Projeto da Forrester Consulting
encomendado pela Veeam

Maio de 2020

Guia dos compradores de backup moderno

A adoção da nuvem está em ascensão, com mais de um terço das empresas adicionando infraestrutura/serviços baseados em nuvem e/ou migrando cargas de trabalho existentes para a nuvem (pública, privada ou hospedada) como estratégia principal para garantir objetivos e metas de negócios. Os tomadores de decisão de TI estão adotando uma abordagem de múltiplas nuvens para aproveitar serviços baseados em nuvem. Esses serviços complementam e podem estimular a reconsideração de estratégias mais amplas de proteção de dados para obter maior disponibilidade, backup/recuperação de dados e melhor desempenho de aplicações sensíveis à latência.

Com o aumento da adoção da nuvem, mais empresas veem a necessidade de modernizar suas plataformas de backup e proteção de dados a partir de várias perspectivas: uso da nuvem como destino de armazenamento, proteção de dados e aplicações hospedadas na nuvem pública e proteção de dados consistente em ambientes híbridos. 80% dos tomadores de decisão estão ansiosos para lidar com os riscos relacionados à privacidade, segurança cibernética e integridade dos dados, mas com os ambientes de TI mudando tão rapidamente para a maioria das organizações, as empresas devem considerar vários atributos de qualquer nova solução de proteção e backup de dados, procurando garantir a proteção e a capacidade de recuperação das plataformas e serviços de produção em todo o ambiente, incluindo:

- Proteção abrangente.
- Recuperação em escala.
- Facilidade de gerenciamento.
- Automação e orquestração.
- Reutilização de dados e insights.
- Segurança.

Este guia fornece orientações sobre quais recursos procurar em cada uma dessas categorias e oferece questões que os tomadores de decisão de TI e de negócios devem se perguntar ao avaliar as necessidades específicas de suas empresas em relação às soluções de backup e proteção de dados.

FORRESTER®

Proteção abrangente: Continuidade dos negócios, heterogeneidade e amplo suporte à plataforma

Embora as empresas líderes de tecnologia tenham modernizado aplicações usando tecnologias nativas da nuvem, como infraestrutura como serviço (IaaS) e software como serviço (SaaS), elas ainda mantêm inúmeras tecnologias e plataformas locais que hospedam uma variedade de aplicações críticas. A heterogeneidade de aplicações e arquiteturas de dados cria requisitos complexos de proteção de dados que as empresas devem atender para proteger os negócios de qualquer crise.

Uma estratégia abrangente e heterogênea deve ser aplicada não apenas ao que as organizações protegem (físico, virtual, hospedado na nuvem), mas também ao local onde protegem seus dados (disco, fita, armazenamento de objetos). Além disso, as soluções de proteção de dados devem oferecer uma abordagem abrangente para backup, snapshots e replicação para conjuntos de dados de produção inteiros, permitindo flexibilidade para transportar esses conjuntos de dados facilmente entre plataformas, com base nas necessidades dos negócios.

Figura 1

34%

enfrentam dificuldades com o gerenciamento de dados em vários ambientes na nuvem

34%

não têm certeza de que podem proteger dados confidenciais/ privados, armazenados no local, com terceiros ou na nuvem*

Base: 206 tomadores de decisão de TI nos EUA, Reino Unido e Alemanha responsáveis por decisões de tecnologia de backup e recuperação de dados
Fonte: um estudo encomendado pela Veeam e realizado pela Forrester Consulting, dezembro de 2019
*Base: 3.741 tomadores de decisão de segurança de empresas de todo o mundo
*Fonte: Forrester Analytics' Global Business Technographics® Security Survey, 2019

Considerações técnicas e funcionais	Considerações organizacionais e operacionais
• Quais novas aplicações minha organização planeja implantar? Quais são as necessidades de proteção de dados de cada uma delas? • Como protejo as fontes de dados heterogêneas da minha organização? • Como protejo os dados armazenados em vários serviços SaaS que minha organização consome? • Que tipo de dados serão armazenados para cada aplicação? Qual nível de proteção e capacidade de recuperação cada um precisa? • Como posso melhorar meus backups e restaurações de armazenamento conectado à rede (NAS)?	• Como minha organização planeja utilizar as tecnologias em nuvem nos próximos um a dois anos? • Quais são os requisitos de tempo de atividade e retenção para todas as nossas aplicações? • Quais riscos de negócios minha empresa enfrenta à medida que os dados se espalham por vários ambientes em nuvem? Como meu licenciamento muda à medida que movemos cargas de trabalho entre plataformas e nuvens? • Quais partes da minha organização são ou serão dependentes dos dados que agora residem na infraestrutura ou nos serviços hospedados na nuvem?

O QUE PROCURAR EM UMA SOLUÇÃO

Procure uma solução que possa suportar infraestrutura virtualizada e física local, infraestrutura de nuvem pública e SaaS. À medida que as plataformas de plataforma como serviço (PaaS) crescem no uso da produção convencional, procure fornecedores de proteção de dados contemporâneos que incluam contêineres em sua estratégia e roteiro. Além disso, procure a capacidade de aproveitar diversas plataformas de armazenamento para ter snapshots e replicações na mesma estrutura de gerenciamento de proteção de dados. Procure ferramentas de proteção de dados que suportem cargas de trabalho modernas, incluindo NAS, sistemas de arquivos distribuídos, dados não estruturados e plataformas baseadas na nuvem, e que suportem recuperação granular para objetivo de tempo de recuperação (RTO) aprimorado.

OUTRAS CONSIDERAÇÕES

Os volumes de dados — estruturados e não estruturados, nativos na nuvem — estão crescendo rapidamente. Os profissionais de infraestrutura e operações (I&O) enfrentam pressão constante para alcançar e manter um equilíbrio de conformidade, custo e equação de velocidade. Considere uma combinação de técnicas de otimização de armazenamento e novas arquiteturas em sua lista para alcançar esse equilíbrio, incluindo armazenamento de objetos para ajudar a reduzir o custo, uma arquitetura em expansão para fornecer uma arquitetura resiliente e destinos de armazenamento em nuvem pública, que podem atender às suas necessidades de retenção a longo prazo.

FORRESTER®

Recuperação em escala: Confiabilidade de backup e restauração

As organizações devem manter cópias de seus dados, apesar do crescimento exponencial dos volumes de backup, considerando o tipo de dado, a frequência de backup e as necessidades de retenção de dados. As empresas devem manter os backups e outras cópias por anos, exigindo flexibilidade e adaptabilidade para gerenciar o armazenamento subjacente. Dependendo do estágio do ciclo de vida, as empresas podem ter que colocar dados em discos ou armazenamento de arquivos em nuvem pública.

Granularidade e velocidade são dimensões importantes das perspectivas de backup e recuperação. Dependendo da circunstância, as necessidades de recuperação vão desde recuperar algumas mensagens de e-mail ou um único arquivo até um data center inteiro. Em exemplos específicos, como a recuperação de ransomware, as organizações precisam estar atentas ao desenvolver uma estratégia de retenção que garanta a imutabilidade dos dados, bem como garantias de que não se deve reinfectar ambientes durante restaurações. As empresas devem otimizar as ferramentas de backup para reduzir os requisitos de tempo, custo e armazenamento e ainda atender aos níveis de serviço comprometidos e aos requisitos normativos. O ponto principal de qualquer solução de backup é a confiabilidade com que pode operar em diferentes situações e se suas recuperações podem atender às necessidades dos negócios.

Figura 2

22% relatam níveis de serviço inconsistentes em ambientes em nuvem

24% estão adotando a nuvem híbrida para aproveitar diferentes níveis de serviço/desempenho em diferentes plataformas na nuvem

26% citam a capacidade de aproveitar o armazenamento na nuvem para recuperação como um dos principais impulsionadores da adoção da nuvem híbrida

Base: 2.275 tomadores de decisão de infraestrutura de empresas de todo o mundo que estão implementando ou planejando implementar a nuvem híbrida
Fonte: Forrester Analytics' Global Business Technographics® Infrastructure Survey, 2018

Considerações técnicas e funcionais

- Quais opções de otimização de backup são aplicáveis correspondendo às minhas fontes de dados?
- Minhas técnicas atuais de otimização (custo e armazenamento) ainda se aplicam à implantação em nuvem ou híbrida?
- Minhas janelas de backup foram compactadas no passado, e como elas serão moldadas nos próximos dois a três anos?
- Quais processos eu tenho para verificar se meus dados são recuperáveis?

Considerações organizacionais e operacionais

- Como as expectativas de desempenho da minha equipe variam entre ambientes na nuvem e no local?
- Quais SLAs minha organização tem atualmente para proteção de dados?
- Minha organização não está apenas preparada para impedir ataques cibernéticos, mas também está adequadamente preparada para se recuperar de ransomware?
- Posso suportar uma recuperação em massa de uma paralisação em grande escala do data center?

O QUE PROCURAR EM UMA SOLUÇÃO

Encontre uma solução que escale bem para oferecer proteção e recuperação de dados com velocidade e confiabilidade. Procure uma solução que ofereça as técnicas de otimização corretas para tempo, custo e armazenamento. Sua solução deve ser igualmente adepta às opções de recuperação granular e de todo o local, proteger a restauração de dados de ransomware e outras invasões de malware e oferecer suporte a vários modos de recuperação, incluindo recuperações centradas em aplicações, específicas do usuário e em nível de arquivo. Procure uma solução que possa executar automaticamente testes de recuperação em segundo plano para garantir que a recuperação ocorra quando você realmente precisar.

OUTRAS CONSIDERAÇÕES

Com qualquer nova solução, as empresas buscam consistentemente o tempo mais rápido e nenhum aprisionamento ao fornecedor, mas esse caminho parece diferente para cada empresa com base no ambiente atual. Uma abordagem centrada em software fornece flexibilidade para escolher os melhores componentes da categoria. O surgimento de appliances de backup convergentes mostra interesse em soluções que combinam software de backup com hardware, pois os dispositivos podem ter um tempo de implantação mais rápido. Avalie seu ambiente atual e determine a combinação certa de software e hardware para sua organização para oferecer suporte à orquestração em todos os ambientes esperados.

FORRESTER®

Facilidade de gerenciamento: Uso e operações diárias que fornecem análises e insights operacionais

A TI atualmente gerencia várias tecnologias — vários sistemas de armazenamento, tecnologias de virtualização, bancos de dados e serviços em nuvem (IaaS, SaaS) — todos operando de maneiras distintas e exigindo diferentes métodos de proteção. As ferramentas de backup devem se integrar e oferecer suporte a esse portfólio diversificado de fontes de dados e repositórios em diferentes níveis.

O gerenciamento de operações de backup não deve aumentar a complexidade existente que os administradores de TI enfrentam hoje. O entendimento das características de integridade, desempenho e capacidade da infraestrutura de backup é fundamental para as operações diárias, planejamento de capacidade e estratégia operacional de longo prazo. Análise preditiva e resolução de problemas assistida são essenciais.

As equipes de TI precisam de sistemas de backup mais fáceis de gerenciar para reduzir a complexidade. 32% dos tomadores de decisão de tecnologia acreditam que a facilidade de uso aprimorada seria o principal fator para alterar/melhorar suas soluções de backup primário.

Figura 3

Base: 206 tomadores de decisão de TI nos EUA, Reino Unido e Alemanha responsáveis por decisões de tecnologia de backup e recuperação de dados
Fonte: um estudo encomendado pela Veeam e realizado pela Forrester Consulting, dezembro de 2019

Considerações técnicas e funcionais	Considerações organizacionais e operacionais
• Quantas ferramentas diferentes estou usando para proteger minhas diversas fontes de dados de produção? • Minhas ferramentas de backup operam de maneira diferente para origens e destinos diferentes, ou elas aumentam a complexidade? • Minhas ferramentas de backup atuais podem fornecer recomendações com base no desempenho histórico ou nas condições de status? • Qual é o meu nível de visibilidade nas operações de backup? Isso é suficiente?	• Tenho a capacidade ou o requisito de proteger, gerenciar e relatar todos os ativos em um único painel? • Tenho recursos dedicados, com o treinamento adequado, para gerenciar sistemas e operações de backup em escala? • Quais dados e relatórios operacionais estão disponíveis na solução de backup? • Posso usar efetivamente os relatórios para otimizar a proteção, backup e recuperação de dados? • Os relatórios da minha solução de backup melhoram minha capacidade de garantir a conformidade normativa e passar com êxito em minhas auditorias internas e externas?

O QUE PROCURAR EM UMA SOLUÇÃO

Procure soluções que ofereçam gerenciamento e relatórios globais usando um console operacional unificado para produzir relatórios abrangentes nos ativos protegidos heterogêneos e na infraestrutura de proteção de dados distribuída. Procure soluções que ofereçam visibilidade imediata ou permitam a criação personalizada de relatórios operacionais para se adequar ao seu ambiente específico. Os relatórios devem ser intuitivos para guiar os profissionais de TI e as equipes de conformidade/auditoria a executar ações de reparação, analisando as realizações históricas.

FORRESTER®

Automação e orquestração: Integração, proteção baseada em política e restaurações baseadas em fluxo de trabalho

As empresas estão gerando muito mais dados do que há apenas alguns anos. A tolerância ao tempo de inatividade ou à perda de dados reduziu drasticamente. Os requisitos normativos e a concorrência aumentaram a dependência e o rigor da proteção de dados pela TI. Os desenvolvedores de aplicações estão adotando rapidamente novas tecnologias que introduzem novas plataformas de produção para atendimento ao cliente em um ritmo nunca antes visto. Gerenciar todas essas alterações de maneira tradicional — um planejamento e execução manuais de tarefas de backup — quase certamente resultará em falhas de proteção que deixam as organizações expostas.

As organizações estão testemunhando mudanças rápidas em um mercado altamente competitivo, enquanto os usuários têm expectativas cada vez maiores. Para atender a essas demandas em evolução, as equipes de TI devem procurar soluções de proteção de dados orientadas por políticas que possam afetar as alterações automaticamente. As equipes de TI precisam de soluções modernas de proteção de dados que possam se integrar às ferramentas de orquestração de TI, para que os fluxos de trabalho possam executar tarefas de backup automaticamente. 58% dos entrevistados pesquisados classificam a proteção automatizada entre os cinco principais recursos que mais influenciam a escolha das soluções de proteção de dados de suas empresas.

Figura 4

Apenas 29% dos tomadores de decisão acham muito fácil automatizar e gerenciar SLAs de recuperação de dados em ambientes

37% relatam que as ferramentas de backup não têm gerenciamento baseado em políticas para automatizar tarefas

34% dos tomadores de decisão não acham fácil integrar ferramentas de backup com sistemas e processos existentes

Base: 2.275 tomadores de decisão de infraestrutura de empresas de todo o mundo que estão implementando ou planejando implementar a nuvem híbrida
Fonte: Forrester Analytics' Global Business Technographics Infrastructure Survey, 2018

Considerações técnicas e funcionais

- Quanto tempo minha equipe de TI gasta na configuração e no gerenciamento de planos de proteção de dados?
- Quais tarefas de recuperação podem ser orquestradas ou programadas? A interação humana pode ser reduzida à decisão única de "invocar" o(s) plano(s) de recuperação?
- Minhas tarefas de backup podem ser orquestradas por meus fluxos de trabalho mais amplos de gerenciamento ou provisionamento de sistemas?
- Meu plano de recuperação de proteção de dados pode ser testado usando a orquestração para obter consistência?

Considerações organizacionais e operacionais

- Estamos protegendo todas as nossas fontes de dados?
- Como minha organização garante salvaguardas de dados em tempo hábil?
- Qual é a eficácia dos planos e políticas atuais para atender às necessidades de negócios?
- Como sabemos quando nossos planos e políticas precisam ser alterados?

O QUE PROCURAR EM UMA SOLUÇÃO

Procure uma solução que ofereça automação integrada para tarefas de rotina como backup, restaurações/validações de teste e recuperações. Uma abordagem automatizada à proteção de dados deve relatar desvios das políticas de proteção ou deficiências de RTO/RPO para garantir a conformidade com as políticas corporativas de retenção e recuperação. Esses recursos devem estar disponíveis independentemente da heterogeneidade no(s) ambiente(s) de produção. Portanto, procure soluções que suportem a chamada de tarefas operacionais usando APIs REST, aproveitem fluxos de trabalho orquestrados para realizar tarefas repetitivas e garantir consistência, e que possam ser controladas por políticas.

FORRESTER®

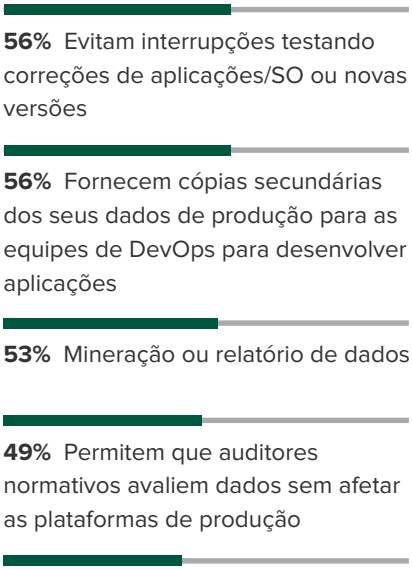
Reutilização de dados e insights: Uso de dados/infraestrutura de backup para necessidades de negócios, além de casos de uso de recuperação

As organizações devem investir na manutenção de cópias de dados para necessidades de negócios e normativas. Para muitas, o ROI de uma solução de backup moderna não vem apenas da garantia da capacidade de recuperação, mas também da capacidade de fazer mais, aproveitando os dados nos repositórios de backup para qualquer outro uso comercial, além da retenção ou recuperação "justa". Testes de desenvolvimento de aplicações, segurança de TI e verificações de conformidade são alguns dos casos de uso mais procurados pelas equipes de negócios fora da TI. 56% dos entrevistados relatam que suas organizações reutilizam dados de backup para testar patches de aplicações/SO ou novas versões. Uma porcentagem semelhante de entrevistados informa que fornece cópias secundárias dos dados de produção para equipes de teste de desenvolvimento para desenvolver aplicações e 53% dos entrevistados relatam usar cópias de backup para fins de mineração ou relatório de dados.

Para habilitar a reutilização de dados, as ferramentas de backup devem poder gravar segmentos de dados solicitados nos repositórios de backup. Elas devem permitir que aplicações de terceiros solicitem, consumam e gerenciem com segurança esses dados de teste.

Figura 5

"De que maneira sua organização reutiliza dados de backup?"



Base: 206 tomadores de decisão de TI nos EUA, Reino Unido e Alemanha responsáveis por decisões de tecnologia de backup e recuperação de dados
Fonte: um estudo encomendado pela Veeam e realizado pela Forrester Consulting, dezembro de 2019

Considerações técnicas e funcionais	Considerações organizacionais e operacionais
• Quais equipes internas poderiam utilizar o acesso secundário aos dados de produção e para quais finalidades? – Auditorias de conformidade? – Teste de desenvolvimento? – Teste de correção? – Cibersegurança? – Teste de penetração? • Posso satisfazer esses cenários de capacitação hoje e com que dificuldade ou regularidade?	• Tenho os processos alinhados que permitirão a reutilização de dados de backup? • Como vou abordar e garantir a segurança e a conformidade dos dados para esses casos de uso? • Quanto valeria (em ROI) para as outras equipes da minha organização poder aproveitar esses dados inativos para auditorias, testes, DevOps, etc.?

O QUE PROCURAR EM UMA SOLUÇÃO

Explore soluções que oferecem uma interface nativa padrão e/ou APIs padrão que ferramentas de terceiros ou scripts personalizados possam chamar para enviar as solicitações de dados. A solução deve ser capaz de extrair partes específicas dos dados. A segurança dos dados é obrigatória, tanto para permitir o acesso quanto para preservar a capacidade de recuperação dos dados. Procure maneiras automatizadas de criar "sandboxes" ou ambientes de teste semelhantes que permitam a reutilização off-line e isolada de dados desativados para fins secundários.

FORRESTER®

Segurança: Integração de backup e recuperação em uma estratégia abrangente de segurança cibernética

O ransomware é um risco global que as empresas enfrentam em termos de probabilidade de ocorrência e impacto. O ransomware é conhecido não apenas por criptografar os dados de produção, mas também por eliminar os sistemas de backup e as cópias de backup, ou seja, a última linha de defesa das vítimas. As organizações devem proteger os sistemas e dados como parte de suas estratégias de segurança cibernética. As empresas de setores regulamentados usaram cópias impenetráveis, sistemas de arquivos imutáveis e repositórios de armazenamento WORM (write-once, read-many) para garantir que os dados sejam inalteráveis. Os líderes de TI têm exercitado a prática de proteger as cópias de dados, movendo-as para locais remotos desconectados dos sistemas de produção. Agora, eles precisam garantir que os sistemas de backup não reintroduzam o malware restaurando acidentalmente as cópias infectadas.

Figura 6

consideram a segurança cibernética e privacidade ao desenvolver sua estratégia de tecnologia

têm fortes preocupações sobre ataques de segurança de agentes não estatais

enfrentam desafios de segurança ao usar várias plataformas em nuvem*

Base: 3.741 tomadores de decisão de segurança
Fonte: Forrester Analytics' Global Business Technographics® Security Survey, 2019
*Base: 2.515 tomadores de decisão de infraestrutura cujas empresas estão usando estratégias de nuvem híbrida
Fonte: Forrester Analytics' Global Business Technographics® Infrastructure Survey, 2019

Considerações técnicas e funcionais	Considerações organizacionais e operacionais
• Como protegerei minha solução de backup e recuperação e como evitarei que ela seja comprometida? • Como protegerei as cópias de backup de serem comprometidas ou excluídas? • Posso proteger a solução de backup adicionando autenticação multimétodo para tarefas que podem destruir as cópias de backup? • Durante a operação de recuperação, como posso ter certeza de que vestígios de ransomware não estão sendo (re)injetados nas instâncias recuperadas?	• Como trabalho com colegas de negócios e de segurança de TI para criar um plano mutuamente acordado que lide com riscos de ransomware? • Com que frequência devo testar a capacidade de recuperação? • Como as ferramentas de segurança de TI compartilharão inteligência com as ferramentas de backup?

O QUE PROCURAR EM UMA SOLUÇÃO

Verifique se há soluções de backup que fornecem inerentemente segurança multidimensional. Primeiro, descubra quais recursos a solução de backup tem para se proteger de acessos não autorizados, elementos nocivos e ataques de malware. Segundo, determine como o software de backup armazena e protege as cópias de backup. Dependendo da aplicação e do seu perfil de risco de dados, encontre uma solução que possa salvar dados de backup com requisitos de retenção específicos em um sistema de arquivos imutável a uma frequência definida. Um projeto meticuloso usando sistemas imutáveis aumentará a resiliência dos dados.[1] Você também deve procurar a autenticação multicamada para garantir que uma ação destrutiva não possa ser executada simplesmente obtendo acesso ao sistema. Pode ser um recurso nativo da ferramenta ou alcançado através da integração com outras ferramentas de segurança

FORRESTER®

Conclusão

À medida que as organizações distribuem cada vez mais suas aplicações e dados entre sistemas hospedados, públicos e locais para seus sistemas essenciais para negócios e missão, elas devem prestar muita atenção para garantir que os dados armazenados nesses sistemas sejam protegidos e adequadamente armazenados em backup. Isso não é pouco, pois os dados estão constantemente em movimento entre os sistemas locais e na nuvem e entre diferentes aplicações. O aumento do volume de dados, que continua a crescer sem sinais de desaceleração, apenas exacerba esse desafio.

Os líderes das equipes de TI devem avaliar cuidadosamente suas necessidades e requisitos de proteção de dados para garantir que eles tenham as ferramentas e processos certos para proteger e fazer backup de todos os seus ativos de dados. Sempre haverá mais dados a serem protegidos, mas sua capacidade de gerenciar operações de dados e extrair informações dos processos atuais para gerar melhorias é um fator fundamental para o sucesso. À medida que você e sua equipe consideram suas futuras arquiteturas de TI em um modelo de implantação distribuída que inclui vários serviços em nuvem e como deseja proteger seus dados daqui para frente, faça a si mesmo as principais perguntas destacadas nas várias seções deste documento para entender exatamente o que sua organização precisa de uma solução de proteção e backup de dados.

Apêndice A: metodologia

Em dezembro de 2019, a Veeam contratou a Forrester Consulting para realizar uma pesquisa sobre o uso e requisitos atuais das empresas para soluções de backup e proteção de dados. A pesquisa consistiu em dois componentes:

1) A Forrester conduziu uma pesquisa com 206 tomadores de decisão de TI nos EUA, Reino Unido e Alemanha, responsáveis pelas decisões de tecnologia de backup e recuperação de dados, e os entrevistados foram perguntados sobre uma série de questões sobre suas necessidades de negócios atuais de proteção e backup. A pesquisa foi duplamente cega e os entrevistados receberam um pequeno incentivo como agradecimento pelo tempo dispensado.

2) A Veeam encomendou o uso das pesquisas Business Technographics® da Forrester para obter informações específicas sobre proteção de dados, backup de dados e computação em nuvem. As pesquisas usadas incluem a Forrester Analytics' Global Business® Technographics Infrastructure Survey, 2018 e 2019; Security Survey, 2019; e Networks And Telecommunications Survey, 2019.

Apêndice B: observações finais

[1] Fonte: "Four Technologies Combine To Protect You From Ransomware Attacks", Forrester Research, Inc., 18 de outubro de 2019.

Diretora de projeto:
Chris Taylor,
consultora sênior de impacto de mercado

Pesquisas contributivas:
grupo de pesquisa em infraestrutura e operações da Forrester

FORRESTER®