451 Research® | PATHFINDER REPORT

Diminuindo riscos na jornada para a multinuvem híbrida

IMPERATIVOS DA RESILIÊNCIA

ENCOMENDADO POR

IBM

NOVEMBRO DE 2019

Sobre este artigo

Um artigo inovador que auxilia os tomadores de decisão em questões que envolvem uma tecnologia ou caso de negócios específico, explora o valor comercial da adoção e recomenda diversas considerações e as próximas etapas concretas do processo de tomada de decisão.

SOBRE O AUTOR

ERIC HANSELMAN

ANALISTA CHEFE

Eric Hanselman é o analista chefe da 451 Research. Ele tem um vasto conhecimento prático de uma ampla gama de assuntos em TI e tem experiência direta nas áreas de redes, virtualização, segurança e semicondutores. Ele coordena a análise de mercado em todo o amplo portfólio de disciplinas da 451 Research. A convergência de forças no cenário tecnológico está provocando grandes mudanças no mercado, incluindo SDN/NFV, hiperconvergência e Internet das Coisas (IoT). Eric ajuda os clientes da 451 Research a lidar com esse cenário turbulento e a determinar o impacto e a melhor forma de capitalizá-lo. Eric também é membro do Centro de Excelência para Tecnologias Quânticas da 451 Research.

Resumo executivo

A migração para um ambiente híbrido de multinuvem já pode ser uma realidade para alguns e parecer inevitável para muitos. Essa mudança acaba trazendo à tona um conjunto de complexidades que pode pressionar as abordagens tradicionais de disponibilidade, segurança econformidade. A expansão natural que está atraindo as empresas para ambientes fora de seus data centers tradicionais também está fazendo com que componentes e dados críticos de aplicações necessitem de proteções superiores às já implementadas. É necessário estabelecer essas proteções nesses novos locais, mas isso pode ser desafiador e caro para as empresas que talvez não tenham tido tempo de desenvolver a profundidade técnica para fazê-lo de maneira eficaz.

Principais descobertas

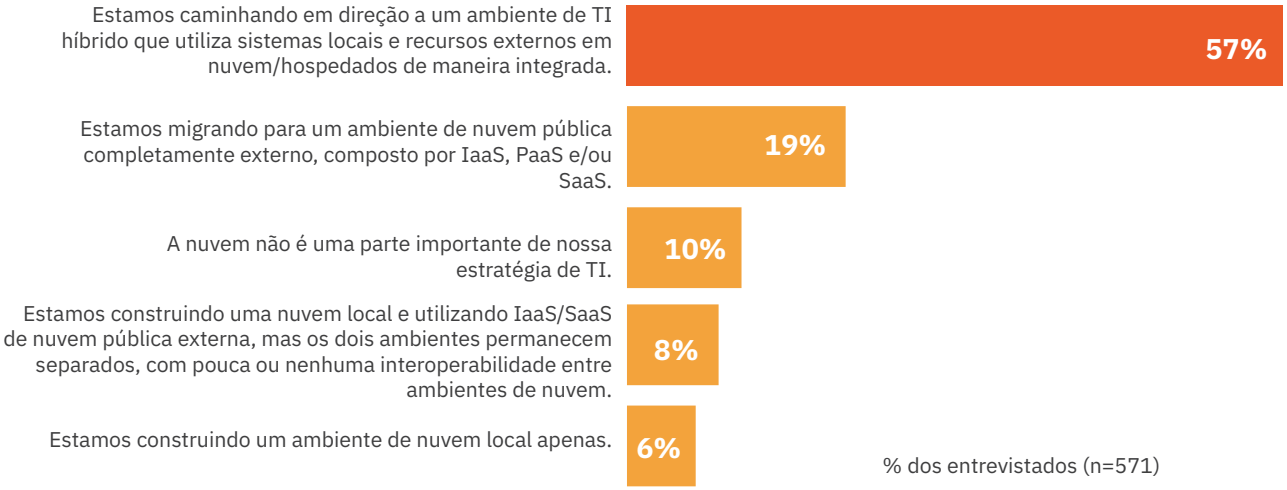
- Ambientes híbridos de multinuvem demandam novas estratégias para gerenciar os riscos.
- A resiliência requer ações imediatas para diminuir os riscos para os negócios.
- Mudanças nos padrões e nas ferramentas de ataque demandam proteções de dados para diminuir novas ameaças.
- A proteção de dados na multinuvem híbrida requer vigilância aprimorada para novos riscos.
- As melhorias no gerenciamento de dados híbridos são imperativas diante do cenário regulatório, como o Regulamento Geral sobre a Proteção de Dados da UE e a Lei de Privacidade do Consumidor da Califórnia.
- A automação e a orquestração são necessárias para lidar com a escala dos ambientes híbridos de forma eficaz.

Benefícios da multinuvem híbrida

À medida que a transformação digital e a migração para a nuvem continuam se expandindo, as empresas estão ampliando sua infraestrutura em grande escala. A criação de um ambiente híbrido multinuvem deve estimular a interoperabilidade e permitir uma variedade de parcerias e colaborações nas nuvens. De acordo com a pesquisa "Voice of the Enterprise: Cloud, Hosting Managed Services, Workloads and Key Projects de 2019" feita pela 451 Research, 57% das empresas descreveriam sua abordagem e estratégia de TI como híbridas.

Figura 1: O futuro é híbrido para a maioria

Fonte: 451 Research, Voice of the Enterprise: Cloud, Hosting & Managed Services, Workloads and Key Projects de 2019
P: Qual das opções a seguir melhor descreve a abordagem e a estratégia geral de TI da sua empresa?



Para os 19% dos entrevistados que relatam a migração para um ambiente de nuvem pública, pode ser difícil permanecer exclusivamente em nuvens públicas. Prevemos que os ambientes híbridos se tornarão tão difundidos que será improvável que empresas não tenham algum nível de colaboração híbrida, mesmo que somente para algumas aplicações.

O crescente uso da infraestrutura em nuvem cria um ambiente no qual podem ser usadas inúmeras configurações de recursos virtuais. Uma grande variedade de recursos disponíveis significa que, para obter sucesso, as empresas precisam criar ativos que possam existir em diversos ambientes. Uma estratégia de TI híbrida permite mais espaço para colaboração e interoperabilidade.

Para operar com sucesso no modo da multinuvem híbrida, as empresas precisam conseguir mover os dados no âmbito da infraestrutura sem sacrificar a fluidez. À medida que avançam rumo ao uso de arquiteturas de contêineres e microsserviços, os próprios componentes de aplicações leves podem ser facilmente transferidos entre as nuvens. Em um ambiente no qual os dados talvez precisem ser armazenados na borda, como uma implementação de IoT ou um factory inteligente, é imperativo que esses dados possam ser facilmente transferidos entre as nuvens para permitir um uso mais eficiente da infraestrutura distribuída.

As tecnologias que permitem a operação da multinuvem híbrida estão disponíveis e são amplamente utilizadas. As estratégias para a movimentação e a disponibilidade de dados podem ser customizadas de acordo com as necessidades das aplicações que estão sendo suportadas. As técnicas de replicação e publicação/assinatura oferecem abordagens básicas para garantir que os dados estejam disponíveis onde quer que sejam necessários. Caminhos mais complexos, como bancos de dados distribuídos como o MongoDB ou o Cassandra, podem se estender por locais e automatizar a tarefa de distribuição de dados.

Mais um impulsionador da mudança para o mundo híbrido é a expansão do ecossistema de tecnologia de uma empresa. Existem dois caminhos comuns: a adoção de uma tecnologia importante e a presença de um parceiro ou fornecedor. Em ambos os casos, a empresa estabelece uma presença em um novo local para aproveitar a tecnologia ou o serviço. Os provedores em nuvem pública oferecem tecnologias especializadas, como reconhecimento de imagem ou fala e recursos de machine learning. Para usá-los, os dados precisam estar disponíveis nesse ambiente de nuvem e os resultados também são entregues nele. Os serviços oferecidos pelos parceiros do ecossistema, como marketing ou engajamento do cliente, podem ser hospedados em um provedor específico, o que possibilita ter componentes de aplicações hospedadas nele para melhorar o desempenho. Todos esses fatores podem levar as empresas a diversos ambientes nos quais elas precisam gerenciar a confiabilidade e a disponibilidade dos dados.

Complexidades da multinuvem híbrida

À medida que a infraestrutura em nuvem se expande, ela se torna cada vez mais complicada, abrindo portas para erros e falhas. Uma empresa que opera em um modo de multinuvem híbrida pode desenvolver exposições a riscos em sua infraestrutura sem estar operacionalmente consciente da existência delas. Esse é um desafio que pode se desenvolver com o crescimento orgânico da infraestrutura. Se a empresa não tiver processos para integrar novos recursos que reavaliem o risco a cada etapa, poderão surgir ameaças à resiliência. Não é incomum que o uso de diversos ambientes de nuvem ou de hospedagem seja descoordenado. Além disso, muitas cargas de trabalho conectadas podem criar vetores de ataque estranhos às equipes e ao software de segurança da informação existentes.

Trabalhar em ambientes em nuvem também cria uma necessidade específica da interconexão, a qual não apresenta confiabilidade perfeita. Os ambientes híbridos estendem os caminhos dos dados por meio de tecnologias tipicamente diferentes e com ferramentas inconsistentes para gerenciá-los e monitorá-los. O gerenciamento de caminhos de dados importantes pode ser bastante desafiador em um data center. Uma vez que esses dados são dispersados por uma infraestrutura de escala gigantesca, eles se tornam um desafio ainda mais complexo.

Uma das maiores dificuldades apresentadas pela interconexão é que os modos de falha introduzidos podem ser muito mais complexos. Isso pode dificultar a detecção de falhas e sua recuperação. Por exemplo, um caminho que compartilha o tráfego de diversas origens pode ficar congestionado, criando aumentos na latência ou na perda de pacotes. Para aplicações que dependem da sincronização oportuna, o aumento da latência acima do limite de desempenho pode ter um efeito semelhante à falha do caminho, mas, mesmo assim, as ferramentas de monitoramento ainda podem estar funcionando. É complexo diagnosticar problemas como esse, principalmente porque eles costumam acontecer apenas quando há uma carga significativa, o que pode tornar sua ocorrência intermitente.

Os modos de falha de uma aplicação podem ser complicados devido aos fatores nos diferentes ambientes nos quais os componentes estão localizados. Os problemas de desempenho local podem ser causados por uma série de questões que abrangem erros de aplicações, variabilidade de E/S de armazenamento, erros de dimensionamento de instância e falhas simples.

A complexidade surge ao tentar determinar a ocorrência de uma falha e sua recuperação em ambientes nos quais os mecanismos de detecção e recuperação são únicos. Se a empresa quiser resolver esse problema, poderá ter de gastar recursos consideráveis para desenvolver habilidades em cada novo ambiente operacional.

A infraestrutura de TI híbrida também pode ser uma dor de cabeça para as equipes de operações que precisam monitorar mais ambientes do que nunca. Embora os especialistas em operações de TI sejam conhecedores do gerenciamento de servidores locais privados de suas empresas, em uma configuração de multinuvem híbrida, eles precisarão ter interoperabilidade com nuvens públicas e, potencialmente, uma nuvem privada de outro provedor. É difícil manter a eficiência operacional quando as equipes são encarregadas de dominar diferentes conjuntos de habilidades e integrar os resultados em um processo de trabalho.

Um dos maiores desafios dos ambientes híbridos é que os riscos subjacentes podem ser mascarados pela complexidade das estruturas de aplicações construídas através deles. A combinação de todos esses fatores pode resultar em um conjunto oculto de possíveis problemas que não são levados em consideração no planejamento de continuidade de negócios e recuperação de desastre, que analisa cada ambiente de forma independente.

Imperativos da resiliência

Com a combinação de expansões de ecossistemas e um conjunto de benefícios que impulsiona a adoção de ambientes híbridos, as empresas precisam abordar a resiliência desse novo ambiente para garantir que seja possível manter os mesmos níveis de disponibilidade nas principais aplicações usadas tradicionalmente. Essa tendência de expansão não é um evento único, mas uma nova realidade. Novos ambientes continuarão agregando valor de novas maneiras. As nuvens de IaaS tradicionais deram lugar a ambientes de contêineres. Além disso, os ambientes funcionais e sem servidor estão desempenhando um papel mais importante. Isso significa que as empresas precisam criar recursos que simplifiquem a extensão das proteções necessárias para fornecer resiliência a novos serviços ou locais de execução.

Isso deve ser feito imediatamente. Não se trata somente de adiar um único projeto que torne um novo ambiente resiliente. Qualquer atraso adia o desenvolvimento de uma habilidade importante que pode suportar uma estratégia de infraestrutura ágil por meio da garantia de que, independentemente de como as necessidades de infraestrutura sejam atendidas, seja garantida a robustez dos serviços e aplicações em execução. Há muita discussão sobre a orquestração e a automação necessárias para ter uma infraestrutura ágil, mas a resiliência ágil é tão importante quanto elas.

Há diversos componentes necessários que precisam ser cobertos para fornecer resiliência de forma eficaz e operacionalmente eficiente em implementações de multinuvem híbrida. Alguns deles podem ser abordados expandindo a continuidade de negócios e a recuperação de desastre existentes para incluir recursos de parceiros. A maioria dos exercícios de planejamento de continuidade de negócios e recuperação de desastre considera ativos próprios, o que limita a contabilização da capacidade fornecida por provedores de hospedagem ou nuvens públicas. Parte disso ocorre porque, historicamente, isso sempre foi complicado de alcançar. A maioria das práticas tradicionais de continuidade de negócios e recuperação de desastre não podia se estender facilmente para fora do local e aquelas que podiam requeriam intervenção manual significativa. Com a automação e a orquestração adequadas, as infraestruturas local e externa agora podem ter os mesmos níveis de proteção.

Outro componente significativo da resiliência necessária é impulsionado pelas necessidades de segurança da informação. Os ambientes híbridos de multinuvem têm uma superfície de ataque muito maior. Devido ao rápido aumento no uso de ferramentas de ataque automatizadas pela comunidade de invasores, ficou muito mais fácil encontrar e apontar como destino diferentes elementos de uma infraestrutura de aplicações mais distribuída. Um benefício adicional dos recursos de resiliência que oferecem suporte a diversos ambientes é que eles possibilitam a recuperação em uma infraestrutura que não esteja sob ataque. Isso pode reduzir o risco de qualquer elemento único da implementação completa do processo de negócios poder desativar uma aplicação.

Requisitos para a resiliência

Para fornecer os níveis de funcionalidade necessários para o suporte a ambientes híbridos de multinuvem, existe um conjunto de requisitos que qualquer abordagem de resiliência precisa atender. Em primeiro lugar, ele precisa ampliar a conscientização e a visibilidade em todo o ambiente híbrido. Ter um ponto de referência comum que possa atuar como um recurso compartilhado pode reunir equipes e fornecer uma perspectiva mais completa do estado atual da infraestrutura de uma empresa. Para isso, ele deve abranger recursos físicos e virtuais e fornecer perspectivas equivalentes. Nessas regiões, é necessário criar abstrações de serviço que possam simplificar as operações, traduzindo recursos de alto nível na funcionalidade nativa em cada ambiente. As abordagens que requerem conhecimento especializado para diferentes domínios não podem ter a escala ajustada e tornarão caro o processo de integração de novos ambientes. Ter serviços comuns que as equipes de aplicações possam esperar em locais diferentes oferece vários benefícios: aplicações e serviços podem ser entregues mais rapidamente devido à pouca adaptação necessária e reduzem o potencial de bloqueio a um ambiente específico devido a uma redução na dependência da funcionalidade específica do ambiente.

Qualquer abordagem também precisa ser flexível o suficiente para funcionar bem em diferentes ambientes operacionais. Ter a agilidade para ser implementado rapidamente pode significar que o estabelecimento de proteções não impede a experimentação ou reações rápidas às mudanças do mercado. A escalabilidade deve ser um subproduto natural desse nível de agilidade. Um dos principais desafios dos ambientes híbridos é a escala.

Um dos aspectos dos recursos de resiliência que devem impulsionar o suporte em maior escala é a automação/orquestração. É aconselhável considerar a escala como um requisito em si, porque ela é um elemento muito importante em qualquer implementação. A automação e a orquestração eficazes devem ser o veículo que fornece abstrações e reduz a carga de trabalho da equipe de operações.

A pontualidade da recuperação e a variedade de opções de recuperação também são requisitos importantes. Em muitos casos, os dois andam de mãos dadas, porque ter mais opções de recuperação pode permitir a otimização do processo de recuperação a fim de atender às necessidades de diferentes situações. Em ambientes híbridos, as interrupções podem ter muitos fatores interligados, criando dependências que podem impedir certos caminhos de recuperação. Abordagens eficazes poderão oferecer alternativas para solucionar quaisquer problemas de bloqueio.

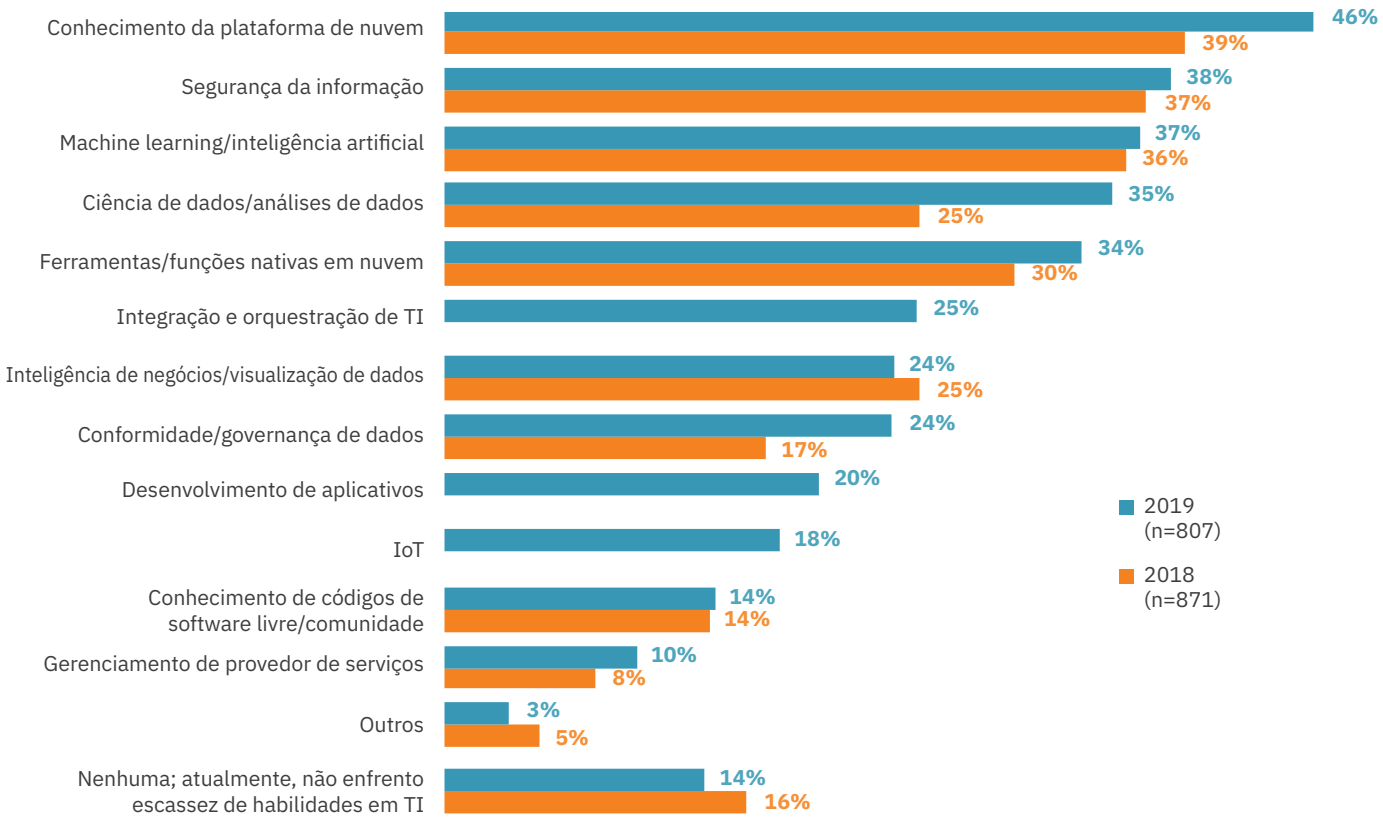
Uma abordagem de resiliência que atenda a esses requisitos pode tornar as empresas mais ágeis, permitindo que se adaptem e se recuperem mais rapidamente de problemas.

Abordagens para obter maior resiliência

Os ambientes híbridos de multinuvem têm facetas diferentes o suficiente para dificultar a identificação de como garantir a resiliência geral. Decidir entre estender as proteções de dados existentes, aproveitar serviços nativos em novos ambientes ou adotar métodos totalmente novos não é simples. Tomar decisões detalhadas também pode requerer um conhecimento profundo dos detalhes técnicos de diversos ambientes que podem estar fora do conjunto de habilidades das equipes de TI. É altamente provável que as equipes de TI não sejam especializadas em serviços de nuvem ou hospedagem novos para a empresa e dedicar algum tempo para desenvolver essas habilidades atrasaria novos serviços e aplicações ou deixaria aberta a possibilidade de riscos operacionais não serem identificados e mitigados. Essa é uma área na qual um provedor de serviços parceiro capaz pode ser particularmente útil para identificar problemas e fornecer perspectivas sobre como lidar com eles.

Figura 2: Escassez atual de habilidades por categoria de TI– 2019 e 2018

Fonte: Voice of the Enterprise: Digital Pulse, Organizational Dynamics Quarterly Advisory Report, 451 Research
P: Em qual das categorias de TI a seguir, se houver alguma, sua empresa está atualmente enfrentando grande escassez de habilidades? Selecione todas as opções aplicáveis.



A maioria das empresas está lutando para acompanhar as habilidades necessárias para gerenciar novos modelos de infraestrutura. No estudo da 451 Research "Voice of the Enterprise: Digital Pulse" do 1º trimestre de 2019, os entrevistados disseram que o conhecimento da plataforma de nuvem era sua escassez de habilidades mais crítica, superando a segurança da informação (de 46% a 38%), líder nas pesquisas anteriores. Em situações como essa, pode ser difícil contratar e reter o talento necessário para atender às necessidades operacionais, além dos membros de equipe para tomar decisões estratégicas. Trabalhar com um provedor de serviços parceiro especializado pode ampliar as habilidades da equipe existente e aumentá-las com recursos de serviço capazes de abordar as complexidades que os modelos híbridos apresentam. Uma parceria de trabalho permite que as empresas obtenham a escala necessária em seus próprios termos.

Esse é um processo que pode trazer benefícios significativos para a empresa. A implementação de amplos recursos de resiliência híbrida pode ajudar as empresas a atender antecipadamente às necessidades de suas equipes de desenvolvimento. Atualmente, eles são capazes de gerenciar as necessidades de resiliência de dados, no entanto, podem fornecer uma base que as equipes de desenvolvimento podem utilizar ao longo do tempo, o que é mais importante, tornando os desenvolvedores menos dependentes das opções nativas e proprietárias existentes em provedores de nuvem individuais. Isso pode expandir as opções de uma empresa quanto à escolha da infraestrutura, facilitando a otimização de ambientes para atender às necessidades dos negócios. Ao mesmo tempo, pode permitir que as empresas respondam mais rapidamente às mudanças nas condições de mercado e nos relacionamentos com fornecedores.

Conclusões e recomendações

A migração para os modelos de infraestrutura de multinuvem híbridos está bem encaminhada para muitas empresas. Ela oferece benefícios que podem ser atrativos e muitas empresas adotarão esse modo de operação sem considerar completamente seu impacto na confiabilidade e na resiliência de seus ambientes de aplicações.

Todas as empresas, principalmente aquelas que ainda não adotaram completamente esse modelo, precisam considerar como abordarão os riscos associados e os gerenciarão de maneira operacionalmente eficiente. Lidar com isso agora pode ajudar a gerenciar o ambiente atual, além de fornecer um meio de lidar com a expansão da infraestrutura com confiança. É um processo cujo valor pode ser maximizado trabalhando com um parceiro capaz que forneça orientação em uma área na qual geralmente há faltas consideráveis de habilidades.

O aumento da resiliência de aplicações em um mundo híbrido oferece muitas complexidades e é um objetivo extremamente valioso que deve ser alcançado.

Perfil do patrocinador

A obtenção da resiliência em um ambiente híbrido de multinuvem complexo exige uma plataforma integrada para proteger dados, manter a alta disponibilidade e recuperar rapidamente a infraestrutura e os sistemas de tecnologia vitais em caso de desastre. A construção dessa plataforma começa com uma estratégia e um plano de resiliência integrados, que abrangem tecnologias, processos de negócios, pessoas e políticas.

O IBM Services ajuda os clientes a desenvolver e implementar estratégias e soluções de resiliência corporativa, a fim de auxiliar na diminuição os riscos na jornada para a multinuvem híbrida. Isso ajuda os clientes a otimizar a disponibilidade e a continuidade dos negócios e da TI no dia a dia, nas operações de negócios e de TI ou sob condições inesperadas, como ataques cibernéticos, falhas de hardware e software, falhas de fornecedores e desastres naturais ou causados por pessoas. Ele suporta negócios em ambientes híbridos multinuvem, incluindo nuvem pública, nuvem privada e ambientes de data center local e de colocação. Também tem uma forte prática de multinuvem nos provedores de nuvem populares, incluindo o Red Hat OpenShift, a AWS, o Azure, o Google Cloud e a IBM Cloud.

O portfólio de ofertas de resiliência da IBM inclui consultoria, infraestrutura, design/construção, implementação e serviços gerenciados, da proteção de dados, virtualização, recuperação de desastre e resiliência cibernética à computação em larga escala, resiliência de dados e aplicações, alta disponibilidade e instalações e data centers eficientes. Usando abordagens definidas por software, ferramentas baseadas em nuvem e soluções de orquestração, os serviços da IBM são desenvolvidos para ajudar os clientes a proteger sistemas de TI, manter aplicações críticas em execução e obter recuperação rápida e confiável em caso de interrupções. Para mais informações, acesse: *ibm.biz/multicloud-resiliency*.

CONTEÚDO FORNECIDO POR: IBM

Sobre a 451 Research

A 451 Research é uma empresa líder em consultoria e pesquisa em tecnologia da informação com foco em inovação tecnológica e inovação no mercado. Mais de 100 analistas e consultores disponibilizam informações essenciais para mais de 1.000 empresas clientes em todo o mundo por meio de uma combinação de pesquisa e dados sindicados, serviços de consultoria e entrada no mercado e eventos em tempo real. Fundada em 2000 e sediada em Nova York, a 451 Research é uma divisão do The 451 Group.

NOVA YORK
Chrysler Building
405 Lexington Avenue,
9° andar
Nova York, NY, EUA – 10174
+1 212 505 3030

SÃO FRANCISCO
505 Montgomery Street,
Suite 1052
São Francisco, CA, EUA – 94111
+1 212 505 3030

LONDRES
Paxton House
30, Artillery Lane
Londres, E1 7LS, Reino Unido
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA, EUA – 02110
+1 617 598 7200