



Relatório Global de Tendências de Redes de 2020



Conteúdo

Introdução: situação das redes para a era digital

4

O papel em evolução da rede de TI	7
Tendências globais que definem as demandas da rede	9
Globalização	9
Transformação empresarial digital	9
Automação de negócios	10
Resiliência comercial e operacional	10
Sustentabilidade	10
Tendências de tecnologia que promovem a evolução da rede	11
A transformação do cenário de aplicativos	11
IoT	12
IA	13
Mobilidade	13
Segurança	14
Experiências imersivas	14
A necessidade de um novo tipo de rede	16
Os especialistas da Cisco vislumbram a nova arquitetura de rede	17
O estado da arquitetura de rede	19

Tendências em tecnologia de rede

20

Automação de rede em escala	23
Rede definida por software: apenas o começo	25
Rede baseada em intenção: fechando o loop	25
Virtualização de funções de rede	27
Programabilidade como um fundamento de rede	27



Tendências em tecnologia de rede (continuação)

Controladores de IBN de plataforma aberta: Integração de processos de TI e negócios	28
Alinhamento de garantia e política entre domínios: cliente para carga de trabalho	29
Garantia viabilizada pela inteligência artificial	30
O que são IA, ML e MR?	31
A complexidade da rede promove a adoção da IA	32
Como a ML e o MR são aplicados em um contexto de rede?	34
Estado atual e futuro da IA para a garantia da rede	34
Considerações para avançar com a IA	36
Rede para dados e aplicativos em ambientes multicloud	37
O impacto sobre a rede da transformação dos modelos de aplicativos	39
Otimização da conectividade, de um usuário para multicloud	41
Rede para um data center em qualquer lugar	45
Considerações ao arquitetar uma rede multicloud	48
Acesso à rede com e sem fio	49
Como proporcionar uma experiência de usuário agradável em dispositivos móveis	51
Como preparar a TI para o sucesso da rede sem fio	53
Situação atual e futura da disponibilidade de acesso à rede	53
Considerações sobre a viabilização do acesso e da rede sem fio na era digital	55
A transformação do papel da segurança de rede	56
Desafios com a segurança da rede	59
Enfrentando desafios de segurança com uma rede inteligente	61
Estado atual e futuro da segurança da rede	64



Tendências em operações de rede

65

Estado atual e futuro das operações de rede	69
Como os avanços estão transformando as operações de rede	69
Integração de operações de rede ao processo de TI	69
Alinhamento total com a equipe de TI e a intenção de negócios	71
Automação para reduzir a complexidade das operações de rede	72
Gerenciamento de incidentes e problemas reativo x preventivo	72
Trazendo a conectividade da tecnologia operacional para as operações de rede	73
Apresentando uma estrutura de operações de rede de última geração	73
Gerenciamento do ciclo de vida	74
Gerenciamento de políticas	75
Gerenciamento de garantia	76
O futuro das previsões de operações de rede para 2025	77

Tendências em talentos de redes

78

Como se preparar para as mudanças nos conjuntos de habilidades para rede	82
As maiores defasagens de qualificações profissionais em tecnologia da informação	82
As maiores defasagens de qualificações profissionais para rede	83
Aumento da necessidade de qualificações de negócios e pessoais	84
Funções cruzadas mais proeminentes no futuro	84
Novas funções para estrategistas de redes	85
Estrategista do futuro: proporcionando valor além da rede	85
Novas funções para profissionais de rede	87
Engenheiros de rede do futuro: proporcionando valor além da conectividade	87
Líderes de TI: medidas para resolver a escassez de talentos de rede	88
Recomendações para líderes de TI: como formar a equipe de rede do futuro	90

Introdução: situação das redes para a era digital

Resumo da seção



Revelações principais

- Tendências como globalização, transformação digital, automação e resiliência empresariais e sustentabilidade estão moldando os requisitos para um novo tipo de rede.
- O cenário tecnológico em evolução – modelos emergentes nativos da nuvem, Internet das Coisas, inteligência artificial (IA), tecnologia móvel, ameaças à segurança cibernética e aplicativos imersivos – está afetando drasticamente as arquiteturas e operações de rede de TI.
- A escala, a complexidade e a natureza dinâmica dessas demandas estão excedendo a capacidade dos operadores humanos.
- As novas redes estão usando tecnologias emergentes como IA, aprendizado de máquina e automação para simplificar e assegurar operações, viabilizar uma rápida adaptabilidade e aumentar a tomada de decisão humana.

Tendências globais de negócios e tecnologia que definem a nova rede

700
milhões

de contêineres
hospedados
na borda da
rede até 2021¹

50%

das cargas
de trabalho
fora do
data center
corporativo
até 2021²

14,6
bilhões

de dispositivos
na IoT
até 2022³

42%

de crescimento
anual no
tráfego móvel
empresarial de
2017 a 2022³

53%

dos ataques
à segurança
cibernética
causam mais
de US\$ 500.000
em prejuízos⁴

12

vezes
de tráfego
de RA/RV
até 2022³

Resumo da seção
(continuação)

Orientação essencial

- Os líderes de TI e estrategistas de rede devem conduzir uma abordagem passo a passo para transformar cada um dos seus domínios de rede em um modelo baseado em controlador, com base em tecnologias de automação e IA.
- Os líderes de TI devem construir um plano de negócios e tecnologia que se alinhe às prioridades comerciais e abranja arquitetura, tecnologia, operações e talentos.
- Os estrategistas e os profissionais de redes devem identificar percursos de carreira e de aprendizagem que lhes proporcionem os conjuntos de habilidades necessários para liderar esta transformação das redes e incrementar o seu valor.



Principal previsão

“Até 2025, as equipes de redes de ponta terão redes baseadas em intenção operando em vários domínios: campus, filial, WAN, data center, nuvem, provedor de serviços e segurança. Suas redes poderão compreender as exigências de aplicativos e empresariais e traduzi-las em políticas de rede e segurança. Pode-se melhorar consideravelmente a agilidade com uma automação inteligente de redes, e as redes podem operar com um poderoso loop de feedback que apresente monitoramento, segurança e otimização contínuos. A rede baseada em intenção garantirá que os serviços empresariais sejam entregues e protegidos de forma contínua por meio da rede. Esses avanços gerarão benefícios significativos tanto para as empresas quanto para a sociedade em geral”.

– John Apostolopoulos, CTO de rede corporativa, Cisco

Introdução: situação das redes para a era digital

Em uma série de memorandos redigidos em 1962, J.C.R. Licklider, diretor da Agência de Projetos de Pesquisa Avançada do Departamento de Defesa dos EUA, propôs uma “rede intergaláctica de computadores”, onde computadores de todo o mundo estariam interconectados para proporcionar acesso rápido a dados e programas em qualquer lugar.⁵

Apenas alguns anos mais tarde, em 1965, Leonard Kleinrock, Lawrence Roberts e Thomas Merrill usaram linhas telefônicas para conectar quatro computadores, criando efetivamente a primeira rede de área ampla e dando início à Internet.⁶

Mais de 50 anos depois, a visão original de Licklider permanece a mesma, pois a rede continua conectando consumidores globais de informações e serviços a aplicativos e fontes de dados.

É claro que todo o resto mudou.





O papel em evolução da rede de TI

O mundo de hoje, impulsionado pelo crescimento exponencial do desempenho tecnológico, está cada vez mais conectado, digitalizado, distribuído e diversificado. Com todas as “coisas” capazes de processar dados, os modelos computacionais têm tudo para serem muito mais distribuídos e conectados em rede. Como indica a lei de Metcalfe, com mais dispositivos e usuários adicionados, o valor e a importância da rede continuam crescendo exponencialmente.

Os negócios digitais continuam alimentando as inovações conectadas em rede. A IDC estima que haverá 48,9 bilhões de dispositivos conectados em uso em todo o mundo até 2023,⁷ e o relatório *2018 Cisco Complete VNI Forecast* de 2018 prevê que a quantidade média de dados consumidos em uma rede será de quase 60 GB por computador pessoal por mês.³





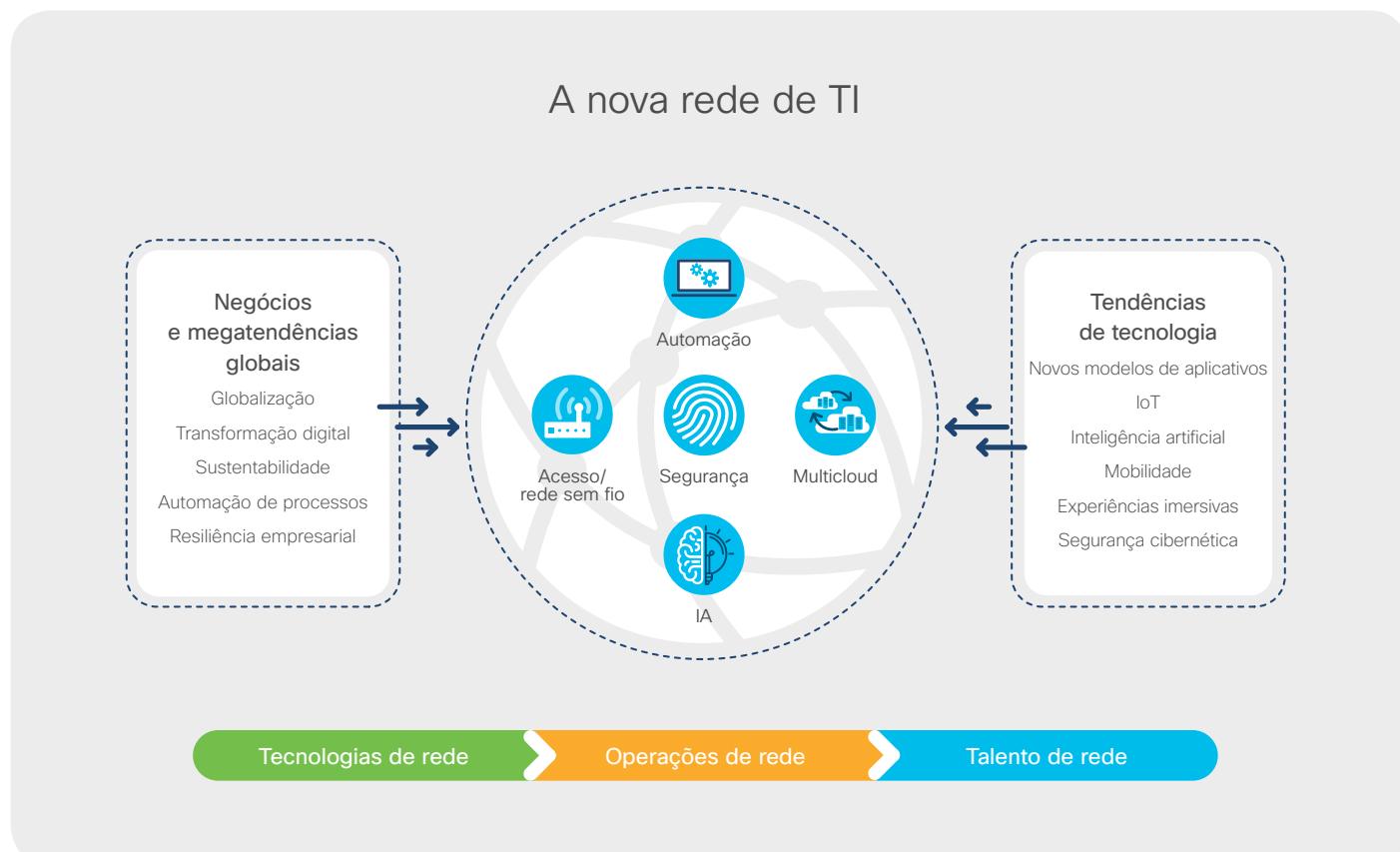
Não é surpresa nenhuma que, dado esse crescimento implacável, as equipes de TI estejam chegando a um ponto em que a escala e a complexidade das redes estão excedendo sua capacidade de gerenciá-las e protegê-las de forma eficaz. Precisamos agora de novos sistemas que combinem tecnologias como aprendizado de máquina, raciocínio de máquina e automação, a fim de simplificar as operações e melhorar a tomada de decisão humana.

Estamos no limiar de uma nova era de redes, em que a TI pode romper com as formas tradicionais de construir e operar

redes e abraçar um futuro alimentado por tecnologias que podem superar esses desafios de maneiras vastamente novas.

Antes de examinarmos as tendências de talentos, operações e tecnologias de rede emergentes que formam a base desta nova rede, vamos pensar brevemente nas tendências globais de negócios e tecnologia que impulsionam essa evolução.

Figura 1 Tendências globais de negócios e tecnologia que definem a nova rede



Tendências globais que moldam as demandas de redes

Uma série de tendências globais e de negócios estão moldando o papel que a rede desempenha em uma organização. Compreender essas tendências pode ajudar os líderes de TI a se prepararem melhor para as crescentes expectativas que os líderes de negócios estão atribuindo à rede.



60%

De acordo com o Gartner, até 2023, mais de 60% das empresas considerarão a rede algo fundamental para suas estratégias digitais, em comparação a menos de 20% hoje, considerando a rede como um facilitador estratégico.⁸

Um breve olhar sobre algumas dessas megatendências globais revela as demandas que elas provavelmente impõem sobre as redes.



Globalização

De acordo com o Fórum Econômico Mundial, estamos entrando agora em uma nova era de globalização digital, conhecida como “Globalização 4.0”. Nessa era, bens e serviços *digitais* possibilitados por recursos digitais e pela inteligência artificial, são as principais exportações.⁹

Impacto na rede

Conforme as conexões entre sistemas, pessoas, processos, locais e dispositivos ficarem mais distribuídas e complexas, o valor econômico da rede para a organização aumentará. E a segurança e o gerenciamento da rede se tornarão mais estratégicos e mais difíceis.



Transformação dos negócios digitais

Cada vez mais empresas estão usando tecnologias digitais como análise, mobilidade, soluções em nuvem e a IoT como base para transformar seus negócios. De acordo com o relatório *Digital Vortex 2019* da IMD e da Cisco, 88% dos executivos acreditam que a inovação digital terá um impacto importante ou transformador em seus setores, em comparação com apenas 27% em 2015.¹⁰

Impacto na rede

A imprevisibilidade inerente aos negócios exige uma rede que possa se ajustar rapidamente às necessidades em evolução para possibilitar novos serviços, processos e modelos.



Automação de negócios

O uso de automação e robótica nos próximos anos continuará aumentando, pois as empresas buscarão melhorar a qualidade, a produtividade da força de trabalho, a satisfação do cliente e muito mais. O Capgemini Research Institute prevê que a adoção em larga escala da automação pode gerar uma economia de custos de até US\$ 471 bilhões até 2022 nas indústrias automotiva, de varejo, de serviços públicos e de transformação.¹¹

Impacto na rede

Como a automação de processos é sensível ao tempo e de missão crítica, a rede precisa assegurar que os pacotes sejam entregues de forma confiável e pontual.



Resiliência comercial e operacional

Por causa da globalização e da transformação digital, as organizações de hoje em dia são

dependentes de uma rede cada vez mais complexa de tecnologias, sistemas, processos, cadeias de fornecimento e infraestrutura. Uma resiliência empresarial eficaz exige avaliação contínua e proativa de riscos operacionais, estabelecimento e auditoria de planos de contingência e administração de treinamento de resposta a incidentes.

Impacto na rede

Uma arquitetura de rede ágil, resiliente e segura é fundamental para proteger funcionários, clientes e parceiros e é vital para recuperar dados e restabelecer rapidamente serviços e acesso.



Sustentabilidade

À medida que nosso mundo fica mais interconectado, as empresas estão sendo desafiadas a elevar a sustentabilidade ambiental. Além das métricas já conhecidas, as empresas serão julgadas em função do quanto reduzirem as emissões de gases de estufa, preservarem a biodiversidade e os recursos naturais e projetarem produtos para minimizar ou reciclar resíduos.

Impacto na rede

As redes avançadas oferecem a promessa de maior eficiência em praticamente todos os aspectos do negócio, desde o consumo de energia até a utilização de recursos e a redução de emissões.

Tendências de tecnologia que impulsionam a evolução das redes

Atualmente, várias tendências emergentes estão transformando drasticamente o cenário de TI. Um olhar mais atento sobre algumas destas tendências-chave revela o impacto que elas podem ter na rede corporativa.



A transformação do cenário de aplicativos

É óbvio que aplicativos e dados estão no âmago dos negócios digitais. A forma de desenvolvimento, hospedagem e consumo de aplicativos está em constante mudança para atender às novas necessidades de negócios.

Eis alguns exemplos de como os aplicativos estão evoluindo e, de certa forma, reformulando a rede:

Aplicativos e dados estão saindo das instalações físicas: aplicativos e dados estão sendo distribuídos em microsserviços

e movidos para várias nuvens públicas. Em alguns casos, também estão sendo distribuídos para a extremidade da rede. E estão sendo cada vez mais consumidos por vários provedores de software como serviço (SaaS).

Os aplicativos são modulares e distribuídos em diferentes ambientes:

aplicativos monolíticos estão, em muitos casos, dissolvendo-se em microsserviços interconectados que são entregues por meio de uma série de cargas de trabalho virtuais e físicas, incluindo contêineres, em toda a empresa.



De acordo com o Uptime Institute, metade de todas as cargas de trabalho será executada fora do data center corporativo até 2021, seja em infraestruturas de nuvem e data center ou na borda da rede.²

O desenvolvimento de aplicativos vem sendo contínuo e rápido: no caso de aplicativos desenvolvidos e hospedados no local, a TI precisa acelerar a própria criação e o fornecimento de serviços de infraestrutura para atender às necessidades de aplicativos e usuários, tudo isso com custos operacionais mais baixos.

Os aplicativos estão migrando do físico para o virtual, para contêineres e para fora do servidor: a ascensão dos contêineres está expondo os paradigmas de design e implantação

de aplicativos a uma inovação muito maior: as arquiteturas sem servidor, que estão forçando as empresas a reavaliarem como os aplicativos são desenvolvidos, o papel da infraestrutura e o design de processos operacionais.



Estima-se que, até 2021, as instâncias de contêineres instaladas e em uso excederão 3,5 bilhões, com mais de 20% delas sendo executadas em locais distribuídos que atendem a cargas de trabalho de borda de rede e de IoT.¹



IoT

O uso cada vez maior da IoT em dispositivos, em aplicativos e nos dados que os acompanham está impulsionando a criação de novos modelos computacionais distribuídos que consistem em níveis exponencialmente maiores de escala e complexidade. Conforme o relatório “VNI Forecast Highlights Tool” da Cisco, os dispositivos machine-to-machine (M2M) representarão 51% (14,6 bilhões) de todos os dispositivos em rede no mundo até 2022.¹²

Impacto na rede

Com o surgimento de aplicativos e microsserviços em todos os diferentes domínios, a rede deve ser vista mais como um conjunto crescente de “clusters nervosos” interconectados e situados onde os dados estão, o que pode ser qualquer lugar ao longo do continuum entre extremidade e nuvem. A nova rede precisa ser capaz de se conectar com segurança dentro “clusters nervosos” interconectados e também entre eles, bem como de compreender fundamentalmente como esses novos modelos de aplicativos funcionam e de estender dinamicamente as políticas de aplicativos através da rede para onde quer que os aplicativos estejam hospedados.

Impacto na rede

Além de proporcionarem conectividade e segurança para uma gama incrivelmente diversificada de dispositivos de IoT, os administradores de rede precisarão criar formas escaláveis e eficientes de identificar, classificar e aplicar políticas automaticamente e monitorá-las para garantir a funcionalidade adequada sem afetar ou comprometer outros serviços executados na rede.



IA

O surgimento de aplicativos que utilizam a IA para uso empresarial e de consumidores está nos levando a um mundo totalmente novo, com dispositivos conectados, inteligentes e automatizados que estão sendo implantados em todos os lugares.



Mobilidade

De acordo com o relatório “VNI Forecast Highlights Tool” da Cisco, o tráfego global de dados móveis de negócios crescerá seis vezes de 2017 a 2022, a uma taxa de crescimento anual de 42%.¹² Os usuários de dispositivos móveis corporativos continuarão tendo expectativa de conectividade imediata e de alto desempenho em qualquer lugar, a qualquer hora e em qualquer dispositivo por meio de Wi-Fi e de redes públicas 4G e 5G. Ao mesmo tempo, os dispositivos de IoT sem fio se tornarão cada vez mais onipresentes em todos os aspectos das nossas vidas.

Impacto na rede

Para liberar todo o potencial da IA nos negócios, é preciso haver mais processamento computacional e tomada de decisão mais perto da extremidade da rede. Dependendo de desempenho, capacidade, privacidade e até mesmo de considerações de custo, o posicionamento de processamento e dados de IA irá variar da nuvem a data centers locais e até a extremidade da rede.

Impacto na rede

O acesso de funcionários a aplicativos de nuvem a partir de dispositivos corporativos e privados quando estão fora da rede está criando uma falta de visibilidade e controle que os administradores de rede e segurança ainda não enfrentaram. E uma onda de dispositivos de IoT se somará aos requisitos de rede sem fio em termos de escala, diferentes padrões de tráfego e segurança.



Segurança

As ameaças à segurança cibernética estão se tornando cada vez mais sofisticadas e perigosas ao longo de uma superfície de ataque mais ampla que não está mais contida em perímetros bem definidos e defendidos. Em particular, à medida que cargas de trabalho se deslocam para fora das instalações físicas, há o perigo de que a TI perca visibilidade.



Experiências imersivas

O uso crescente do vídeo e o surgimento da realidade virtual (RV) e da realidade aumentada (RA) para melhorar a colaboração, o treinamento, a produtividade e as experiências de trabalho remoto exigirão cada vez mais das redes das empresas.

Impacto na rede

Embora a rede continue a ser um aliado poderoso na identificação e contenção de ameaças, as operações de rede e segurança precisam compartilhar dados e integrar ferramentas e fluxos de trabalho para melhor combater o aumento contínuo do número e da sofisticação dos ataques. Além disso, a rede pode estender o alcance da TI a ambientes de nuvem para ajudar a proteger aplicativos e dados, mesmo quando estes não estão diretamente sob seu controle.

Impacto na rede

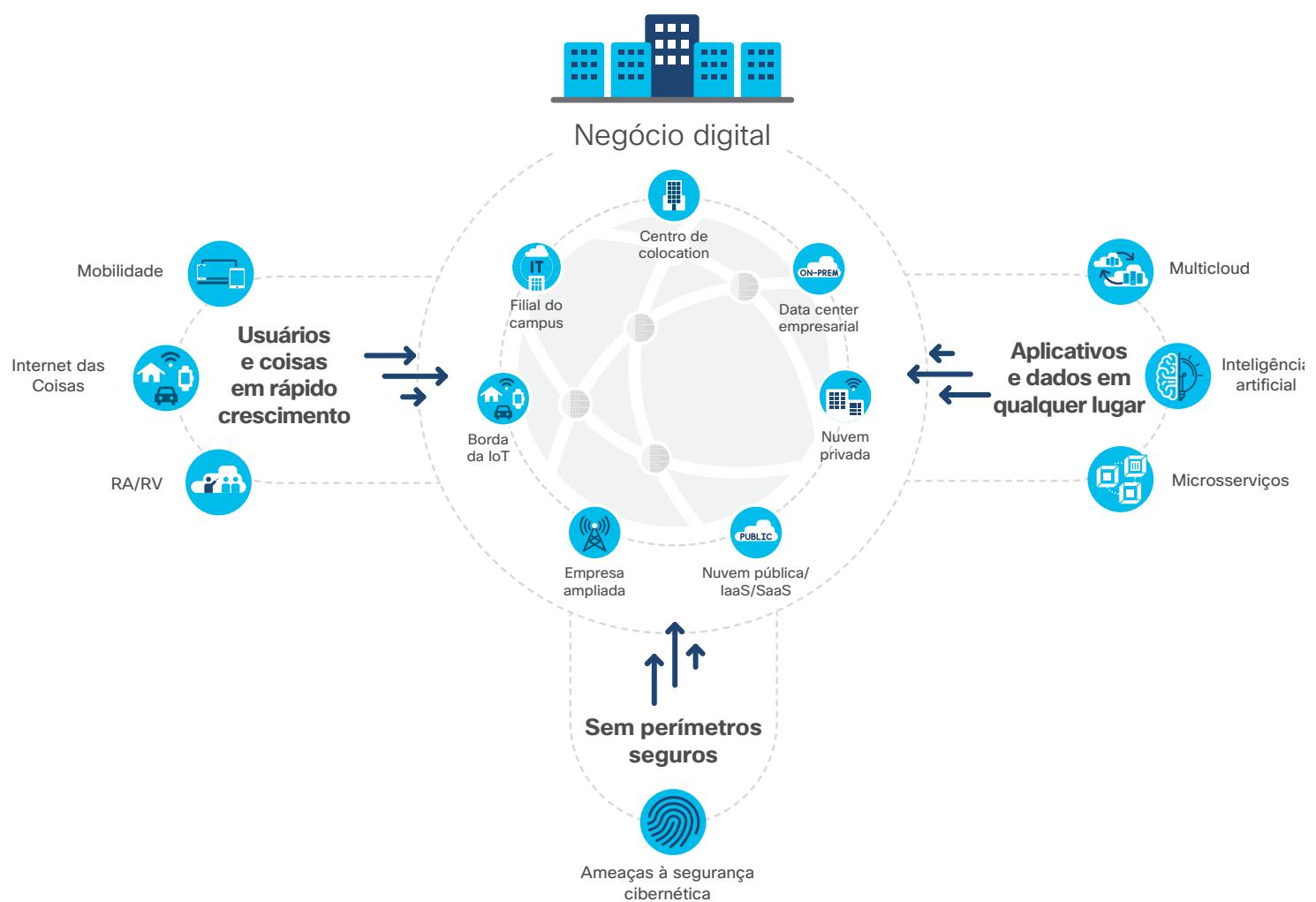
A rede terá de fornecer a largura de banda de ponta a ponta, comunicação de baixa latência e os controles de desempenho dinâmicos necessários para viabilizar tais experiências imersivas.



Até 2022, o vídeo representará 82% de todo o tráfego empresarial na Internet, o tráfego de RV/RA aumentará em 12 vezes e o tráfego de vigilância por vídeo na internet aumentará em sete vezes.¹³

Este cenário de tecnologia dinâmico não é apenas uma realidade para todas as empresas e seus clientes. É também o motor da economia digital. Por isso, não é nenhuma surpresa que a TI esteja sentindo a pressão para abordar todas essas tendências com as estratégias de tecnologia de rede, modelos de operações e talentos corretos.

Figura 2 Tecnologias determinando novas exigências de rede



A necessidade de um novo tipo de rede

Neste ambiente cada vez mais exigente, há uma necessidade crucial de que os líderes de TI migrem para uma abordagem radicalmente nova das redes.

Para que uma empresa cresça na economia digital, a rede precisa ser capaz de se adaptar rapidamente a exigências empresariais em constante mudança. A rede precisa comportar um conjunto de usuários,

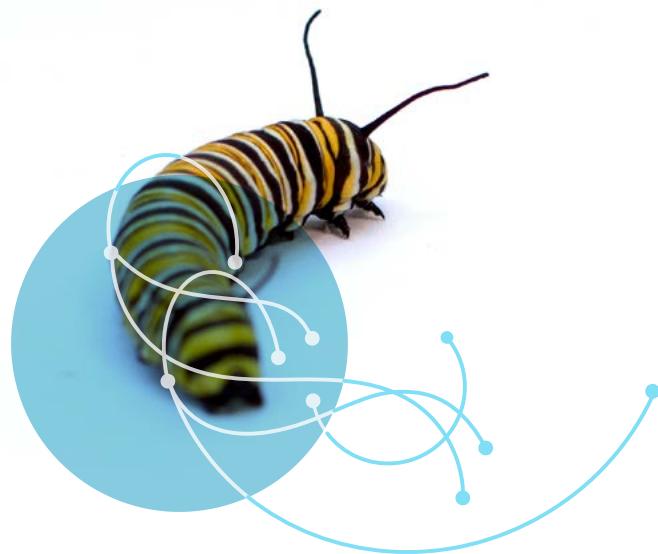


Figura 3 Quatro objetivos principais da nova rede

Alinhar com a empresa	Complexidade abstrata	Assegurar o desempenho	Reducir riscos
<ul style="list-style-type: none">• Proporcionar novas iniciativas de negócios digitais• Alinhar-se dinamicamente às necessidades de aplicativos dinâmicas	<ul style="list-style-type: none">• Simplificar as operações de TI em face do aumento das demandas• Permitir que a equipe de TI concentre recursos na criação de valor comercial	<ul style="list-style-type: none">• Atender de modo constante aos requisitos de desempenho de serviço e experiência do usuário• Evitar interrupções de rede	<ul style="list-style-type: none">• Prevenir ou conter ameaças à segurança antes que elas causem danos• Cumprir os requisitos regulamentares e de conformidade

dispositivos, aplicativos e serviços cada vez mais diversificados e em rápida mudança. Ela precisa incorporar de forma transparente e segura esse conjunto diversificado de dispositivos e fornecer a experiência desejada do usuário e do aplicativo.

Também precisa garantir um acesso rápido e seguro às cargas de trabalho e entre elas, onde quer que estejam. E, para que a rede funcione de forma otimizada, tudo isso precisa ser alcançado de ponta a ponta entre usuários, dispositivos, aplicativos e serviços em todos os domínios de rede: campus, filial, remoto/home, WAN, provedor de serviços, tecnologia móvel, data center, nuvem híbrida e ambientes com várias nuvens.

Isso significa que as empresas precisam de uma nova arquitetura integrada para cada domínio de rede. Ela deve ser personalizada para atender às necessidades específicas daquele domínio e propor uma maneira de comunicar e aplicar políticas consistentes em todos os domínios.



Os especialistas da Cisco vislumbram a arquitetura de rede emergente.

A maioria das redes atuais ainda não está pronta para atender às demandas desta era digital emergente. Na nossa *Pesquisa global de tendências de rede de 2019*, descobrimos que, enquanto 39% dos líderes de TI acreditam que suas redes estão muito bem alinhadas para atender às demandas dos negócios digitais, apenas 19% dos estrategistas de rede pensam da mesma forma.¹⁴

No entanto, há razões para otimismo.

John Apostolopoulos, CTO de rede corporativa da Cisco, prevê uma transição relativamente breve das atuais infraestruturas, em grande parte rígidas e operadas manualmente, para arquiteturas mais ágeis e orientadas por software que possam “adaptar-se continuamente para atender à transformação das exigências dos aplicativos e serviços dos quais a empresa depende”.

“As redes vão operar como um sistema com níveis cada vez maiores de autonomia, levando em conta o seu próprio estado, o estado dinâmico de todos os usuários e aplicativos e a vasta gama de opções possíveis”.

- Ravi Chandrasekaran, SVP de engenharia de rede corporativa, Cisco

Como será essa arquitetura de rede emergente? De acordo com Ravi Chandrasekaran, SVP de engenharia de rede corporativa da Cisco, “as redes vão operar como um sistema com níveis cada vez maiores de autonomia, levando em conta o seu próprio estado, o estado dinâmico de todos os usuários e aplicativos e a vasta gama de opções possíveis”.



Descobrimos que, enquanto 39% dos líderes de TI acreditam que suas redes estão muito bem alinhadas para atender às demandas dos negócios digitais, apenas 19% dos estrategistas de rede pensam da mesma forma.¹⁴

A chave para alcançar esse estado mais autônomo será a IA, que ajudará as equipes de TI a responderem rapidamente a condições de rede em transformação, quer isso signifique mudar automaticamente rotas de tráfego, solicitar mais largura de banda, exigir uma mudança de política ou até mesmo recusar uma nova solicitação de serviço.

Com o passar do tempo, aproveitando a inteligência e a automação de todo o sistema, a rede se tornará completamente transparente para o usuário. Ela simplesmente estará lá, fornecendo conectividade segura para os serviços de que eles precisam, no nível exigido, em todos os lugares e em todos os momentos.



Embora Apostolopoulos admita que ainda há um longo caminho a percorrer antes que as redes tenham toda a inteligência e o poder necessários para cumprir essa promessa, ele acredita que os avanços técnicos imprescindíveis para reunir garantia de serviço habilitada para IA, automação baseada em controlador, processamento de linguagem natural e melhorias significativas na segurança de rede estão bem encaminhados.

Caso de uso para a nova rede

Em 2025, uma rede corporativa de ponta será capaz de atender a uma solicitação comunicada em linguagem natural a partir de qualquer linha de negócios e traduzi-la automaticamente em um conjunto de políticas e ações automatizadas

que garantirão que a necessidade empresarial seja continuamente atendida em toda a rede – tudo isso sem afetar nenhum outro serviço disponível. Uma rede com esses tipos de capacidades é comumente conhecida como rede baseada em intenção.

Aqui está o exemplo de um caso de uso hipotético de uma rede baseada em intenção.

Visão geral: uma empresa deseja usar sensores ópticos de IoT sem fio para atender a uma inovação comercial proporcionada por meio de um aplicativo de RA. Veja aqui como a necessidade e a intenção empresariais seriam traduzidas em uma ação de rede.

Figura 4 Caso de uso para a nova rede

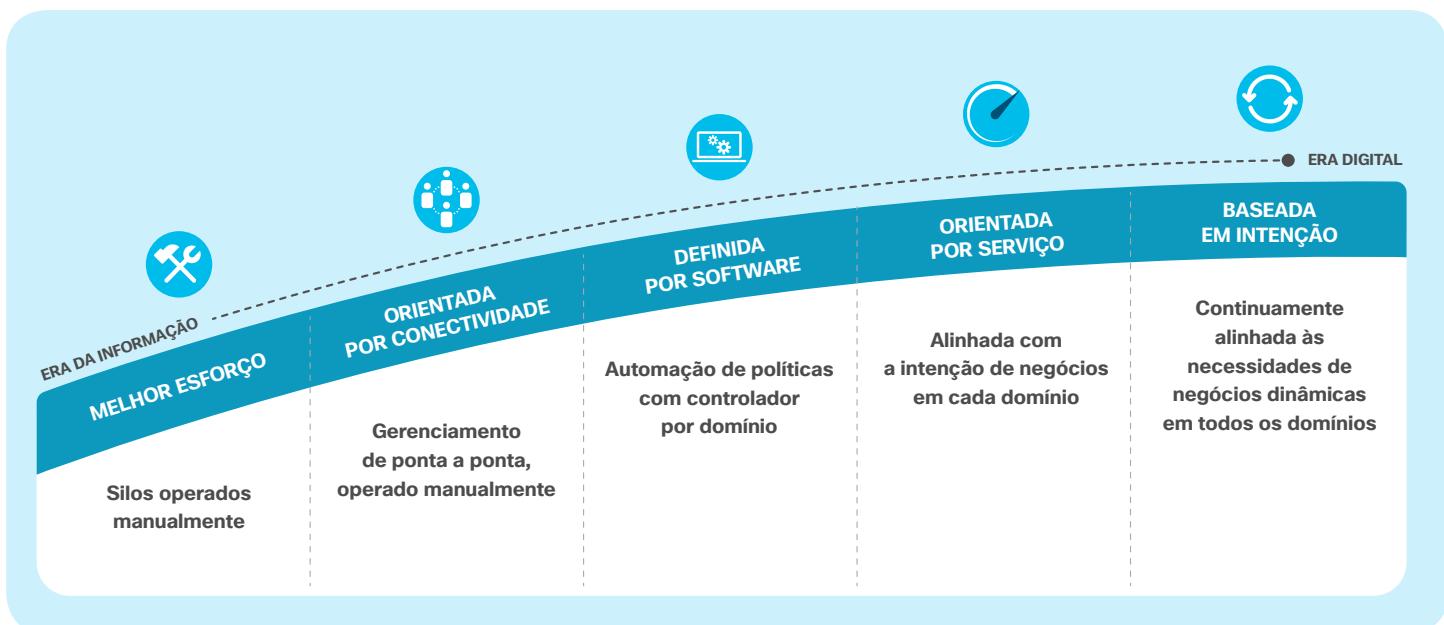


O estado da arquitetura de rede

Onde estão hoje as empresas em sua jornada rumo a uma rede mais avançada que possa atender às demandas da era digital? O modelo de prontidão de rede digital da Cisco é um modelo padrão de maturidade em cinco estágios para ajudar as empresas de TI a avaliarem o seu nível atual de prontidão de rede e ajudá-las a planejar onde precisarão estar no futuro.

O modelo pode ser aplicado em várias categorias de prontidão de rede, como arquitetura, acesso, WAN, garantia, segurança de rede, etc.

Figura 5 Modelo de capacidade de rede digital da Cisco





Relatório Global de
Tendências de Redes de 2020

Tendências em
tecnologia de rede

Cinco tecnologias que estão definindo a nova rede

Neste exato momento, uma série de grandes desenvolvimentos em tecnologia de rede estão ocorrendo para formar a base de um novo modelo de rede. Avanços em cinco áreas tecnológicas em especial – **automação, IA, redes multicloud, rede sem fio, e segurança de rede** – prometem impulsionar a maior onda de transformação de rede vista em décadas. Essas tecnologias comportarão as necessidades do mercado aumentando a escala, a agilidade e a segurança e, assim, viabilizarão as novas tendências que estão mudando o mundo como o conhecemos.



Áreas tecnológicas

- Automação
- IA
- Redes em várias nuvens
- Redes sem fio
- Segurança da rede

“As empresas do mundo todo percebem a necessidade de se transformarem digitalmente para acompanhar o ritmo do mercado e satisfazer as demandas de funcionários, parceiros, clientes e representantes”, revela Brandon Butler, analista sênior de pesquisa de redes corporativas da IDC. “Os líderes de TI também percebem que, sem uma rede mais robusta, segura e ágil, a transformação digital de suas empresas está em risco, o que estimula a refatoração simultânea de vários aspectos de suas redes.”

Um olhar mais atento à situação de cada uma dessas áreas tecnológicas fornece informações sobre como elas estão reformulando a rede, a situação atual de sua adoção e as mudanças que podemos esperar no futuro próximo.

Figura 6 Cinco tecnologias que definem a transformação da rede



Automação de rede em escala



Resumo da seção



Revelações principais

- Juntos, a rede definida por software (SDN), a rede baseada em intenção (IBN), a virtualização de rede, a programabilidade e os controladores de rede de plataforma aberta estão tornando realidade o alinhamento automatizado dos serviços de rede com as necessidades das empresas e os processos de TI.
- A IBN aumenta os recursos de automação da SDN e é capaz de traduzir a intenção em política, coletar dados, dar visibilidade, corrigir problemas e garantir que as políticas estejam realmente fazendo o que foi planejado.
- O objetivo da IBN é aplicar e garantir continuamente os requisitos de desempenho dos serviços, as políticas de conformidade e segurança e também os processos operacionais de TI em toda a rede.
- As interfaces de programação de aplicativos (APIs) em um controlador de plataforma aberta permitem que este integre e troque inteligência com redes e serviços de TI adjacentes, outros domínios de TI, aplicativos empresariais e infraestrutura heterogênea.



Principais descobertas

- Segundo os líderes de TI, automação de redes (25%), SDN (23%) e IBN (16%) estão entre as tecnologias que terão maior impacto nas redes nos próximos cinco anos.
- Cerca de 27% dos líderes de TI identificaram um design em silos e abordagem operacional em todos os domínios de acesso, WAN, DC, nuvem e segurança como um obstáculo à adoção de tecnologias de rede avançadas.
- 34% dos líderes de TI identificaram a obtenção de uma melhor coordenação e integração de rede com outras equipes de TI como uma área importante para melhoria.
- Apesar de apenas 4% dos estrategistas de rede e líderes de TI classificarem sua rede como uma rede baseada em intenção atualmente, 35% planejam que sua rede seja um modelo baseado em intenção em até dois anos.



Resumo da seção (continuação)



Orientação essencial

- Os líderes de TI devem avaliar a prontidão de sua rede para fornecer serviços de rede no ritmo que a empresa precisa.
- Explore a criação de um roadmap que ofereça uma estratégia de redes de loop fechado baseada em intenção em cada domínio de rede em etapas incrementais de forma que cada uma ofereça o melhor retorno sobre o investimento para a empresa.
- Identifique e priorize os processos de TI e aplicativos empresariais que mais se beneficiarão com a integração com um controlador de rede de plataforma aberta.



Principal previsão

“A visão de longa data da aplicação de políticas baseadas em intenção de ponta a ponta passará a ser realidade em 2025. As equipes de redes poderão automatizar políticas de segmentação e otimização de serviços dinâmicas em escala em diferentes domínios (acesso, WAN, DC, várias nuvens, IoT) desde o cliente até o aplicativo e entre cargas de trabalho distribuídas.”

– Ronnie Ray, vice-presidente de experiência do cliente em redes de negócios, Cisco

Automação de rede em escala

A automação de redes, obviamente, é o processo de automatizar a configuração, o gerenciamento, os testes, a implantação e a operação de dispositivos físicos e virtuais em uma rede. Mesmo a otimização da rede em si pode ser automatizada para criar melhorias contínuas no serviço.



De acordo com o Gartner, “cerca de 70% das tarefas de rede de data center são feitas manualmente, o que aumenta o tempo, o custo e a probabilidade de erros e reduz a flexibilidade”.¹⁵

A automação pode melhorar a disponibilidade e liberar as equipes de operações de rede (NetOps) de tarefas diárias demoradas; logo, não é surpresa que, quando perguntados sobre quais tecnologias teriam o maior impacto na rede nos próximos cinco anos, 25% dos líderes de TI indicaram a automação da rede.¹⁴

Inovações nas áreas de SDN, IBN, virtualização, programabilidade e controladores de plataforma aberta estão transformando a automação em realidade nas redes atualmente.



Cerca de 25% dos líderes de TI acreditam que a automação terá o maior impacto nas redes nos próximos cinco anos.¹⁴

Redes definidas por software: apenas o começo

Ao longo dos últimos anos, a SDN tem dado um grande passo para permitir a automação em toda a rede. A SDN permite que as equipes de rede gerenciem as redes como sistemas end-to-end, tornando o gerenciamento mais eficiente e flexível ao separar os planos de encaminhamento e controle.

Consequentemente, o plano de controle é diretamente programável. Ele abstrai a infraestrutura e os dispositivos subjacentes de aplicativos e serviços de rede. A inteligência de rede é centralizada logicamente por meio de controladores de SDN programáveis.

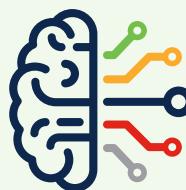


A SDN foi inicialmente apresentada para simplificar ambientes complexos de data center que precisavam ser compatíveis com migrações de carga de trabalho portáteis e dinâmicas e tráfego de servidor para servidor. Os mesmos princípios servem de base para o acesso definido por software (SD-Access), que ajuda a proteger com mais eficiência o acesso de usuários e dispositivos, e para a WAN definida por software, que é capaz de disponibilizar melhores experiências de acesso a aplicativos e serviços em nuvem.

Redes baseadas em intenção: fechando o loop

O principal objetivo das equipes de rede é fornecer desempenho de aplicativos e serviços e proteção de forma contínua para as empresas. Assim, embora a SDN ofereça avanços importantes em automação, ela é apenas parte da solução. As empresas também precisam de monitoramento e otimização contínuos de rede para comportar modelos empresariais cada vez mais dinâmicos e digitais.

Para tal, as redes devem entender a mudança de intenção da empresa e monitorar as condições dinâmicas da rede para que possam se adaptar a essa intenção de forma contínua. De acordo com um projeto da Força-tarefa de engenharia de Internet (IETF), “a intenção constitui uma política declarativa com um âmbito de aplicação a toda a rede. Um operador humano define ‘o que’ é esperado, e a rede computa uma solução para satisfazer esses requisitos.”¹⁶



Redes baseadas em intenção são um modelo de rede relativamente novo apresentado pela primeira vez ao mercado em 2017. Desde então, elas têm sido amplamente adotadas no segmento de redes.

Para que possam ser usadas, o sistema também precisa verificar continuamente se a intenção



está sendo atendida e, caso contrário, fornecer orientações sobre como fazer a correção. O Gartner afirma que “as configurações com base em políticas farão a transição para soluções de rede baseada em intenção (IBN), com uma automação que fará um automonitoramento, garantindo que a rede realmente atenda à intenção das políticas definidas no momento da configuração.”¹⁵

Em nossa *Pesquisa global de tendências de rede*

de 2019, concluímos que 26% dos estrategistas de rede identificaram a implantação de redes baseadas em intenção em um ou mais domínios como uma prioridade tecnológica para implantar a rede ideal. E apesar de apenas 4,3% dos entrevistados terem classificado sua rede como uma rede baseada em intenção atualmente, 35% planejam que ela seja um modelo baseado em intenção em até dois anos.¹⁴

John Apostolopoulos explica que um controlador de IBN amplia a SDN para fornecer um sistema mais completo, a fim de adaptar continuamente a rede de forma que a intenção desejada pela empresa seja alcançada. Esse controlador aumenta os recursos de automação da SDN e é capaz de traduzir a intenção em política, coletar dados e dar visibilidade e insights relevantes, garantindo então que a rede esteja realmente

Figura 7 IBN: Aproveitando os princípios fundamentais da SDN

	DEFINIDA POR SOFTWARE	BASEADA EM INTENÇÃO
TRADUÇÃO		
Inserir intenção		●
Traduzir para política		●
Verificar integridade		●
ATIVAÇÃO		
Orquestrar políticas	●	●
Automatizar configurações de rede	●	●
GARANTIA		
Visibilidade		●
Insights (contexto + política)		●
Verificação contínua		●
Ações corretivas		●

fazendo o que foi planejado. O feedback de loop fechado fornecido pela IBN é fundamental para que os benefícios desejados sejam alcançados.¹⁷

Uma rede baseada em intenção captura a intenção empresarial e usa análise, aprendizagem de máquina, raciocínio de máquina e automação para alinhar a rede contínua e dinamicamente às necessidades empresariais em constante mudança, bem como para se adaptar às cargas de rede em transformação e a outros efeitos ambientais. Isso pode significar aplicar e garantir continuamente os requisitos de desempenho de serviços e as políticas de usuários, segurança, conformidade e operações de TI em toda a rede.

Como funciona o trabalho das redes baseadas em intenção? A definição de redes baseada em intenção (IBN) da Cisco envolve três componentes básicos funcionais: tradução, ativação e garantia.¹⁸

Figura 8 Elementos de uma rede baseada em intenção



Os líderes de TI são pressionados a fornecer serviços de forma mais rápida e eficiente em colaboração e competição com os serviços em nuvem. Do ponto de vista tecnológico,

a experiência em computação, o poder de processamento e a expertise em IA necessários para as IBNs estão se tornando mais prontamente disponíveis.



Rohit Mehra, da IDC, afirma: “A rede baseada em intenção é um desenvolvimento significativo para o segmento de redes. Ela não apenas abrange níveis avançados de visibilidade, automação e garantia, como também é a plataforma sobre a qual a nova funcionalidade de gerenciamento de rede baseada em aprendizagem de máquina será construída.”¹⁹

Virtualização de funções de rede

O modelo de virtualização que alterou radicalmente os serviços de computação foi adotado nas redes na forma de virtualização de funções de rede (NFV). Ele permite que NetOps forneçam ou alterem rapidamente serviços de rede e os implantem e administrem remotamente. Além da agilidade da TI, a NFV proporciona uma consolidação física substancial, economizando espaço e energia e criando menos pontos de possíveis falhas.

Programabilidade como um fundamento de rede

Para que os controladores e sistemas de IBN sejam escaláveis e alcancem todo o seu potencial, eles precisam construir uma infraestrutura de rede física ou virtual programável. Dispositivos e interfaces

programáveis e circuitos integrados programáveis específicos ao aplicativo (ASICs) são o fundamento de uma rede inteligente.



Para adotar sistemas mais eficientes e automatizados, as equipes de TI continuam se afastando das abordagens tradicionais de gerenciamento manual baseadas em interface de linha de comando (CLI). Em vez disso, estão adotando interfaces acionadas por modelos de dados (DMI). Essas interfaces padronizadas baseadas em modelos proporcionam consistência, abertura, estrutura e eficiência.

Liderando o caminho para um modelo operacional sustentável que oferece consistência e facilidade de uso, modelos padronizados IETF, como o YANG, fornecem um conjunto completo de interfaces programáticas de subida.

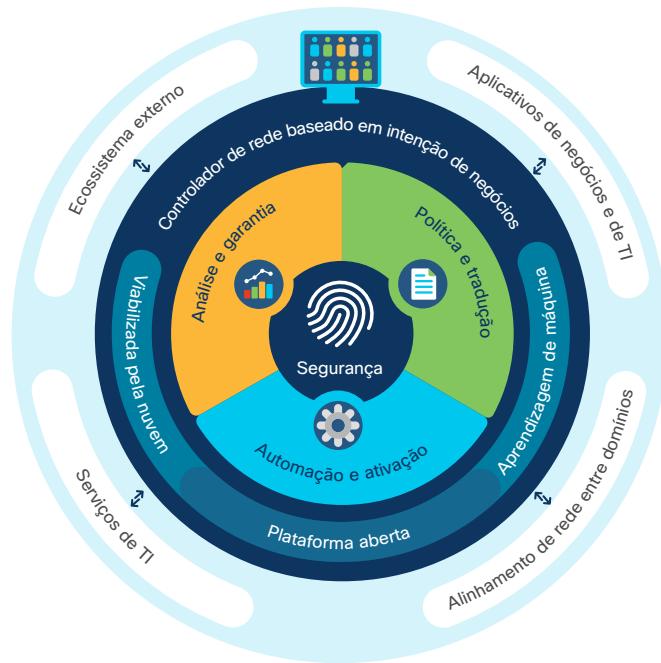
Controladores IBN de plataforma aberta: Integração de processos de TI e negócios

As interfaces de programação de aplicativos (APIs) no controlador permitem que este integre e troque inteligência com serviços de TI e redes adjacentes, outros domínios de TI, aplicativos empresariais da linha de negócios e infraestrutura heterogênea.

Isso transforma a rede em uma plataforma aberta que pode aceitar especificações de políticas a partir de aplicativos e dispositivos, lançar mão da automação centralizada de políticas entre domínios e verificar se o sistema está atendendo às necessidades da empresa. Isso melhora a disponibilização de serviços de TI, simplificando os fluxos de trabalho entre domínios de rede, sistemas de TI e processos da linha de negócios que costumavam ser gerenciados de forma independente.

Em nossa *Pesquisa global de tendências de rede de 2019*, 34% dos líderes de TI identificaram a obtenção de uma melhor coordenação e integração de rede com outras equipes de TI como uma área importante de melhoria.¹⁴

Figura 9 Controlador de plataforma aberta para integração com aplicativos de negócios, serviços de TI e domínios de rede



Com a extensibilidade de rede da API e do kit de desenvolvimento de software (SDK), a TI pode ter um melhor alinhamento com as necessidades dos aplicativos de negócios e de TI, agilizar as operações e garantir a proteção do investimento.

Alinhamento de garantia e política entre domínios: Cliente para carga de trabalho

As equipes de redes precisam trabalhar em conjunto para conseguir um alinhamento de rede de ponta a ponta com a intenção empresarial. Isso significa criar uma ligação uniforme de onde quer que o cliente ou “coisa” esteja se conectando à rede para onde quer que o serviço ou aplicativo esteja hospedado.



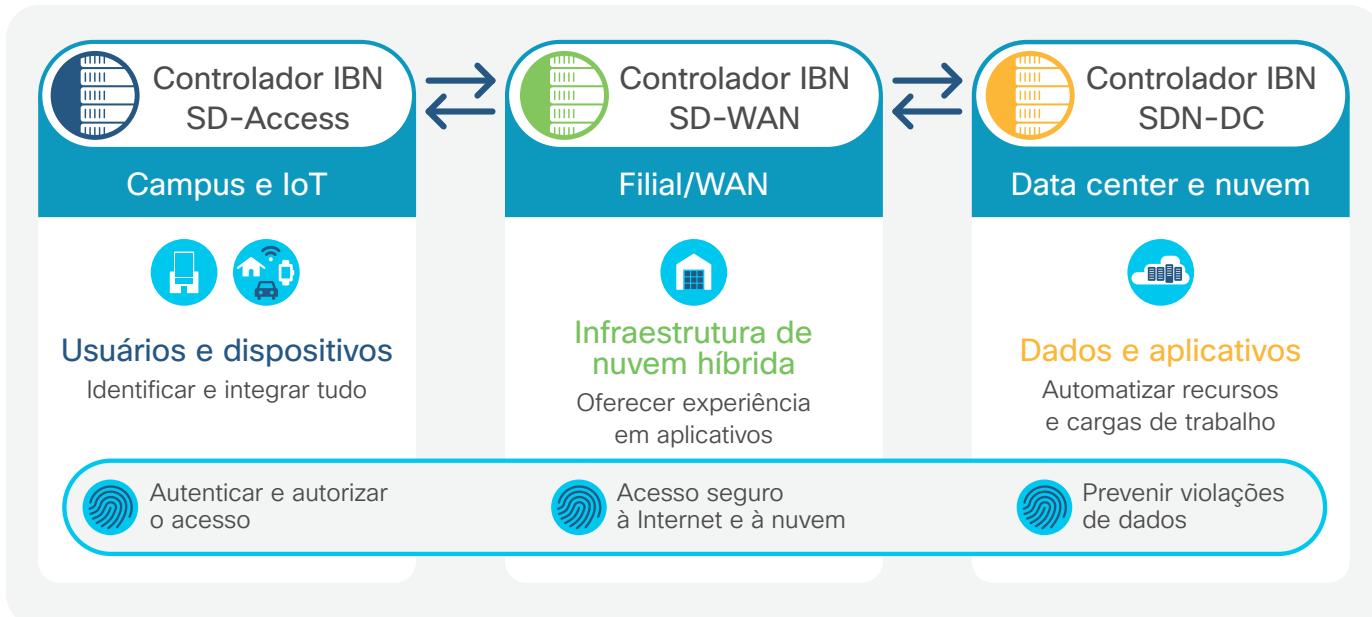
Análise atual: para que uma empresa tenha sucesso com a rede baseada em intenção, ela precisa adotar totalmente a automação no data center, no campus, na rede de área ampla e na filial.²⁰

No entanto, em muitos casos, isso não é fácil de conseguir. Em nossa *Pesquisa global de tendências de rede de 2019*, 27% dos líderes de TI identificaram um “design em silos e abordagem operacional em todos os domínios de acesso, WAN, DC, nuvem e segurança” como um obstáculo à adoção de tecnologias de rede avançadas.¹⁴

Por uma boa razão, a rede é normalmente dividida em domínios que são geralmente organizados em torno do objetivo principal do domínio. No entanto, para obter verdadeira visibilidade, controle e validação de ponta a ponta da intenção empresarial, recursos de política e garantia precisam ser orquestrados em todos os domínios.

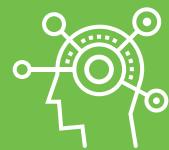
Os líderes de TI estão adotando medidas para conseguir isso, com 26% deles identificando a “garantia e a aplicação de políticas de rede multidomínio integradas” como uma prioridade máxima para o aumento do investimento.¹⁴

Figura 10 Política e garantia: alinhamento entre todos os domínios da IBN





Garantia viabilizada pela inteligência artificial



Resumo da seção



Revelações principais

- O uso de inteligência artificial (IA) está se tornando essencial em operações, disponibilização de serviços e garantia de rede, algo em que AIOps – a combinação de recursos e operações de IA – está se tornando uma categoria bem consolidada.
- O crescimento explosivo de volume de tráfego, dispositivos móveis e de IoT conectados, aplicativos e microsserviços interconectados, e também as ameaças à segurança cada vez maiores, está sobrecarregando as equipes de rede.
- Grandes quantidades de dados, telemetria e eventos gerados por redes que comportam um número cada vez maior de dispositivos e serviços estão excedendo a capacidade de ação dos operadores humanos por si só.
- Fundamental para um modelo de rede baseada em intenção (IBN), a IA utiliza os volumosos dados fornecidos pela rede para explorar a complexidade do ambiente e propor ajustes à rede de forma dinâmica.
- A aprendizagem de máquina e o raciocínio de máquina complementam-se para fornecer processamento de eventos complexos, insights correlacionados e correção guiada.



Principais descobertas

- Mais de 50% dos estrategistas de redes identificam a IA como um investimento de rede prioritário.
- Apenas 17% dos estrategistas de redes acreditam que a falta de maturidade nas tecnologias de IA representa um obstáculo à modernização da rede.
- Atualmente, apenas 22% das equipes de redes utilizam alguma IA para garantir a segurança da rede, possivelmente porque a disponibilidade de ferramentas genuínas viabilizadas por IA é ainda bastante recente.
- Cerca de 68% dos estrategistas de rede projetam que usarão insights preditivos ou correção prescritiva viabilizados por IA nos próximos dois anos.



Orientação essencial

- Utilize a aprendizagem de IA baseada em nuvem: Em alguns casos, serão necessárias mudanças nas políticas de dados corporativos para usufruir dos benefícios das ferramentas de IA viabilizadas pela nuvem.
- Interação humana e de IA: Definir progressivamente até onde a IA pode ir na tomada de decisões ou ações antes que um operador humano precise se envolver para monitorar, aprovar ou aplicar uma mudança.

Resumo da seção (continuação)



- Conhecimento de IA: O conhecimento especializado em redes será um conjunto de habilidades premium necessário para verificar se a IA está alcançando os objetivos comerciais e de TI conforme pretendido.



Principal previsão

“Até 2025, as ferramentas de garantia de rede viabilizadas por IA automatizarão totalmente várias tarefas bem definidas e específicas. No entanto, a maioria das tarefas operacionais que exigem uma tomada de decisão mais flexível e contextual continuará exigindo a especialização e a intervenção de operadores humanos.”

– JP Vasseur, especialista da Cisco

Garantia viabilizada pela inteligência artificial

A inteligência artificial está promovendo grandes transformações em vários setores e agora está se tornando essencial para operações de TI, em que os AIOps estão se tornando uma categoria bem estabelecida.

O que são IA, ML e MR?

Simplificando, inteligência artificial (IA) é um campo de estudo que confere a computadores inteligência semelhante à humana ao executar uma tarefa. Duas das categorias mais importantes de IA são a aprendizagem de máquina (ML, de Machine Learning) e o raciocínio de máquina (MR, de Machine Reasoning). A aprendizagem de máquina pode ser descrita como a capacidade de “aprender estatisticamente” a partir de dados sem uma programação explícita. O raciocínio de máquina usa o conhecimento adquirido para navegar por uma série de opções possíveis em direção a um resultado ideal.

Dessa forma, a ML permite que um sistema examine os dados e deduza o conhecimento. Ela vai além de simplesmente aprender ou extrair conhecimento. Ela utiliza e aperfeiçoa o conhecimento ao longo do tempo e com a experiência. Essencialmente, o objetivo da ML é identificar e explorar padrões ocultos em dados de “treinamento”.

O MR é bastante adequado para resolver problemas que exigem profundo conhecimento do domínio. Os humanos precisam capturar explicitamente todo o conhecimento antecipadamente para que um raciocinador de máquina possa operar com novos dados. O MR é um complemento maravilhoso para a ML porque pode utilizar as conclusões apresentadas pela ML e analisar possíveis causas e potenciais opções de aprimoramento.

A complexidade da rede promove a adoção da IA.

Vários fatores estão alimentando o impulso rumo a redes viabilizadas pela IA. Com aumentos sem precedentes na complexidade e na escala da rede, a IA está se tornando cada vez mais necessária para ajudar as equipes de TI a proporcionarem níveis confiáveis de serviço e rede.

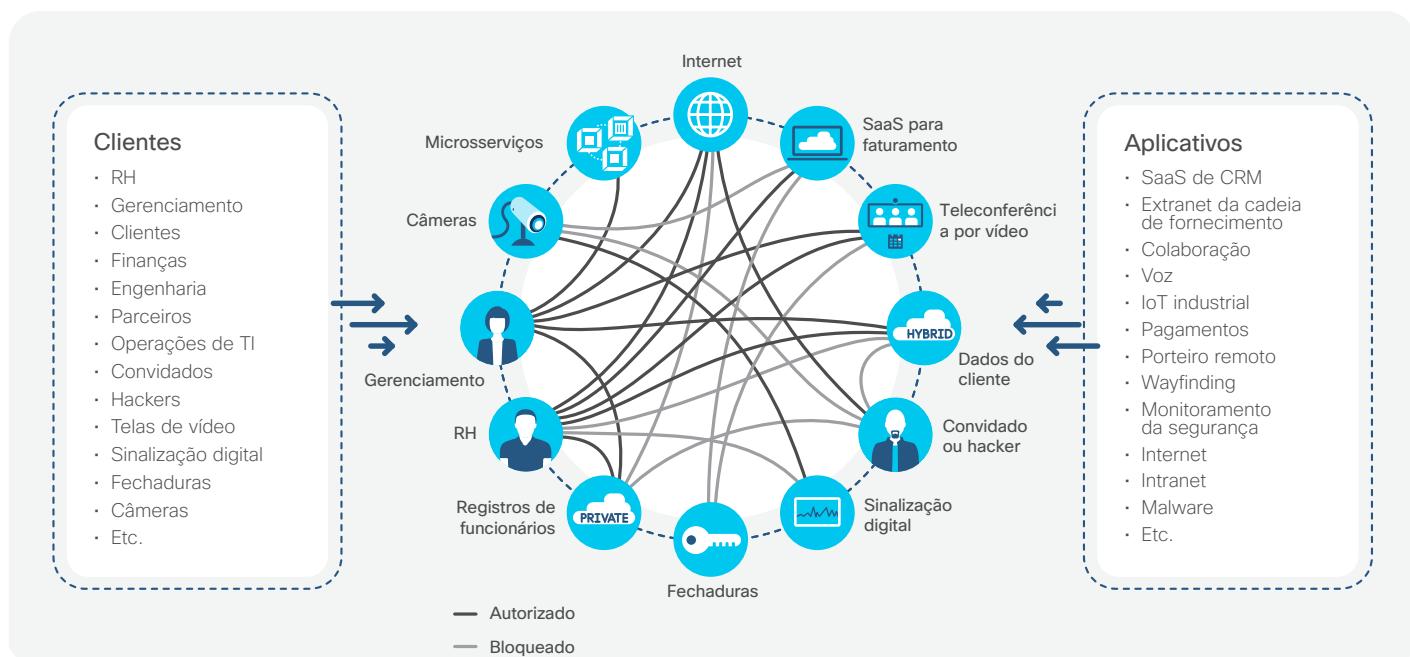
As redes estão comportando um crescimento explosivo de volume de tráfego, dispositivos de IoT e móveis conectados, e aplicativos e microserviços interconectados. As redes atuais também estão gerando enormes quantidades de dados que excedem a capacidade de gerenciamento – e ainda mais de compreensão – dos operadores humanos em tempo hábil.



O custo das interrupções de rede

97% dos líderes globais de TI que participaram da entrevista disseram que tiveram problemas de desempenho relacionados a aplicativos essenciais aos negócios nos seis meses anteriores. O custo médio por interrupção de rede? US\$ 402.542 nos Estados Unidos e US\$ 212.254 no Reino Unido.²¹

Figura 11 Complexidade de rede de empresas hiperconectadas



A IA oferece o potencial para que as equipes de rede usem melhor esses dados a fim de garantir que suas redes funcionem de forma eficaz e em alinhamento contínuo com as necessidades empresariais. Por exemplo, ela pode ajudar a criar melhores parâmetros, prever problemas com precisão e ajudar na solução de problemas de sistemas complexos.

Os estrategistas de redes já reconhecem esse fato. Mais de 50% identificam a IA como um investimento prioritário necessário para disponibilizar a rede ideal,¹⁴ enquanto apenas 17% acreditam que a falta de maturidade em tecnologias de IA representa um obstáculo à modernização da rede.¹⁴

Usando os volumosos dados obtidos pela rede, a IA aprende sobre a complexidade do ambiente

de comunicações e redes e pode propor ajustes à rede de forma dinâmica. Esta capacidade torna a IA fundamental para um modelo de IBN.

A inteligência artificial e tecnologias avançadas de redes como a IBN estão claramente desestruturando a forma como as coisas são feitas, especialmente quando tratamos de operações de redes. Testes de novos aplicativos podem acontecer em minutos em vez de semanas. A solução de problemas de rede fica significativamente mais fácil quando um mecanismo de garantia identifica as causas raiz e recomenda correções. De fato, armado com poderosos painéis de controle que oferecem informações açãoáveis, um futuro operador de rede só vai precisar procurar em poucos lugares, em vez de percorrer pilhas de possíveis causas.

Figure 12 Rede baseada em intenção alimentada por IA





Como a ML e o MR são aplicados em um contexto de rede?

Conforme observado acima, um elemento importante das operações de rede e da rede baseada em intenção é a garantia de rede, que é a verificação contínua de que o estado e o comportamento da rede estão de acordo com a intenção desejada. A aprendizagem de máquina e o raciocínio de máquina oferecem recursos exclusivos que os operadores podem usar para garantir o desempenho de rede necessário, especialmente nas três principais áreas de garantia a seguir (ver Figura 13 abaixo).

Processamento de eventos complexos:

ao aplicar a ML à telemetria de rede, é possível estabelecer parâmetros dinâmicos das condições normais de operação para uma dada intenção.

Insights correlacionados: a ML oferece visibilidade e insights mais profundos sobre

a operação da rede e prevê quando uma condição anômala pode ocorrer no futuro. O MR aumenta o poder da ML, aplicando conhecimento especializado pré-carregado e capturado de fluxos de trabalho de solução de problemas semelhantes.

Remediação: a remediação permite o alinhamento constante com a intenção, identificando as ações corretivas mais adequadas por meio de bases de conhecimento fornecidas, por exemplo, com o MR.²²

Estado atual e futuro da IA para a garantia da rede

Os dados da nossa *Pesquisa global de tendências de rede de 2019* esclarecem em que ponto as empresas estão na adoção da garantia de rede viabilizada pela IA.

Usando o nosso modelo padrão de prontidão em cinco estágios para medir o estado

Figura 13 Casos de uso de ML e MR para garantia de rede

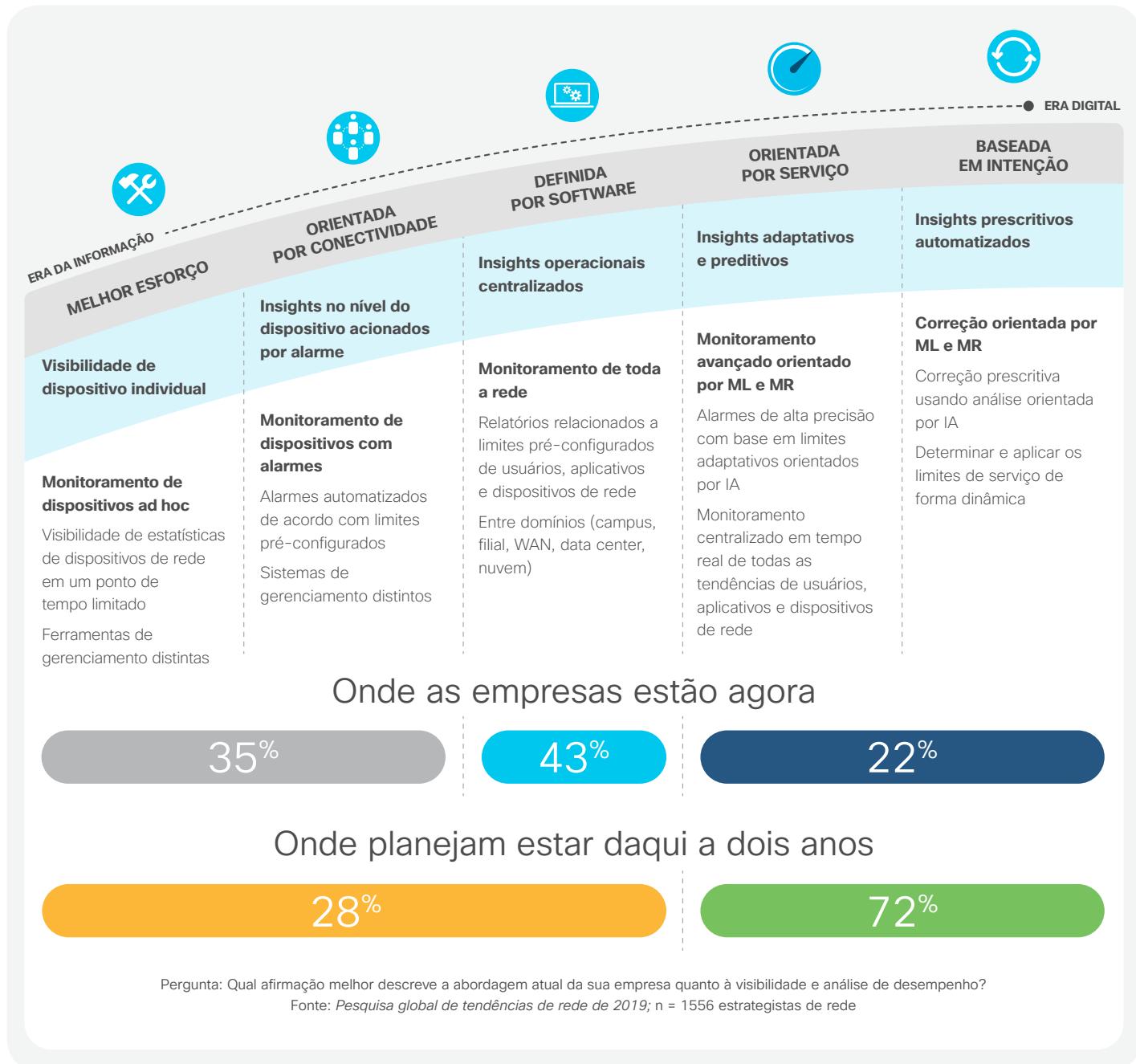
	Aprendizagem de máquina	Raciocínio de máquina
Abordagem tecnológica	Modelo matemático a partir de grandes conjuntos de dados	Captura de conhecimento humano, a lógica simbólica
Aplicabilidade	Análise preditiva, detecção de anomalias, classificação, regressão	Mecanização de fluxos de trabalho determináveis
Função de garantia de rede	<ul style="list-style-type: none">Identificação de problemas e linha de base dinâmicaInsights e visibilidadeAnálise preditiva	<ul style="list-style-type: none">Solução automática de problemasCorreção automática



de prontidão estimado, apenas 22% dos estrategistas de redes entrevistados relataram utilizar capacidades de IA para garantia de rede atualmente. Isso pode ser atribuído ao fato de as verdadeiras soluções de garantia de rede

baseadas em IA serem ainda relativamente novas. No entanto, 72% dos entrevistados planejam alcançar insights preditivos ou remediação prescritiva viabilizados pela IA nos próximos dois anos.¹⁴

Figura 14 Capacidade de garantia viabilizada pela IA





Considerações para avançar com a IA

De acordo com o especialista da Cisco JP Vasseur, ao avaliar o uso da IA na infraestrutura de rede, os seguintes itens devem ser levados em consideração:

1 Criar boas práticas operacionais: saber o que a IA **não pode** e **não deve** fazer é tão importante quanto entender o que ela **pode** fazer. Ao determinar quais áreas dos negócios poderiam se beneficiar mais da IA, não se esqueça de identificar também as áreas que apresentam o risco e a exposição mais elevados.

2 Definir uma função objetiva clara: não existe um algoritmo capaz de extrair fatos interessantes de um conjunto de dados sem que a equipe de ML especifique claramente os objetivos. É importantíssimo poder afirmar claramente a meta e as métricas de desempenho antes de iniciar a jornada de ML.

3 Limite da interação humana com a IA: definir até onde a IA pode ir na tomada de decisões ou ações antes que um humano precise se envolver para monitorar, aprovar ou fazer uma mudança é fundamental para o negócio e para a capacidade da equipe de rede de permanecer no controle.

4 Conhecimento de IA: uma dependência cada vez maior da IA pode criar lacunas de conhecimento. Por isso, o conhecimento especializado em redes será um conjunto de habilidades de excelência necessário para verificar se a IA está alcançando os objetivos de TI e de negócios pretendidos e para ajudar os operadores a fazerem a escolha certa entre as opções recomendadas pelo sistema de IA.

5 Dependência de dados: como melhorar a coleta. A IA depende de cálculos matemáticos para criar insights com base nos quais é possível realizar ações, e esses cálculos são tão bons quanto a qualidade dos dados que estão utilizando. Os especialistas em redes terão de trabalhar em várias funções e domínios para garantir que a qualidade dos dados seja confiável para as iniciativas de IA.

6 Onde aplicar a IA: a aplicação da IA depende do desempenho, da segurança, da capacidade dos dados e da privacidade de um aplicativo e dos dados. Embora haja algumas instâncias de treinamento de modelos no local, a aplicação mais comum hoje em dia é a aprendizagem de máquina baseada em nuvem. A nuvem fornece capacidade de computação e armazenamento para aprender e executar a ML a partir de grandes quantidades de dados agregados e anonimizados provenientes de várias fontes. Em alguns casos, isso pode suscitar preocupações em termos de privacidade, em termos de quem tem acesso a esses dados e mesmo em que geografia esses dados estão armazenados. Além disso, esteja ciente das implicações de latência que podem afetar os insights em tempo real no caso de grandes conjuntos de dados, o que pode ocorrer, por exemplo, com sensores de vídeo que produzem grandes quantidades de dados.

7 Mudança no paradigma corporativo: o ideal é alinhar as políticas de dados da sua empresa para lançar mão da IA na nuvem. Ao vincular milhões de sistemas a um único mecanismo de análise de IA, é possível alcançar um tamanho de amostra de dados que pode proporcionar resultados exponencialmente melhores do que a mesma tecnologia quando alimentada por dados de uma única experiência de rede. As equipes de TI podem ser fundamentais para plantar hoje as sementes que levarão às políticas favoráveis à nuvem que sustentarão a implantação da IA.

Redes para dados e aplicativos em ambientes com várias nuvens



Resumo da seção



Revelações principais

- Todas as empresas precisarão de serviços baseados em nuvem, mas sempre haverá necessidade de manter alguns dados e cargas de trabalho no local.
- Aplicativos monolíticos estão, em muitos casos, dissolvendo-se em microsserviços interconectados que são prestados por meio de uma série de cargas de trabalho virtuais e físicas localizadas em contêineres, no local, na nuvem e na extremidade da rede corporativa.
- Um data center distribuído não funciona como um data center tradicional. Portanto, as empresas de TI precisam se adaptar para atender às crescentes demandas de conectividade de aplicativos e redes dessa nova arquitetura.
- SD-WAN, acesso direto à nuvem, instalações de colocation e trocas de nuvem, juntamente com serviços de banda larga elevada e 5G a preços mais acessíveis, estão surgindo como novos elementos de arquitetura importantes para garantir que os serviços de nuvem possam atender às exigências comerciais de forma acessível e efetiva.



Principais descobertas

- 23% do tráfego dentro dos data centers corporativos já está sendo transportado por SDN/NFV, um número que deve crescer para 44% até 2021.

- 29% dos líderes de TI e estrategistas de redes acreditam que, dentro de dois anos, eles terão recursos de rede baseados em intenção em seus ambientes locais, híbridos e com várias nuvens.
- A maior dependência da nuvem está impulsionando o aumento do tráfego WAN. Espera-se que o tráfego WAN IP empresarial duplique até 2022, atingindo 5,3 hexabytes por mês.
- Mais de 58% das empresas em nível global já implantaram a SD-WAN de alguma forma, e mais de 94% dos entrevistados acreditam que terão uma SD-WAN baseada em intenção básica ou mais avançada implantada nos próximos dois anos.



Orientação essencial

- Identifique os aplicativos e serviços baseados em nuvem mais fundamentais e coloque em ordem de prioridade quaisquer planos de SD-WAN para acessar e proteger esses aplicativos primeiro.
- Estenda a automação baseada em política de forma consistente em redes híbridas e de várias nuvens, tomando o cuidado de levar em consideração qualquer plataforma, qualquer hipervisor ou qualquer estrutura de contêiner em qualquer local e com qualquer carga de trabalho (nativo da nuvem, metal puro, hipervisor, contêiner e sem servidor).



Resumo da seção (continuação)



- Mapeie serviços de aplicativos, cargas de trabalho e componentes de serviços na rede “expandida” para obter uma melhor compreensão de quais aplicativos, serviços e microsserviços estão na rede.
- As equipes de data center, nuvem e rede devem colaborar para desenvolver a constância do serviço em domínios de campus, filial, data center, extremidade/IoT e provedor de nuvem pública/SaaS.
- Os aplicativos e serviços exigirão integração e entrega contínuas entre cargas de trabalho no local e na nuvem, e as empresas que implementarem os processos operacionais para interconectar e comportar esse modelo colherão a velocidade e a flexibilidade prometidas pela nuvem.



Principal previsão

“Até 2025, espero ver 20% das cargas de trabalho distribuídas na borda das redes fora dos ambientes de data center em várias nuvens e corporativos. Isso significa que um quinto do tráfego que geralmente estaria confinado em um data center agora precisará ser assegurado e protegido em toda a rede corporativa e de várias nuvens.”

— **Vijoy Pandey, vice-presidente e CTO do Grupo de Soluções e Plataforma de Nuvem da Cisco**

Redes para dados e aplicativos em ambientes com várias nuvens

A necessidade de velocidade e inovação está levando as empresas de TI a modernizarem os aplicativos existentes e a desenvolverem rapidamente novos aplicativos que permitam o acesso a informações em qualquer dispositivo a qualquer momento. Hoje em dia, os desenvolvedores de aplicativos e usuários corporativos apreciam a agilidade, a escalabilidade e o autoatendimento da nuvem.

No entanto, embora 85% dos departamentos de TI estejam avaliando ou já estejam usando a nuvem pública, a migração para a nuvem não representa a realidade.²³ Na verdade, a frase “a migração para a nuvem” não se mostrou completamente precisa. Vijoy Pandey, vice-presidente e CTO do Grupo de Soluções e Plataforma de Nuvem da Cisco, diz: “Nos últimos anos, à medida que cargas de trabalho valiosas tentavam migrar para a nuvem pública, ficou claro que a situação não era binária e que havia cargas de trabalho e, principalmente, alguns dados que precisavam ser locais”.²⁴

Das empresas que estão usando a nuvem pública hoje, 85% estão seguindo uma estratégia multicloud. A previsão é de que esse número aumente para 94% em 12 meses.²⁵

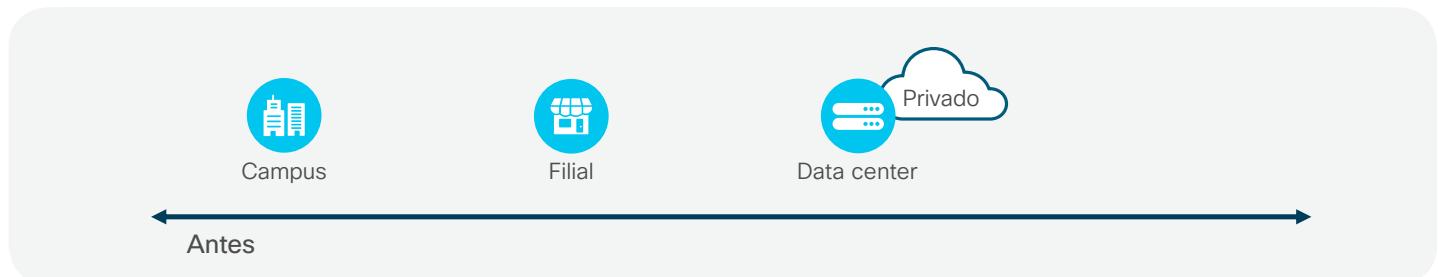
Pandey também observa que a decisão de manter os dados no local decorre de uma série de preocupações, inclusive regulamentos e proteção de dados: “Outra preocupação é que, quando você precisa de muitas informações dos seus dados, precisa fazer muitos cálculos de dados.” Para todas essas cargas de trabalho, você precisa de computação local e de redes locais. Embora todas as empresas precisem de serviços baseados em nuvem, a necessidade de serviços no local nunca desaparecerá. É por isso que acho que fazer a aposta em ambientes com várias nuvens e híbridos é o caminho a seguir.”

O impacto sobre a rede da transformação dos modelos de aplicativos

Antigamente, o desempenho de uma rede centrava-se em dois elementos principais:

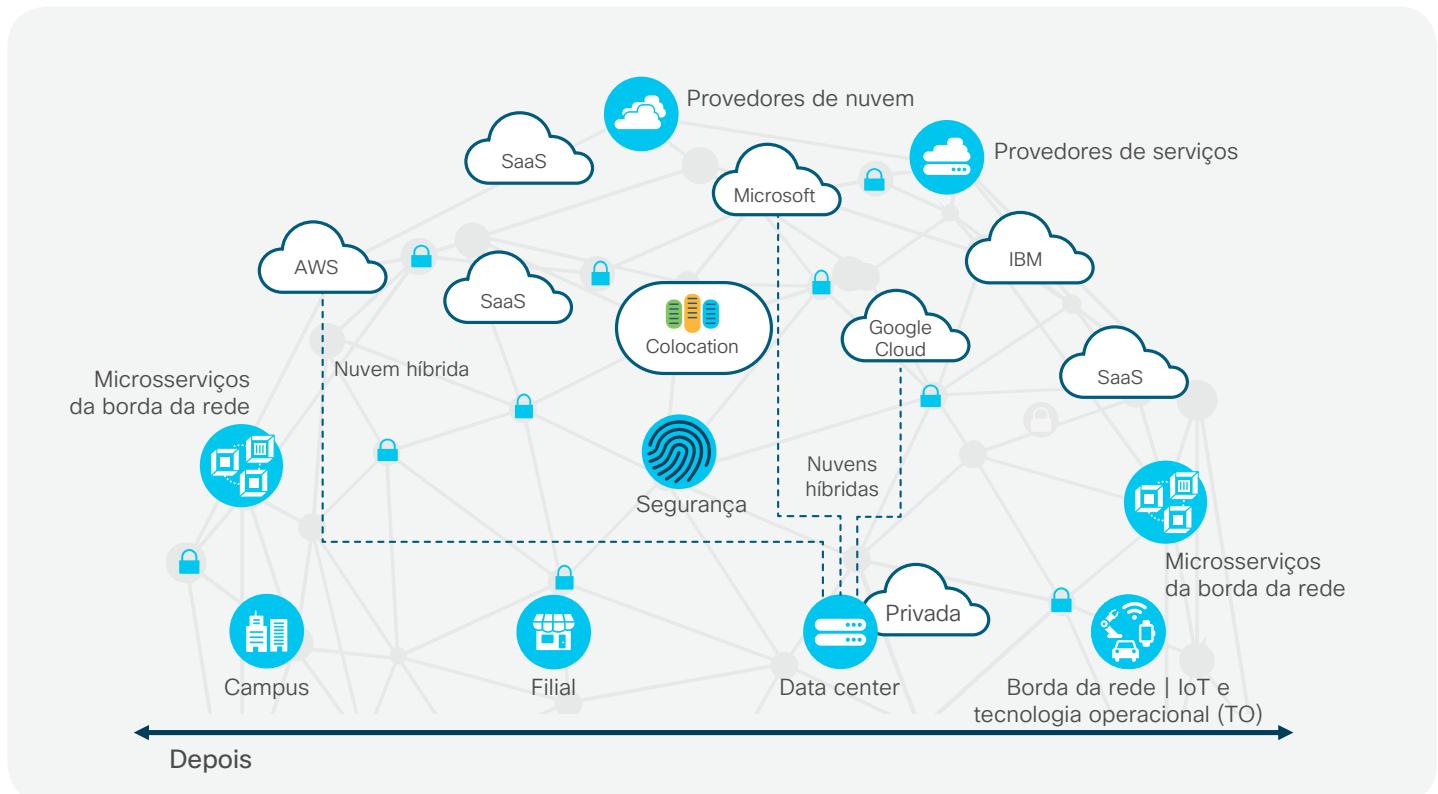
- A comunicação entre o cliente e o aplicativo ou serviço monolítico, normalmente com hospedagem em um data center centralizado
- A comunicação dentro do data center entre servidores e armazenamento em rede

Figura 15 Antes: comunicação de clientes com serviços e entre cargas de trabalho



Mas essa abordagem não é mais suficiente, pois as equipes de aplicativos continuam adotando modelos de aplicativos mais ágeis, menos monolíticos e compostos de várias cargas de trabalho ou componentes de serviço que nem sempre são colocados, mas sim distribuídos, para além dos ambientes locais e do data center.

Figura 16 Depois: comunicação de clientes com serviços e entre cargas de trabalho





Embora algumas equipes de TI possam acreditar que uma mudança para a nuvem significa que a rede se torna menos importante, nada pode estar mais longe da realidade. As equipes de data center e de nuvem não podem mais trabalhar em separado das equipes de redes,

um fato que os líderes de TI já reconheceram. Eles agora identificam investimentos em rede para comportar ambientes multicloud (públicos, infraestrutura como serviço [IaaS] ou SaaS) como uma de suas maiores prioridades.¹⁴

Figura 17 As equipes de TI priorizam o investimento em rede para ambientes multicloud



Pergunta: Se você pudesse reduzir o tempo gasto na manutenção de atividades de status quo, em qual dos seguintes serviços de valor agregado você colocaria mais foco?

Fonte: *Pesquisa global de tendências de rede de 2019*; n = 505 líderes de TI

De acordo com Tom Edsall, CTO da Cisco para data center e consultor emérito: “À medida que aplicativos, cargas de trabalho, serviços e dados se tornam mais distribuídos em todo o continuum entre a borda da rede e a nuvem, há uma responsabilidade a mais para a TI como um todo para garantir que os serviços sejam prestados de forma segura e confiável e com o desempenho desejado,

independentemente da sua localização física. Os profissionais de data center devem agora colaborar mais estreitamente do que nunca com as equipes responsáveis pelas redes em nível de filial/extremidade, WAN e campus”.

Considerando essas mudanças contínuas, onde os líderes de TI e de redes precisam concentrar seus esforços hoje?

A expansão para o mundo híbrido e com várias nuvens significa gerenciar variáveis em constante mudança (aplicativos, dados, usuários e dispositivos) que abrangem todos os domínios da empresa. Como resultado, as equipes de infraestrutura e operações (I&O) e de redes devem trabalhar juntas para lidar com tudo, desde as implicações de redes dos provedores de nuvem pública e de SaaS até o impacto em seus ambientes locais.

Para ajudar a compreender o desafio, vamos analisar os requisitos de rede através de duas lentes:

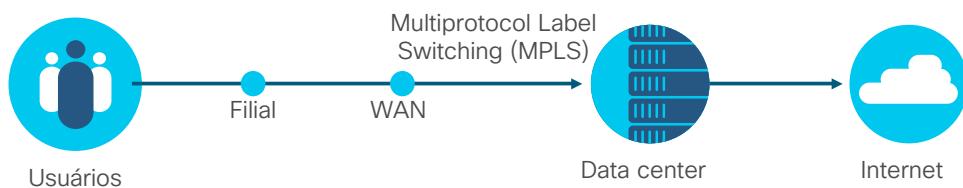
- Otimização da conectividade, de um usuário para várias nuvens
- Redes para um data center em qualquer lugar

Otimização da conectividade, de um usuário para várias nuvens

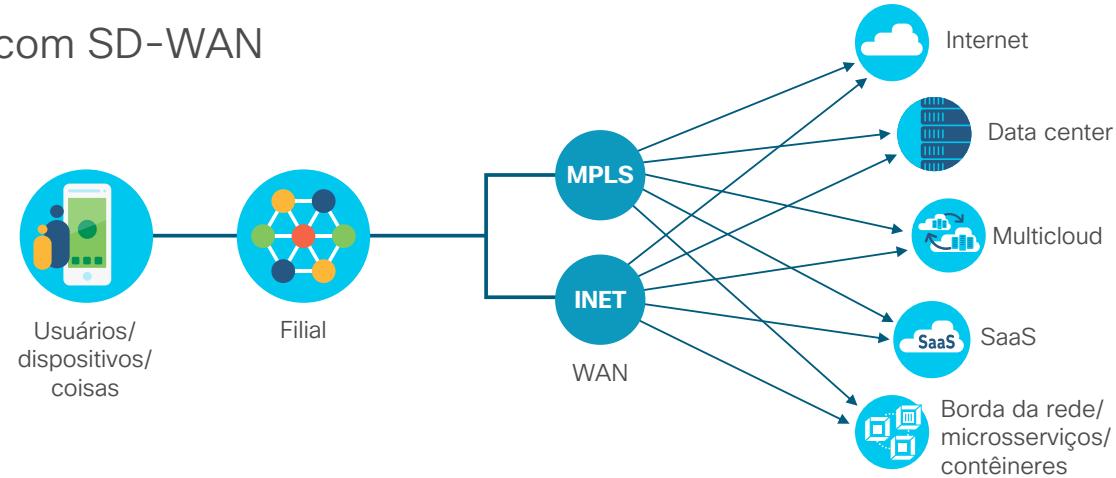
A predominância emergente de serviços em nuvem significa que a conectividade remota a esses serviços está mais crucial do que nunca. Também significa que as tradicionais arquiteturas de rede de área ampla que se concentravam em conectar locais remotos a data centers centralizados não são mais ideais.

Figura 18 O cenário da WAN em transformação

Antigo



Hoje com SD-WAN





Agora que SaaS, IaaS e serviços distribuídos de extremidade podem ser hospedados em qualquer lugar onde haja uma conexão de rede, uma arquitetura WAN antiquada de hub-and-spoke pode atrasar as empresas.



A maior dependência da nuvem também está promovendo o aumento do tráfego de WAN. A previsão é de que o tráfego de WAN IP empresarial global duplique até 2022, atingindo 5,3 hexabytes por mês.¹²

SD-WAN, acesso direto à nuvem, instalações de colocation e trocas de nuvem, juntamente com a disponibilidade de serviços de banda larga elevada a preços acessíveis, estão surgindo como novos elementos de arquitetura importantes para garantir que os serviços de nuvem possam atender às exigências comerciais de forma acessível.



As equipes de TI precisam do mesmo controle em ambientes multicloud e em suas próprias redes para que possam continuar prestando o serviço que a empresa espera.

SD-WAN

A SD-WAN é uma abordagem definida por software para gerenciar a WAN. Ela permite que um controlador centralizado otimize a experiência de aplicativo em várias nuvens e simplifique muito as operações da WAN.

A recente adoção rápida da SD-WAN indica que ela fornece muitas respostas às crescentes demandas da nuvem. E, na verdade, a nuvem é o maior impulsionador desta adoção da SD-WAN. Quase 75% dos entrevistados na pesquisa de SD-WAN da IDC afirmaram que os serviços em SaaS/nuvem são importantes (ou muito importantes) para as escolhas atuais da tecnologia WAN.²⁶

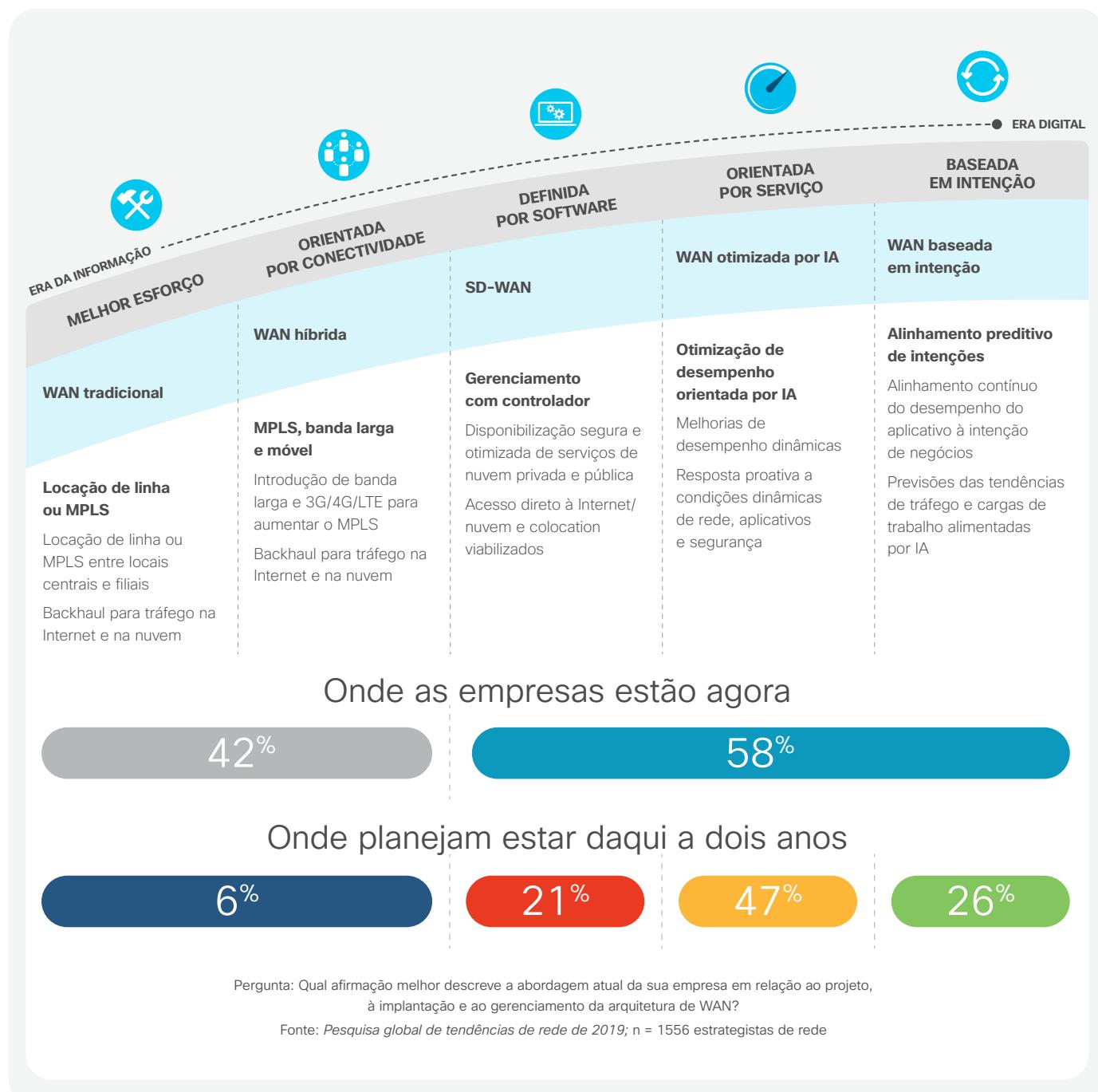
Isso não é surpreendente, pois as opções e os serviços tradicionais usados para se conectar à nuvem privada virtual fornecida pelos provedores de serviços de nuvem deixam as equipes de rede corporativa com controle limitado em um cenário com várias nuvens.

De acordo com a nossa *Pesquisa global de tendências de rede de 2019*, mais de 58% das empresas no mundo todo já implantaram a SD-WAN de alguma forma, e mais de 94% dos entrevistados acreditam que implantarão algum tipo de implementação básica ou mais avançada de SD-WAN nos próximos dois anos.¹⁴

Além disso, à medida que os serviços 5G se tornarem mais amplamente disponíveis, a SD-WAN irá integrá-los perfeitamente em uma estrutura independente de transporte para oferecer máxima flexibilidade e desempenho, um backup aprimorado e sempre conectado e um custo reduzido.



Figura 19 Capacidade da WAN em um ambiente multicloud

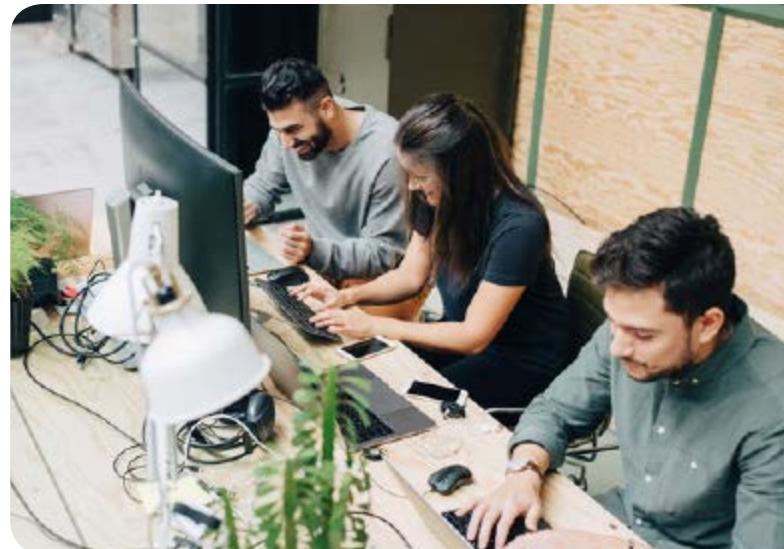


Acesso direto à nuvem

A abordagem tradicional de backhauling de tráfego de filial ao longo de circuitos WAN caros rumo ao data center ou um gateway de Internet centralizado por meio de uma arquitetura hub-and-spoke pode dificultar a transição para serviços em nuvem. Ela também gera despesas e introduz uma latência que degrada a experiência do usuário.

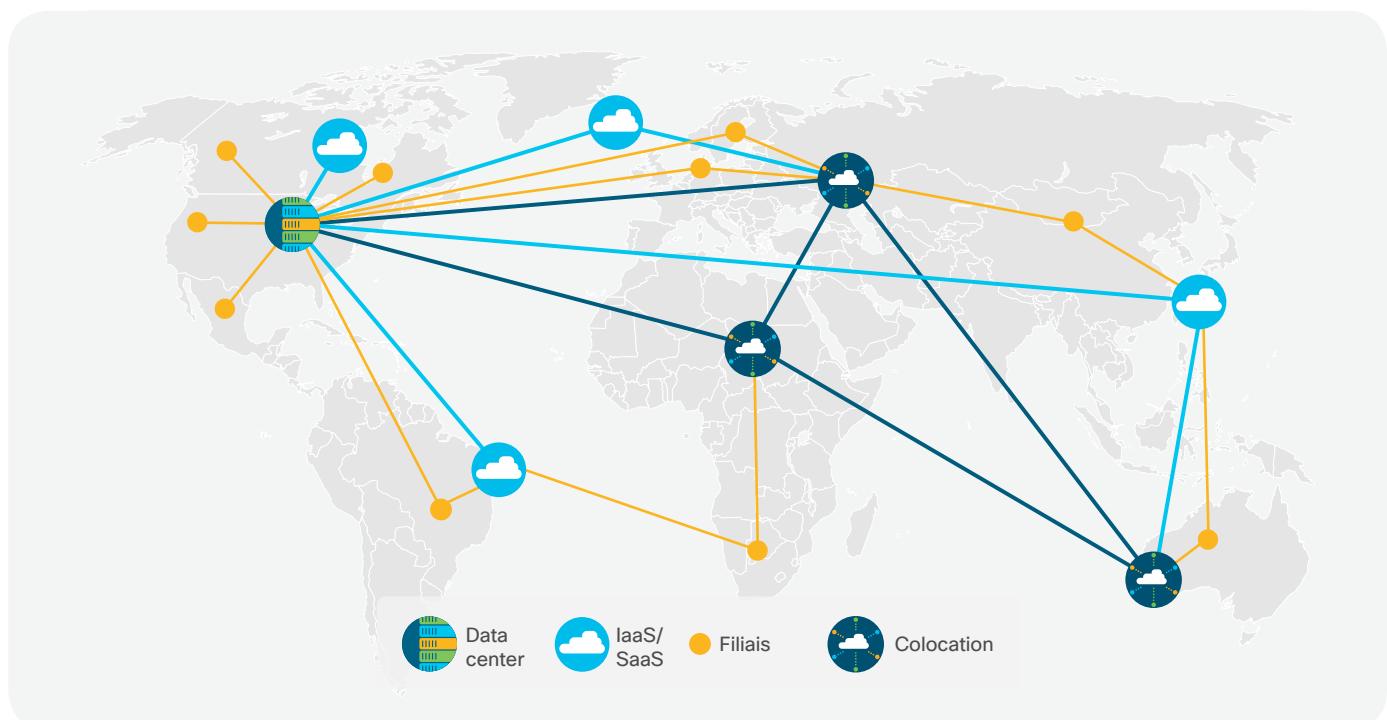
Até agora, as arquiteturas de rede estavam presas a essa abordagem por causa do custo e da complexidade da alternativa, que exige a implantação e o gerenciamento de recursos de segurança distribuídos, como firewalls, filtragem de URL e proteção DNS em cada roteador da filial.

Agora, porém, os recursos de “acesso direto à nuvem” ou “acesso direto à Internet” podem conectar com segurança os usuários diretamente da filial aos serviços em nuvem. Isso simplifica o gerenciamento de políticas em



loais remotos e automatiza o provisionamento de novos serviços de rede em poucos minutos, ao mesmo tempo em que reforça a segurança em várias camadas, incluindo criptografia, autenticação, segmentação, firewall e aplicação de DNS.

Figura 20 SD-WAN segura com acesso direto à nuvem e hubs de colocação





Colocation e troca de nuvens

Embora as instalações de colocation (colo) de operadoras neutras não sejam novas, elas assumem um papel muito expandido na era de várias nuvens e são um componente essencial da nova arquitetura de WAN otimizada para a nuvem. Em essência, instalações colo, como as fornecidas pela Equinix e outros serviços de interconexão, tornam-se uma extensão da WAN corporativa, fornecendo visibilidade, acesso de alto desempenho e segurança centralizada para múltiplos provedores de SaaS e IaaS. (Ver Figura 20 acima.)

Redes para um data center em qualquer lugar

Os data centers de hoje já não são mais locais isolados. O emergente “data center distribuído” é resultado de aplicativos e dados que vivem dentro e fora da instalação em ambientes híbridos, com várias nuvens e de extremidade de rede. Mas um data center distribuído não funciona como um tradicional. As empresas de TI precisam adaptar e mudar suas tecnologias e operações para atender às crescentes demandas de conectividade de rede e aplicativos desta nova arquitetura.

Um data center em qualquer lugar exige que as equipes de TI assegurem a constância tecnológica e operacional no local, em toda a borda da rede corporativa e em ambientes híbridos e com várias nuvens.

Automação

A crescente escala, complexidade e portabilidade da carga de trabalho nos data centers está forçando os administradores de rede a substituírem processos manuais e aplicarem ferramentas de automação para gerenciar conectividade e políticas de rede.

A adoção de serviços de rede, automação e NFV para as camadas 4 a 7 definidos por software coloca as redes de data centers em uma posição viável para comportar um ambiente de nuvem ágil no local.



Quase 60% dos líderes de TI e estrategistas de rede afirmam que já implantaram alguma forma de SDN em seus data centers.¹⁴

Isso permite a orquestração centrada da carga de trabalho da rede, juntamente com serviços de computação e armazenamento. Na verdade, você pode considerar atrasada uma rede de data center que ainda não adotou um modelo de DevOps baseado em controlador e acionado por API.

Quase 60% dos líderes de TI e estrategistas de rede afirmam que já implantaram alguma forma de SDN em seus data centers.¹⁴ O SDN/NFV já está transportando 23% do tráfego dentro dos data centers corporativos, um número que deve crescer para 44% até 2021.²³ Esses data centers sem SDN terão dificuldades para comportar modelos de aplicativos ágeis e flexíveis.



Rede baseada em intenção para o data center

Com base nos fundamentos da SDN, a rede baseada em intenção permite que as equipes de data center obtenham uma arquitetura holística de validação de ciclo fechado que analisa o comportamento do data center em tempo real em relação às políticas definidas e disponibiliza um método eficiente e confiável para fazer mudanças na rede. Isso permite que as equipes de TI acompanhem as mudanças dinâmicas de carga de trabalho e se alinhem continuamente às necessidades de aplicativos da empresa.

Em um cenário de data center, também é muito importante validar as políticas antes de ativá-las. Com a IBN, isso pode ser alcançado por meio de uma verificação contínua, automatizada e em toda a rede, incluindo políticas de conformidade.

Extensão da IBN para ambientes com várias nuvens

Para assegurar a segurança e os níveis de serviço desejados para as empresas atuais, as equipes de data center precisam estender o controle e a visibilidade para além dos ambientes locais. As equipes de TI podem estender a automação e a aplicação baseadas em políticas da IBN para ambientes com várias nuvens, a fim de que possam implantar políticas de forma confiável nas cargas de trabalho, independentemente do local.

Em dois anos, 29% dos entrevistados da nossa *Pesquisa global de tendências de rede de 2019* planejam ter recursos de rede baseada em intenção que mantenham o alinhamento da intenção de negócios, garantindo ações de rede automatizadas em ambientes multicloud.¹⁴

Tom Edsall, CTO da Cisco do setor de data center, explica que “a IBN é a mais ousada e mais abrangente iniciativa do setor para criar um modelo de rede em todo o sistema que aborde todas as últimas tendências tecnológicas e necessidades dinâmicas de empresas ágeis”.

“A rede baseada em intenção é o mais ousado e mais abrangente esforço do setor de redes para criar um modelo de redes em todo o sistema que aborde todas as últimas tendências tecnológicas e necessidades em rápida mudança de empresas ágeis.”

– Tom Edsall, CTO para data center e consultor emérito, Cisco

A chave para uma implementação bem-sucedida no local, com várias nuvens ou híbrida é manter a simplicidade. Para isso, os arquitetos de rede devem considerar:

- Nenhuma rede de sobreposição na nuvem
- Nenhuma dependência de agentes, o que permite ampla aplicabilidade para qualquer carga de trabalho
- Adaptabilidade à escala da nuvem



Infraestrutura de rede subjacente

No data center, a infraestrutura de rede subjacente precisa proporcionar programabilidade e telemetria abertas para comportar a automação e a análise que são centrais para os sistemas de IBN. A infraestrutura de rede do data center também precisa acompanhar os enormes aumentos de tráfego.

3X O tráfego de IP do data center global triplicará nos próximos cinco anos.²³

O tráfego de IP do data center global triplicará nos próximos cinco anos. No geral, o tráfego de IP do data center crescerá a 25% (taxa de crescimento anual composta) até 2021.²³

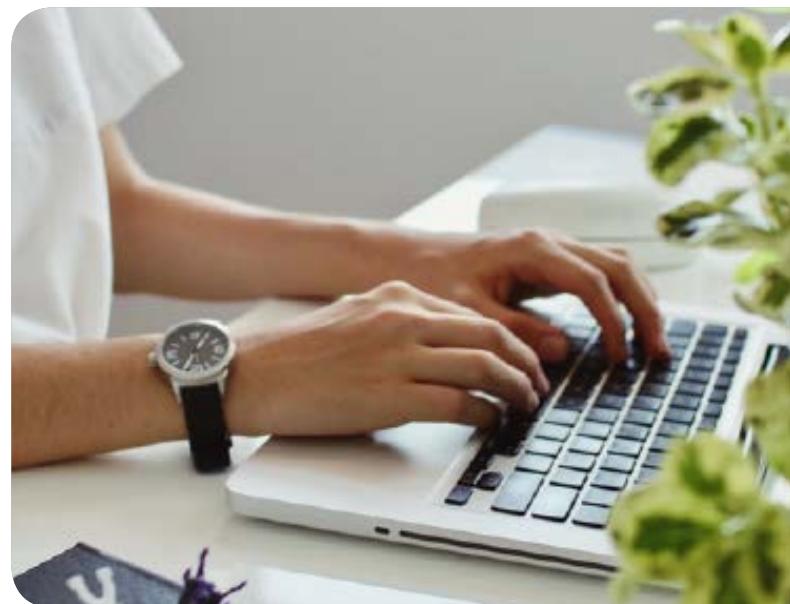
72%

Até 2021, o tráfego dentro do próprio data center será responsável por 72% de todo o tráfego do data center.²³

As infraestruturas de rede precisam de flexibilidade e capacidade para comportar o tráfego de alto desempenho de cliente para aplicativo (norte-sul) e, cada vez mais, de servidor para servidor ou de VM para VM (leste-oeste). Hoje em dia, isso é feito normalmente com uma arquitetura plana “spine-and-leaf” apoiada por um ou mais protocolos de sobreposição da camada de controle.

De acordo com o *Cisco Global Cloud Index*, até 2021, o tráfego dentro do próprio data center será responsável por 72% de todo o tráfego do data center e excederá muito o tráfego de data center para usuário (15%) e de data center para data center (14%).²³

Serão necessários aumentos contínuos no desempenho do switching de Ethernet para comportar as necessidades crescentes de tráfego de computação, bem como de tráfego de armazenamento baseado em arquivos e até mesmo de tráfego de armazenamento baseado em blocos.



Com a popularização da velocidade de 400 Gbps comutada, e com especificações IEEE para 800 Gbps e até mesmo para 1,6 Tbps em preparação, o capital atrativo e os benefícios operacionais da Ethernet farão com que ela seja inevitavelmente uma alternativa ao switching de canal de fibra mais tradicional para algumas cargas de trabalho.



Considerações ao arquitetar a sua rede para várias nuvens

Nesse ambiente de aplicativos expandido e mais distribuído, os arquitetos de rede e de nuvem, os executivos de data center e as equipes de infraestrutura e operações precisam desenvolver uma estratégia de rede que otimize a experiência do aplicativo. Aqui estão alguns passos iniciais para se levar em consideração ao fazê-lo:

- 1 Oriente-se pela estratégia de aplicativo da empresa:** ela começa com o aplicativo. Os estrategistas de TI e de rede devem ter uma boa compreensão da expansão da carga de trabalho e do volume de dados da empresa.
- 2 Trabalhe em colaboração com outras áreas para ter estabilidade em um ambiente multicloud:** as empresas precisam que seu ambiente multicloud (e também no local) funcione como um só. Em meio a toda a complexidade, as equipes de data center e rede devem colaborar para desenvolver constância em seus domínios de campus, filial, data center, extremidade/IoT e provedor de nuvem pública/SaaS, de forma a obter custos, desempenho, visibilidade, segurança e experiências de forma otimizada para os usuários.
- 3 Estenda a regularidade da automação com base em política às redes híbridas e em ambiente multicloud:** as equipes devem levar em consideração a implementação da automação com base em políticas em qualquer plataforma, qualquer estrutura de hipervisor ou contêiner, qualquer local e qualquer carga de trabalho (nativo da nuvem, bare-metal, hipervisor, contêiner e sem servidor).

- 4 Mapeie serviços de aplicativos e cargas de trabalho e componentes de serviços para a rede expandida:** os estrategistas e profissionais de rede precisam de uma boa compreensão dos aplicativos, serviços e microsserviços que estão na rede.

- 5 Priorize o desempenho do aplicativo em sua estratégia de SD-WAN:** identifique os aplicativos e serviços de missão crítica na nuvem e priorize o plano de SD-WAN para dar respaldo a esses aplicativos primeiro.

- 6 Aproxime a política de acesso e a política de aplicativos em todos os silos da rede:** para oferecer segmentação segura com base em política em todos os lugares, considere como os sistemas de IBN podem mapear grupos e políticas entre diferentes domínios de rede, como WAN e data center.

- 7 Desenvolva conjuntos de habilidades de NetDevOps:** como as cargas de trabalho e os serviços exigem serviços de rede sob demanda, não apenas dentro de um data center, mas também entre locais remotos, eles precisarão deixar suas necessidades claras para a rede. Isso exigirá conjuntos de habilidades de NetDevOps que compreendam como fazer a ponte entre os requisitos do aplicativo e as políticas da rede.

- 8 Melhore a SDN com avanços de IA:** use recursos de IA para acelerar a solução de problemas, melhorar o gerenciamento de mudanças e garantir a conformidade.



Acesso à rede e rede sem fio



Resumo da seção



Revelações principais

- Recursos emergentes, como o OpenRoaming, fornecerão roaming global contínuo, sempre conectado e seguro entre diferentes redes de Wi-Fi 6 e redes de 5G públicas.
- As equipes de redes precisam de análises aprimoradas e recursos viabilizados por IA para planejamento de redes sem fio, monitoramento de integridade, solução de problemas e correção.
- As equipes de TI precisam gerenciar, administrar e propagar políticas de acesso consistentes automaticamente em diferentes redes de acesso para proteger melhor aplicativos, dados, usuários e dispositivos.
- As redes sem fio precisarão identificar e comportar dinamicamente as demandas de novos dispositivos de IoT e aplicativos de mídia imersivos.



Principais descobertas

- Globalmente, os dispositivos sem fio representarão 43% de todos os dispositivos em rede até 2022.
- Os dispositivos de IoT M2M representarão 51% de todos os dispositivos em rede até 2022, com a maioria deles conectados sem fio.

- 35% dos estrategistas de redes reconhecem que a solução de problemas de rede é a atividade mais intensiva em recursos e que mais consome tempo para as operações de redes atualmente.
- 34% das empresas ainda usam uma abordagem manual para gerenciar o acesso em redes com e sem fio.
- 40% das empresas fornecem automação e segmentação de políticas para reduzir a superfície de ameaça, com outros 15% aproveitando soluções de acesso viabilizado por IA.
- Dentro de dois anos, 27% das empresas planejam ter em vigor um modelo de acesso à rede baseado em intenção.



Orientação essencial

- Avalie como o Wi-Fi 6 e o 5G afetarão os requisitos de negócios futuros da sua empresa e baseie nessa avaliação a sua estratégia de redes sem fio.
- Crie um roteiro para automatizar a integração e segmentação seguras de todos os dispositivos móveis e de IoT.
- Explore o uso da classificação automatizada de dispositivos para viabilizar a integração segura e em larga escala de todos os tipos de dispositivos de IoT.
- Avalie como os serviços baseados em localização e as ferramentas de mensuração de redes podem proporcionar benefícios comerciais à sua empresa.



Resumo da seção (continuação)



- Explore como qualquer tecnologia sem fio especializada necessária para casos de uso exclusivos ou exigentes (como Bluetooth, Zigbee e Thread) pode ser gerenciada por meio de uma camada de gerenciamento comum.



Principais previsões

“Até 2025, federações de tecnologia sem fio como a OpenRoaming serão onipresentes, permitindo que empresas de TI e provedores de serviços usem sistemas de acesso zero-trust, compartilhem credenciais de identidade com segurança e viabilizem que os usuários finais façam roaming de forma ininterrupta e segura em qualquer rede de acesso sem fio – tanto privada quanto pública. A experiência do usuário será isenta de atritos e aplicada por política. Ela será a melhor onde quer que eles se conectem.”

– Matt MacPherson, CTO de tecnologias sem fio, Cisco

“Até 2025, redes de Wi-Fi 6 baseadas no padrão IEEE 802.11ax, juntamente com extensões planejadas de Wi-Fi 6, se tornarão a forma predominante de Wi-Fi em todos os lugares. Já por volta de 2024, a próxima geração de Wi-Fi baseada no padrão IEEE 802.11be em desenvolvimento (provavelmente comercializada como Wi-Fi 7) começará a aparecer no mercado.”

– Andrew Myles, diretor e ex-presidente da Wi-Fi Alliance, Líder técnico da Cisco

Acesso à rede e rede sem fio

O tráfego de IP corporativo atingirá 63,3 hexabytes por mês até 2022 no mundo todo, um aumento de três vezes em relação a 2017.³ O acesso com fio, iniciado de modo relativamente desprestensioso em redes locais cabeadas compartilhadas, como Ethernet (10 Mbps), token ring (16 Mbps) e FDDI (100 Mbps), se beneficiou de inovações contínuas em silício e fibra óptica para se tornar a rede central Ethernet de 400 Gbps comutada para ambientes de rede LAN e área metropolitana que os clientes podem implantar hoje.

Em um futuro não muito distante, as inovações contínuas prometem a Terabit Ethernet e novos recursos avançados, como Time-Sensitive Networking (TSN), para aplicativos de IoT determinísticos. No entanto, no mundo majoritariamente móvel de hoje, é no acesso wireless que grande parte da atenção está concentrada. O acesso à rede wireless via LAN sem fio (Wi-Fi) ou via redes públicas móveis continua mudando as nossas vidas de maneiras que poucos poderiam imaginar.

“Descobrimos que a inovação comercial digital exige e impulsiona avanços na inovação da rede sem fio, ao mesmo tempo em que os próprios avanços na inovação da rede sem fio estão abrindo possibilidades para novas inovações comerciais. É um ciclo virtuoso.”

– Guillermo Diaz, SVP de transformação do cliente, Cisco

“A ‘experiência’ de hoje é a moeda dos negócios, e os avanços em conectividade sem fio serão o viabilizador de muitas experiências da próxima geração. Ao combinar o melhor do Wi-Fi 6 e do 5G, as equipes de rede têm potencial para tornar essas experiências uma realidade.”

– Matt MacPherson, CTO de tecnologias sem fio, Cisco

Globalmente, os dispositivos sem fio representarão 43% de todos os dispositivos em rede até 2022, com os smartphones representando 24% (6,7 bilhões) de todos os dispositivos em rede. Ao mesmo tempo, o número de dispositivos de IoT M2M aumentará para 14,6 bilhões e representará 51% de todos os dispositivos em rede até 2022, sendo a grande maioria conectada sem fio.¹²

Como proporcionar uma experiência deliciosa ao usuário de dispositivo móvel

Pessoas em todo o mundo se acostumaram a usar aplicativos móveis, como Uber, Waze e WebEx, que fazem uma grande diferença em seu trabalho e vida particular. Elas querem que a sua experiência móvel seja uma experiência

imediata (sempre disponível, sem amarras e onipresente), bem como uma experiência satisfatória que possibilite acesso ininterrupto a vídeo 4K sem vibrações, navegação ultrarrápida e VOIP cristalina.

Tão importante quanto tudo isso, as redes sem fio precisam dar respaldo a novas inovações comerciais. Enquanto as empresas cada vez mais adotam aplicativos de mídia imersivos, como vídeo de alta definição, RA e RV, os líderes querem saber se a rede tem desempenho, capacidade, cobertura e segurança para comportar novas iniciativas digitais para que possam se movimentar rapidamente quando surgirem oportunidades.



“Imagine que um comprador possa receber uma experiência personalizada e relevante alimentada por serviços locais e realidade aumentada”, explica Matt MacPherson, CTO da Cisco para tecnologias sem fio. “Ou que um depósito possa ser equipado com milhões de sensores para permitir que robôs e veículos elétricos autônomos cumpram ordens e enviem produtos.”



As novas redes Wi-Fi 6 e as redes públicas de tecnologia móvel 5G prometem um desempenho consideravelmente superior para comportar esses requisitos. O Wi-Fi 6 traz taxas de dados mais altas, menor latência, maior densidade de dispositivos e um desempenho geral muito melhor. Da mesma forma, até 2022, as redes públicas móveis 5G, cuja implantação comercial está prevista para 2020 em alguns países específicos, oferecerão velocidades quatro vezes maiores do que as disponibilizadas com o 4G.¹²



70%

O Wi-Fi é amplamente utilizado como um mecanismo de descarregamento de tecnologia móvel e será ainda mais necessário na era 5G. A previsão é de que o 5G descarregue mais de 70% do seu tráfego, acima dos 59% descarregados pelas redes 4G.²⁷

Os usuários de dispositivos móveis também querem uma experiência transparente ao acessarem aplicativos empresariais, na nuvem e na internet pública. Isso inclui onboarding e roaming entre diferentes redes.

Ao complementar o 5G com o Wi-Fi 6, os usuários terão uma experiência transparente e sempre conectada em áreas públicas e privadas internas ou externas. Isso inclui um respaldo para novos aplicativos com alta demanda de dados, que podem facilmente superar os limites dos planos de dados móveis de muitos usuários.

Para dar vida a essa visão, o OpenRoaming se baseou na tecnologia Passpoint da Wi-Fi Alliance.²⁸ Mesmo ainda em um estágio inicial, a OpenRoaming Foundation, um consórcio composto pela Cisco e vários líderes de tecnologias sem fio, está tornando realidade o objetivo ambicioso de fornecer roaming dinâmico e seguro através de redes sem fio públicas e privadas.

O OpenRoaming disponibiliza aos usuários um roaming global fácil e seguro entre diferentes redes Wi-Fi 6 e redes públicas 5G por meio de uma federação baseada em nuvem formada por redes de acesso e provedores de identidade, incluindo operadoras móveis. O OpenRoaming foi apresentado em um recente Congresso Mundial de Tecnologia Móvel e foi bem-sucedido.²⁸

Ao usarem dispositivos de modo duplo, como smartphones e tablets, os usuários poderão alternar entre redes Wi-Fi corporativas ou domésticas privadas, hotspots Wi-Fi públicos e a rede pública 5G sem problemas.

“Com o OpenRoaming, os usuários de dispositivos móveis não precisarão mais adivinhar qual rede Wi-Fi usar, se estressar em um portal que surge para autenticação ou usar um nome de usuário e senha inseguros novamente. Eles serão conectados onde quer que estejam e poderão fazer download e transmissões por streaming, bater papo por vídeo, jogar e até mesmo trabalhar se quiserem.”

– Matt MacPherson, CTO de tecnologias sem fio, Cisco



Como preparar a TI para o sucesso das redes sem fio

As operações de rede precisarão estar à frente dessas novas exigências das empresas para que possam fornecer as experiências que os usuários de dispositivos móveis desejam, visto que as abordagens tradicionais de implantação e manutenção de redes sem fio não serão sustentáveis.

Em especial, a solução de problemas de redes sem fio é geralmente uma atividade reativa, complexa e com uso intensivo de recursos para a maioria das equipes de rede. Não é de surpreender que a solução de problemas de rede seja considerada pelos líderes a atividade que mais consome tempo nas operações atualmente.¹⁴



Para complicar ainda mais as coisas, existe o fato de que, além das novas redes Wi-Fi 6 e 5G, os dispositivos de IoT podem se comunicar por meio de vários protocolos de nicho sem fio, incluindo BLE, Zigbee e Thread. A TI terá o desafio de assegurar que os esforços de gerenciamento de redes não sejam repartidos por essas diferentes redes.

Muitos casos de uso da IoT convergirão para as principais redes Wi-Fi 6 e 5G, mas as equipes de TI devem levar em conta como podem gerenciar tecnologias sem fio mais específicas necessárias em casos de uso exclusivos ou exigentes por meio de uma camada de gerenciamento comum.

Para estarem à frente, as equipes de NetOps precisam de uma abordagem mais proativa ao planejar, monitorar, fornecer solução de problemas e remediar redes sem fio. Essa abordagem exige uma visibilidade muito melhor do desempenho e da integridade das redes sem fio usando ferramentas de mensuração e monitoramento viabilizado por IA.

Situação atual e futura da disponibilidade de acesso à rede

A TI não pode depender das operações tradicionais de rede de acesso manual para dar respaldo aos usuários de dispositivos móveis. Em vez disso, as empresas precisam de uma abordagem orientada por software que abranja todos os domínios da rede.

O sistema de gerenciamento de rede precisa ser capaz de gerenciar, administrar e propagar políticas de acesso consistentes de forma automática em diferentes redes de acesso, mesmo que os usuários e as cargas de trabalho continuem em movimento. Também precisa liberar dados e insights que permitirão que a TI auxilie as empresas em tempo real e empregue a IA para melhorar a previsão de problemas e a automação de tarefas rotineiras. E, à luz da crescente prevalência de aplicativos de IoT, a rede precisa reconhecer e classificar automaticamente os dispositivos de IoT e aplicar políticas pertinentes.

Juntos, esses recursos permitirão que funcionários, clientes e líderes empresariais aproveitem ao máximo o que o Wi-Fi 6 e o 5G oferecem. Paralelamente, eles permitirão que a TI não apenas sobreviva ao dilúvio da tecnologia sem



fio, mas também garanta a segurança e a melhor experiência ao usuário em um mundo móvel.

Em nossa *Pesquisa global de tendências de rede de 2019*, perguntamos a estrategistas de rede em qual posição eles estão na adoção de uma arquitetura de acesso seguro com relação ao modelo de capacidade de cinco estágios. Cerca de 72% dos entrevistados

planejam implantar acesso viabilizado por IA ou baseado em intenção em até dois anos, contra apenas 18% dos que já contam com uma dessas opções hoje. Essa implantação permitirá que eles criem e alterem políticas de forma dinâmica e, consequentemente, alinhem de forma consistente as políticas de acesso à intenção de negócios de ponta a ponta, entre usuários e serviços, onde quer que estejam localizados ou em roaming.¹⁴

Figura 21 Capacidade de acesso seguro





Considerações sobre a viabilização do acesso e das redes sem fio na era digital

1 Ferramentas de garantia sem fio

serão uma necessidade: na maioria dos setores, a conectividade de acesso de clientes e coisas está se tornando predominantemente sem fio. Os estrategistas de redes precisam contar com sistemas e ferramentas avançados de garantia sem fio para que possam fornecer experiências sem fio consistentes em todas as redes de acesso de TI e IoT.

2 A segmentação com e sem fio com base em políticas poupará muitas dores de cabeça:

a automação com base em políticas nas redes de acesso, de núcleo e filiais permite que segmentos e microsegmentos sejam criados e gerenciados dinamicamente de acordo com grupos de usuários e aplicativos para que as redes formem uma barreira dinâmica zero-trust contra ataques e ameaças.

3 Use a classificação de dispositivos orientada por IA antes de implantar a IoT de forma ampla demais:

do ponto de vista econômico, não faz sentido proteger sensores, monitores e outros dispositivos de IoT de baixo custo com soluções de segurança caras. No entanto, com o uso de uma classificação automatizada de dispositivos e uma automação baseada em políticas, segmentos e microsegmentos de IoT podem ser criados e gerenciados dinamicamente com base em grupos de aplicativos e dispositivos de IoT.

4 Prepare-se para Wi-Fi 6, 5G

e OpenRoaming: os líderes de rede devem se certificar de que seu roadmap sem fio leve em conta como o Wi-Fi 6 e o 5G se complementarão e funcionarão com dispositivos, operadoras Wi-Fi e provedores de serviços para oferecer os recursos do OpenRoaming.

5 Considere serviços com base na localização:

muitos executivos de negócios dos setores de varejo, serviços de saúde e ensino já estão aproveitando os benefícios dos serviços com base na localização interna para melhorar a experiência do cliente. De acordo com a nossa pesquisa, 51% dos entrevistados já estão usando redes sem fio com local reconhecido para viabilizar uma experiência mais personalizada ao cliente por meio de aplicativos móveis. Outros 40% estão avaliando a oportunidade.¹⁴

6 Prepare-se para a execução de microserviços em dispositivos de rede de borda:

com o Kubernetes e outros recursos de gerenciamento e orquestração para cargas de trabalho em contêineres, está se tornando cada vez mais atraente para as equipes de aplicativos começar a hospedar componentes de serviço de aplicativos ou de rede em dispositivos de rede com capacidade de carga de trabalho na borda da rede. Considere como isso afetará os requisitos de políticas, desempenho, segurança e segmentação da sua rede.



A transformação do papel da segurança de rede



Resumo da seção



Revelações principais

- À medida que aplicativos, dados e identidades mudam para a nuvem e a extremidade da rede, a segurança baseada em perímetro por si só não consegue mais proteger de forma eficaz contra as ameaças atuais.
- A combinação de muitos tipos diferentes de dispositivos e usuários de dispositivos móveis conectados de qualquer lugar a aplicativos em rede em qualquer lugar resulta em novos desafios, como perda de visibilidade e controle.
- A integração da segurança com recursos de redes baseados em intenção resulta em uma combinação poderosa que simplifica a aplicação de política, a proteção e a correção de maneira eficaz em toda a rede.



Principais descobertas

- Os estrategistas de redes identificaram a segurança como uma das principais áreas de investimento, atrás apenas da IA.
- 43% das equipes de rede identificaram como prioridade a melhoria dos recursos integrados de segurança da rede.
- Em 2019, 48% dos CISOs identificaram o “tempo até a correção” como o principal indicador-chave de desempenho (KPI), em comparação aos 30% de 2018.

- Quase 75% dos líderes de rede estavam confiantes de que em dois anos teriam definição e aplicação de políticas adaptativas ou automatizadas viabilizadas por IA.



Orientação essencial

- Desenvolva recursos de segurança de rede em cinco áreas principais: visibilidade e detecção de ameaças, acesso zero-trust, proteção contínua, infraestrutura de rede confiável e fluxos de trabalho de SecOps e NetOps integrados.
- Certifique-se de que uma estratégia de segurança zero-trust esteja incluída em qualquer plano de automação e garantia de rede para gerenciar efetivamente as ameaças à segurança, independentemente de onde elas existam na rede distribuída.
- Ao modernizar a infraestrutura e os processos, as equipes de redes devem levar em conta requisitos confiáveis que ajudem a garantir que a própria rede seja resistente a violação.
- As equipes de SecOps e NetOps precisam avaliar como compartilhar dados e devem integrar ferramentas para simplificar a prevenção, a detecção e os fluxos de trabalho de resposta a ameaças.



Resumo da seção (continuação)



Principais previsões

“Até 2025, algumas empresas de TI de ponta terão implantado um conjunto limitado de fluxos de trabalho de segurança viabilizados por redes totalmente automatizados os quais ajudarão a acelerar a correção e a reduzir a carga de trabalho da equipe de SecOps. O aumento da maturidade das plataformas de IBN, das tecnologias de inteligência artificial e de aprendizagem de máquina e da integração entre ferramentas de rede e segurança viabilizará a automação de alguns casos de uso bem definidos que não acarretam riscos à rede ou à postura de segurança da empresa.”

– Wendy Nather, chefe da equipe de Consultoria de CISOs, Cisco

“Em 2025, a computação quântica ainda estará na sua infância. No entanto, já haverá esforços para enfrentar o novo perigo de a computação quântica ser utilizada para superar os atuais métodos de criptografia.”

– David McGrew, especialista da Cisco

A transformação do papel da segurança de rede

A adoção de modelos móveis, de várias nuvens e de IoT está criando novos desafios e oportunidades na segurança de rede.

O perímetro tradicional da rede corporativa é agora apenas um elemento de um modelo mais distribuído em que a identidade de todos os usuários, coisas e aplicativos deve ser questionada, independentemente de estarem no campus ou na filial, em uma VPN, na rede pública ou na nuvem.

As equipes de TI precisam aproveitar os poderes combinados da rede e da segurança para enfrentarem os desafios da segurança cibernética de forma eficaz. Os estrategistas de redes reconhecem prontamente a importância de investir em segurança de rede. Quando perguntados sobre como as equipes de rede podem atender melhor às necessidades das empresas, os entrevistados em nossa *Pesquisa global de tendências de rede de 2019* identificaram a segurança como a segunda principal área de investimento após a IA, com 43% identificando como prioridade a melhoria dos recursos integrados à segurança da rede.¹⁴

A convergência da segurança com um modelo de redes baseado em intenção permite que as empresas apliquem e imponham políticas de função empresarial e respondam mais rapidamente às ameaças em todos os serviços de rede.

Nesta nova realidade, as equipes de NetOps e as redes que elas controlam têm um papel vital na segurança em cinco áreas-chave:

Visibilidade: os CISOs estão preocupados em manter a visibilidade neste novo modelo distribuído de aplicativos e dados.

Acesso zero-trust: a rede é um elemento integrante para implementar um modelo de confiança consistente em que todos os usuários, dispositivos e aplicativos sejam igualmente suspeitos, independentemente de onde estejam acessando a rede.



De acordo com uma pesquisa da Forrester, um modelo de rede zero-trust deve fazer três coisas:²⁹

1

Segmentar redes para aplicar controles granulares e evitar movimentos laterais.

2

Fornecer análise e visibilidade granular da rede para detecção e resposta a ameaças.

3

Oferecer um gerenciamento de segurança de rede consolidado e estabelecer as bases para a automação.

Fluxos de trabalho contínuos de SecOps e NetOps:

os CISOs entendem que suas equipes de SecOps e NetOps atuam juntas, com 95% dizendo que suas equipes são muito ou extremamente colaborativas.³⁰ No entanto, essas equipes ainda tendem a usar dados, fluxos de trabalho e ferramentas de

forma separada ao coletar e analisar dados. As equipes de SecOps e NetOps precisam repensar o jeito de simplificar os fluxos de trabalho, compartilhar dados e integrar ferramentas para atingir uma meta comum de prevenção, detecção e resposta automatizadas a ameaças.

Proteção contínua: a rede precisa funcionar como um agente de detecção distribuída e um agente de aplicação que possa tomar medidas de forma automática e rápida para conter dispositivos infectados.

Infraestrutura de rede confiável: com o aumento da ameaça de agentes mal-intencionados que buscam informações privilegiadas ou tentam interromper operações de rede, as empresas devem proteger o sistema e os dispositivos de rede individuais de ataques.



48%

Em 2019, 48% dos CISOs identificaram o “tempo até a correção” como um indicador-chave de desempenho em comparação aos 30% de 2018.³⁰

De acordo com pesquisas do Gartner, “para SecOps, o acesso ao tráfego de rede comporta análise retrospectiva de fluxos de tráfego, identificação de tentativas de exfiltração, computação forense de redes e fluxos de trabalho de microssegmentação”.³¹

Desafios com a segurança da rede

Aumento da escala e da complexidade

A TI deve proteger a empresa e seus dados em ambientes com prioridade à nuvem e prioridade à tecnologia móvel maiores, mais complexos e em rápida transformação, e de ameaças à segurança contra as quais é cada vez mais difícil se defender.

Cargas de trabalho: à medida que aplicativos, dados e identidades migram para a nuvem ou para a Internet, o modelo de TI continua indo além do perímetro tradicional da empresa. Esse aumento da computação híbrida e em várias nuvens e dos microsserviços hospedados na borda da rede exige uma mudança da maneira como protegemos as cargas de trabalho. A segurança baseada em perímetro por si só não é capaz de oferecer proteção eficaz contra as ameaças atuais.

Clientes: além disso, a combinação de diversos tipos de dispositivos (dispositivos de usuário e dispositivos de IoT interconectados), bem como diferentes tipos de usuários (funcionários, contratados, terceirizados), que se conectam de qualquer lugar a aplicativos em rede em qualquer lugar, apresenta ainda mais complexidade.³⁰



Infraestrutura: por fim, à medida que a sofisticação das ameaças evolui, os invasores procuram cada vez mais subverter a infraestrutura subjacente de switching e roteamento para escutar, roubar ou manipular dados e iniciar ataques contra outras partes da rede.³²

“Como qualquer outra grande empresa, precisamos lidar com a complexidade em escala. Inspecionamos 47 TB de tráfego da Internet, analisamos 28 bilhões de fluxos e registramos 1,2 trilhão de eventos de segurança diariamente.”

– Marisa Chancellor, diretora de segurança de infraestrutura, Cisco

O cenário da ameaça: inovação contínua dos invasores

À medida que o potencial de retorno em ataques de segurança cibernética continua ficando mais atraente, a natureza desses ataques está se tornando mais sofisticada. Dentre as tendências de ameaça mais preocupantes estão as seguintes:

- Ransomware autopropagável com base na rede
- Ataques de malware criptografados e ocultos no tráfego criptografado representaram 70% de todos os ataques mal-intencionados em 2017⁴
- Redes de botnets de IoT implantados em dispositivos de IoT desatualizados e não monitorados



Figura 22 Ameaças atuais à segurança cibernética



Para obter as mais recentes informações sobre o cenário cada vez mais sofisticado de ameaças, consulte o último Cisco Cybersecurity Series Threat Report.³³

Conformidade

As equipes de segurança também se veem diante da adesão a regulamentações novas e emergentes. Ou seja, precisam assegurar e demonstrar que contam com políticas de segurança eficazes.

O Regulamento Geral de Proteção de Dados (RGPD) da União Europeia entrou em vigor em 2018 e determina uma abordagem proativa em relação à privacidade de dados. Além disso, setores como saúde, serviços financeiros, varejo e governo federal estão exigindo novos padrões de conformidade, mediante risco de aplicação de multas pesadas por não conformidade.

Proliferação de dispositivos de IoT: crescimento da superfície de ataque
Os dispositivos de IoT conectados continuam se proliferando sem a segurança adequada, em grande parte porque muitas vezes são desconhecidos ou não detectados pela TI. Cada dispositivo conectado expande a superfície de ataque de uma empresa. No caso dos dispositivos de IoT, os ataques em nível de rede podem incluir distributed denial-of-service (DDoS), spoofing de identificação por radio-frequência (RFID) e ameaças direcionadas a senhas e com software mal-intencionado.

Lacunas na visibilidade

A proliferação de novos microsserviços e aplicativos de nuvem pode apresentar lacunas na visibilidade e no controle da TI sobre sua superfície de ataque. Os usuários agora podem instalar e ativar sem auxílio aplicativos que podem ser inseguros ou exigir permissões de acesso excessivas.



“Muitos dispositivos de IoT oferecem pouca segurança intrínseca, raramente usam credenciais ou certificados digitais e podem ser facilmente comprometidos. Por isso, a automação do reconhecimento de dispositivos, da classificação e da ativação de políticas de acesso à rede é fundamental para prevenir ou conter violações de segurança.”

– Tim Szigeti, engenheiro principal, Cisco IoT

O número e o alcance dos dispositivos móveis (corporativos e pessoais) continuarão crescendo, e a tendência “traga seu próprio dispositivo” significa que mais smartphones, laptops, tablets e outros dispositivos pessoais estão acessando aplicativos cruciais, o que resulta em maior falta de visibilidade e controle.

Enfrentando desafios de segurança com uma rede inteligente

A equipe de NetOps capacitada com uma rede inteligente apresenta um forte aliado a SecOps na luta contínua para manter a empresa e seus dados seguros. Ao adotar um modelo de rede baseado em intenção em que os recursos de segurança são fundamentais, a TI pode fazer

com que a rede determine de forma automática e eficaz o que é novo, o que é importante e o que é incomum, independentemente de sua posição na rede distribuída.

Em última análise, a combinação de segurança e redes baseadas em intenção fornece visibilidade e controle contínuos sobre quem e o que está na rede. Contribui para um modelo de acesso zero-trust completo e também integra dentro da rede (em vez de agregar posteriormente) recursos de prevenção, detecção e resposta rápida a ameaças, proporcionando proteção constante em todos os lugares. (Ver Figura 23 abaixo.)

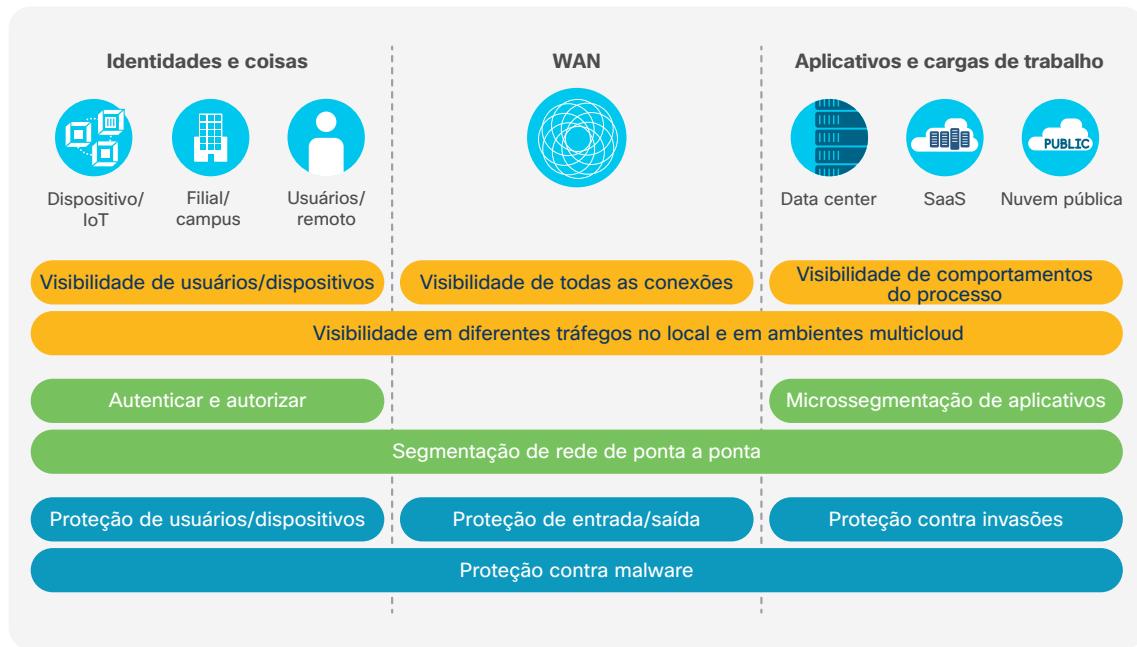
Visibilidade de rede e detecção de ameaças

Nunca foi tão verdade que não dá para proteger o que não se pode ver. A visibilidade é fundamental para que as equipes de TI protejam os ativos e as informações da rede. Isso inclui a visibilidade de usuários, dispositivos, aplicativos e coisas, onde quer que estejam, para monitorar atividades anômalas e definir políticas.

“Estamos lidando com um movimento em grande escala em relação a SaaS e perdendo a visibilidade e o controle que tínhamos no passado.”

– Marisa Chancellor, diretora de segurança de infraestrutura, Cisco

Figura 23 Modelo de segurança de rede integrada



Uma visualização completa de redes de acesso, WAN, data center, de várias nuvens e em IoT permite o mapeamento de cada fluxo que percorre a rede para que as equipes possam determinar um parâmetro dinâmico de comportamento normal de rede. Com uma rede inteligente que disponibilize total visibilidade, a equipe de rede tem um recurso inestimável para ajudar a equipe de segurança a detectar e corrigir ameaças com mais rapidez e precisão, mesmo com tráfego criptografado.

Acesso zero-trust

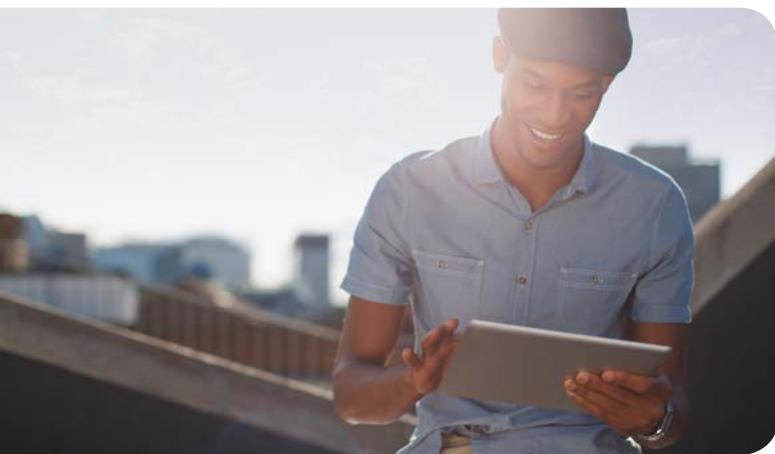
Aproveitando-se de uma base avançada de visibilidade, um modelo holístico de segurança zero-trust permite que as equipes de NetOps gerenciem o acesso independentemente do tipo e da localização dos dispositivos e das cargas de trabalho em questão. Quando aplicado adequadamente, esse modelo pode proteger cargas de trabalho e dados dentro da nuvem pública ou privada e a força de trabalho, mesmo quando os usuários não estão na rede. Os principais recursos de um modelo zero-trust abrangem:

Proteção do acesso à rede: em um modelo de acesso zero-trust, a equipe de TI aplica controles precisos sobre quem, o que, quando, onde e como usuários e endpoints de IoT têm permissão de acesso à rede com e sem fio. A TI também pode aplicar uma abordagem zero-trust usando controles de política baseados em grupo e segmentação cliente-para-aplicativo de ponta a ponta, a fim de restringir o acesso a recursos em sua rede.

Contenção proativa de violações de aplicativos: a equipe de TI pode mitigar a movimentação lateral não autorizada entre as cargas de trabalho dentro ou além do data center, o que pode ajudar a reduzir a superfície de ataque caso um invasor já esteja na rede.

Mitigação do risco de acesso não autorizado a aplicativos: quando qualquer tipo de usuário (funcionário, contratado, terceirizado, etc.) fizer login em um aplicativo dentro ou fora do local, será necessário verificar sua identidade

com autenticação de dois fatores (2FA) e também a segurança do dispositivo, o que mitigará o risco de acesso não autorizado a aplicativos e dados causado por senhas roubadas ou fracas.



Proteção constante em qualquer lugar

Para fornecer proteção a todos os sistemas e usuários corporativos, a rede precisa se adaptar aos novos tempos fazendo com que a proteção vá além de perímetros tradicionais. Arquiteturas baseadas em intenções, como SD-WAN, apresentam uma plataforma com controle centralizado para implantar e gerenciar uma pilha de segurança completa na borda da rede que estende a proteção a todas as entradas ou saídas da rede. Para oferecer proteção total, essa pilha deve incluir segmentação de rede, firewall, gateway Web seguro, proteção contra malware e segurança na camada de DNS.

Caso algum arquivo mal-intencionado consiga passar, a detecção do malware pode instruir rapidamente a rede para que encaminhe os dispositivos infectados de forma automática a um segmento de rede restrito ou em quarentena. E, ao atualizar continuamente a inteligência de ameaças para bloquear arquivos mal-intencionados e estender essa inteligência aos endpoints e até a nuvem, o sistema pode bloquear essas ameaças caso ocorram novamente.

Construção de uma infraestrutura de rede confiável

Conforme as empresas se digitalizam e as ameaças aumentam, há uma necessidade cada vez maior de verificar a segurança e a integridade da infraestrutura da rede e dos dispositivos de rede individuais.

A construção de uma infraestrutura de rede “confiável” exige que seja implementada uma segurança de forma holística em todo o ciclo de vida do produto. Isso ajuda a proteger contra adulteração e manipulação durante a fabricação, a distribuição, a implantação e a operação contínua, que é especialmente importante porque revendedores terceirizados, integradores de sistemas ou managed service providers (MSPs) costumam se envolver nesses processos.

Ao atualizarem os equipamentos, as equipes de rede devem buscar uma série de recursos importantes, como inicialização segura ancorada por hardware, identificadores de dispositivos seguros e exclusivos, e também a capacidade de destruir chaves e ativar a redefinição de fábrica.

Em resumo, as redes estão se tornando cada vez mais capacitadas para enfrentar ameaças atuais e futuras. Cabe a NetOps e a SecOps tomar medidas para incorporar esses recursos de segurança avançada em seus projetos e operações de rede para que possam trabalhar juntos e obter visibilidade, proteção e confiança contínuas.

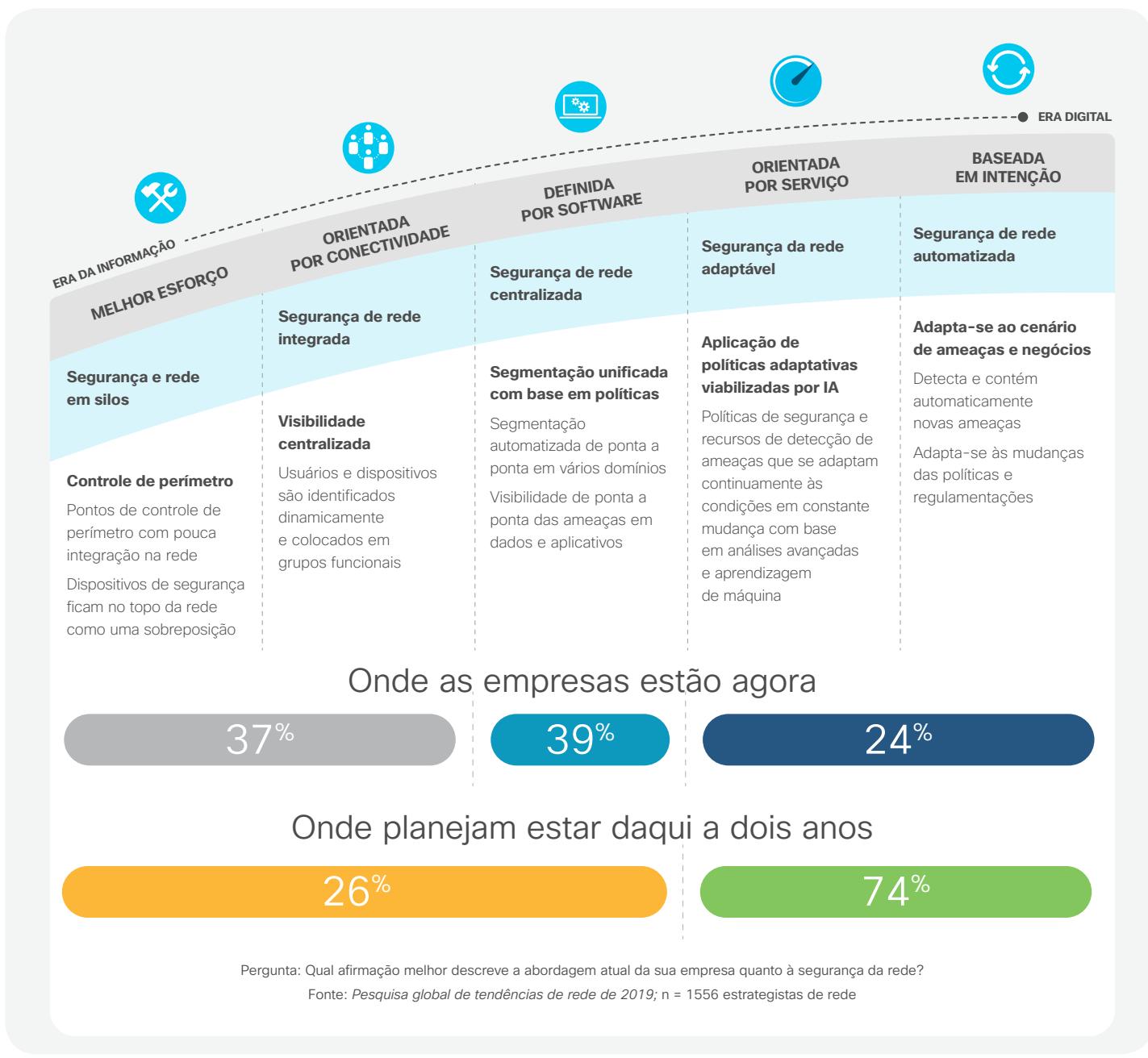


Estado atual e futuro da segurança da rede

Então, qual é a posição atual das empresas na construção de seu modelo de segurança geral da rede para obter proteção contínua?

Em nossa *Pesquisa global de tendências de rede de 2019*, perguntamos aos líderes de rede como eles avaliariam sua abordagem atual de segurança em relação ao nosso modelo de capacidade de cinco estágios. Embora as empresas estejam atualmente distribuídas de forma bem uniforme em todos os estágios, quase três quartos estavam confiantes de que teriam alguma forma de definição e implementação de política de segurança automatizada viabilizada pela IA nesse período.¹⁴

Figura 24 Capacidade de segurança da rede baseada em intenção





Relatório Global de
Tendências de Redes de 2020

Tendências em
operações de rede

Transição de reativo para otimizado para empresas



Resumo da seção



Revelações principais

- Os modelos tradicionais de operações de rede não são sustentáveis para comportar os serviços empresariais necessários face às crescentes demandas digitais.
- As equipes de TI estão modernizando as operações de TI e adotando abordagens de DevOps para aproveitar sistemas baseados em controlador e ferramentas habilitadas para IA que automatizam ou eliminam muitas tarefas de rede tradicionalmente repetitivas.
- Novas e avançadas plataformas de rede aberta permitem uma melhor integração com outros sistemas de TI e segurança e processos operacionais, além de oferecerem novas oportunidades para desenvolvedores de aplicativos empresariais.
- Nesta próxima era de operações de rede, líderes e equipes estarão mais bem posicionados para se afastarem de modelos operacionais reativos e oferecerem continuamente os serviços precisos necessários para a empresa.



Principais descobertas

- 73% das equipes passam mais da metade do tempo apenas mantendo o status quo da rede.
- Os líderes de TI iriam priorizar os recursos das suas equipes de rede para se concentrar em várias nuvens; acelerar implantações de aplicativos; e proteger melhor a rede, os aplicativos e os dados, se pudesse liberar recursos das tarefas diárias de manutenção que garantem a continuidade dos serviços.
- Mais de um terço dos líderes de TI priorizou a importância de alcançar uma melhor coordenação e integração de rede com outras equipes de TI e linhas de negócios.

Resumo da seção
(continuação)

Orientação essencial

- Ao adotarem modelos de automação e garantia baseados em controlador, as equipes de redes devem concentrar seus esforços em três áreas cruciais do processo: gerenciamento do ciclo de vida, gerenciamento de políticas e gerenciamento de garantia.
- Para melhorar a qualidade do serviço, o custo, a agilidade e a segurança, os administradores de redes devem se afastar do gerenciamento de dispositivos individuais e concentrar sua atenção no controlador de rede e no gerenciamento do sistema de rede de ponta a ponta por meio do controlador.
- As equipes de rede devem adotar uma abordagem DevOps de plataforma aberta a fim de integrar a rede aos processos de TI e agilizar os fluxos de trabalho de ponta a ponta para que possam ganhar eficiências e ser mais responsivas às necessidades das empresas.
- As equipes de operações de rede devem se equipar com recursos de AIOps emergentes para oferecer melhores resultados de rede e de negócios.



Principais previsões

Aproximação de negócios e TI:

“As equipes irão reequilibrar o tempo gasto na manutenção da rede com um foco externo de como a rede pode atender melhor às necessidades de negócios e apoiar a inovação comercial. Novas funções operacionais serão organizadas com a tradução das intenções comerciais e das exigências de aplicativos em políticas de rede.”

NetOps estendendo o monitoramento à nuvem:

“À medida que os serviços de negócios multicloud se tornam o padrão, as equipes de NetOps estenderão a visibilidade e o monitoramento preditivo em redes públicas e WAN e até o ponto de presença na nuvem. Para obter insights ainda melhores, os sistemas corporativos de redes com base em intenção começarão a integrar dados de sistemas do provedor de serviços e do provedor da nuvem para garantir a qualidade contínua da experiência para serviços em nuvem.”

– Rich Plane, CTO de Experiência do Cliente da Cisco

Transição de reativo para otimizado para empresas

Segundo pesquisas da Cisco, as equipes de liderança de TI estão encabeçando a transformação digital em suas empresas. Para que isso seja possível, elas estão conduzindo uma transformação igualmente importante à parte, modernizando as operações e a infraestrutura de TI para atender às novas exigências digitais.³⁴

Pela primeira vez, ao adotarem uma abordagem DevOps de plataforma aberta, as equipes de redes possuem as ferramentas e tecnologias para integrar a rede em processos de TI e agilizar os fluxos de trabalho de ponta a ponta para que possam obter eficiências e ser mais responsivas às necessidades das empresas.

Essa abordagem também oferece uma chance de construir pontes operacionais entre os domínios de rede e fazer uma integração direta com aplicativos de modo a dar respaldo às necessidades dinâmicas das linhas de negócios.

Ao adotarem novas formas de pensar em operações de redes e novas maneiras de trabalhar, os líderes e equipes de TI estarão mais bem posicionados para oferecer exatamente os serviços dos quais as linhas de negócios precisam, sejam estes melhores serviços atuais ou novos serviços que viabilizam os negócios.

63%

De acordo com a nossa *Pesquisa global de tendências de rede de 2019*, 63% dos líderes de TI planejam implementar redes avançadas capazes de atender às necessidades de negócios de forma dinâmica em até três anos.¹⁴





Estado atual e futuro das operações de rede

Prontidão operacional para apoiar a transformação digital

Em nossa *Pesquisa global de tendências de rede de 2019*, perguntamos a estrategistas de rede e líderes de TI como eles classificariam a capacidade operacional de suas redes atuais com relação ao gerenciamento de garantia em cinco estágios de maturidade, que vão de reativo a otimizado para os negócios.

Embora apenas 23% se considerem atualmente preditivos ou otimizados para os negócios, 71% deles planejam atingir esse estágio em dois anos, o que destaca a urgência que as empresas têm para se preparar para as demandas cada vez maiores na rede corporativa.¹⁴

Como os avanços das redes estão transformando as operações de rede

A recente onda de tecnologias de rede avançadas mudará praticamente todos os aspectos das operações de rede, e as seguintes áreas devem sofrer grandes mudanças.

Integração de operações de rede ao processo de TI

Os velhos tempos em que as redes eram operadas em silos de tecnologia por engenheiros com experiência principalmente em uma área estão cada vez mais distantes. Segundo a nossa pesquisa, quase um terço dos líderes de TI enfatizou a importância de atingir uma melhor coordenação e integração de rede com outras equipes de TI, enquanto 26%

Figura 25 Capacidade das operações de rede: gerenciamento de garantia



revelaram a importância de melhorar a capacidade de atuar com linhas de negócios.¹⁴ Outros 27% identificaram que estavam ficando para trás devido ao design em silo e à abordagem operacional em domínios de rede separados.¹⁴

Graças às interfaces abertas proporcionadas pelos controladores de rede baseados em intenção, as equipes de NetOps abrirão mão de seus silos operacionais isolados para se tornarem uma parte totalmente integrada dos fluxos de trabalho de TI. Cerca de 34% dos líderes de TI

identificaram essa mudança como a que mais ajudaria a equipe de rede a atender melhor às necessidades da empresa.¹⁴

No entanto, para atingir os níveis desejados de agilidade de TI e alinhamento contínuo de intenções, as equipes de NetOps ficarão encarregadas de melhorar a integração entre domínios de rede (acesso, WAN, data center [DC], nuvem etc.), como também com outros domínios de TI, como gerenciamento de serviços de TI (GSTI) e sistemas de SecOps.

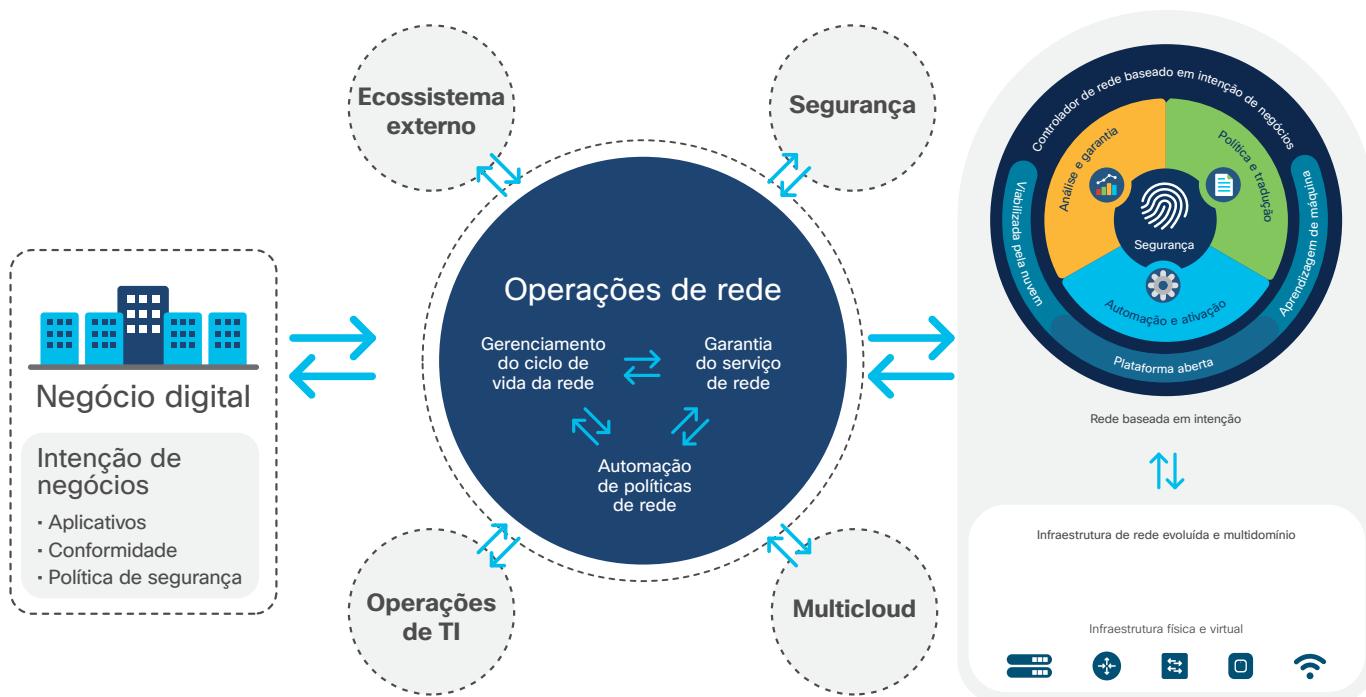
Esta figura ilustra como a NetOps poderá usar uma abordagem DevOps de rede de plataforma aberta para integrar tecnologias e processos de rede a outros sistemas internos e até mesmo externos.

Alinhamento total com TI e intenção de negócios

Essencialmente, a rede existe para fornecer os serviços necessários para auxiliar funcionários, clientes e parceiros, ou seja, administrar o negócio. Mas a realidade é que as abordagens tradicionais de operações manuais muitas vezes não atendem às necessidades dinâmicas das empresas. Essa realidade está prestes a mudar.

Com redes baseadas em intenção, as operações de rede serão muito mais automatizadas e dinâmicas e também diretamente informadas pela intenção do TI e das empresas. Essa intenção incluiria necessidades de desempenho de aplicativos, política de segurança e conformidade e processos de TI.

Figura 26 Oportunidades de integração com a abordagem de DevOps de rede de plataforma aberta





Com o tempo, a tradução de intenção de TI e de negócios em política de rede se tornará parte integrante da função de operações de rede.

Automação para reduzir a complexidade das operações de rede

Não há dúvida de que a automação das tarefas de operações está mudando o aspecto das operações de rede. Um a cada quatro líderes de TI e estrategistas de rede identificou a automação como a tecnologia que teria o maior impacto no design e na estratégia de rede nos próximos cinco anos.¹⁴

Por outro lado, isto significará deixar para trás as abordagens manuais tradicionais de configuração e manutenção de rede. Algumas equipes acharão essa tendência preocupante. Cerca de 20% dos líderes de TI reconhecem que a resistência das equipes de NetOps em adotar tecnologias de automação e IA será um grande obstáculo à modernização.¹⁴

Gerenciamento de incidentes e problemas reativo x preventivo

Conforme abordado anteriormente, muitas empresas se encontram em um estágio reativo de prontidão operacional. A questão é que 25% dos entrevistados indicaram que uma mentalidade operacional reativa os impedia de atingir os objetivos de rede.³⁵ Esse cenário também está prestes a mudar. Ao usarem a IA e fazerem uma integração com outros sistemas de TI, as equipes de NetOps serão capazes de atingir um

estado de manutenção preditiva que corrige problemas muito antes que eles se tornem incidentes e afetem os serviços.

Inteligência humana e artificial trabalhando lado a lado

Os engenheiros de rede precisam de toda a ajuda que estiver ao seu alcance para enfrentarem a complexidade da rede.



É por isso que as equipes de NetOps estão se armando com novos recursos de operações de IA (AIOps), como aprendizagem de máquina e raciocínio de máquina, os quais podem proporcionar maior precisão em definição de linha de base de desempenho, detecção de anomalias, análise automatizada de causa raiz, orientação de correção e insights preditivos.

Em vez de fazer triagem por milhares de eventos, as equipes de NetOps dependerão cada vez mais dessas tecnologias para apresentar com precisão apenas os mais importantes, assim como as principais opções de correção. A equipe de AIOPS também pode trabalhar para ajustar esse resultado, enriquecer o conteúdo e integrar o conhecimento com os principais sistemas de gerenciamento de negócios e serviços.

42%

A mudança para AIOps está ganhando força, já que 42% dos líderes de TI acreditam que a IA terá mais impacto em suas operações automatizadas no futuro.³⁵

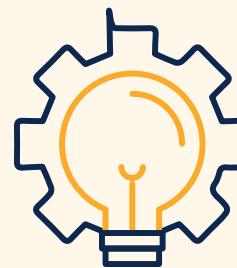
Trazendo a conectividade da tecnologia operacional para as operações de rede

O fato de que os dispositivos de IoT são considerados ativos de negócios e que os dados operacionais que eles produzem são vitais para as operações de negócios deixa bem clara a necessidade de novas abordagens para o gerenciamento de infraestrutura.

- Em casos de uso de IoT, como monitoramento em tempo real, os problemas operacionais podem ter consequências graves, até mesmo fatais.
- Com redes de grande porte, os dispositivos na IoT podem chegar aos milhões, de modo que a automação é a única maneira de gerenciá-los com eficiência.
- Em alguns casos, não se pode garantir uma conexão constante entre o HQ e dispositivos remotos na IoT – o que está impulsionando o investimento em análise de neblina e borda da rede.

Apresentando uma estrutura de operações de rede de última geração

Para se preparar para um futuro de operações conduzidas por redes baseadas em intenção, os especialistas em tecnologia da Cisco Customer Experience criaram uma estrutura que oferece orientação estratégica, boas práticas, designs validados, processos comprovados e ajustes recomendados.

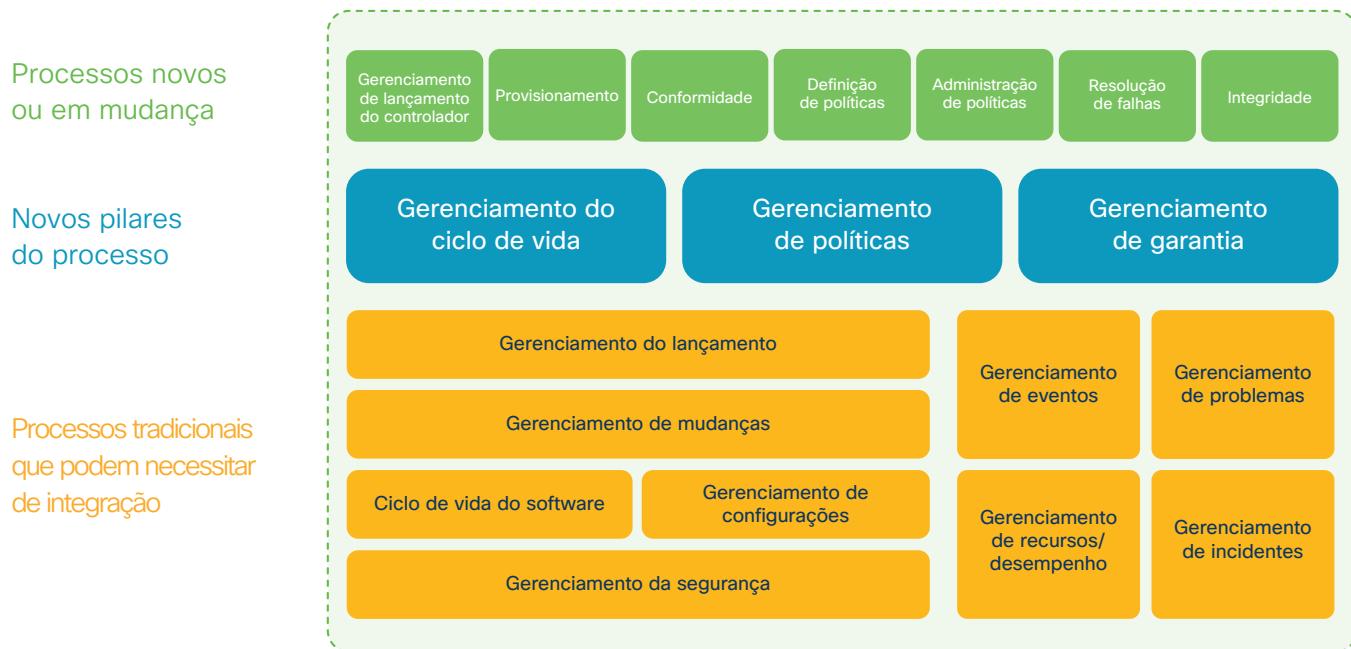


Uma nova mentalidade: gerenciamento do controlador de rede

De acordo com Jake Hartinger, arquiteto de soluções da Cisco Customer Experience, uma das mudanças mais profundas nas operações de rede será a mudança de foco – do dispositivo para o controlador. Até agora, os administradores de rede normalmente fornecem e coletam informações da rede fazendo login em dispositivos.

Com modelos de garantia e automação baseados em controladores, os administradores se concentrarão em gerenciar o controlador, as integrações e os processos em relação ao controlador. Quanto mais uma empresa for capaz de adotar essa mudança, mais rápido ela conseguirá melhorar a qualidade, o custo, a agilidade e a segurança do serviço.³⁶

Figura 27 Novos modelos de operações para a nova rede



Existem três áreas de processo cruciais no cerne deste modelo: gerenciamento do ciclo de vida, gerenciamento de políticas e gerenciamento de garantia. A simplificação operacional que o IBN oferece permite planejar e construir uma transformação operacional em torno desses processos centrais.

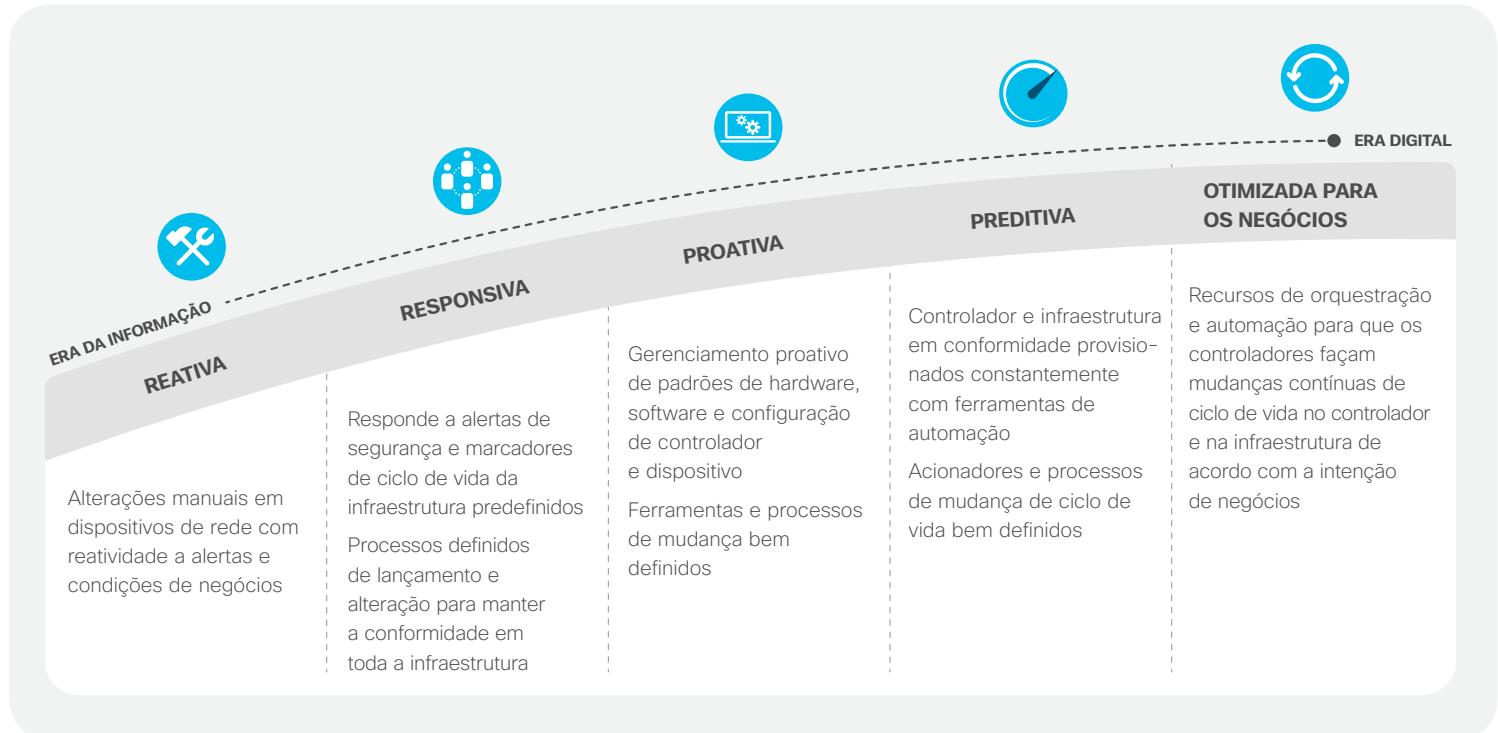
Gerenciamento do ciclo de vida

A mudança para sistemas de provisionamento e a automação conduzidos por controladores exige uma adesão muito mais criteriosa às normas de segurança, hardware e software. Um usuário que faz uma alteração na interface de linha de comando (CLI) pode achar que o controlador substituirá o comando em atualizações futuras porque ele não foi definido como política.

Para evitar este cenário, a empresa precisará contar com práticas bem definidas de gerenciamento do ciclo de vida com relação ao gerenciamento de lançamentos e de mudanças, especialmente com automações que foquem na rede ou no serviço como sistema.

Para simplificar, o gerenciamento do controlador de rede envolve o gerenciamento de novas APIs, pontos de integração, software e hardware de controlador, como também a configuração da interface de usuário que gerencia os recursos de garantia e política. Uma vez que os recursos do controlador mudarão de forma contínua no futuro próximo, será fundamental definir um processo de gerenciamento do ciclo de vida exclusivo para o controlador de rede e as integrações.

Figura 28 Capacidade das operações de rede: Gerenciamento do ciclo de vida



Gerenciamento de políticas

O gerenciamento de políticas de rede também é essencial porque, para serem bem-sucedidos e sustentáveis, os controladores de rede dependem de diretrizes e padrões de rede mais rígidos para hardware, software, configurações e até mesmo integrações de dispositivos de rede. A política deve primeiro ser definida para então ser atualizada. Também deve ser configurada nos controladores de rede para garantir que os padrões definidos sejam continuamente provisionados. Além disso, a política deve ser validada utilizando métodos de verificação de conformidade.

Uma vez que as mudanças de políticas podem ter uma presença de ativação muito ampla, capaz de afetar as configurações de milhares de dispositivos, elas precisam ter uma natureza prescritiva para que possam ser testadas e consideradas válidas e aprovadas. Consequentemente, com a maior difusão de modelos de verificação de políticas modelares que simulam quaisquer alterações antes da ativação, haverá a necessidade de mais flexibilidade nas opções de configuração.

Figura 29 Capacidade das operações de rede: gerenciamento de políticas



Gerenciamento de garantia

Redes de pequeno porte tendem a ser facilmente gerenciadas por mãos e cérebros humanos, mas é quase impossível gerenciar redes maiores sem ferramentas, dados de rede e processos bem definidos. Atualmente, apenas uma em cada cinco equipes de operações é capaz de usar análises avançadas para identificar e corrigir possíveis problemas com impacto no serviço antes que eles aconteçam.¹⁴

Com um modelo de rede baseado em intenção habilitado para IA, o gerenciamento de garantia melhora e integra esses recursos com análises, integrações de API, recursos de correlação, inventário e relatórios avançados e enriquecimento. Em especial, a análise e o enriquecimento fornecem detalhes adicionais sobre falhas de rede que facilitam a resolução rápida ou a melhoria da integridade. E, com

a expectativa de que o sistema habilitado por IA continue sendo aperfeiçoado com base nas aprendizagens de grandes números de implantações adicionais, as equipes de operações continuarão se beneficiando.

Em redes maiores, o resultado é uma melhor qualidade de serviço, resolução rápida de problemas e eficiência operacional. Uma equipe de AIOps pode se concentrar em filtragem, enriquecimento e APIs com sistemas de gerenciamento de negócios ou serviços para automatizar totalmente os fluxos de trabalho de garantia.

Além dessas três principais áreas de processo, recomendamos que sejam examinadas as possíveis interações com processos tradicionais de ITSM, domínios de TI e sistemas para identificar outras possíveis oportunidades de integração.



O futuro das previsões de operações de rede para 2025

De acordo com Rich Plane, CTO de Experiência do Cliente da Cisco, dentro de cinco anos as equipes de operações de rede serão muito mais eficientes na execução daquilo que suas empresas precisam que elas façam. Aqui estão as suas previsões de como isso vai acontecer.

1 Garantia de ponta a ponta: as equipes de operações de rede poderão fazer a detecção preditiva de problemas e análise de causa raiz entre qualquer cliente ou dispositivo e qualquer serviço comercial, hospedado em qualquer lugar, e identificar rapidamente se e onde a rede é a causa de eventual degradação do desempenho do serviço.

2 Aproximação de negócios e TI: as operações de rede serão capazes de reequilibrar o foco, que deixará de ser quase exclusivo em monitoramento e solução de problemas e passará também a ter um direcionamento externo sobre o negócio e sobre como a rede pode melhor atender às necessidades de negócios. Novas funções operacionais serão organizadas com a compreensão e a tradução das intenções comerciais e das exigências de aplicativos em políticas de rede.

3 NetOps e SecOps trabalham com uma única fonte de verdade: as equipes de NetOps e SecOps desenvolverão fluxos de trabalho integrados e otimizados habilitados por compartilhamento de dados, entregas automatizadas e interações entre plataformas e ferramentas.

4

NetOps estendem o monitoramento

à nuvem: à medida que os serviços de negócios multicloud se tornam o padrão, as equipes de NetOps estenderão a visibilidade e o monitoramento preditivo em redes públicas e WAN e até o ponto de presença na nuvem. Para obter insights ainda melhores, os sistemas corporativos IBN começarão a integrar dados de sistemas do provedor de serviços e do provedor da nuvem para garantir a qualidade contínua da experiência para serviços em nuvem.

5

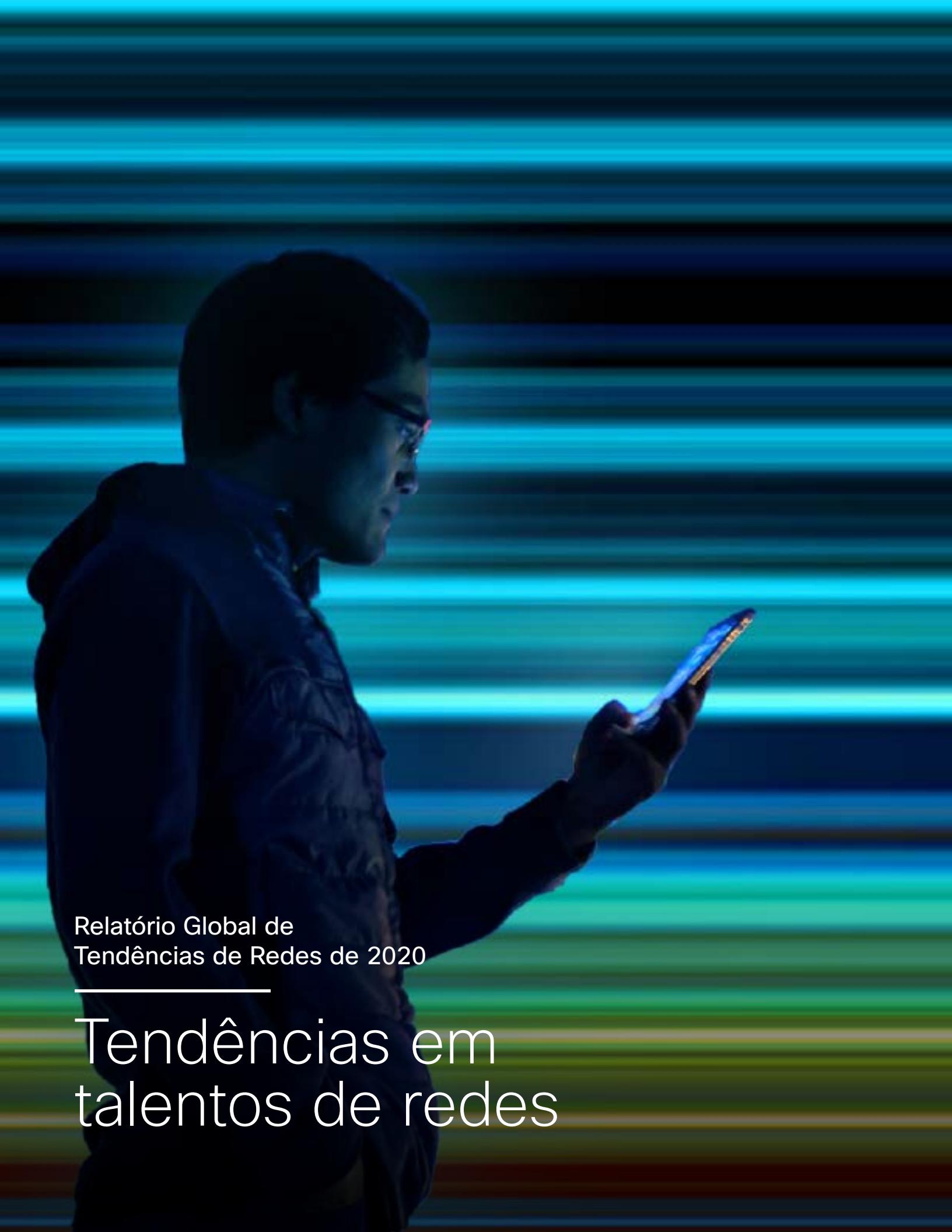
Gerenciamento de mudanças com base

em modelos: os processos de NetOps mais avançados, como a análise “e se” de qualquer alteração feita na rede, se estenderão além do data center e se tornarão mais difundidos.

6

Fluxos de trabalho autogerenciados

e autorreparáveis: alguns fluxos de trabalho menos impactantes serão totalmente automatizados, permitindo que a rede realize ações corretivas ou de gerenciamento do ciclo de vida sem a intervenção do operador humano. Esta abordagem baseada em dados e validada pela intenção produzirá níveis muito mais elevados de continuidade do serviço devido à minimização das oportunidades de erro.



Relatório Global de
Tendências de Redes de 2020

Tendências em
talentos de redes

Novos conjuntos de habilidades para a rede moderna



Resumo da seção



Revelações principais

- As novas tecnologias estão eliminando muitas tarefas manuais em muitos setores, e a área de TI não é exceção.
- A boa notícia para a área de TI e de rede é que a demanda por empregos continua forte para aqueles que adquirem novos conjuntos de habilidades com alta demanda, como programabilidade de rede.
- Conforme as operações de rede se tornam mais automatizadas, os administradores de redes assumem funções alinhadas às novas práticas operacionais relacionadas com gerenciamento do ciclo de vida, política e garantia de rede.
- Os estrategistas de redes assumirão funções de grande importância que visam a melhorar o alinhamento das empresas, integrar processos de TI, aumentar a segurança e fazer melhor uso dos dados.



Principais descobertas

- Em média, as tarefas de manutenção de rede ocupam hoje 55% do tempo e dos recursos de uma equipe de rede.

- 27% dos líderes de TI identificaram a falta de qualificações profissionais necessárias como um obstáculo importante para a transição para uma rede avançada.
- 22% dos líderes de TI preferem a requalificação com investimento em treinamento, conhecimento e certificações continuadas.
- Os estrategistas de redes identificam IA, integração TI/TO, automação e DevOps de rede como as principais áreas de aprimoramento de qualificações profissionais.



Orientação essencial

Estrategistas: considerem adquirir conhecimentos técnicos, comerciais e de software que façam com que vocês se desenvolvam em pelo menos uma destas áreas:

- O tradutor empresarial se concentrará em alinhar o desempenho de TI à intenção empresarial dinâmica.
- O guardião de rede se concentrará em conectar arquiteturas de segurança e de rede.
- O arquiteto de dados de rede focará em utilizar ferramentas de mensuração de rede e IA.
- O arquiteto de integração de rede se concentrará na integração de domínios de rede e TI.

Resumo da seção (continuação)



Profissionais: adquiram de maneira proativa a combinação certa de qualificações técnicas e de software para que vocês se desenvolvam em pelo menos uma destas novas áreas:

- O chefe de rede focará no gerenciamento do ciclo de vida da rede.
- O orquestrador da rede se concentrará na tradução e na automação de políticas.
- O detetive da rede se concentrará em garantir o serviço e a segurança da rede.

Líderes: considerem estas recomendações para formar a equipe de rede do futuro:

- Cultivem uma cultura de aprendizagem contínua.
- Busquem o equilíbrio entre requalificação e contratação.
- Invistam mais em treinamento e desenvolvimento.
- Façam rodízios de talentos para aumentar o tino comercial.
- Promovam um ambiente de trabalho inclusivo.



Principal previsão

“Até 2025, 75% das equipes de rede gastarão menos de 1/3 do tempo fazendo a manutenção do status quo da rede e 2/3 proporcionando inovação e criando valor para a empresa.”

– Joe Clarke, engenheiro eminentíssimo, Cisco

Novos conjuntos de habilidades para a rede moderna

Nos próximos dois anos, as tecnologias de redes avançadas alterarão quase todas as funções de redes. Com a TI assumindo um papel mais central na transformação empresarial, os profissionais de TI precisam se adaptar.

60% dos líderes empresariais acreditam que a TI está liderando a estratégia de transformação da empresa. No entanto, 93% dos executivos afirmam que a defasagem das qualificações profissionais os impede de fazerem as transformações com a rapidez necessária.³⁴

Quer uma linha de negócios esteja implantando um novo aplicativo de IoT, um novo serviço em nuvem ou uma nova política de conformidade, os profissionais de TI precisam entender o que é exigido da rede e qual será sua função para que possam fornecer os serviços de rede necessários a tempo e com segurança.

Nesta parte do relatório, examinaremos a transformação de três papéis-chave de TI: estrategista de rede, profissional de rede e líder de TI. Também identificaremos os novos conjuntos de habilidades de que esses profissionais precisarão para supervisionar um ambiente de rede corporativa em rápida evolução.

Líder de TI

- Supervisão geral de TI e rede
- Supervisão da estratégia de rede e orçamento

Títulos: CIO, VP de infraestrutura de TI, diretor de TI

Estrategista de rede

- Responsável por definições da estratégia da rede em relação a roteiro, arquitetura e preferências de tecnologia

Títulos: estrategista de rede, arquiteto de rede/TI, gerente de rede

Profissional de rede

- Responsável pela implantação, configuração, manutenção e solução de problemas da rede

Títulos: Engenheiro de rede, administrador de rede, engenheiro de suporte de rede



Como se preparar para a transformação dos conjuntos de habilidades de redes

Não é de surpreender que, à medida que a rede corporativa evolui, o mesmo aconteça com as qualificações profissionais necessárias



Figura 30 Principais defasagens de qualificações profissionais de TI

51% Especialização em nuvem

46% Arquitetura empresarial

43% Big data e análises

42% DevOps

41% Segurança cibernética

41% Internet das Coisas

37% Desenvolvimento de aplicativos

35% Desenvolvimento de aplicativos nativos da nuvem

30% Automação

29% Programação/scripting

27% Design de interface e experiência do usuário

26% RA/RV

9% Inteligência artificial e ML

para a sua construção e gerenciamento.

Em duas pesquisas recentes, líderes de TI e estrategistas de rede revelam as defasagens de qualificações profissionais que estão observando em lugares habituais e não tão habituais.

As maiores defasagens de qualificações profissionais em tecnologia da informação

Os dados da nossa pesquisa de talentos de TI revelam que, de modo geral em toda a equipe de TI, tecnologias avançadas, como experiência em nuvem, arquitetura empresarial, big data e análise, DevOps e segurança cibernética, encabeçam a lista de qualificações profissionais técnicas e conhecimentos necessários.³⁴ Aliás, a necessidade de expertise nos primeiros quatro tópicos de defasagens de qualificações profissionais – nuvem, arquitetura empresarial, análise de dados e DevOps – demonstra uma forte evidência das mudanças nas funções de TI.

Pergunta: Quais são as qualificações profissionais tecnológicas ou especializações mais importantes de que o seu departamento de TI precisa para dar respaldo à transformação empresarial?

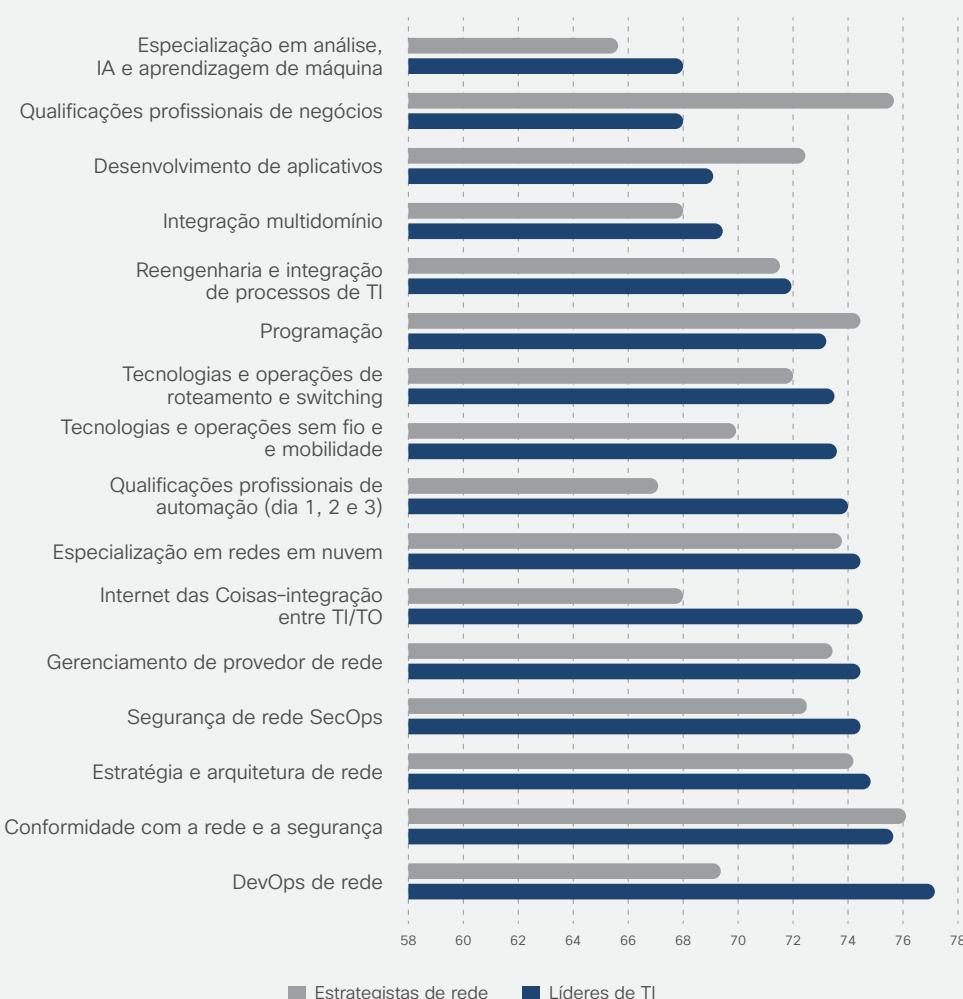
Fonte: *Estratégias de Talentos de TI da Próxima Geração*, Cisco, outubro de 2018; n = 600 executivos de negócios e de TI

As maiores defasagens de qualificações profissionais para redes

Na nossa *Pesquisa global de tendências de rede de 2019*, pedimos aos líderes de TI e estrategistas de rede que avaliassem a capacidade de sua equipe em desenvolver e manter uma rede que atenda às demandas futuras da empresa em que atuam.

Em geral, os líderes e estrategistas expressam um nível razoável de confiança nas capacidades da sua equipe de rede. Os líderes de TI identificaram análise e IA, juntamente com qualificações profissionais empresariais e habilidades de desenvolvimento de aplicativos, como itens que precisam de mais atenção. Embora os estrategistas de rede também reconheçam a análise e a IA como uma defasagem, eles identificaram a integração de TI/TO, a automação e DevOps de rede como as outras áreas-chave que precisam ser aperfeiçoadas.¹⁴

Figura 31 Confiança na capacidade da equipe de rede em diferentes conjuntos de qualificações profissionais



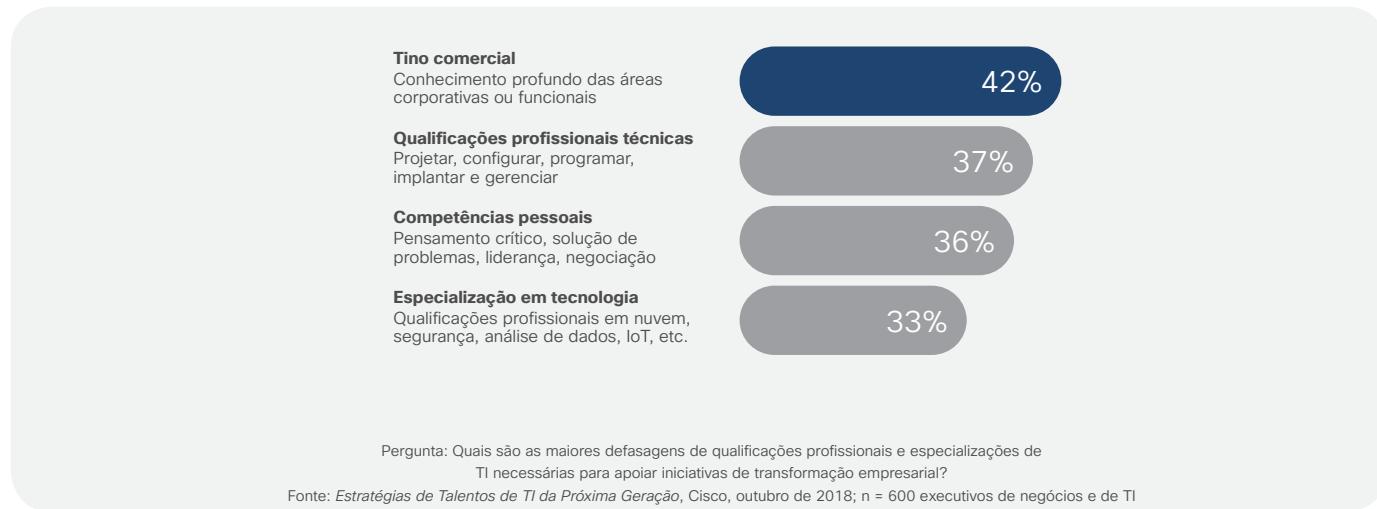
Pergunta: Pensando nas habilidades e qualificações profissionais atuais de sua equipe de rede, como você classificaria o nível de capacidade da equipe para construir e manter uma rede que atenda às demandas futuras da sua empresa em cada uma das seguintes áreas?

Fonte: *Pesquisa global de tendências de rede de 2019*; n = 2061 (505 líderes de TI; 1.556 estrategistas de rede)

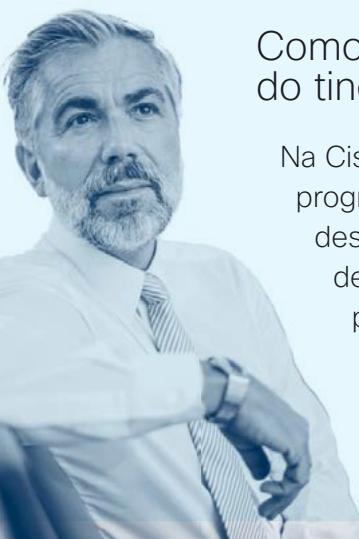
Necessidade crescente de qualificações profissionais empresariais e pessoais

Nossa própria pesquisa de talentos de TI revela que a falta de tino comercial é a principal lacuna de habilidades na área de TI atualmente.³⁴ Preencher essa lacuna será fundamental à medida que as empresas fizerem a transição para redes baseadas em intenções. Ao falar a linguagem empresarial, a TI pode traduzir efetivamente os objetivos ou intenções empresariais em políticas de TI de alto nível, as quais, por sua vez, podem determinar configurações de infraestrutura e dispositivos.

Figura 32 O tino comercial é identificado como a principal lacuna de habilidades na área de TI



Como a Cisco faz: desenvolvimento do tino comercial



Na Cisco, criamos o “Cliente Zero”, um programa que coloca os profissionais de TI no desenvolvimento de produtos, onde eles podem desenvolver tino comercial e qualificações pessoais, como pensamento crítico e resolução de problemas em profundidade. Isso incentiva os funcionários a se adaptarem e se transformarem, de forma a ajudar a nos mantermos competitivos.

Funções transversais mais proeminentes no futuro

Em um futuro próximo, algumas funções de TI evoluirão para posições cruzadas que abrangem mais de uma área. Por exemplo, administradores de

rede que agregarem recursos de análise de dados ou programação ao seu conjunto de qualificações profissionais poderão exercer uma nova função, de uma forma que amplie efetivamente a sua contribuição e aumente o valor de seu trabalho.

Essas funções transversais exigirão combinações singulares e muito procuradas de diferentes áreas técnicas e qualificações profissionais relacionadas

a linguagens. Por exemplo, os profissionais podem programar a rede por meio de APIs e linguagens de programação. Ou as equipes de NetOps e SecOps podem colaborar para criar fluxos de trabalho operacionais otimizados entre ambas.

“Precisamos de engenheiros de redes e infraestrutura que sejam motivados a projetar, construir e operar infraestruturas cruciais para a missão. Precisamos de desenvolvedores de software que sejam motivados a criar aplicativos inovadores que rodem com base na infraestrutura e que automatizem fluxos de trabalho e tarefas.

As empresas mais eficientes terão equipes de especialistas em domínios, tanto em software quanto em infraestrutura, que poderão trabalhar juntas com eficiência.”³⁷

– Susie Wee, SVP e CTO de DevNet da Cisco

Novos papéis para estrategistas de redes

Sem dúvida, o trabalho mais urgente para os estrategistas de redes será construir um roadmap eficaz e de baixo risco para uma arquitetura de rede mais ágil e alinhada aos negócios. Os estrategistas também precisarão otimizar a TI, criando catálogos de rede de autoatendimento, integrando a rede aos processos de TI, integrando fluxos de trabalho de NetOps e SecOps e convergindo TI e tecnologia operacional (TO). As empresas

precisarão de ajuda para projetar inovações comerciais habilitadas para rede, como personalização baseada em localização, otimização da utilização do local de trabalho ou aplicativos remotos especializados.



Estrategista do futuro: Proporcionando valor além da rede

Joe Clarke, engenheiro da Cisco, acredita que o cargo de estrategista de rede abrangerá cada vez mais funções que estão atualmente fora do radar da maioria dos estrategistas. Os estrategistas de redes provavelmente evoluirão ao longo de um ou mais dos seguintes caminhos:

O **tradutor de negócios** concentrado em alinhar o desempenho da equipe de TI com a intenção de negócios:

O tradutor trabalhará para melhor transformar as necessidades empresariais em requisitos de nível de serviços que podem ser aplicados e monitorados em toda a rede. O tradutor também trabalhará para melhor utilizar a rede e os dados da rede para o valor comercial e a inovação.

Qualificações de negócios: averiguar os requisitos de negócios e traduzi-los em requisitos de rede.

Qualificações de

DevOps: entender como as APIs de plataforma de rede e as tecnologias de processamento de linguagem natural (NLP) podem aproximar a intenção de negócios e a TI.

O arquiteto de integração da rede concentrado na integração de domínios de rede e TI:

Os integradores trabalharão para integrar a rede no processo de TI e com sistemas externos. O integrador também será responsável pela integração entre domínios de rede para assegurar que a intenção esteja presente em todos os domínios relevantes.

Reengenharia e integração de processos

de TI: entender os processos e fluxos de trabalho de TI para mudar e integrar as operações de rede para aumentar a eficiência.

Operações de serviço de ITSM: entender os processos da biblioteca de infraestrutura de tecnologia da informação (ITIL) para vincular efetivamente os sistemas de garantia de rede aos recursos de ITSM.

Qualificações de DevOps: compreender as APIs oferecidas por uma plataforma de rede aberta e como elas podem disponibilizar fluxos de trabalho integrados com outros sistemas de TI.

O guardião da rede concentrado em conectar arquiteturas de rede e segurança:

Os guardiões incorporarão a inteligência distribuída da rede na arquitetura de segurança e nos processos de SecOps. O guardião da rede



Como a Cisco faz: caminhos de aprendizagem continuada em TI

Na Cisco, desenvolvemos vários caminhos de aprendizagem de TI relacionados a temas como sistema empresarial, segurança, data center, provedor de serviços, colaboração, DevNet e outros tópicos avançados, proporcionando aos engenheiros a oportunidade de desenvolver qualificações profissionais de ponta. Também oferecemos educação continuada em todos os níveis de associados, especialistas, profissionais e especializados, bem como treinamento gratuito ou com desconto e certificações para funcionários.

terá um papel fundamental na convergência de redes e segurança.

Qualificações de segurança: definir arquiteturas de segurança de rede, implantar tecnologias de segurança de rede e compreender o papel que a rede tem na contribuição para a segurança geral.

Qualificações de DevOps: entender como as APIs de plataforma de rede podem viabilizar a integração com sistemas SecOps.

O arquiteto de dados de rede concentrado na análise de rede e IA:

O arquiteto de dados de rede trabalhará para aproveitar melhor as grandes quantidades de dados que atravessam a rede e as ferramentas emergentes habilitadas para IA a fim de melhorar os serviços de TI e informar a empresa.

Qualificações de análise e IA: coletar dados para tomar decisões melhores e com mais rapidez. Compreender as tecnologias de IA e como elas podem ser aplicadas para

garantia de rede e integradas com outros sistemas de TI em prol de uma garantia geral de serviços.

Qualificações de visão empresarial:

entender os negócios e como eles podem usar dados acessíveis pela rede para embasar decisões e criar novas oportunidades.

Novos papéis para profissionais de redes

À medida que a transformação digital se torna central para a estratégia de uma empresa, os profissionais de redes precisarão se concentrar menos em tarefas de gerenciamento repetitivas e mais em serviços agregados que deem respaldo às metas comerciais. Isso se tornará mais fácil à medida que os níveis crescentes de automação em redes avançadas começarem a eliminar as tarefas mais demoradas dos engenheiros de TI.



Engenheiros de redes do futuro: proporcionando valor além da conectividade

À medida que as redes baseadas em intenções se tornam mais prevalentes, os papéis dos profissionais de redes evoluirão para apoiar um ou mais pilares das operações de rede: ciclo de

“Hoje, um engenheiro de redes bem-sucedido é aquele que é bom em integrar as novas tecnologias com as tradicionais, e que preenche a lacuna entre redes e desenvolvimento de software. Essa nova abordagem exige uma mentalidade voltada para DevOps e uma melhor compreensão de como a tecnologia está ligada aos objetivos de negócios.”

– Joe Clarke, engenheiro eminentíssimo, Cisco

vida, processo ou garantia. Nesse cenário, os profissionais de redes terão de desenvolver qualificações profissionais a fim de desempenhar um ou mais destes papéis potenciais:

O **comandante da rede** concentrado no gerenciamento do ciclo de vida da rede:

O comandante será responsável pelos processos e pelas práticas que asseguram a integridade geral e o funcionamento contínuo do controlador de rede e da rede subjacente.

Qualificações necessárias: operar, manter e ajustar um controlador que proporcione automação e orquestração em ambientes de rede baseados em intenção. Garantir a sustentabilidade das integrações de plataformas com outros



Tarefas repetitivas de gerenciamento podem ocupar 55% do tempo e dos recursos dos profissionais de rede atualmente.¹⁴

sistemas. Compreender o ciclo de vida destes controladores e assegurar a saúde, segurança, conformidade e estabilidade contínuas dos controladores e da rede subjacente.

O **orquestrador da rede** concentrado na tradução e automação de políticas:

Os orquestradores precisam entender como as necessidades de negócios se traduzem em políticas de rede e, em seguida, gerenciar a automação dessas políticas. Os orquestradores também serão responsáveis pelo alinhamento das políticas com outros domínios de redes e TI.

Qualificações necessárias: dominar como empregar ferramentas de automação de infraestrutura, protocolos de automação e modelos de dados. Obter proficiência em Linux, Python e ferramentas de desenvolvimento de programação de rede. Compreender formatos de dados comuns. Familiarizar-se com metodologias ágeis de desenvolvimento de software e sentir-se confortável usando APIs e kits de ferramentas para interagir com controladores e dispositivos de rede.

O **detetive da rede** concentrado na garantia da rede e dos serviços:

Os detetives serão adeptos do uso e da otimização de ferramentas de garantia de rede que usam análise avançada e inteligência artificial para garantir que a rede cumpra a intenção de

negócios prometida. Os detetives precisarão se integrar aos processos de gerenciamento de serviços de TI e também trabalharão em estreita colaboração com a equipe de SecOps para assegurar que anomalias de rede sejam sinalizadas e que possíveis falhas de segurança sejam resolvidas.

Qualificações necessárias: identificar e priorizar tendências com base em insights de IA para que a empresa possa agir proativamente. Sintonizar e fornecer feedback aos sistemas de análise para que a detecção e correção de anomalias seja continuamente aprimorada. Integrar os processos de detecção e resolução de problemas de rede aos processos de TI e segurança.



Líderes de TI: medidas para resolver a escassez de talentos de redes

A construção de qualificações profissionais técnicas é hoje fundamental para proporcionar uma transformação digital bem-sucedida no futuro. Na nossa *Pesquisa global de tendências de rede de 2019*, convidamos os líderes de TI a compartilhar o que estão fazendo atualmente para desenvolver seus talentos. A requalificação, a expansão e o reequilíbrio são as principais abordagens aqui apresentadas.



Figura 33 Abordagens preferenciais para solucionar defasagens de qualificações em rede



Pergunta: Qual é a principal abordagem que a liderança de TI da sua empresa deve priorizar para abordar as atuais defasagens de talentos necessários para planejar, implantar e manter as suas futuras necessidades de rede?

Fonte: Pesquisa global de tendências de rede de 2019; n = 505 líderes de TI

Embora os líderes tenham preocupações com requalificação, esta continua sendo a abordagem prioritária tanto para as qualificações profissionais de empresas de TI quanto para as qualificações profissionais técnicas de TI.

Figura 34 Maiores preocupações com requalificação



Pergunta: Ao considerar planos para requalificar a equipe de rede da sua empresa para oferecer melhor estrutura e suporte a uma rede mais avançada, qual é a sua maior preocupação?

Fonte: Pesquisa global de tendências de rede de 2019; n = 505 líderes de TI

Recomendações para líderes de TI: como montar a equipe de rede do futuro

De acordo com Guillermo Diaz, SVP de transformação de clientes na Cisco, estas cinco estratégias podem ajudar os líderes a montar uma equipe de rede preparada para desenvolver um negócio digitalmente transformado.

1 Promover uma cultura de aprendizagem contínua

contínua: é absolutamente essencial que os líderes de TI promovam uma cultura de aprendizagem contínua. Isso ajudará os estrategistas e profissionais de redes a dominar regularmente as qualificações profissionais necessárias para se adaptarem às novas tecnologias e processos operacionais. Isso pode ser feito combinando oportunidades de desenvolvimento internas e externas que proporcionem uma variedade de conhecimento, experiência e exposição às suas equipes.

2 Encontrar o equilíbrio entre requalificação e contratação

e contratação: nossa pesquisa mostra que os líderes estão confiando cada vez mais na requalificação para preencher lacunas de qualificações profissionais. No entanto, quando se trata de novas tecnologias, o oposto parece ser o caso. Muitas empresas estão buscando novos talentos para preencher vagas de trabalho emergentes em tecnologia, especialmente em inteligência artificial e aprendizagem de máquina. Encontrar o equilíbrio certo entre desenvolvimento e contratação dependerá das metas operacionais e comerciais e da sua posição na transformação de sua rede.

3 Investir mais em treinamento

e desenvolvimento: em uma pesquisa recente com líderes de TI, descobrimos que as empresas mais bem-sucedidas em transformação digital investem cerca de 10% a mais no treinamento

“Investir em requalificação é menos dispendioso do que recorrer ao mercado externo para contratar um novo especialista, certamente em termos de salário e honorários de recrutamento, mas também em termos de custo de integração, transferência de conhecimento tácito organizacional e familiaridade com o processo. O seu pessoal atual pode não ter certas qualificações profissionais e habilidades novas, mas provavelmente tem muito do que você precisa para estar em uma posição de vantagem.”³⁸

– Colin Seward; CIO da Cisco, Europa, Oriente Médio, África e Rússia

e desenvolvimento da sua equipe de TI.³⁴ Quando a equipe de TI é capaz de acompanhar o ritmo da mudança tecnológica, também consegue tomar decisões melhores, mais rápidas e mais inteligentes orientadas por dados para dar respaldo aos objetivos de negócios.

Satisfazendo novas necessidades: pacote de certificação expandido da Cisco

Para satisfazer esses novos requisitos de treinamento, grades curriculares e certificações de rede (como as oferecidas pela Cisco) estão sendo rapidamente atualizadas.³⁷

Nível de associado Nível de especialista Nível de profissional Nível de expert

Engenharia



Software



Futuro
Produto

4 Faça um rodízio de talentos para aumentar o tino comercial

o tino comercial: fazer um rodízio de curto prazo com equipes de TI e de negócios amplia o conhecimento, desenvolve um contexto mais amplo e permite interações mais produtivas posteriormente. Mais especificamente, a capacidade de disponibilizar redes, aplicativos e rodízios nas empresas proporciona uma combinação de habilidades de tecnologia, programabilidade e tino comercial.

5 Promova um ambiente de trabalho inclusivo

inclusivo: as recomendações anteriores são concentradas no talento. Criar um local de trabalho que seja altamente inclusivo significa aproveitar ao máximo os talentos que a sua empresa tem à disposição. As empresas que priorizam a diversidade e a inclusão na forma como recrutam, gerenciam, desenvolvem e recompensam seus funcionários demonstram melhor desempenho frente às concorrentes que não priorizam esses valores. Essa atitude começa pela liderança executiva com compromisso com políticas, programas e padrões de comportamento, bem como treinamentos que criam as condições para um ambiente inclusivo na empresa.

A empresa de TI da próxima geração tem de servir como exemplo de uma cultura diversificada e inclusiva na forma como atua todos os dias.

Como a Cisco faz: atrair novos talentos

Não se encontram bons talentos por acaso. É por isso que usamos programas como a nossa IT University, a Cisco Networking Academy e o Cisco International Internship Program para descobrir e contratar novos talentos, bem como o Cisco Veterans Program, que nos ajuda a capacitar e empregar veteranos interessados em carreiras tecnológicas.

Sobre este relatório

O *Relatório global de tendências de rede de 2020* oferece aos profissionais, estrategistas e líderes de TI insights sobre as tendências atuais e futuras da rede em toda a empresa e oferece orientação essencial sobre tecnologia, operações e talentos de rede. O relatório tem como base pesquisas originais da Cisco e inclui novos dados da *Pesquisa global de tendências de rede de 2019* com 2.061 líderes e estrategistas de TI de 13 países. Além disso, líderes, membros e engenheiros de renome da Cisco fornecem análises e recomendações especializadas para empresas que estão fazendo a transição a tecnologias de rede avançadas.



Este relatório é dedicado a Cliff Apsey, cuja dedicação em oferecer as melhores experiências digitais para os clientes nos inspirou a fazer com que este relatório seja uma experiência melhor para você. Agradecemos o tempo que estivemos com o Cliff. Nunca nos esqueceremos dele.

© 2019 Cisco e/ou suas afiliadas. Todos os direitos reservados. Cisco, o logotipo da Cisco e Webex são marcas comerciais ou marcas comerciais registradas da Cisco e/ou de suas afiliadas nos EUA e em outros países. Para ver uma lista das marcas comerciais da Cisco, consulte a página “Marcas comerciais” no site da Cisco. As marcas comerciais de terceiros citadas pertencem aos seus respectivos proprietários. O uso da palavra “parceiro” não implica uma relação de parceria entre a Cisco e qualquer outra empresa. (1909R)

Fontes

1. *IDC FutureScape: Worldwide Enterprise Infrastructure 2018 Predictions*, IDC, 2017.
2. *Uptime Institute Annual Data Center Survey*, 2019.
3. *Previsão de VNI completa da Cisco de 2018*, Cisco, 2018.
4. *Relatório anual de segurança cibernética da Cisco de 2018*, Cisco, 2018.
5. “J.C.R. Licklider,” Internet Hall of Fame, 2013.
6. “History of Online Education,” The Quad, 2019.
7. *Previsão global de dispositivos e dados de IoT DataSphere da IDC, 2019–2023*, IDC, maio de 2019.
8. Dennis Smith, Dale Kutnick, Lisa Pierce, *Invest in Networks to Achieve Digital Business Success*, Gartner, May 2019
9. “A Brief History of Globalization,” Fórum Econômico Mundial, janeiro de 2019.
10. *Digital Vortex 2019: Continuous and Connected Change*, IMD, 2019.
11. *Reshaping the Future* (pesquisa de caso de uso de automação), Capgemini Research Institute, 2018.
12. “Ferramenta de destaque de previsão de VNI,” Cisco, 2017.
13. *Índice visual de redes da Cisco: previsão e tendências, 2017–2022 (white paper)*, Cisco, fevereiro de 2019.
14. *Pesquisa global de tendências de rede de 2019*, Cisco, 2019.
15. Jonathan Forest, Neil Rickard, *2019 Roadmap estratégico para redes*, Gartner, 10 de abril de 2019
16. *Distinção entre modelos de intenção, política e serviços*, IETF, 3 de maio de 2018.
17. “Por que as redes baseadas em intenção são uma boa notícia para redes definidas por software?” Cisco, 1 de junho de 2018.
18. *Redes baseadas em intenção: a ponte entre os negócios e a TI*, Cisco, janeiro de 2018.
19. *Rede baseada em intenção: evolução da rede em campus corporativo*, IDC, junho de 2018.
20. “Empresas não podem ter problemas de comprometimento de automação e terem sucesso,” IT Connection, 21 de julho de 2017.
21. “A ascensão dos AIOps: como dados, aprendizado de máquina e IA transformarão o monitoramento de desempenho,” AppDynamics, 17 de dezembro de 2018.
22. “Garantia de rede com raciocínio de máquina e aprendizado de máquina,” Cisco, 25 de julho de 2019.
23. *Cisco Global Cloud Index: previsão e metodologia, 2016–2021 (white paper)*, Cisco, 19 de novembro de 2018.
24. “Previsões para 2019: para infraestrutura,” Cisco, 11 de fevereiro de 2019.
25. *Agora o ambiente multicloud é o padrão*, IDC, março de 2018.
26. *SD-WAN: segurança, experiência em aplicativos e simplicidade operacional promovem o crescimento do mercado*, IDC, abril de 2019.
27. “Conectando o desconectado: 5G e Wi-Fi 6 desempenharão um papel fundamental na redução da divisão digital,” Cisco, 19 de março de 2019.
28. “OpenRoaming: roaming automático e contínuo nas redes Wi-Fi 6 e 5G” Cisco, 29 de abril de 2019.
29. *O ecossistema Zero Trust eXtended: redes*, Forrester, 2 de janeiro de 2019.
30. *Antecipando o desconhecido: estudo de referência com o diretor de segurança da informação*, Cisco, março de 2019.

31. Sanjit Ganguli, Lawrence Orans, alinhamento dos objetivos das ferramentas NetOps e SecOps com casos de uso compartilhado, Gartner, 24 de julho de 2018
32. Atores cibernéticos patrocinados pelo Estado russo visando a dispositivos de infraestrutura de rede, CISA, 16 de abril de 2018.
33. “Série de relatórios de segurança cibernética da Cisco,” Cisco, 2019.
34. *Estratégias com talentos de TI da próxima geração, Cisco, outubro de 2018.*
35. *Transforming IT Operations, Cisco Connected Futures, 2018.*
36. *Operações de rede da próxima geração, Cisco, setembro de 2019.*
37. “Trazendo práticas e habilidades de software para as redes com certificações da Cisco e para DevNet,” Cisco, 10 de junho de 2019.
38. *Evolving the IT Team, Cisco, 2019.*