netskope

A transformação digital exige uma excelente integração

O business case para uma maior colaboração entre a equipe de redes e segurança na era SASE

Não é nenhum segredo que na maioria das empresas existe um conflito entre as equipes de rede e segurança; em alguns casos, são apenas diferentes prioridades, mas em outras, elas estão em pé de guerra. Em uma era de silos, onde cada equipe tinha uma estratégia, um orçamento, um conjunto de recursos e de prioridades, esse conflito era visto como uma consequência normal do trabalho. Mas estamos na era da arquitetura Secure Access Service Edge (SASE), onde as equipes de redes e segurança e os produtos e serviços que elas gerenciam convergem em um conjunto compartilhado de prioridades, vinculadas aos objetivos corporativos. Nesse cenário, as equipes de redes e segurança precisam não apenas se alinhar, mas colaborar para garantir que a força de trabalho, cada vez mais remota, possa acessar dados com segurança de qualquer lugar usando aplicações na nuvem e ter uma boa experiência, sem perda de conectividade da rede.

Falar é fácil, executar são outros quinhentos. Mas a colaboração entre as equipes de redes e segurança não é só um momento "paz e amor". Na verdade, a falta de colaboração custa tempo e dinheiro e, de um ponto de vista executivo, limita a habilidade das empresas de entregar projetos bem-sucedidos de transformação digital que estimularão o crescimento dos negócios e manterão as empresas mais competitivas.

Uma nova pesquisa da Censuswide, encomendada pela Netskope, destaca as tensões muito reais entre as equipes de redes e segurança e mostra como CIOs e líderes de redes e segurança encaram o cenário atual dessa integração — ou, melhor dizendo, da falta dela.

Este documento destaca as principais descobertas e indica um caminho para equipes que busquem melhorar a colaboração para aproveitar os benefícios de uma arquitetura SASE cloud-first e segura.

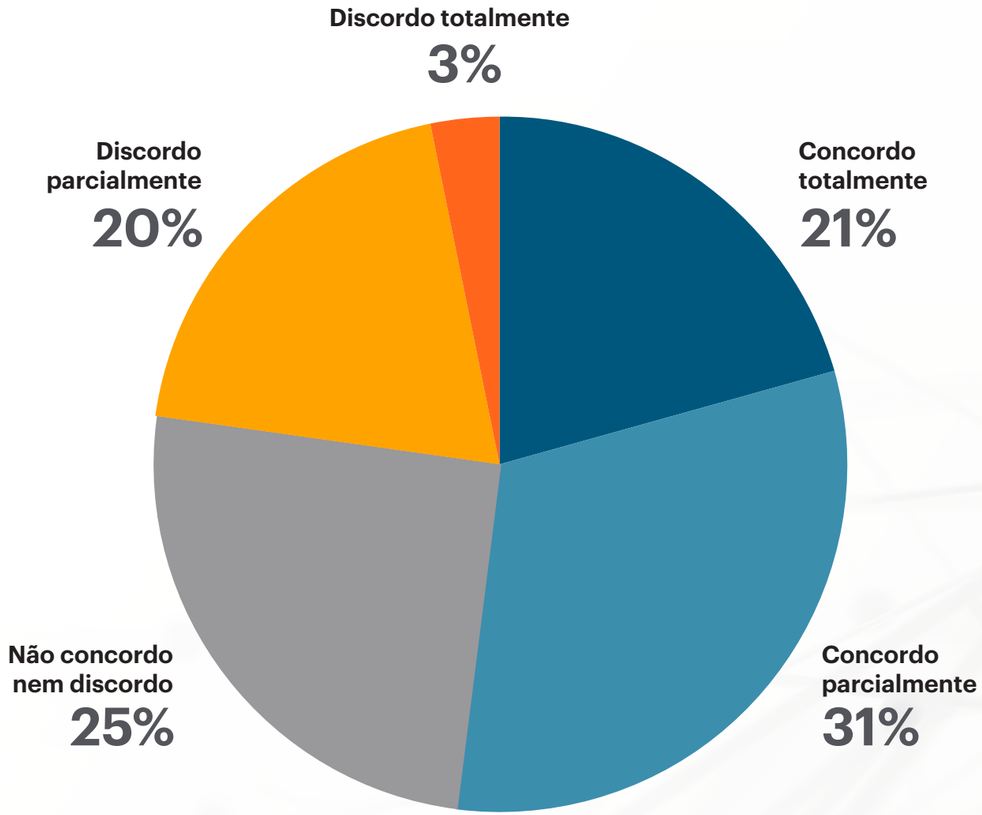
50% dos CIOs acreditam que a falta de colaboração entre equipes especializadas impede que suas empresas materializem os benefícios da transformação digital.

As empresas gastarão cerca de US$ 6,8 trilhões em projetos de transformação digital (Dx) até 2023* — um valor que deve aumentar nos três anos subsequentes. Os benefícios da transformação digital, mesmo que definidos de forma vaga, garantem que as empresas permanecerão ágeis, competitivas e cloud-first, transformando os centros de custos funcionais de TI e segurança em verdadeiros facilitadores de negócios. Na pesquisa da Censuswide, 87% dos entrevistados afirmaram que estão trabalhando em um projeto de Dx ou que terminaram um recentemente.

No entanto, o abismo entre profissionais de redes e segurança aponta desafios que inibem o sucesso tempestivo de projetos de Dx. Isso não é novidade para os CIOs, que geralmente são responsáveis por definir as prioridades de Dx com a aprovação da diretoria executiva.

*IDC FutureScape: Worldwide Digital Transformation 2021 Predictions

A FALTA DE COLABORAÇÃO ENTRE EQUIPES ESPECIALISTAS NOS IMPEDE DE APROVEITAR OS BENEFÍCIOS DA TRANSFORMAÇÃO DIGITAL



Ponto-chave

Projetos isolados de Dx podem evoluir mesmo na ausência da importante colaboração entre equipes de rede e segurança. Mas isso não é verdade para mudanças significativas na arquitetura, onde a colaboração é requisito implícito para o sucesso – um exemplo é a mudança rumo a uma arquitetura SASE, para preparar as empresas para uma adoção segura da nuvem.

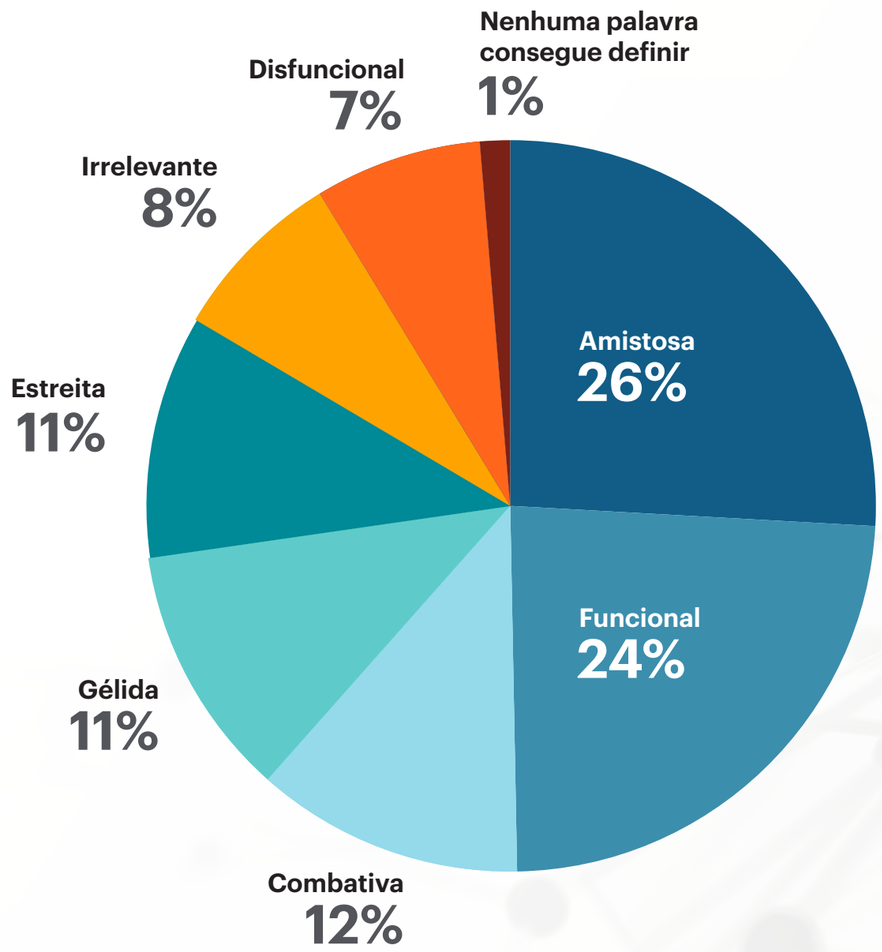
Quase metade dos profissionais de rede e segurança descrevem a relação entre as duas equipes em termos muito negativos, como “combativa”, “não funcional”, “gélida” ou “irrelevante”.

Sabia que 45% dos profissionais de rede e segurança nunca conheceram um membro da outra equipe? Isso pode parecer mentira, já que quase metade (49%) está sob o mesmo grupo e se reporta aos mesmos líderes, mas esses mesmos entrevistados afirmam claramente que “as equipes de segurança e rede não costumam trabalhar juntas”.

O problema pode ser uma questão de liderança e priorização. Os profissionais de rede e de segurança entrevistados pela Censuswide selecionaram as mesmas três principais prioridades para 2021:

- Ajudar no aumento da produtividade da empresa como um todo
- Expandir a infraestrutura para apoiar o crescimento da empresa
- Aumentar a visibilidade e o controle

QUAL PALAVRA, SE HOUVER UMA, MELHOR DEFINE PARA VOCÊ A RELAÇÃO ENTRE AS SUAS EQUIPES DE SEGURANÇA E REDE:



Ponto-chave

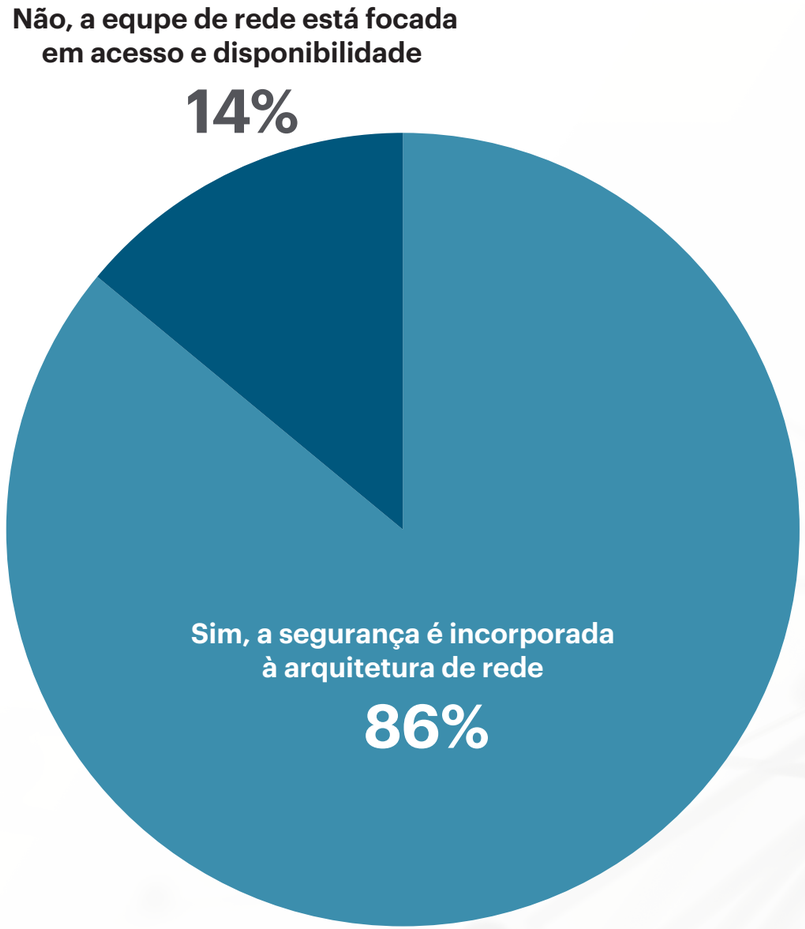
As equipes de redes e segurança costumam trabalhar em separado e o relacionamento entre elas costuma ser improdutivo, mesmo estando sob a mesma estrutura na empresa, trabalhando para os mesmos diretores e identificando as mesmas prioridades corporativas, o que destaca o valor que essas equipes podem trazer.

86% dos profissionais de redes e segurança entrevistados afirmaram que a segurança é responsabilidade da equipe de redes.

A segurança e as redes costumavam ser parte de um órgão unificado dentro das empresas. Apesar das aparências, elas continuam inextricavelmente unidas, mesmo que cada função tenha crescido e aumentado individualmente. Considere que o papel da segurança é de identificar problemas (geralmente na infraestrutura da rede) e de organizar a solução. Por outro lado, parte do papel da equipe de redes é manter o tempo de atividade e a conectividade, usando ferramentas e técnicas que a equipe de segurança ajudou a escolher (ou no mínimo foi consultada).

A pesquisa mostra que as equipes não são ideologicamente contrárias à ideia de colaboração. A maioria dos grupos de segurança e redes afirmaram que a equipe de redes é parcialmente responsável pela segurança, que deve ser inserida na arquitetura da rede. Mais da metade dos entrevistados informou que projetos de Dx costumam ter padrinhos tanto nas equipes de segurança quanto de redes.

A SEGURANÇA FAZ PARTE DA RESPONSABILIDADE DA EQUIPE DE REDE?



Ponto-chave

As bases para uma colaboração mais profunda já existem. Cabe às equipes de liderança propiciar uma ativação eficaz.

Até 2025, **60% das empresas** terão implementado uma estratégia SASE*

Quer se chame SASE, o termo criado pelo Gartner em 2019, quer tenha outro nome, a evolução que a nuvem traz para TI e segurança caminha a passos rápidos. Como o termo "nuvem" há 10 anos ou os princípios Zero Trust há 5 anos, o termo SASE está cercado de ruídos e muito marketing, mas poucos conselhos práticos como um passo-a-passo do tipo "é assim que se faz".

Mas, como as pessoas, processos e tecnologia estão evoluindo para um futuro SASE, qualquer definição de sucesso depende de uma convergência entre redes e segurança.

Ponto-chave

O caminho certo rumo à SASE tem sido fervorosamente debatido desde que o termo foi criado pelo Gartner e deve continuar assim no futuro próximo. Mas todos concordam que a convergência entre redes e segurança é fundamental para uma arquitetura SASE bem-sucedida – e que a arquitetura SASE é o futuro.

*Gartner, "2021 Strategic Roadmap for SASE Convergence," publicado em 25 de março de 2021

O que você pode fazer agora

Mudar a gestão não é fácil em tempos "normais" e ficou ainda mais difícil devido a importantes tendências tecnológicas (adoção da nuvem, arquitetura SASE) e crises únicas com efeitos corporativos e interpessoais significativos, como a pandemia da COVID-19. A seguir, listamos sugestões de processos vindas de CIOs de empresas Fortune 500 que estão conseguindo resolver o problema da colaboração entre redes e segurança, conduzindo eficazmente projetos de Dx e criando um caminho com suas equipes para um futuro com SASE.

Implemente os ensinamentos do DevOps
DevOps (e suas variantes, incluindo DevSecOps) virou um movimento, porque ele entende os conflitos e desalinhamentos inerentes entre as equipes de desenvolvimento e operações em grandes empresas com vários níveis. Boa parte das premissas e táticas inspiradas pelo DevOps, da criação de equipes de projeto multifuncionais ao uso de quadros kanban e processos ágeis, podem ser facilmente transportadas para uma colaboração entre equipes de redes e segurança ou para qualquer outro ponto na empresa que possa se beneficiar de uma maior colaboração entre equipes e funções.

Avalie a possibilidade de um SNOC
A ideia de combinar SOC e NOC, conhecida em alguns círculos como centro de operações de segurança e rede (SNOC), tem sido cada vez mais adotada, à medida que as equipes percebem que o objetivo corporativo prioritário de uma infraestrutura de rede corporativa segura, robusta e resiliente é compartilhado entre todos. Um SNOC une funções essenciais em um só lugar e se baseia cada vez mais em tecnologias de próxima geração, como AI/ML, para aprofundar a análise humana e garantir que nada passe despercebido.

Foque em uma lista (curta) de métricas essenciais aos negócios que transcendam as fronteiras entre redes e segurança
Qual a melhor maneira de comunicar aos diretores executivos, especialmente com os diretores não técnicos, que as equipes de redes e segurança estão trabalhando em harmonia para a manutenção da infraestrutura e para ajudar a empresa a alcançar seus objetivos? Nesse tipo de relatório, não há espaço para destaques pontuais, muito menos para histórias do tipo "paz e amor"!

As métricas exatas dependerão da natureza dos negócios e da maturidade das equipes, mas os CIOs recomendam que as seguintes métricas sejam consideradas:

- Melhor tempo médio de resposta (MTTR)
- Melhor tempo médio até a falha (MTTF) ou melhor tempo médio entre falhas (MTBF)
- Melhor satisfação de clientes (externos ou internos - medição realizada por pesquisa robusta)

Para mais informações

Visite netskope.com

“O progresso da Netskope no framework de SASE é o mais avançado entre os fornecedores no Quadrante Mágico.”
– Gartner, Quadrante Mágico para Cloud Access Security Brokers, novembro de 2020

Netskope, a líder em SASE, conecta com rapidez e segurança usuários diretamente à internet, qualquer aplicação, e suas infraestruturas de qualquer dispositivo, dentro ou fora da rede. Com CASB, proxy, e ZTNA incorporados nativamente em uma única plataforma, a Netskope é rapida em todos os lugares, centrada nos dados, e pensada estratégicamente para a nuvem, tudo isso enquanto mantém boa cidadania digital e custos mais baixos de propriedade.

netskope.com

©2021 Netskope, Inc. Todos os direitos reservados. Netskope é uma marca registrada e Netskope Active, Netskope Discovery, Cloud Confidence Index, Netskope Cloud XD e SkopeSights são marcas registradas da Netskope, Inc. Todas as outras marcas registradas são propriedade de seus respectivos donos. 04/21 EB-451-1