The bridge to possible

Relatório de tendências globais de rede para 2021

Edição especial sobre resiliência de negócios: veja as cinco tendências que promovem a agilidade e a resiliência em tempos de transformação.

Conteúdo

Uma introdução – resiliência

Introdução: da continuidade dos negócios à resiliência de negócios

Nem como indivíduos nem como empresas poderíamos prever ou estávamos preparados para uma transformação geral de longo prazo como a causada pela COVID-19. Praticamente da noite para o dia, toda a força de trabalho começou a funcionar remotamente, enquanto algumas empresas se esforçavam para colocar seus produtos e serviços on-line e outras mudavam as cadeias de fornecimento estratégicas para novos fornecedores e regiões.

É evidente que a pandemia foi um alerta para todas as nações, municípios e empresas. Mas o que mudou? Afinal, não é a primeira situação difícil que as empresas enfrentam. 7 entre 10 empresas sofreram pelo menos uma crise grave nos últimos 5 anos e 95% estão convencidas de que não será a última.[1]

As empresas sofreram pelo menos uma crise grave nos últimos 5 anos.

Fonte: “PwC: Global Crisis Survey 2019”

Interrupções causadas por pessoas, como ataques cibernéticos, mandatos regulatórios e agitação social, tornaram-se uma parte cada vez mais comum da nossa rotina. No mundo todo, estamos enfrentando os impactos implacáveis de furacões, incêndios florestais, inundações e outras **catástrofes naturais** com cada vez mais frequência.

Obter sucesso nos próximos eventos de interrupção exige que os líderes de TI adotem uma nova abordagem. Uma abordagem que dê ênfase à agilidade de TI necessária para alcançar a **resiliência de negócios** em vez da abordagem mais prescritiva e reativa, que tem sido a base do planejamento tradicional da **continuidade dos negócios**. Diferente das iniciativas atuais da continuidade dos negócios, a resiliência de negócios prepara as empresas para o inesperado.

[1] PwC, “PwC’s Global Crisis Survey 2019.”

Continuidade dos negócios versus resiliência de negócios

Continuidade dos negócios: a capacidade de uma empresa de continuar entregando produtos ou serviços em níveis predefinidos aceitáveis após uma interrupção. *

Resiliência de negócios: a capacidade de uma empresa de absorver e se adaptar em um ambiente dinâmico para cumprir os objetivos, sobreviver e prosperar. **

* International Organization for Standardization, "Security and Resilience-Vocabulary", ISO 22300-2018

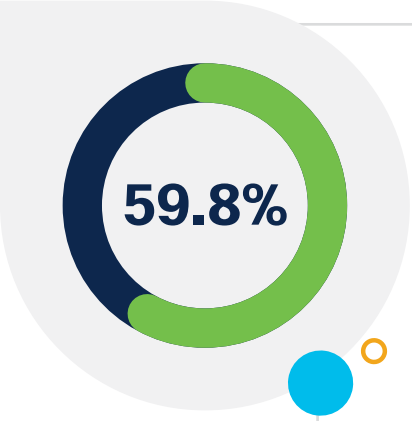
** International Organization for Standardization, "Security and resilience - Organizational resilience - Principles and attributes", ISO 22316-2017

Figura 1. Da continuidade dos negócios à resiliência de negócios

Cinco tendências da rede

A rede: cinco tendências para viabilizar a resiliência de negócios

Os processos corporativos essenciais dependem de uma rede cada vez mais complexa de tecnologias digitais que fornecem a base para alcançar a resiliência organizacional.



A maioria dos profissionais da continuidade dos negócios (59,8%) avalia a resiliência de TI como o fator mais importante na resposta à pandemia atual.

Fonte: BCI, “The Future of Business Continuity and Resilience”

Como a única plataforma que une, protege e permite um conjunto cada vez mais dinâmico e distribuído de usuários, dispositivos, aplicações e cargas de trabalho cada vez mais dissociadas e diluídas, a rede desempenha um papel fundamental em ajudar as empresas a criar resiliência.

Em outras palavras, a resiliência de rede que mantém a conectividade e o tempo de atividade da rede não é mais suficiente. As empresas precisam da resiliência proporcionada por uma plataforma de rede avançada capaz de responder rapidamente a qualquer circunstância, habilitar novos modelos operacionais e serviços, integrar-se aos processos de TI e proteger os funcionários, as atividades essenciais, os clientes e a marca. Na verdade, esta é a mesma rede avançada necessária para oferecer suporte às iniciativas de transformação digital.

Resiliência de rede versus rede de resiliência de negócios

Resiliência de rede: a capacidade de fornecer e manter um nível aceitável de serviço diante das falhas e dos desafios da operação normal de determinada rede de comunicações, com base em instalações preparadas.*

Rede de resiliência de negócios: rede criada para permitir que as empresas respondam com rapidez, segurança e eficiência diante de interrupções esperadas ou inesperadas.

* International Telecommunication Union, “Requirements for network resilience and recovery”

Como criar agilidade e resiliência para a força de trabalho, o local de trabalho, a carga de trabalho e as operações

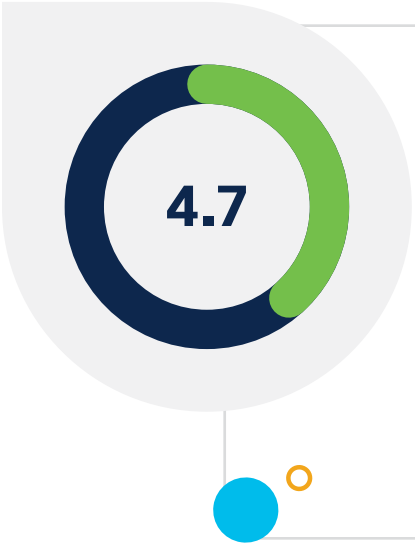
Escolhemos destacar cinco tendências que os líderes de rede devem considerar como parte das iniciativas para sustentar os planos de resiliência da empresa. Elas estão relacionadas ao aumento da resiliência de quatro esferas principais: **força de trabalho, local de trabalho, carga de trabalho e operações de TI.**

Figura 2. Base da rede para força de trabalho, local de trabalho, carga de trabalho e resiliência operacional

Força de trabalho – remota, segura

Tendência nº 1: força de trabalho – mais segurança para a força de trabalho remota

A maioria das empresas está percebendo que abordagens de trabalho novas e mais flexíveis se tornarão uma realidade permanente para os funcionários.



Em média, 4,7 vezes mais funcionários estão trabalhando em casa agora, em comparação ao cenário anterior à pandemia. Muitas equipes de TI tiveram dificuldade com a escalabilidade para lidar com a demanda repentina.

Fonte: Freeform Dynamics, "A New Perspective on the Modern Workplace", relatório patrocinado pela Cisco, julho de 2020

Como resultado, a equipe de TI se depara com um novo conjunto de requisitos de negócios:

- Dar autonomia aos funcionários para serem produtivos e colaborativos em qualquer lugar
- Otimizar o desempenho da equipe de TI, o custo e a segurança de cada funcionário
- Estender as operações de TI e a administração de nível empresarial até em casa

Mas o cumprimento desses requisitos tem seus próprios desafios. Especificamente, a segurança do funcionário remoto e o **comportamento do usuário final** continuam sendo preocupações e desafios constantes para a maioria dos departamentos de TI.

Os quatro principais desafios do departamento de TI para viabilizar o trabalho remoto:

Segurança (65%)

Comportamento do usuário final (52%)

Desempenho das aplicações (43%)

Operações de TI (35%)[2]

[2] "Pesquisa sobre rede de resiliência de negócios da Cisco para 2020"

Quando usam dispositivos e conexões pessoais para acessar aplicações e dados corporativos, os funcionários remotos ficam especialmente vulneráveis a ataques de segurança cibernética. Muitos evitam a VPN e se conectam diretamente a serviços e aplicações na nuvem pública, que continua sendo o ambiente mais difícil de proteger.[3]

Considerações de rede: quando viabilizam modelos de trabalho remoto seguros em escala, as equipes de TI devem adotar algumas ou todas as abordagens a seguir:

- **Disponibilizar VPNs escaláveis para proteger os funcionários remotos:** as VPNs corporativas continuam oferecendo uma das maneiras mais eficientes e rápidas de estender o controle e a proteção de nível corporativo para os funcionários remotos.
- **Use a autenticação multifatorial (MFA) para proteger as aplicações:** a MFA, que verifica a identidade de cada usuário antes de permitir que ele entre na rede ou acesse aplicações e dados confidenciais, é essencial para proteger a empresa.
- **Implante uma borda de serviço de acesso seguro (SASE) para garantir proteção ao acesso multicloud:** a segurança em nuvem e a SASE ajudam na defesa contra ameaças na Internet, independentemente da conexão, dispositivo do usuário ou ambiente de nuvem.

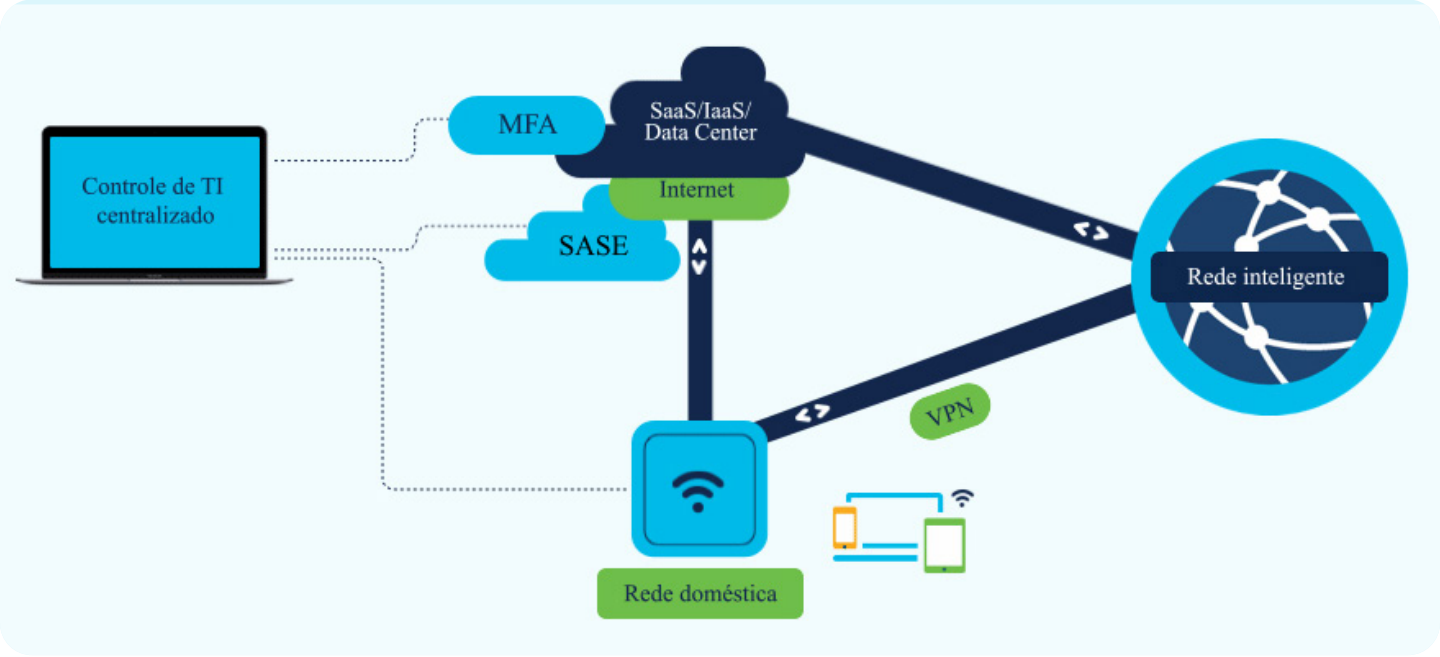


Figura 3. Força de trabalho remota segura com VPN, MFA e SASE

Saiba como conectar e proteger a força de trabalho remota

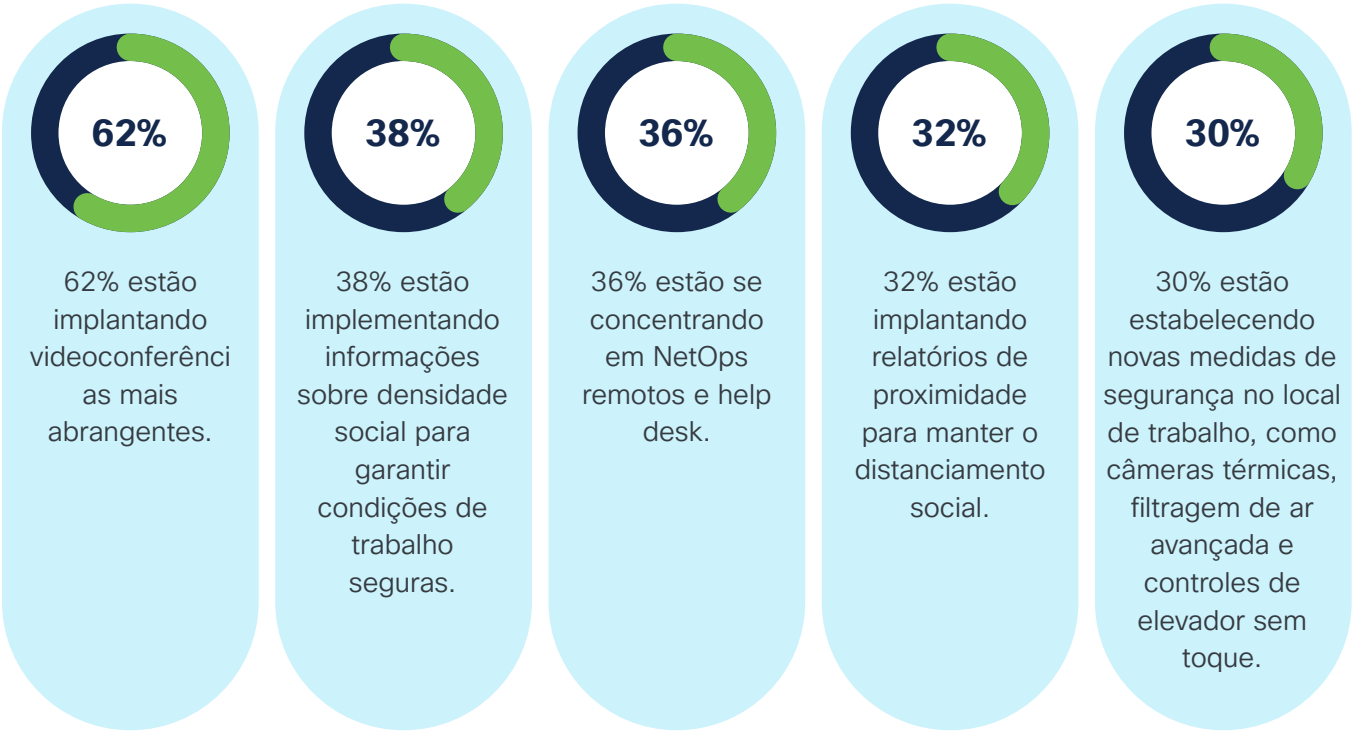
[3] Cisco Umbrella, "2019 Cybersecurity Trends."

Local de trabalho – seguro, confiável

Tendência nº 2: local de trabalho – como viabilizar o retorno seguro aos espaços de trabalho presenciais

Embora muitas perguntas permaneçam, está claro que os locais de trabalho e os espaços de trabalho vão evoluir com a pandemia. Várias empresas estão no processo de aumentar os serviços atuais, como videoconferência e Wi-Fi com base em localização. Outras estão implantando novos serviços e proteções, como monitoramento de distância física, relatórios de proximidade, maior automação do local de trabalho e até mesmo robôs que oferecem suporte à produtividade humana e à comunicação.

Como as equipes de rede estão se preparando para um retorno seguro ao local de trabalho



Fonte: “Pesquisa sobre rede de resiliência de negócios da Cisco para 2020”

Considerações sobre a rede: uma rede moderna e ágil é um mecanismo essencial que facilita a reintrodução segura e contínua de funcionários nas instalações.

- **Teste de resistência da rede:** em muitos casos, a rede está inativa há várias semanas. Não pense que ela ainda pode fornecer os serviços com e sem fio necessários.
- **Automatizar o acesso seguro de acordo com a identidade:** as empresas precisam da capacidade de gerenciar, proteger e segmentar a integração de usuários e dispositivos e o acesso a serviços de maneira constante, estejam eles conectados em redes locais, domésticas ou públicas.
- **Aumente a segurança dos funcionários e clientes por meio de análises com base na localização:** habilite o monitoramento do local de trabalho, alertas e percepções para ajudar a proteger a saúde e a segurança de funcionários, parceiros, convidados e clientes usando as redes Wi-Fi atuais.

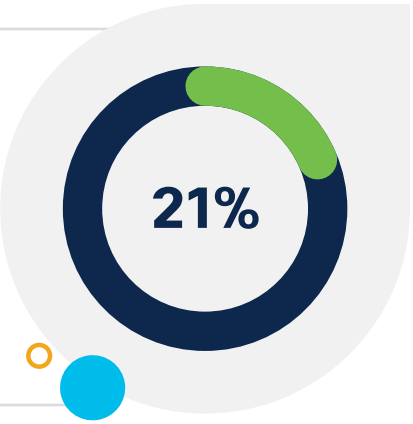
Saiba mais sobre a criação de um ambiente de trabalho seguro

Carga de trabalho – multicloud

Tendência nº 3: carga de trabalho – estímulo a ambientes multicloud para oferecer mais resiliência

Os líderes de TI estão usando os serviços em nuvem para melhorar a resiliência de negócios após a pandemia global. Isso inclui uma maior adesão ao modelo multicloud, como a distribuição de aplicações, cargas de trabalho e dados em data centers locais e provedores de nuvem pública, para reduzir custos, aumentar a flexibilidade e proteger e disseminar o risco de falhas catastróficas.

> "21% das empresas estão migrando cargas de trabalho adicionais para a nuvem pública devido aos problemas de CapEx relacionados à pandemia."
>
> IDC, "COVID-19 Impact Survey, Wave 5," 2020



Considerações sobre a rede: para garantir uma experiência confiável para usuários e equipes de DevOps, as empresas precisam de uma estratégia de rede proativa e multicloud que alinhe a rede com a nuvem, segurança e prioridades das operações de TI.

As estratégias de rede multicloud de sucesso se baseiam em três pilares principais:

- **Carga de trabalho:** adote um modelo operacional na nuvem para simplificar as políticas, a segurança e o gerenciamento de cargas de trabalho e serviços em data centers locais, várias nuvens distintas e outros ambientes de computação.
- **Acesso:** adote abordagens de SD-WAN e SASE para garantir o acesso multicloud (incluindo SaaS) constantemente seguro para usuários e dispositivos em redes públicas e corporativas no campus, na filial, em casa ou em trânsito.
- **Segurança:** reduza o risco associado a usuários, dispositivos e aplicações distribuídas em várias nuvens e outros ambientes de computação.

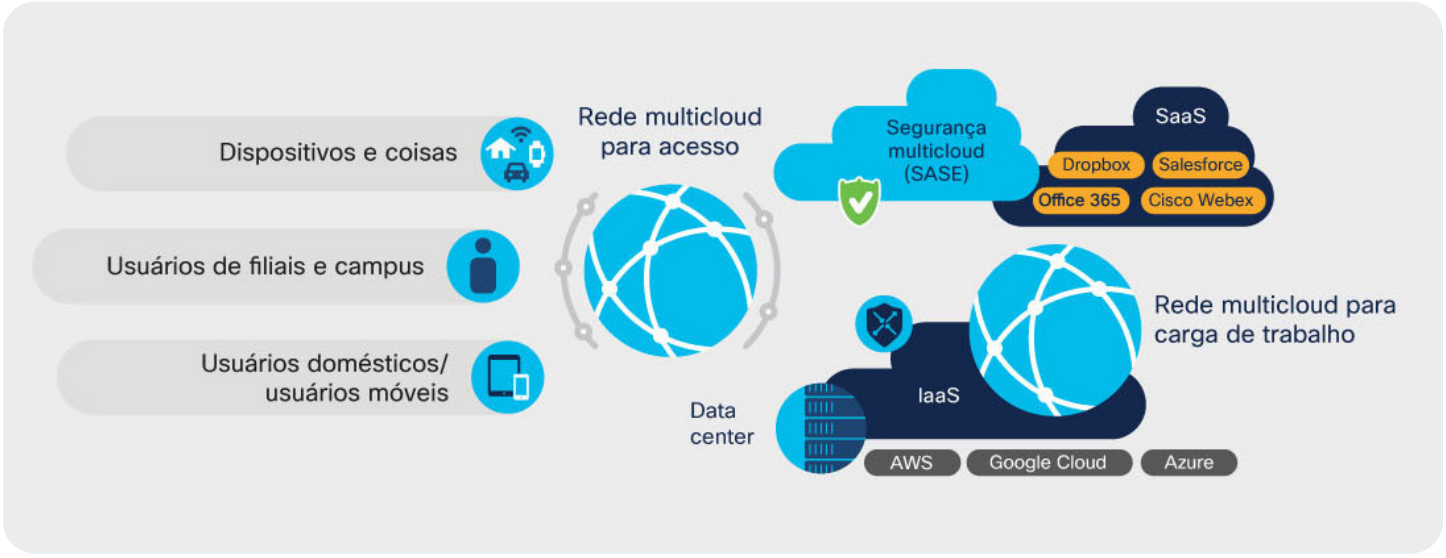


Figura 4. Rede multicloud: carga de trabalho, acesso e segurança

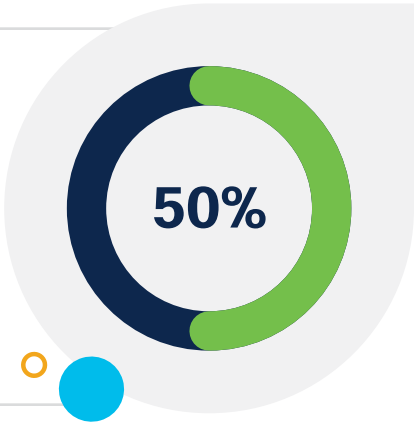
Saiba como elaborar uma estratégia de rede multicloud segura e eficiente

Operações – automatizadas

Tendência nº 4: operações – automação de operações para agilizar a recuperação

Não é só a explosão no número de funcionários remotos distribuídos que coloca uma pressão extraordinária nas equipes de NetOps hoje em dia. A pandemia também gerou níveis sem precedentes de grandes flutuações em contagens de clientes, padrões de tráfego de aplicações e novos casos de uso, como e-learning, videoconferência, eventos virtuais, atendimento remoto, automação de processos e outros serviços que dependem da rede.

> "50% priorizam a automação de rede para lidar com as interrupções atualmente."
>
> Pesquisa sobre rede de resiliência de negócios da Cisco para 2020



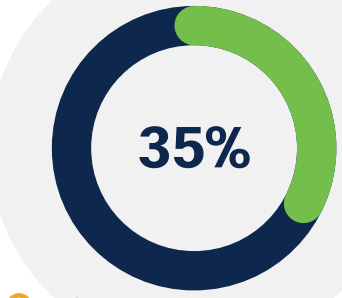
Não é surpresa que hoje metade dos profissionais de rede reconheça a automação como requisito fundamental para garantir serviço e desempenho contínuos durante uma interrupção.

Fonte: Relatório de tendências globais de rede da Cisco para 2020

Considerações sobre a rede: as equipes de NetOps podem obter melhoria contínua e responder rapidamente ao aumento de interrupções e ameaças adotando uma abordagem passo a passo:

- **Automatize tarefas administrativas repetitivas,** como provisionamento de rede, configuração e gerenciamento de imagens para reduzir a carga administrativa e melhorar a conformidade em cada domínio.
- **Automatize o acesso à rede, a integração e a segmentação** para proteger grupos de usuários e dispositivos distribuídos, bem como mitigar a propagação de ataques de segurança cibernética.
- **Automatize a política de rede no data center corporativo** com segmentação centrada em aplicações que protege aplicativos e dados e segue a carga de trabalho.
- **Automatize a política além do data center para a nuvem** com um modelo operacional na nuvem que oferece uma política de aplicações constante em ambientes de nuvem híbrida e local.
- **Automatize a segmentação com base em políticas de vários domínios de ponta** a ponta para estabelecer um modelo de acesso zero-trust completo e confiável, de usuários e dispositivos a cargas de trabalho.

> “35% planejam que as redes sejam baseadas em intenção em todos os domínios até 2022, em comparação a apenas 4% em 2019.”
>
> Relatório de tendências globais de rede da Cisco para 2020



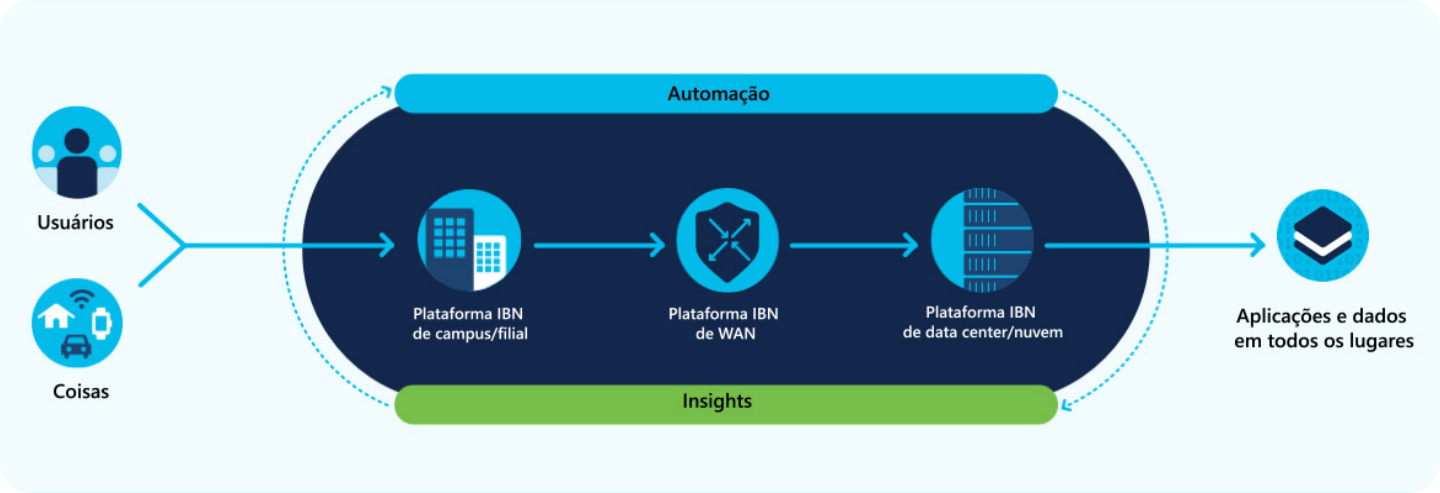


Figura 5. Automação e informações do usuário para a carga de trabalho em qualquer lugar

Saiba como automatizar políticas em vários domínios de rede

Operações – com inteligência artificial

Tendência nº 5: operações – uso de análise de rede alimentada por AI para obter informações mais inteligentes

Gerenciar a complexidade e a escalabilidade das redes modernas e o acúmulo de eventos e problemas resultantes que bombardeiam várias plataformas de monitoramento diferentes pode ser devastador e ineficiente, especialmente quando ocorre uma interrupção.

> "4.400: número médio de eventos mensais sem fio em uma rede corporativa. *"
>
> Fonte: Cisco telemetry: Cisco DNA Center, 2020

* Com base em mais de 600 redes corporativas. Os eventos incluem falhas/tempos de integração, taxa de transferência de rádio e tempo de resposta/falhas de DHCP. Esses números de eventos já foram reduzidos usando a linha de base dinâmica com inteligência artificial.

Claramente, as equipes de NetOps precisam da ajuda de análises avançadas para tomar decisões de correção inteligentes e oportunas.

Ao usar análises de rede com inteligência artificial e técnicas de aprendizado de máquina, as equipes de NetOps estão alcançando um conjunto muito mais gerenciável de problemas que elas podem resolver.

> "Em nível global, o Cisco AI Network Analytics, uma aplicação do Cisco DNA Center, resolve 2,6 milhões de "eventos" mensais em 15.080 "problemas" acionáveis – uma redução de 99,4%. *"
>
> Fonte: Cisco telemetry: Cisco DNA Center, 2020

* Com base em mais de 700 redes corporativas distribuídas globalmente.

Essa redução está permitindo que as equipes concentrem todos os esforços no que realmente importa e que tem potencial para causar impacto negativo nos negócios.

E esse problema não está mais limitado à rede corporativa. Agora que a maioria das transações em rede têm origem na rede corporativa tradicional ou terminam fora dela, as equipes de NetOps também precisam de visibilidade e análise para as redes públicas às quais estão conectadas. Isso é especialmente importante durante períodos de estresse incomum, como a recente pandemia.

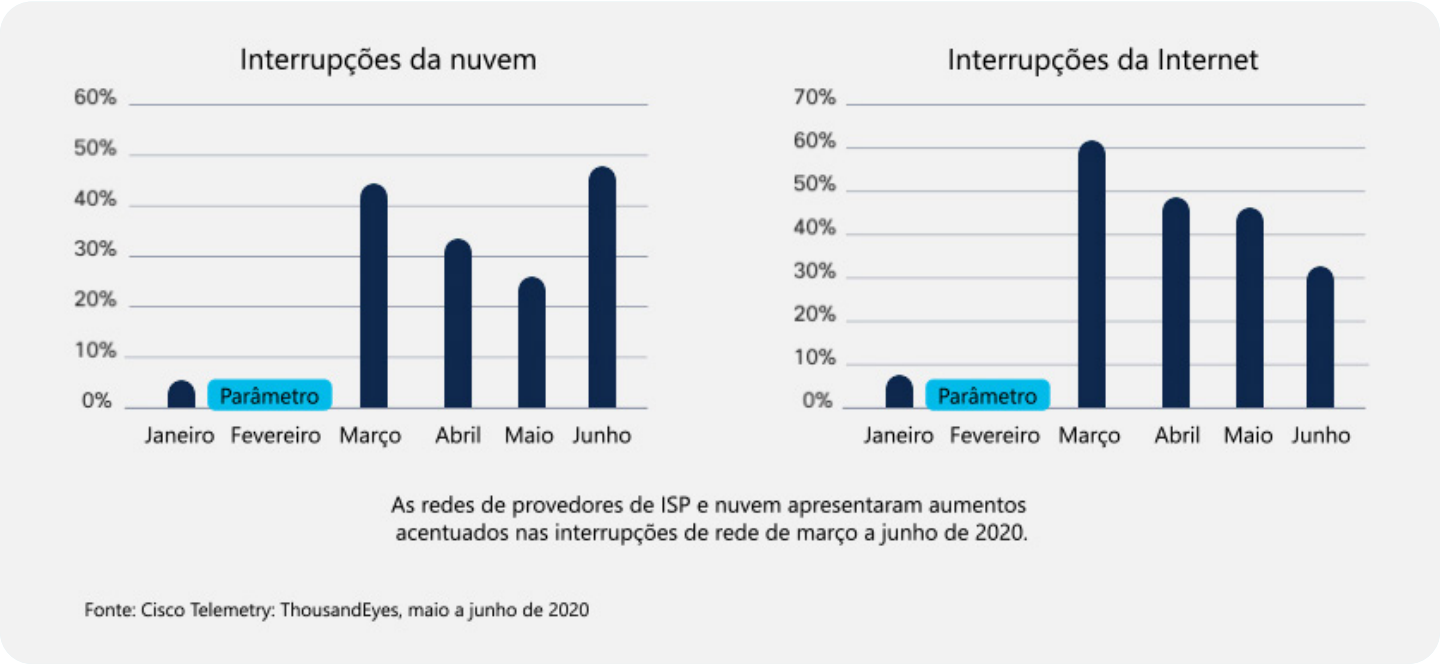
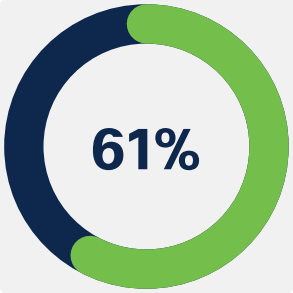


Figura 6. A interrupção de serviço de Internet e nuvem aumenta durante a pandemia

> "A Cisco ThousandEyes identificou um aumento de 61% no número de interrupções em redes de ISP e um aumento de 44% em redes de provedor de nuvem entre fevereiro e março de 2020."
>
> Cisco ThousandEyes, "Internet Performance Report: COVID-19 Impact Edition", 2020



Considerações sobre a rede: para entender um tsunami de eventos, as equipes de NetOps devem adotar análises de rede com inteligência artificial e sistemas de garantia para alcançar o seguinte:

- **Detecção mais precisa:** melhore a precisão da detecção automatizada de problemas e anomalias em domínios e entre eles.
- **Correção mais rápida:** correlacione eventos para detectar e descrever claramente a causa mais provável de problemas e anomalias.
- **Gerenciamento automatizado de políticas:** identifique dispositivos, aplicações e tendências e ofereça atualizações de políticas recomendadas.
- **Menos degradações:** identifique padrões e tendências e forneça informações contextuais que aceleram a ação proativa, corretiva e preventiva.
- **Inteligência de pares:** forneça inteligência e análise que ajudam os administradores de rede a comparar o desempenho de rede com referenciais globais, regionais ou do setor.

Saiba como você pode usar informações com inteligência artificial para gerenciar melhor as redes:

Informações de rede para data center

Concluindo

Conclusão: melhoria da resiliência de negócios com uma plataforma de rede avançada

Eventos desestabilizadores continuarão desafiando a nós e às redes ao longo de nossas carreiras. É hora de repensar como a estratégia de rede viabiliza a estratégia de resiliência de negócios e priorizar os novos recursos de rede mais necessários para ficar à frente do próximo grande acontecimento.

A automação e as informações com inteligência artificial oferecidas por redes baseadas em intenção fornecem uma plataforma eficiente para ajudar a se adaptar a qualquer circunstância. Elas oferecem agilidade, segurança, inteligência e velocidade necessárias para dar suporte ao seguinte:

- **Força de trabalho:** capacitar os funcionários com desempenho seguro de nível corporativo e acesso às aplicações enquanto trabalham em casa, no escritório e em qualquer lugar
- **Local de trabalho:** permitir que os funcionários voltem com segurança ao escritório com monitoramento, alertas e informações habilitadas para Wi-Fi
- **Carga de trabalho:** estimular modelos de resiliência multicloud e proteger dados e aplicações, estejam as cargas de trabalho em nuvens públicas e data centers locais
- **Operações:** automatizar políticas de rede de ponta a ponta e segmentação, bem como simplificar tarefas administrativas, melhorando a visibilidade, reduzindo alertas e permitindo uma correção mais rápida

No novo normal, basta ter uma rede que possa se adaptar para enfrentar o futuro. À medida que você pensa na estratégia de resiliência de negócios, considere como a rede pode ser um facilitador fundamental dessa estratégia.

Para obter mais informações sobre a resiliência de negócios

Outros assuntos em que você pode estar interessado

Resiliência de negócios | Webinars

Cisco Digital Network Architecture (Cisco DNA)

C96-744694-00 01/21