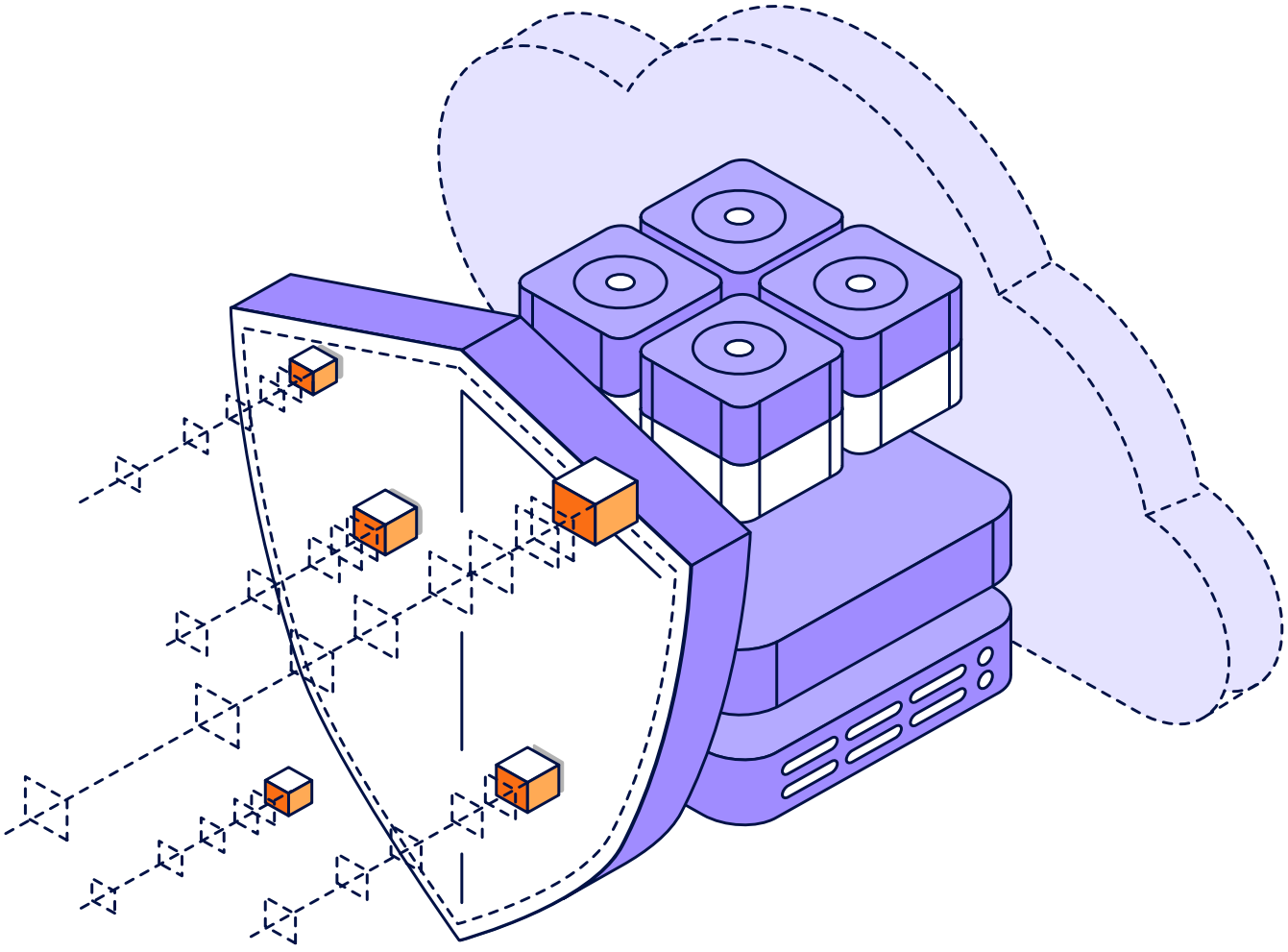
Resiliência Virtual para a Nuvem Híbrida

Lições aprendidas a partir de mais de 7.000 profissionais de TI e segurança



Nos últimos anos, houve uma mudança de data centers locais para '***a nuvem, quando isso faz sentido***', depois para estratégias de ***nuvem em primeiro lugar***, para ***híbridos em todos os lugares***, e então, para onde a maioria das empresas está hoje: com '***múltiplas nuvens estratégicas***' como o modo normal de fornecer TI moderna. Em 2024, as perguntas não são sobre se devemos usar serviços baseados em nuvem, nem quais serviços de nuvem usar. Em vez disso, as empresas estão se perguntando quantas nuvens são necessárias, e como suas equipes de TI vão gerenciar todas as suas nuvens, garantindo a segurança virtual, a proteção de dados e outros controles essenciais de TI.

Para responder a essas perguntas, este relatório de pesquisa seleciona três fontes independentes de pesquisa consultadas entre agosto de 2022 e março de 2023, incluindo:

- **Tendências em Proteção na Nuvem em 2023**
  Entrevistando 1.700 administradores de IaaS, PaaS e SaaS sobre suas estratégias de proteção de dados.
- **Relatório sobre Tendências em Proteção de Dados em 2023**
  Entrevistando 4.200 líderes de TI responsáveis pelas estratégias de proteção de dados de suas empresas.
- **Relatório sobre Tendências de Ransomware em 2023**
  Entrevistando 1.200 profissionais de Segurança, Backup e CISOs cujas empresas tenham sofrido um ataque virtual em 2022.

Todas as três pesquisas foram conduzidas por departamentos independentes de pesquisa ou análise, a partir de seus painéis imparciais, com os dados sendo então adquiridos e publicados de várias maneiras pela Veeam®. Nesse relatório, quatro áreas principais são reveladas de modo consistente:

- Os serviços baseados em nuvem são essenciais para proteger os data centers e as cargas de trabalho hospedadas na nuvem.
- As nuvens são igualmente suscetíveis a ataques de ransomware, talvez até mais.
- Usar uma nuvem para proteger outra é uma boa ideia; usar a mesma nuvem para proteger a si mesma não é.
- As equipes de segurança, DR, nuvem e local não estão alinhadas. Corrija isso primeiro!

Os serviços baseados em nuvem são essenciais para proteger os data centers e as cargas de trabalho hospedadas na nuvem

82%

das empresas agora usam storage baseado na nuvem com recursos de imutabilidade.

As pesquisas revelam de forma consistente que os serviços baseados em nuvem são uma parte indispensável da proteção de cargas de trabalho tradicionais locais tradicionais, além de cargas de trabalho hospedadas na nuvem. *Notavelmente, o storage baseado na nuvem permite* ***repositórios 'com capacidade de sobrevivência'*** *(por exemplo, imutabilidade), além de uma* ***infraestrutura de recuperação de desastres*** *quando você precisar disso.*

Para a maioria das empresas, há verdades praticamente universais na proteção contra o ransomware:

- Para proteger os servidores do data center, tire seus dados do local (por exemplo, off-site ou em uma nuvem).
- Para se recuperar do ransomware, você precisará de cópias de backup que as ameaças virtuais não possam afetar.

Com base na Pesquisa sobre Tendências de Ransomware em 2023, combinar esses dois axiomas tornou-se necessário em 2023 como uma "lição aprendida" – com **82%** das empresas agora utilizando storage baseado na nuvem e com recursos de imutabilidade.[1]

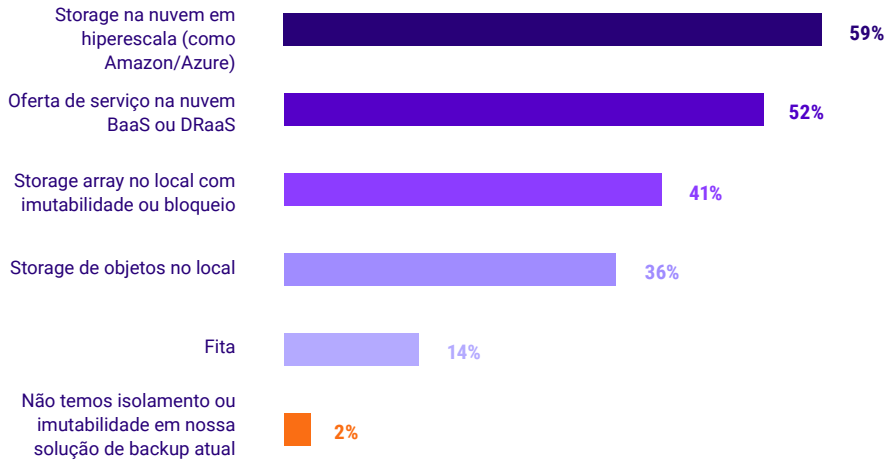


Figura 1.1

Sua empresa utiliza backups off-line, isolados ou imutáveis usando os seguintes sistemas?

Após garantir que a empresa tenha cópias de backup com capacidade de sobrevivência, outros aspectos de uma estratégia tradicional de continuidade dos negócios ou recuperação de desastres (BC/DR) também podem ser considerados. Ao observar que os ataques virtuais são cada vez mais considerados como outra forma (especial) de desastre, não é surpresa que muitos pensem que a resiliência virtual e a recuperação de desastres estejam fortemente inter-relacionadas. Em ambos os casos, a próxima questão mais pragmática é, **"Para onde você vai fazer a recuperação ou o failover?".**

Como lições aprendidas por meio dos depoimentos de vítimas de ataques virtuais, as estratégias de recuperação das empresas incluem a capacidade de recuperar seus servidores de data center para uma infraestrutura hospedada na nuvem ao remediar um ataque de ransomware ou outra crise.[2]

Figura 1.2

Ao recuperar servidores do ransomware, para onde você recupera seus dados?

Os dados acima mostram que a maioria das empresas têm uma estratégia híbrida flexível, baseada no escopo da crise. De fato, **71%** das empresas podem se recuperar usando uma nuvem, enquanto **81%** podem se recuperar usando infraestrutura local. É uma grande sobreposição (flexibilidade). Na gama mais ampla de crises para as quais as empresas se preparam, em seus planos de recuperação de desastres, **54%** planejam fazer failover para um local alternativo, enquanto **46% planejam usar infraestrutura hospedada na nuvem como site de recuperação de desastres**. Dito isso, há mais de uma maneira de criar um site de recuperação de desastres com tecnologia da nuvem.[3]

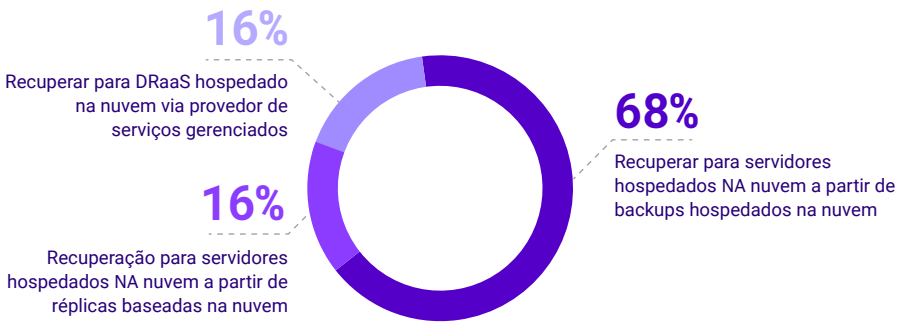


Figura 1.3

Ao usar serviços de nuvem para recuperação de desastres, como as operações são retomadas?

Se o seu plano de recuperação de desastres usa um provedor de recuperação de desastres como serviço (DRaaS) ou uma infraestrutura autogerenciada na nuvem, como a Amazon Web Services ou o Microsoft Azure, existem pelo menos dois recursos essenciais para o sucesso:

- A capacidade de transformar um backup durante a restauração, de forma que um servidor de produção protegido originalmente em formato físico ou virtual seja recuperado e ativado em um host na nuvem.
- A capacidade de orquestrar o processo de recuperação, incluindo o isolamento de quarentena para a detecção durante o fluxo de trabalho de restauração.

Infelizmente, apenas

- **18%** das empresas podem usar scripts para orquestrar fluxos de trabalho para recuperação de failover.[4]
- **44%** usam uma área de teste isolada, ou "sandbox", para verificar se ainda há ocorrência de malware durante a restauração, a fim de garantir que o ambiente não seja reinfectado.[5]

Essas perguntas difíceis devem ser respondidas pela liderança sênior, sobre se a solução ou o serviço de proteção de dados da sua empresa é capaz de automatizar a recuperação em escala e/ou garantir uma restauração segura.

As nuvens são igualmente suscetíveis a ataques de ransomware, talvez até mais

Possivelmente porque os serviços baseados em nuvem são acessíveis em arquiteturas de TI híbridas, a pesquisa revela de modo consistente que **as cargas de trabalho baseadas em nuvem têm a mesma chance de serem afetadas durante um ataque virtual**. *De fato, ao considerar que muitas empresas devem usar tecnologias de segurança diferentes para impedir o acesso a serviços de rede em comparação com seus recursos do data center, mais oportunidades de ataque se tornam possíveis, como interromper a conectividade entre os usuários e suas plataformas de nuvem.*

Da mesma forma que "a nuvem não está chegando, ela já está aqui", também é necessário reconhecer que a TI não está desativando plataformas locais na mesma velocidade que as novas cargas de trabalho estão sendo iniciadas em serviços baseados em nuvem. As empresas continuam adotando a infraestrutura hospedada na nuvem como parte de uma estratégia cada vez mais híbrida para a prestação de serviços de TI.

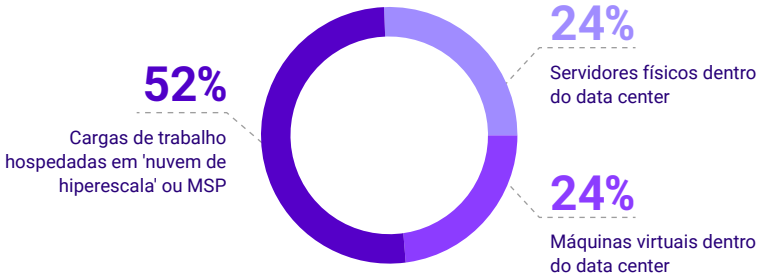


Figura 2.1

Distribuição 'híbrida' de plataformas prevista para cargas de trabalho de servidores de produção em 2024.[6]

Deve-se notar que, diferentemente da evolução das plataformas na TI concentrada no data center, não existe apenas uma arquitetura de "nuvem" para implantar, usar e proteger, independentemente do fornecedor da nuvem. Em vez disso, é necessário considerar muitas arquiteturas na nuvem, cada uma oferecida por uma variedade de provedores, cujas estruturas subjacentes de gerenciamento variam de modo substancial.

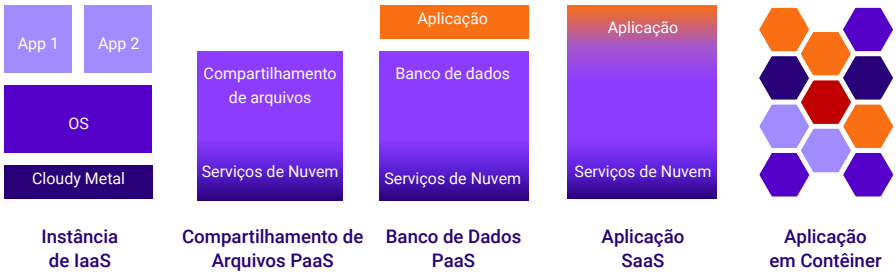


Figura 2.2

Múltiplas arquiteturas de nuvem.

Infelizmente, embora os serviços baseados em nuvem sejam geralmente percebidos como resilientes, as paralisações ainda ocorrem, devido a problemas no provedor de serviços de nuvem, erros de configuração por administradores nos serviços de nuvem e na conectividade entre os usuários e os próprios serviços de nuvem. Dito isso, nos relatórios de pesquisa de 2021 e 2022, as paralisações causadas por ataques virtuais aumentaram anualmente, permanecendo como causa mais impactante de paralisação em 2021 e 2022 (sem sinais de redução em 2023).[7]

- **48%** das empresas sofreram interrupções de TI devido a **"indisponibilidade de recursos da nuvem pública".**
- **52%** das empresas sofreram interrupções de TI devido a **"paralisações de infraestrutura ou rede".**
- **53%** das empresas sofreram interrupções de TI devido a **"eventos de cibersegurança".**

Na maioria dos ataques virtuais, embora a entrada inicial possa ter sido sistematicamente oportunista (por exemplo, enviando e-mails de phishing em massa e esperando que um usuário clique nele), esses mesmos invasores atacam sistemas que possuem vulnerabilidades conhecidas ou possíveis falhas na proteção correta de plataformas de TI populares. A pesquisa do Relatório sobre Tendências de Ransomware em 2023 mostra que os **cibercriminosos tentaram afetar cargas de trabalho hospedadas na nuvem em 38% dos ataques.**[8]

Segundo 1.200 vítimas de ataques virtuais, a quantidade de dados hospedados na nuvem criptografados/afetados foi praticamente igual à quantidade de dados no data center.

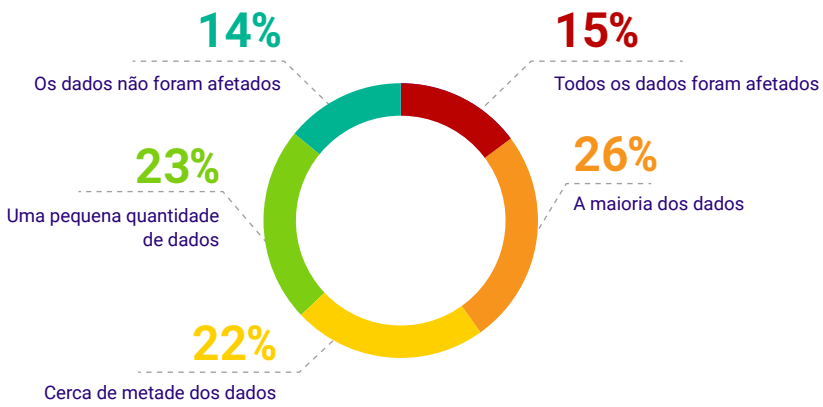


Figura 2.3

% dos dados hospedados em plataformas de nuvem que foram afetados pelo último ataque de ransomware.[9]

É importante notar que as similaridades nas taxas de infecção entre os dados dos data centers, dados das filiais/escritórios remotos e dados hospedados na nuvem sugerem dois fatos importantes:

- Como a TI híbrida é fornecida de modo simplificado, quando uma ameaça virtual está operando no ambiente da vítima, os dados hospedados na nuvem ficam tão vulneráveis a ataques quanto as aplicações e os arquivos no data center físico.
- Por conta da simplicidade e da vulnerabilidade equivalentes, os arquivos, bancos de dados e aplicações hospedados na nuvem devem ser protegidos com o mesmo rigor e metodologias das cargas de trabalho locais.

Até 2024, pela primeira vez, espera-se que mais cargas de trabalho sejam executadas fora de data centers físicos autogerenciados do que nos anos anteriores.

Usar uma nuvem para proteger outra é uma boa ideia; usar a mesma nuvem para proteger a si mesma não é

2 : 1

maioria da proteção de dados feita pela equipe de backup de TI 'tradicional' em comparação com administradores da nuvem.

Quando perguntados sobre 'quem' estava fazendo o backup de seus dados na nuvem e 'como' os dados estão sendo protegidos em 2023, todos os três projetos de pesquisa confirmaram que ***a equipe 'central' de backup (ou seu provedor de serviços) que protege o resto dos dados da empresa no local geralmente também tem o encargo de proteger os dados hospedados na nuvem****. Dito isso, ainda há muita confusão sobre 'como' isso é normal, quando as empresas supõem que sua única opção é usar o utilitário 'integrado' de sua plataforma, em vez de uma solução heterogênea de backup corporativo.*

Antes de observar 'como' as empresas estão protegendo cargas de trabalho hospedadas na nuvem, é importante considerar 'quem' – com uma maioria relativamente consistente, de 2 para 1, da proteção de dados sendo feita pela equipe 'tradicional' de backup, em comparação com os administradores da nuvem.

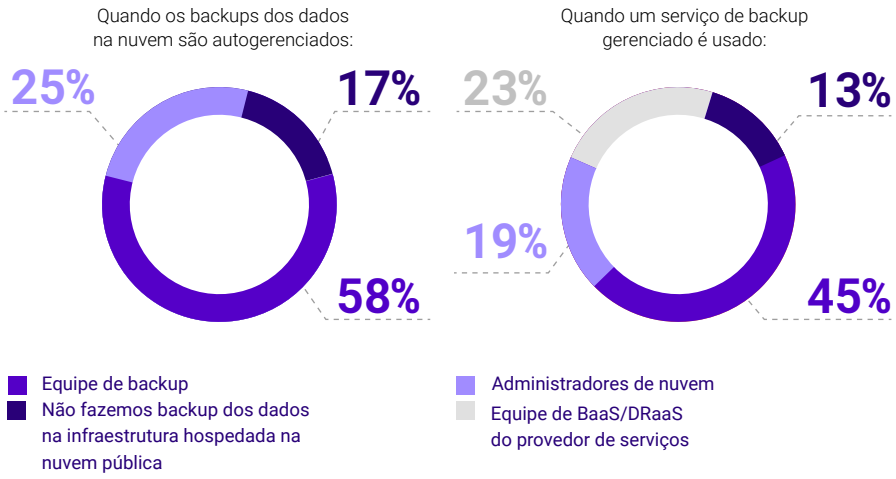


Figura 3.1

Quem gerencia os backups e a proteção de dados de servidores hospedados em nuvem em sua organização?[10]

Surpreendentemente, um em cada oito **(13%)** acredita que as empresas não estão fazendo o backup de sua infraestrutura hospedada na nuvem. Depois disso, para muitas empresas que estão adotando estratégias híbridas, a próxima questão é o reconhecimento de que os backups na nuvem poderiam estar na mesma nuvem, em uma região diferente, em uma nuvem diferente ou até de volta no local.
Essa é uma consideração importante ao escolher uma solução de backup para cargas de trabalho hospedadas na nuvem:

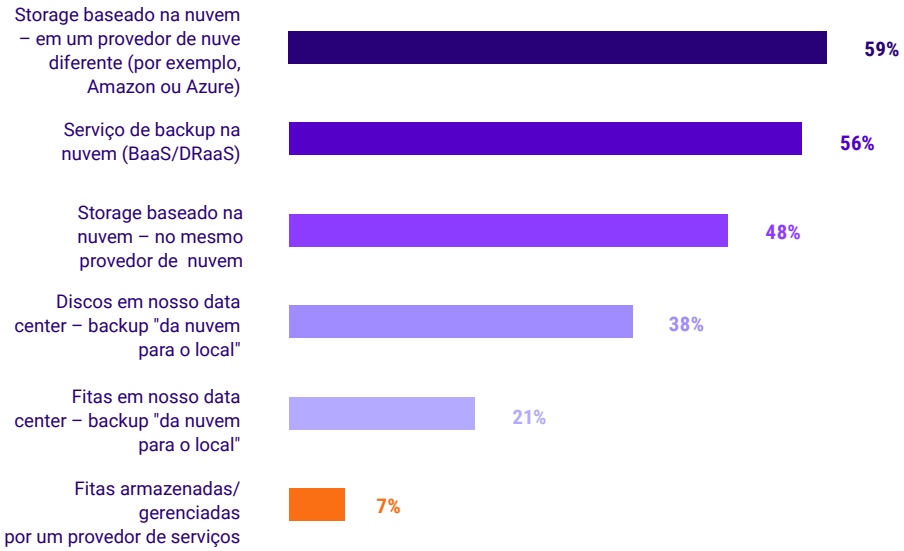


Figura 3.2

Onde são armazenados os backups de dados na nuvem que a sua empresa retém por um ano ou mais?[11]

- **37%** dos líderes de TI consideram a "capacidade de mover cargas de trabalho de uma nuvem para outra" como um aspecto definidor de uma solução de proteção de dados 'moderna' ou 'inovadora'.[12]
- **88%** das empresas levaram cargas de trabalho da nuvem de volta para o local ou as moveram para outra nuvem.[13]

Obviamente, a outra opção ao escolher uma solução de backup para cargas de trabalho hospedadas na nuvem é simplesmente confiar no utilitário 'integrado' ou função de exportação que muitas empresas da nuvem oferecem para cada carga de trabalho específica. Muitas vezes, o fator limitante é simplesmente o desconhecimento de que ferramentas de terceiros com

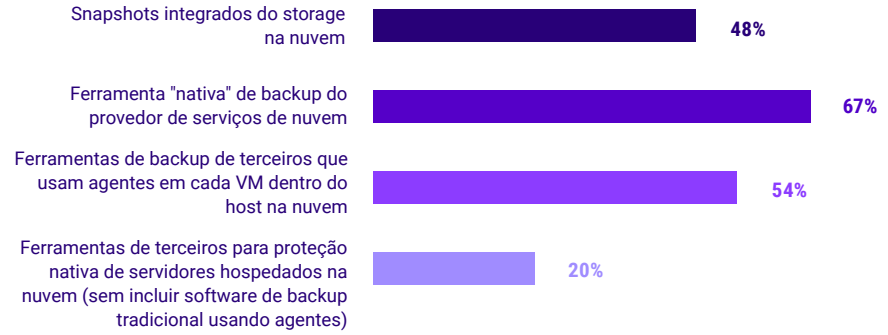


Figura 3.3

Quais mecanismos de proteção de dados hospedados na nuvem você conhece (independentemente de você usá-los ou não hoje)?

proteção abrangente para cargas de trabalho na nuvem estão disponíveis.[14]

Se estiver considerando os snapshots, questione-se: você confiaria apenas em snapshots dos seus servidores de arquivos locais? Os snapshots são ferramentas de recuperação poderosas para obter pontos de recuperação quase em tempo real, para uso instantâneo. Mas os **snapshots nunca foram um substituto para os backups,** porque:

- O mesmo silo de exposição (relacionando o NAS autônomo com uma pilha de storage IaaS, incluindo credenciais comuns).
- Caro para retenção ao longo do tempo. É por isso que a maioria das empresas mantêm alguns dias de snapshots, mas semanas, meses e anos de backups.

Se você está considerando utilitários 'nativos' centrados em cargas de trabalho ou integrados, avalie se as suas plataformas no local são protegidas com:

- O uso apenas de ZDLRA (ou RMAN) para proteger bancos de dados **Oracle**.
- O uso apenas do Utilitário de Backup NT (ou Ferramenta do Sistema) para fazer o backup de **Servidores Windows**.
- O uso apenas de VDPA para fazer backup de hosts de **VMware**.
- O uso apenas de ASB para fazer backup do **Microsoft 365**.

Agora, pergunte-se: quantas ferramentas a sua equipe de TI responsável pelos backups quer gerenciar, e quanto orçamento de storage você tem (pois cada uma dessas ferramentas grava em diferentes repositórios e formatos). Snapshotting e outros utilitários de plataforma única (ou seja, "integrados") são ainda mais problemáticos, considerando-se que a maioria deles é projetada com uma faixa de retenção limitada para permitir reversões rápidas devido a erros recentes – como dados sobrescritos ou uma importação malsucedida. Ao considerar como a empresa vai se recuperar de um ataque de ransomware, que pode ter ficado dormente por semanas, essas abordagens táticas parecem insuficientes (ou com custos proibitivos). Esses sentimentos são quantificados em dois pontos de dados adicionais:

- **35%** dos líderes de TI consideram a **"proteção padronizada de ambientes locais e IaaS/SaaS"** como um aspecto definidor de uma solução de proteção de dados 'moderna' ou 'inovadora'.[15]
- **42%** das empresas acreditam que a **"capacidade de proteger cargas de trabalho hospedadas na nuvem"** é um atributo indispensável das soluções de proteção de dados corporativos.[16] Esse sentimento foi a resposta mais comum e mais importante de 2023.

35%

dos líderes de TI consideram a "proteção padronizada de ambientes locais e IaaS/SaaS" como um aspecto definidor de uma solução de proteção de dados 'moderna' ou 'inovadora'.

As equipes de segurança, DR, nuvem e local não estão alinhadas. Corrija isso primeiro!

Os três projetos de pesquisa entrevistaram várias pessoas, incluindo líderes de TI responsáveis pela proteção de dados, CISOs e executivos similares, profissionais de segurança, administradores de IaaS, PaaS e SaaS e operadores de backup. Todas as três pesquisas revelaram que nenhuma equipe única possuía uma função principal; sempre houve sobreposição em influência e responsabilidade. Ainda assim, ***os dados raramente mostraram que os entrevistados supunham que estavam bem alinhados uns com os outros, em termos de requisitos de estratégia ou da implementação/uso de tecnologias.***

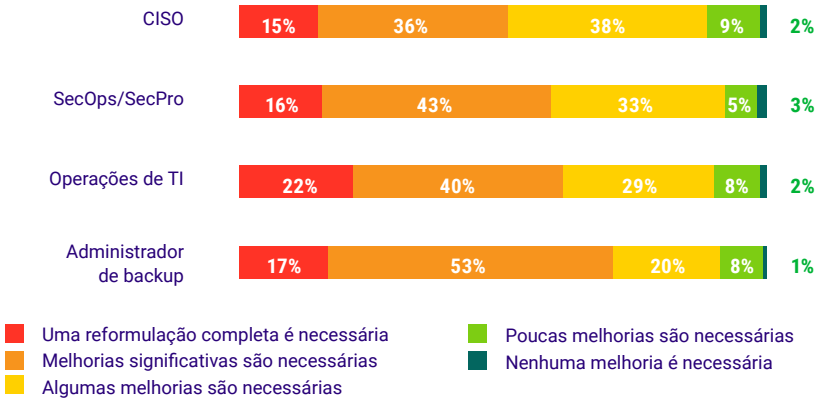


Figura 4.1

Quantas melhorias você acredita que sejam necessárias para a(s) equipe(s) de backup de TI e de cibersegurança da sua organização estarem totalmente alinhadas?

Embora a maioria dessas iniciativas de pesquisa seja centrada nas tecnologias usadas ou nos motivos/estratégias que definem as escolhas de tecnologia, os dados das pesquisas também mostram uma clara e consistente falta de alinhamento entre os profissionais envolvidos nessas funções.[17]

É importante notar que, das quatro personas entrevistadas no **Relatório sobre Tendências de Ransomware em 2023**, quanto mais 'próximo' o profissional estava da remediação do evento (por exemplo, Administrador de Backup vs. CISO), menos satisfeito ele estava com a colaboração e o alinhamento entre as equipes.

Situações similares foram observadas entre administradores de SaaS e administradores de backup ao considerar os motivos e ferramentas para a proteção do Microsoft 365, e novamente entre os administradores de IaaS/PaaS e administradores de backup ao considerar as estratégias e ferramentas para proteger servidores, compartilhamentos de arquivos e bancos de dados hospedados na nuvem.

Questões a considerar!

Com base nas pesquisas que incluíram mais de 7.000 entrevistados em um período de oito meses, algumas perguntas importantes a considerar em sua estratégia de resiliência virtual incluem:

- Seus backups são imutáveis e off-site? Os backups são gerenciados por um provedor experiente, ou nós mesmos gerenciamos os backups?
- Podemos usar a infraestrutura de nuvem como nosso site de recuperação de desastres? Se não, por quê?
- Estamos fazendo o backup de todos os nossos dados hospedados na nuvem, incluindo cargas de trabalho de IaaS, PaaS e SaaS? Caso sim, estamos usando ferramentas separadas por nuvem ou implantadas de modo consistente em nossas nuvens (e cargas de trabalho locais)?
- Quão alinhadas as nossas equipes estão, em relação ao backup no local, IaaS, PaaS e SaaS?
- Quão alinhadas as nossas equipes estão entre a preparação virtual e o backup de dados?
- Quando foi a última vez que testamos a recuperação dos nossos dados baseados na nuvem?
- Quando foi a última vez que testamos uma recuperação de data center em escala?
- Quando foi a última vez que avaliamos e atualizamos nossos manuais de preparação virtual e BC/DR?

Caso tenha alguma dúvida sobre a pesquisa ou seus resultados, entre em contato com StrategicResearch@veeam.com

Para ler os relatórios de pesquisa completos que foram citados aqui, veja os links abaixo:

- **Tendências em Proteção na Nuvem em 2023**
  Entrevistando 1.700 administradores de IaaS, PaaS e SaaS sobre suas estratégias de proteção de dados.
- **Relatório sobre Tendências em Proteção de Dados em 2023**
  Entrevistando 4.200 líderes de TI responsáveis pelas estratégias de proteção de dados de suas empresas.
- **Relatório sobre Tendências de Ransomware em 2023**
  Entrevistando 1.200 profissionais de Segurança, Backup e CISOs cujas empresas tenham sofrido um ataque virtual em 2022.

A perspectiva da Veeam

A plataforma de backup e gerenciamento de dados da Veeam

Agora mais do que nunca, é essencial que as empresas continuem confiantes de que seus dados estejam protegidos e sempre disponíveis, seja no local, na borda ou na nuvem. A Veeam fornece uma única plataforma para ambientes na nuvem, virtuais, físicos, SaaS e Kubernetes. Nossos clientes têm a confiança de que suas aplicações e dados estão protegidos contra ransomware, desastres e agentes maliciosos e sempre disponíveis, com a plataforma mais simples, flexível, confiável e avançada do setor.

A Veeam dá aos clientes a confiança para acelerar a transformação digital, proteger contra o crime virtual e impulsionar a resiliência dos negócios, garantindo que seus dados estejam sempre protegidos e disponíveis. Reduza o custo e a complexidade e alcance seus objetivos de negócio com a Veeam: o melhor backup e recuperação.

Para saber mais, acesse **https://www.veeam.com/br**.

Para se reunir com um especialista da Veeam em nuvem híbrida, solicite uma consultoria **http://vee.am/hybridcloudinquiry**.

Perguntas relacionadas aos dados e insights dessa pesquisa podem ser direcionadas para StrategicResearch@veeam.com

1 Relatório sobre Tendências de Ransomware em 2023, P29
2 Relatório sobre Tendências de Ransomware em 2023, P25
3 Relatório sobre Tendências de Proteção de Dados em 2023, P45
4 Relatório sobre Tendências de Proteção de Dados em 2023, P46
5 Relatório sobre Tendências de Ransomware em 2023, P21
6 Relatório sobre Tendências de Proteção de Dados em 2023, P2
7 Relatório sobre Tendências de Proteção de Dados em 2023, P13 e P14
8 Relatório sobre Tendências de Ransomware em 2023, P9
9 Relatório sobre Tendências de Ransomware em 2023, P6
10 Tendências em Proteção na Nuvem em 2023, P6
11 Tendências em Proteção na Nuvem em 2023, P8
12 Relatório sobre Tendências de Proteção de Dados em 2023, P17
13 Tendências em Proteção na Nuvem em 2023, P4
14 Relatório sobre Tendências de Proteção de Dados em 2023, P35
15 Relatório sobre Tendências de Proteção de Dados em 2023, P17
16 Tendências em Proteção na Nuvem em 2023, P4
17 Relatório sobre Tendências de Ransomware em 2023, P1