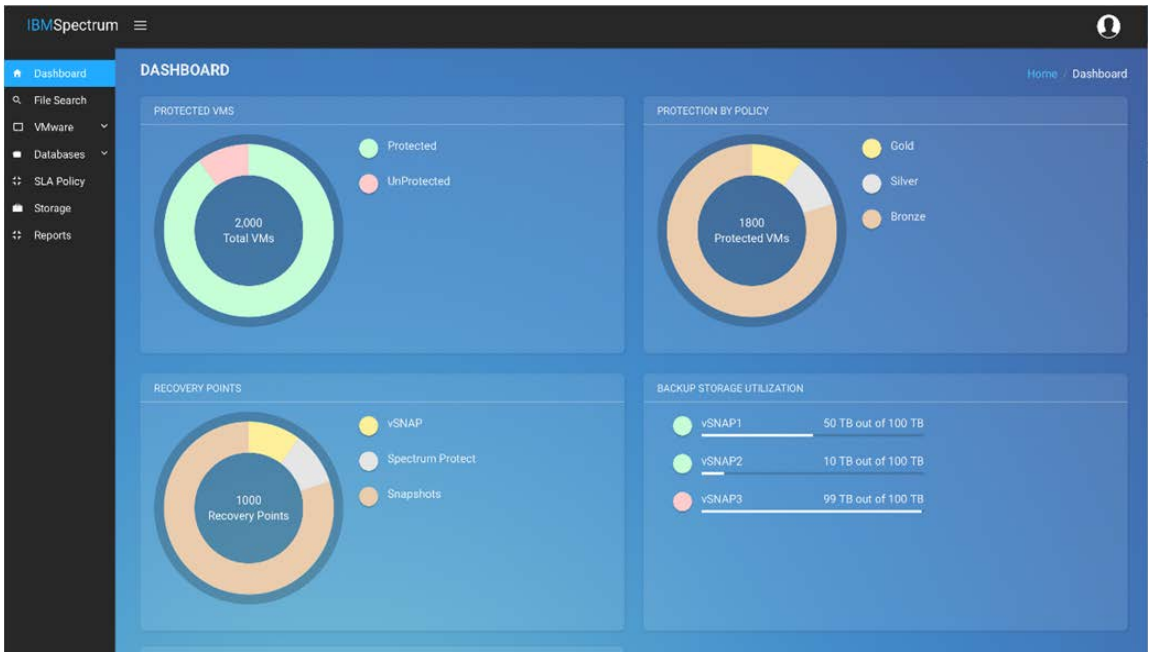
O Spectrum CDM é uma nova adição ao portfólio de proteção de dados IBM Spectrum. Ele foi projetado para permitir casos de uso de não- proteção para dados secundários, por exemplo, DevOps, testes de reparação e relatórios/análises.

Como acontece com outras (embora poucas) ofertas de gerenciamento de cópias de dados no mercado atual, o objetivo básico do Spectrum CDM é simplificar o acesso aos "dados de produção", sem comprometer, sobrecarregar ou alterar os conjuntos reais de dados de produção. Ao aproveitar os recursos do Spectrum CDM, funcionários das unidades de negócios, codificadores/desenvolvedores e muitos outros stakeholders estarão aptos a desbloquear valores comerciais incrementais a partir desses dados. E essa capacidade torna mais fácil para a organização com um todo justificar outros investimentos na moderna proteção e recuperação de dados.

IBM Spectrum Protect Plus

SPP foi projetado tendo em mente generalistas de operações de TI e administradores de virtualização. Ele oferece uma estrutura centrada em SLA para assegurar proteção e recuperação ágil de ambientes altamente virtualizados, tendo uma interface de usuário (ver Figura 4) elegante e contemporânea o bastante para surpreender os clientes fiéis da IBM.

Figura 4. IBM Spectrum Protect Plus–Reporting Dashboard



Fonte: IBM

Ele também possui a "experiência em virtualização" descrita anteriormente, onde as políticas SLA estão definidas pelo administrador de TI e depois simplesmente executadas em VMs ou hosts, conforme as necessidades da empresa.

Como era de se esperar, SPP e Spectrum CDM se integram com o software básico Spectrum Protect e com o restante do portfólio de armazenamento IBM, fornecendo assim uma maior agilidade nos negócios.

A grande verdade

A proteção de dados deverá continuar a evoluir se ela sempre estiver voltada para os desafios que muitas organizações estão enfrentando agora. Mas o interessante é que mecanismos de backup em separado e independentes – e até mesmo

administradores exclusivos de backup – provavelmente diminuirão sua importância à medida que os profissionais de TI aprofundem seu envolvimento na definição e implementação das estratégias de proteção de dados de suas organizações.

Com essa probabilidade em mente, as empresas com quase absoluta certeza continuarão a depender de amplos mecanismos de proteção de dados, como o IBM Spectrum Protect, ainda que busquem mecanismos adicionais acessíveis e criados para essa finalidade para seus trabalhos mais frequentes – mecanismos capazes de desbloquear valores comerciais incrementais apoiando uma estratégia de gerenciamento de dados mais ampla.

Considerando a maneira como essas tendências estão se desenvolvendo, é bom observar que a proteção de dados inovadora e de longa data da IBM continua a se expandir e enriquecer seu portfólio com ofertas adequadas a vAdmins e generalistas de TI. As etapas corretas estão sendo cumpridas para habilitar os casos de uso que as empresas de hoje exigem.