Nuvem segura e *future-proof*

Como a segurança guia
seu caminho na nuvem

accenture

Segurança ajustável à sua jornada de cloud

A corrida para a nuvem está em curso. Com a resiliência das empresas sob ameaça devido à pandemia, o deslocamento para o trabalho remoto fez que muitas organizações precisassem de redes flexíveis, escaláveis e seguras – o que só foi possível graças à nuvem.

Ao mesmo tempo, novas tecnologias baseadas em nuvem oferecem oportunidades para impulsionar inovação, automatizar e perseguir novo crescimento – ou simplesmente economizar e ser mais eficiente. Para complementar o grande panorama da transformação digital significa criar um senso de urgência para que as organizações estejam preparadas na nuvem para abraçar uma continuidade de capacidades.

À medida que estes fatores se juntam, as incertezas históricas sobre cloud foram se dissipando.

No entanto, a acelerada adoção de cloud também expõe as empresas a novos riscos de negócio – especialmente quando se trata de potenciais vulnerabilidades de segurança.

Por exemplo, novas experiências digitais na nuvem podem clarear o caminho para a transformação, mas elas também criam novos vetores. No setor de saúde, descobriu-se recentemente que mais da metade (53%) dos dispositivos médicos e de outros dispositivos de Internet das Coisas (IoT) conectados possuem vulnerabilidades críticas que podem se materializar em incidentes de segurança além de expor a privacidade dos pacientes.[1]

As organizações deverão balancear as necessidades de segurança de hoje com as de amanhã. Elas deverão estar preparadas e ser ágeis para garantir sua pegada de tecnologia existente e se aprontar para gerir o que estiver adiante – onde quer que se encontrem na jornada para a nuvem. E muitas vezes elas precisam fazer isso sem a possibilidade de recorrer a recursos adicionais.

Em qualquer jornada para a nuvem, se a continuidade de cloud for o mapa, segurança é a bússola que orienta as organizações para que naveguem mais efetivamente.

80%

das cargas de trabalho poderão estar na nuvem nos próximos três anos.

Tempos desafiadores

As organizações deveriam considerar seus perfis de segurança em fase do quadro de problemas como:

Aumento do número de ataques

Ameaças de segurança bem-sucedidas estão aumentando – independentemente de setor econômico ou geografia. Nosso estudo de 2021 revela 270 ataques por empresa, um aumento de 31% sobre 2020. Estes ataques ocorreram tanto em ambientes de cloud quanto *on-premise*.

Táticas de ameaças inteligentes

Ataques cibernéticos estão cada vez mais sofisticados com criminosos evoluindo agilmente obtendo vantagem das tecnologias emergentes mais rapidamente que a maioria das organizações.

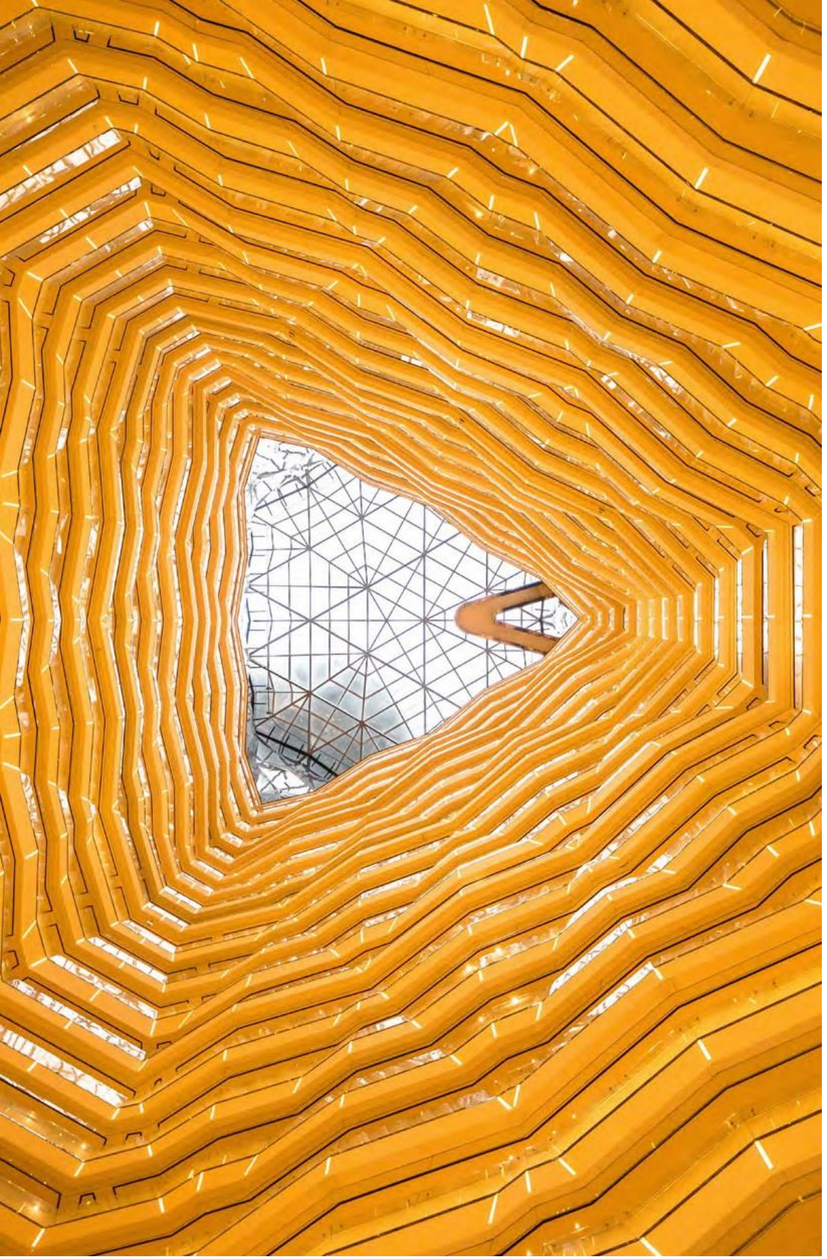
Por exemplo, operadores de ransomware violam a infraestrutura de cloud e introduzem novas técnicas de criptografia para evitar a detecção.

Paralisia da análise de segurança

Garantir visibilidade e controles é necessário, mas as equipes de segurança podem se perder em paralisia de análises ou soluções sofisticadas demais para fechar uma brecha de segurança. Por exemplo, quando um regulador quer evidências de como uma organização protegeu sua cloud, a equipe de segurança pode ter dificuldades para realizar tal demanda, isso porque os antigos modelos estruturados de controles focados em data centers não se alinham nem atendem adequadamente às capacidades digitais modernas atuais.

Nossa pesquisa anual "Estado da Resiliência da Cibersegurança" constatou que essas companhias que alinham bem suas práticas de proteção com a estratégia de negócio obtêm melhores resultados. Elas se saem melhor para suspender ataques, encontrar e consertar brechas de segurança mais rapidamente e reduzir seus impactos.

Equipes de segurança devem ser ágeis e se alinhar ao negócio a fim de estar preparadas para proteger suas organizações e permitir novas oportunidades na nuvem.



Pontos cegos de segurança

Equipes de segurança devem reconhecer onde sua organização está na jornada na nuvem. No entanto, elas são travadas por:

Uma alteração na cultura de segurança

A mentalidade de uma segurança tradicional é baseado em controle; por exemplo, controle do perímetro para limitar quem tem acesso a tecnologia. Mas quando a segurança de rede adota uma abordagem de confiança zero (*Zero Trust*) – onde, por definição, ninguém e nada é confiável sem uma previa análise contextual da utilização do recurso solicitado–, é necessária mudar o controle direto para uma responsabilidade compartilhada. Aprender como renunciar ao controle exige uma mudança da cultura. Além disso, hoje em dia, as equipes de segurança estão muitas vezes mais focadas no processo do que nos resultados; elas precisam estar cientes de que as ações de segurança precisam acompanhar o ritmo do contexto de uma jornada na nuvem evolutiva em constante mutação a fim de evitar novos riscos.

Uma escassez de habilidades

Profissionais de segurança tradicional possuem dois conjuntos de habilidades principais: administradores de segurança (infraestrutura, gerenciamento de vulnerabilidades, capacidades de segurança de redes) e equipes de defesa cibernética (inteligência de ameaças, investigação, resposta a incidentes). Os recursos atuais estão sendo solicitados a executar suas funções de novos modos, que incluem requisitos de novas habilidades. O que falta são profissionais com expertise em domínio de segurança e capacidades tecnológicas em nuvem, como engenheiros de software com competência em gestão de identidade e acesso. Atualizar recursos existentes e somar novas habilidades será necessário a fim de fazer uso completo de uma abordagem de *Cloud Continuum*.

Avanços da automação em software superam segurança

À medida que as iniciativas de nuvem evoluem e estimulam avanços da automação em software, o gerenciamento tradicional do Ciclo de vida de desenvolvimento de (SDLC) tornou-se mais ágil. A segurança precisa acompanhar as demandas de capacidade, e o único modo de alcançar isso é por meio da automação. Aumentar a automação no desenvolvimento de software requer o mesmo das capacidades de segurança para proteger efetivamente serviços emergentes nas plataformas na nuvem. Infelizmente, a escassez de habilidades e capacidade nos domínios da segurança atrasam estes avanços da automação em software.

Uma incapacidade para balancear recursos

A nuvem pode impulsionar tecnologias de segurança, como detecção de parâmetros e resposta, gestão da informação de segurança e eventos (SIEM), arquiteturas baseadas em confiança e inteligência contra ameaças cibernéticas. Mas quando as empresas abrem as portas para essas tecnologias, o estresse sobre recursos e capacidades de segurança existentes podem alcançar um ponto de ruptura, introduzindo novas vulnerabilidades. Os CISOs deverão ajustar diversas alavancas para gerir sua jornada na nuvem – incluindo tecnologia, mão de obra e parceiros estratégicos. Após mais de uma década de segurança na nuvem, existe muito a ser aprendido com aqueles que já passaram por isso. Quando as habilidades faltam dentro de casa, há lições, capacidade e amplo conteúdo *open source* de automação de segurança disponível para as organizações darem inicio a sua jornada.

42%

dos entrevistados afirmaram que segurança e risco de compliance eram grandes problemas para adoção de nuvem.

30%

dos CISOs afirmaram não dispôr das habilidades necessárias para migrar para a nuvem.

Uma jornada na nuvem segura é um evento sem fim

Departamentos de segurança serão desafiados a enfrentar ameaças e a se adaptar continuamente a fim de evitar atrasos nas jornadas de suas empresas na nuvem.

À medida que nos movemos na direção de uma internet mais centrada em humanos e abraçamos avanços como o metaverso, as equipes de segurança devem melhorar suas competências e agilidade em proteção na nuvem para identificar claramente os riscos crescentes e responder o mais rapido possivel.

Os gestores deverão estar confiantes em terem identificado os vetores de ameaças para riscos mais críticos e gerenciar eficientemente a exposição a novos riscos tão rápido quanto os desenvolvedores de software criam novos serviços.

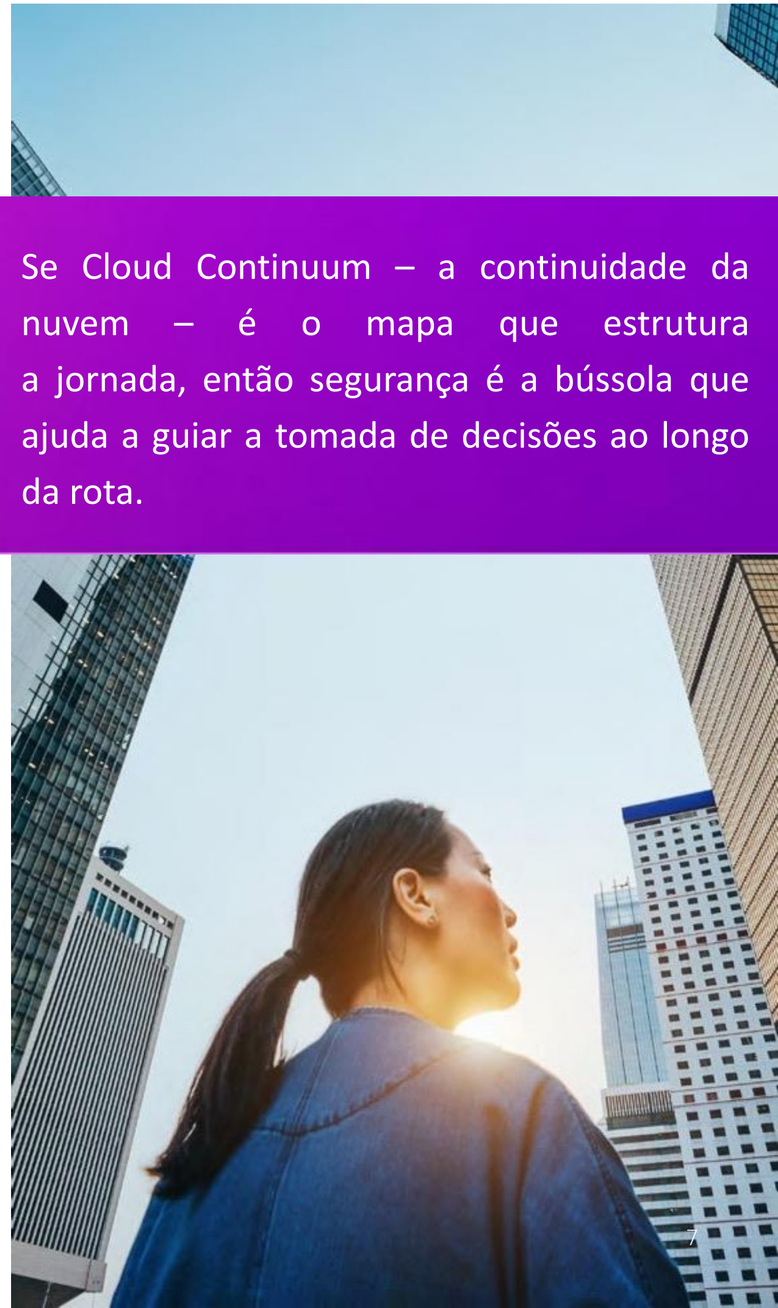
Aonde você está indo?

Não importa se acabou de começar ou se já está no meio da sua jornada na nuvem, as organizações precisam ter uma clara visibilidade dos resultados do negócio, dos riscos residuais ou emergentes e dos modos de os endereçar. Elas deverão compreender o status do progresso atual e ter uma visão abrangente da direção definida.

Os gestores na empresa precisam ter um campo de visão sobre o desempenho de segurança na organização inteira. Eles deverão reconhecer quando as ações de suas equipes de segurança estiverem impulsionando os objetivos de negócio e quando não. Eles deverão ser capazes de identificar a diferença entre equipes de segurança protegendo a organização de ameaças ocultas e bloqueando os avanços.

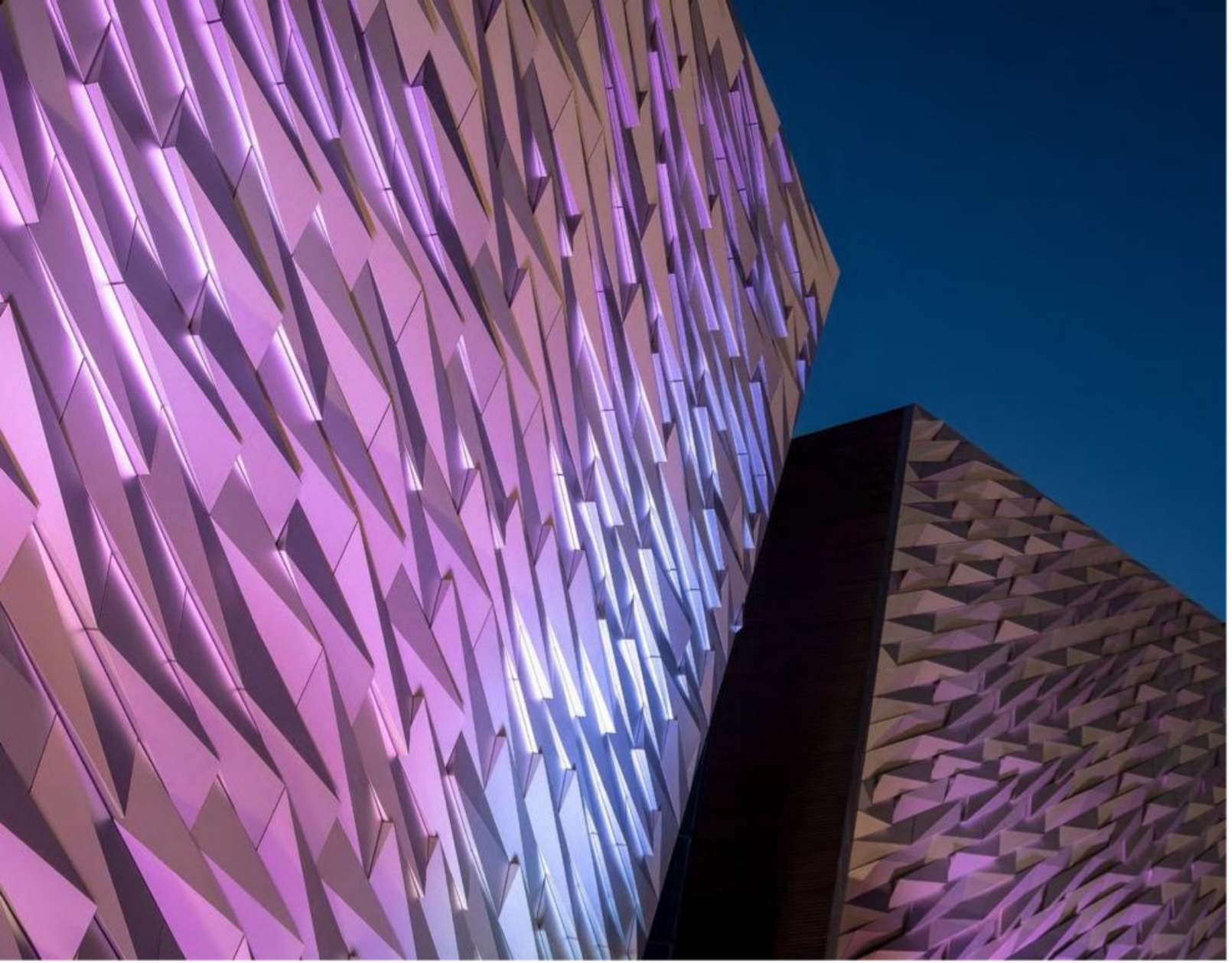
Eles deverão entender a diferença entre acreditar que a empresa está segura e saber que ela está segura. Eles deverão avaliar se a segurança da nuvem está atrasando o seu ritmo ou ajudando a acelerar a jornada.

Por sua vez, os líderes de segurança deverão conhecer o ritmo desejado dos avanços em qualquer jornada na nuvem, de modo que possam aplicar as medidas adequadas para proteger a empresa.



Se Cloud Continuum – a continuidade da nuvem – é o mapa que estrutura a jornada, então segurança é a bússola que ajuda a guiar a tomada de decisões ao longo da rota.

Para se beneficiarem de cloud da maneira mais segura, as organizações precisam se perguntar: nossa capacidade de segurança está nos ajuda a navegar e a progredir na jornada na nuvem?



Definição da rota

Sempre que iniciamos uma jornada, existe um checklist mental que costumamos seguir:

- Sei para onde vou?
- Planejei o meu percurso?
- Arrumei os itens essenciais para a viagem?

Vamos assumir que os fundamentos estão cobertos para uma jornada de cloud de uma organização – a direção geral está estabelecida, um provedor de nuvem está a bordo, a equipe de segurança está comprometida. Agora vem a escolha da rota a seguir e a certeza de que não existe modelo de solução único que atenda a todos os casos.

Se por um lado reconhecemos que existe uma série de abordagens que podem ser adotadas, as rotas a seguir representam os dois fins do espectro normalmente considerado na migração para a nuvem:

A rota direta leva as organizações por terrenos desafiadores – mas usa a autoestrada para ajudar a via expressa da inovação. Esta abordagem 'dirija e aprenda' permite aos executivos visualizar a jornada da nuvem através de lentes incrementais e táticas: menor investimento inicial e maior abordagem '*nuvem-nativa*'. Aqui, as capacidades de segurança podem ser predominantemente extensões de um ecossistema existente.

A rota panorâmica leva as empresas por uma estrada mais sinuosa através de alterações culturais e complexidade da nuvem, mas extrai os benefícios da transformação do negócio ao longo do trajeto. Esta estrada 'intensa e planejada' possibilita aos executivos visualizar a jornada de cloud através de lentes transformadoras – menos 'chave-na-mão' e mais estratégia e governança *North Star*. Aqui, as competências podem ser mais de transformações em termos de migrar redes de segurança para uma abordagem Zero Trust.

Paradas essenciais deverão oferecer visibilidade sobre defesa cibernética e garantia de controles. E "*check-ins*" periódicos podem ajudar a confirmar que a rota definida está alinhada com a estratégia de negócio da organização.

Ambas as rotas verão empresas alcançarem seus objetivos finais, mas criando experiências diferentes. De uma perspectiva de segurança, cada percurso é efetivo e válido, porém possui diferentes riscos e requer uma abordagem diferente.

30%

dos CISOs afirmaram que segurança não fazia parte das discussões iniciais em torno da migração para a nuvem, e que agora eles estavam tentando recuperar o atraso.

Escolha da rota

Cada percurso tem implicações diferentes para o modo como as equipes de segurança orientam os avanços na jornada na nuvem.
Estas rotas destacam como as táticas de segurança atuais podem precisar de ajustes para prosseguir de forma efetiva.

	A ROTA DIRETA **Dirija e aprenda**	**A ROTA PANORÂMICA** **Intensa e planejada**
Jornada na nuvem	Migração para um provedor de nuvem primário em ambiente SaaS, IaaS e PaaS a fim de expandir a presença na nuvem.	Migração para um ambiente híbrido/multicloud; mais complexo, mas oferece resiliência de longa duração.
Foco da segurança	Iniciativas de segurança concentram-se em otimizar a integração e a mudança incremental adicionando segurança ao seu conjunto de ferramentas existente; trabalhando em ambientes nativos e fundindo isso em ferramentas que suas equipes já conhecem; envolve política de engenharia de software como código (DevSecOps).	Iniciativas de segurança focam em romper e modernizar sistemas complexos e envolvem empreender mais atividades do tipo North Star, como adotar Zero Trust para transformar a abordagem de segurança de rede; iniciar migração de talento e cultura para apoiar a arquitetura de proteção.

Para ambas as rotas, empregue gestão de identificação e segurança dos dados.
O grau de complexidade depende da rota escolhida.

Gerenciar riscos

Fatores que influenciam riscos e progressos na jornada na nuvem:

Específicos de setor: Alguns setores econômicos são mais prováveis de ter sucesso numa rota e não em outra. Por exemplo, questões de ordem regulatória ou de compliance são conhecidas por afetar a migração do setor de bancos para a nuvem segura.

Específicos de localização: A presença geográfica pode influenciar os avanços. Por exemplo, organizações globais ou multinacionais *vs* organizações regionais têm demandas de segurança diferentes. Nuvem soberana, que permite que organizações controlem a localização, o acesso e o processamento de dados num ambiente de nuvem, também possuem implicações sobre padrões setoriais emergentes em certos países e setores.

Específicos de engajamento do cliente: Considere os riscos associados aos vários meios de engajamento do cliente. Por exemplo, se comprometer diretamente com clientes por meio de uma plataforma digital como *Uber* ou *Airbnb* implica em diferentes riscos ao gerenciar inumeros fornecedores e processos de pagamento num contexto business-to-business (B2B).

Específicos de inovação: Novos serviços de nuvem precisam de uma avaliação de risco antes de sua adoção; a segurança precisa manter o ritmo das aprovações ou reprovações dos serviços que abrem a porta para riscos incrementais. Por exemplo, a modelagem de ameaças, uma avaliação de risco ou de impacto sobre os negócios e uma determinação de risco residual podem proporcionar a introdução de novos serviços.

À medida que o metaverso se expande, os gestores de segurança deverão se adaptar para atender às necessidades da empresa.

Sua bússola de segurança

As empresas que quiserem se beneficiar das oportunidades trazidas pela continuidade da nuvem precisam entender quais decisões devem ser tomadas e que segurança não é necessária para apoiar o resultado.

Nessa jornada, as organizações têm um número de áreas a considerar em torno do seu compromisso com segurança – relativas às suas pessoas, tecnologias e seu ecossistema de parceiros.

A forma como estes elementos são tratados depende da maturidade específica da sua jornada na nuvem – ainda que no início, acelerado ou já completamente migradas, as organizações precisam ajustar seus esforços de segurança ao longo da migração.

Além disso, riscos e fatores se alteram, por isso é importante pausar durante os *"pit stops"* e continuar se perguntando quanto a jornada:

- Nossa abordagem de segurança ainda está alinhada com a estratégia de negócio?
- Temos as habilidades relevantes?
- Pensamos na questão da capacidade?

Ao fazer estas pausas, os executivos podem checar – e até ajustar – seu rumo para garantir que estão na rota adequada.

Três considerações ao usar segurança como bússola para nortear a jornada na nuvem

Em que ponto você está?

Alinhar segurança com o negócio

Garanta que os CISOs e suas equipes de segurança estejam profundamente alinhados e instigue resultados por meio do uso da segurança como impulsionador para conduzir a jornada na nuvem.

Ação: Acelere a aplicação e a migração de dados; avalie/reequilibre as habilidades adequadas; garanta que os dados estejam apropriadamente autorizados; mostre o que foi feito está dentro dos padrões regulatórios.

O que você deverá fazer?

Garantir a segurança desde o início

Use tecnologia como alavanca para integrar e automatizar as soluções de segurança e conduzir rumo a uma arquitetura nativa de nuvem.

Ação: Teste a tecnologia a ser usada para a postura de segurança atual; beneficie-se de arquitetura e serviços de segurança *"cloud-native"* a fim de liberar seu pessoal para atividades de cibersegurança mais prioritárias.

Com quem você deverá fazer parceria?

Aponte para o seu ecossistema

Faça pausas ao longo da jornada para se engajar com fornecedores estratégicos e seus pares de segurança, aproveite insights e expertise setoriais.

Ação: Aproxime-se do seu ecossistema, incluindo outros CISOs e fornecedores, a fim de entender como eles estão lidando com os desafios comuns; antecipe as demandas por habilidades por meio da criação de comunidades de experiência técnica ou de serviços gerenciados.

As organizações não devem se sentir presas à trilha escolhida; elas podem mudar a direção de rota direta para rota panorâmica e voltar atrás de novo a para corrigir qualquer passo errado dado. O que vai “trazer luz” a rota é um guia consistente de uma bússola de segurança, uma vez que ela proporciona a agilidade para navegar qualquer jornada na nuvem.

O que é a continuidade da nuvem?

Cloud Continuum é uma gama de capacidades e serviços que se estendem de nuvem pública até computação de borda e tudo mais nesse intervalo, perfeitamente conectados por redes *"cloud-first"* e sustentados por práticas avançadas de continuidade na nuvem. O conjunto de tecnologias que integram a *Cloud Continuum* varia conforme o "site" e a localização, de próximas à empresa até totalmente *off-premise*. 5G *cloud-first* e redes definidas por software (SD-WAN) mantêm a unidade da continuidade, permitindo acesso à nuvem virtualmente de qualquer lugar garantindo que não tenha silos entre nuvens privadas, públicas, híbridas, edge ou multicloud.

Para saber mais, visite:
Futuro da Nuvem | Accenture

O que é o metaverso?

A Accenture lança seu olhar para o metaverso como uma evolução da internet que habilita um usuário deslocar-se além do browser para ocupar e/ou participar de uma experiência persistente compartilhada que estenda o espectro do nosso mundo real para o universo totalmente virtual e tudo que possa vir a ter no meio do caminho. A Accenture olha para o metaverso como uma continuidade evolutiva e expansiva sobre múltiplas dimensões; chamamos isso de Metaverse Continuum.

Para saber mais, visite:
Serviços e Soluções em Metaverso Contínuo Corporativas | Accenture

Contatos

Dan Mellen
Diretor executivo,
Accenture Security
daniel.w.mellen@accenture.com

Gretchen Myers
Líder de Cloud Security,
Accenture Security
gretchen.myers@accenture.com

Referência

[1] Health IT Security, janeiro de 2022

Fontes de dados

80% das cargas de trabalho poderão estar na nuvem nos próximos três anos. Accenture Technology Vision 2022

42% dos entrevistados disseram que segurança e riscos de compliance eram problemas graves para adoção da nuvem.
Accenture Cloud Continuum

30% dos CISOs afirmaram não possuir as habilidades necessárias para migrar para a nuvem.
Accenture State of Cybersecurity Resilience 2021

31% dos CISOs afirmaram que a segurança não fazia parte das discussões iniciais em torno da migração para a nuvem e que agora eles tentam recuperar o tempo perdido.
Ibid.

Sobre a Accenture

A Accenture é uma empresa global de serviços profissionais com capacidades líderes em digital, nuvem e segurança. Combinando experiência incomparável e habilidades especializadas em mais de 40 setores, oferecemos serviços nas seguintes áreas: Strategy and Consulting, Technology e Operations, além da Accenture Song. Todas são alimentadas pela maior rede mundial de centros de tecnologia avançada e operações inteligentes. Nossos 721 mil funcionários entregam a promessa de tecnologia e conhecimento humano todos os dias, atendendo clientes em mais de 120 países. Abraçamos o poder da mudança para criar valor e sucesso compartilhado com nossos clientes, funcionários, acionistas, parceiros e comunidades.

Visite-nos em www.accenture.com.br.

Sobre a Accenture Security

Accenture Security é uma provedora líder de serviços de cibersegurança end-to-end, incluindo defesa cibernética avançada, soluções de segurança cibernética aplicada e operações de segurança gerenciadas. Trazemos inovação em segurança, associada a escala global e a uma capacidade de entrega mundial por meio de nossa rede de centros de tecnologia avançada e operações inteligentes. Com nossa equipe de profissionais altamente especializados, possibilitamos aos clientes inovar com segurança, construir resiliência cibernética e crescer com confiança. Siga-nos @AccentureSecure no Twitter ou visite-nos em accenture.com/security.