veeam Insights

Resumo regional

do Relatório sobre Tendências em Proteção de Dados em 2024

Edição das AMÉRICAS

1.200 líderes de TI e implementadores — em 10 países nas regiões EMEA, APJ e Américas — foram entrevistados por uma empresa de pesquisa independente para avaliar seus desafios e estratégias de proteção de dados de TI para 2024, todos eles de empresas com pelo menos 1.000 funcionários. Esse relatório de pesquisa está dividido em dez considerações principais que a liderança sênior deve explorar em suas empresas, com insights globais no relatório e estatísticas regionais das Américas como complemento.

1. As lacunas entre os requisitos de negócios e os SLAs de TI estão aumentando

Uma causa principal da reavaliação ou aderência a SLAs é provavelmente a ameaça constante de ransomware:

2. O ransomware ainda é mais uma questão de 'quando' do que 'se'
3. A preparação virtual e a ESG estão impactando a transformação digital
4. A maioria das empresas não cumprirá seus SLAs de recuperação de desastres/virtuais

Além disso, conforme as empresas continuam com suas estratégias com prioridade para a nuvem, muitas estão descobrindo que suas soluções de proteção de dados legadas são inadequadas:

5. As arquiteturas de produção 'híbridas' estão forçando a reconsideração do 'backup'
6. 74% usam um produto de backup terceirizado ou um serviço de backup para SaaS
7. A maioria das empresas está usando contêineres, mas não faz o backup de todos eles

Com tanta pressão para gerenciar a mudança e minimizar os riscos, as empresas estão melhorando suas ferramentas, mas talvez isso aconteça em detrimento de suas equipes:

8. 92% esperam aumentar seus orçamentos de proteção de dados para 2024
9. Mais de metade das empresas esperam mudar sua solução de backup
10. 2024 verá mudanças significativas de cargos fora da empresa

Após considerar essas estatísticas e implicações, o relatório de pesquisa conclui citando algumas áreas de discussão que os executivos podem considerar com suas equipes de TI.

As lacunas entre os requisitos de negócios e os SLAs de TI estão aumentando

Quando perguntados sobre o alinhamento entre as expectativas das unidades de negócios em relação à prestação de serviços de TI e a capacidade da equipe de TI de cumprir seus SLAs:

- **85%** das empresas reconhecem uma **'lacuna de disponibilidade'** entre a resiliência com que as empresas esperam que seus sistemas de TI sejam recuperados após uma interrupção e a capacidade real de recuperação da TI.
- **76%** das empresas reconhecem uma **'lacuna de proteção'** entre quantos dados a empresa pode perder e a frequência/métodos que a TI usa para proteger de fato os dados.

81%

das organizações nas Américas reconhecem que possuem uma 'lacuna de disponibilidade'

74%

reconhecem que têm uma 'lacuna de proteção' para seus dados

O ransomware ainda é mais uma questão de 'quando' do que 'se'

Pelo terceiro ano seguido, pelo menos três em cada quatro empresas sofreram um ou mais ataques de ransomware nos doze meses anteriores:

- 25% declararam que não foram atacadas, o que deve ser encarado com cuidado, pois muitas empresas de segurança avisam que o invasor pode ficar escondido em seu sistema de 60 a 200 dias antes de causar danos ou pedir um resgate. Se isso for verdade, então uma grande porcentagem desses entrevistados pode simplesmente não ter descoberto ainda a violação
- 26% declararam que foram atacados quatro ou mais vezes no ano passado.

77%

das empresas nas Américas sofreram pelo menos um ataque no ano anterior

A preparação virtual e a ESG estão impactando a transformação digital

Examinando as iniciativas reativas ou obrigatórias (como a conformidade) e as aspirações proativas (como a transformação digital) que as equipes de liderança estão realizando:

- Quando perguntadas sobre conformidade, governança e outras iniciativas corporativas, embora os mandatos normativos, soberania geográfica de dados e requisitos do setor estivessem entre os cinco primeiros, **a principal iniciativa era a educação virtual relacionada ao phishing ou prevenção.**
- Quando perguntados quais fatores serão os maiores inibidores da

realização de suas iniciativas de transformação digital (DX), **as ameaças virtuais** e **objetivos ambientais, sociais e governamentais** tiveram uma pontuação maior do que as dificuldades usuais relacionadas a habilidades, preocupações econômicas, problemas organizacionais, etc. Não por causa de metodologias ou motivações conflitantes, mas devido à quantidade de recursos e esforços sendo desviados dos investimentos em DX ou modernização da TI.

Em outras palavras, a ameaça virtual sempre presente impede muitas iniciativas de responsabilidade das equipes de liderança, ou que são essenciais para o sucesso de suas empresas.

A maioria das empresas não cumprirá seus SLAs de recuperação de desastres/virtuais

Ao considerar os enormes impactos financeiros e à reputação relacionados a crises em escala, incluindo ataques virtuais como o ransomware, ação do clima e outras crises no nível dos sites, a maioria das empresas agora considera a resiliência virtual (CR) como um aspecto fundamental de sua estratégia de continuidade dos negócios ou recuperação de desastres (BC/DR). Infelizmente, a preparação para BC/DR (incluindo a resiliência virtual) ainda não 'cumpre' a maioria das expectativas de SLAs:

- Quando perguntados sobre seu mais recente teste em grande escala sobre desastres/cibersegurança, somente **58%** dos servidores puderam ser recuperados conforme as expectativas. Já imaginou se dois em cada cinco dos seus sistemas de TI não voltassem a ficar on-line após uma crise?
- Quando perguntados sobre quanto tempo a TI precisaria para recuperar 50 servidores, o que não é uma grande quantidade de recursos para as empresas pesquisadas, apenas 32% acreditavam que a TI poderia recuperar os servidores em cinco dias úteis.

De uma perspectiva estratégica, esses desafios provavelmente são causados por duas outras escolhas das equipes de TI e suas lideranças:

- Em média, as empresas só realizam testes de CR/DR a cada 8,1 meses, criando enormes janelas em que as mudanças de sistemas em produção impedem a capacidade de recuperar durante uma crise, abrindo oportunidades para vilões virtuais afetarem os sistemas por meses, antes que a violação seja descoberta
- No momento, 87% das equipes de TI usam métodos manuais de recuperação ou scripts. Essas tarefas não orquestradas são trabalhosas, causando mais relutância em fazer testes, além de inconsistências entre cada teste e quando essas recuperações são necessárias de fato.

Nas Américas, apenas

58%

dos servidores foram recuperados conforme as expectativas

As arquiteturas de produção 'híbridas' estão forçando a reconsideração do 'backup'

Pelo segundo ano seguido, as duas considerações mais importantes para as soluções de 'backup corporativo' são a **confiabilidade** e a **proteção de cargas de trabalho hospedadas na nuvem** (IaaS e SaaS). Isso é problemático para empresas que utilizam soluções de proteção de dados mais antigas, voltadas para o data center. Em 2024, quase metade de todas as cargas de trabalho são executadas em hosts na nuvem, em comparação com aquelas executadas em data centers, incluindo **28%** em servidores físicos, **27%** em máquinas virtuais e **45%** em hosts na nuvem.

Conforme as empresas movem as cargas de trabalho de uma plataforma ou nuvem para outra, as equipes de TI que usam soluções de backup legadas, que não oferecem proteção equivalente para cargas de trabalho hospedadas na nuvem, terão dificuldade para cumprir SLAs, especialmente aquelas que adotam ofertas nativas de nuvem, como o Microsoft 365/Salesforce (SaaS) ou contêineres.

Nas Américas, as arquiteturas híbridas são formadas por:

29%
Servidores físicos

26%
Máquinas virtuais

45%
Instâncias hospedadas na nuvem

74% usam um produto de backup terceirizado ou um serviço de backup para SaaS

A maioria das empresas agora reconhece a necessidade de fazer backup de SaaS. No início da maioria das ondas de adoção do SaaS, existe uma suposição incorreta de que como as plataformas de SaaS são nativamente duráveis, o backup não é mais necessário. Os fornecedores de SaaS têm relembrado repetidamente às empresas que é responsabilidade de cada assinante fazer o backup de seus dados no SaaS, como no modelo de responsabilidade compartilhada da Microsoft.

- Conforme a adoção do SaaS amadurece, as principais expectativas de TI, como acesso baseado em função, zero trust e mandato de backup/retenção, muitas vezes são sobrepostas
- Parte dessa jornada de amadurecimento também inclui as plataformas de produção oferecendo suas próprias ferramentas para fazer o backup dos dados, incluindo a ferramenta de backup do M365, o utilitário do Salesforce, ou os utilitários Windows Backup ou VMware Backup de décadas atrás. Felizmente, em 2024, **74%** delas usam um produto ou serviço terceirizado de backup para proteger o Microsoft 365, enquanto apenas 3% usam a lixeira e 4% ainda acreditam que o backup não é necessário.

67%
das empresas nas Américas protegem dados do Microsoft 365

A maioria das empresas está usando contêineres, mas não faz o backup de todos eles

Para 2024, 59% das empresas informaram que usam contêineres na produção, e outros 37% estavam implantando ou planejando fazer isso, enfatizando que os contêineres não estão vindo — eles já chegaram. Infelizmente, apenas 25% das empresas usam uma solução de backup desenvolvida especificamente para contêineres, enquanto o resto delas (71%) só faz o backup dos repositórios de storage subjacentes ou do conteúdo do banco de dados, nenhum dos quais garante que as aplicações e serviços poderão continuar após uma crise ou mesmo um simples erro de configuração ou importação que precise ser desfeito.

92% esperam aumentar seus orçamentos de proteção de dados para 2024

Os orçamentos de proteção de dados devem aumentar em **6,6%** em 2024. Este é o segundo ano em que a pesquisa revela que o aumento do gasto com proteção de dados vai ultrapassar o aumento do gasto geral com TI, em comparação com a estimativa de 4,3% do Gartner para gastos gerais com TI,[1] ou a previsão do IDC de 5,4% de aumento nos gastos com proteção de dados[2]. Logo, apesar da tendência de aumento dos gastos com TI, a proteção de dados consumirá uma parte maior, provavelmente para continuar a preparação contra ataques virtuais, além das mudanças no panorama de produção que exigem abordagens diferentes à proteção de dados.

Nas Américas, os orçamentos de proteção de dados de 2024 devem aumentar em

6,8%

Mais de metade das empresas esperam mudar sua solução de backup

54% das empresas esperam trocar sua solução de backup primária nos próximos doze meses. Embora muitos talvez suponham que o mercado do backup está maduro e, portanto, não flutua, as mudanças contínuas no relatório semestral do IDC sobre a participação no mercado de backup e replicação[3] provam que esse mito não é verdadeiro há anos. Nos dois últimos anos dessa pesquisa, mais da metade (54% em 2024, 57% em 2023)

56%

das empresas nas Américas planejam trocar sua solução de backup principal em 2024

[1] https://www.gartner.com/document/4714599

[2] https://www.idc.com/getdoc.jsp?containerId=US51037523

[3] Participação de mercado do S1 2023 – IDC

das empresas expressaram que 'muito provavelmente' ou 'certamente' vão mudar de solução de backup. Para ser justo, é igualmente plausível que as empresas escolham mudar do modelo 'autogerenciado de seu próprio software licenciado' para adotar uma oferta de 'backup gerenciado como serviço', mesmo se as tecnologias subjacentes do fornecedor permanecerem constantes. Trocar de modalidade para um serviço gerenciado será, para muitos, o que transformará seus backups "bons o suficiente" em estratégias confiáveis de recuperação.

2024 verá mudanças significativas de cargos fora da empresa

47% dos entrevistados manifestaram interesse em buscar um novo emprego fora de sua empresa atual nos próximos doze meses. Uma grande preocupação relacionada às *'ramificações de um ataque virtual ou outro desastre'* incluía o risco à reputação profissional dos entrevistados. Além disso, os participantes também revelaram sentir ansiedade em relação ao avanço na carreira, desenvolvimento de habilidades ou relevância percebida dentro da organização. Essa mudança do mercado é um desafio e uma oportunidade:

- A liderança sênior precisa reter seus talentos em proteção de dados existentes, a fim de garantir a preparação para a resiliência virtual e outros tipos de preparação para desastres dentro da empresa. Perder esses especialistas coloca a empresa em uma grande desvantagem quando as crises inevitavelmente chegarem
- Existe uma excelente oportunidade de recrutar profissionais que podem trazer novas habilidades para garantir o fortalecimento da proteção de dados contra os criminosos virtuais, além de novos conhecimentos para proteger cargas de trabalho de produção modernas que residem na nuvem, como Microsoft 365, contêineres do Kubernetes ou outras arquiteturas de IaaS/PaaS.

Uma maneira bem estabelecida pela qual as organizações decidem reduzir sua exposição de risco à escassez de habilidades ou de mão de obra em proteção de dados é contratar provedores de **BaaS ou DRaaS.** Os provedores de serviços gerenciados não só garantem um conhecimento atual e profundo, monitoramento operacional e suporte técnico primário, mas também permitem que as empresas evoluam alguns de seus especialistas internos de proteção de dados para supervisionar o monitoramento e o gerenciamento terceirizados da proteção de dados.

55%

dos entrevistados nas Américas declararam interesse em buscar um novo emprego fora de sua empresa atual

O que fazer a respeito disso?

Este relatório de pesquisa chega ao fim com algumas perguntas importantes que a liderança sênior, responsável pela proteção de dados ou prestação de serviços de TI em suas empresas, pode explorar com suas equipes de implementação de TI:

- Quanta confiança nós temos de que seremos capazes de recuperar nossos dados de um criminoso virtual, se ele estiver espreitando em nosso ambiente há três meses ou mais?
- Quanto tempo levaria para recuperar 10% da nossa farm de servidores, se ela fosse infectada por ransomware ou uma crise no site inutilizasse esses servidores?
- Com que frequência nós testamos esses recursos?
- Quais são as nossas métricas de sucesso para esses testes?
- Quais são os nossos processos para melhoria contínua da nossa resiliência virtual ou prontidão para BC/DR?
- Estamos fazendo o backup dos nossos hosts na nuvem? Das nossas aplicações SaaS? Dos nossos ambientes baseados em contêineres?

Sobre os autores

Jason Buffington
VP, Estratégia de Mercado
@JBuff

Dave Russell
VP, Estratégia Corporativa
@BackupDave

Julie Webb
Diretora, Pesquisa de Mercado e Análise

Sobre a Veeam Software

A Veeam®, líder global do mercado em proteção de dados e recuperação de ataque de ransomware, tem a missão de capacitar cada empresa não só a retornar de uma perda ou paralisação de dados, mas de retornar e avançar. Com a Veeam, as empresas têm resiliência radical com segurança, recuperação e liberdade de dados para a sua nuvem híbrida. A Veeam Data Platform fornece uma solução única para ambientes físicos, virtuais, na nuvem, SaaS e Kubernetes, que oferece tranquilidade aos líderes de TI e Segurança, mantendo suas aplicações e dados protegidos e sempre disponíveis. Com sede em Columbus, Ohio, e escritórios em mais de 30 países, a Veeam protege mais de 450.000 clientes no mundo inteiro, incluindo 73% das empresas da lista Global 2.000, que confiam na Veeam para manter seus negócios em operação. A resiliência radical começa com a Veeam. Saiba mais em www.veeam.com ou siga a Veeam no LinkedIn @Veeam-Software e X @Veeam.

Para fazer o download de materiais adicionais desta pesquisa, clique aqui

Para perguntas sobre essa pesquisa ou sua utilização: StrategicResearch@veeam.com