vmware®

Relatório global de informações sobre segurança

Empresas cada vez mais sob ameaça

2021

Introdução

Esta pesquisa foi realizada para compreender os desafios e os problemas enfrentados pelas empresas em todo o mundo no que diz respeito ao aumento dos ataques cibernéticos. Ela identifica as tendências de ataques maliciosos e de hackers, bem como o impacto das violações nas finanças e na reputação de uma empresa em um ano sem precedentes. Ela analisa, ainda, os planos das organizações para proteger novas tecnologias, adotar uma estratégia de segurança que dá prioridade à nuvem e lidar com a complexidade do atual ambiente de gerenciamento de segurança cibernética.

3.542 CIOs, CTOs e CISOs de empresas de diversos setores foram entrevistados para a geração deste relatório. Isso compõe parte de um projeto global de pesquisa em 14 países.

Leia este relatório para descobrir como os profissionais seniores de segurança cibernética planejam se adaptar aos desafios de segurança do local de trabalho distribuído e desenvolver medidas de defesa para tornar a segurança intrínseca à infraestrutura e às operações.w

Resumo do gerenciamento:

Prefácio

INFORMAÇÕES DO CENÁRIO GLOBAL DE SEGURANÇA CIBERNÉTICA

Rick McElroy, estrategista chefe de segurança cibernética, unidade de negócios de soluções de segurança da VMware

Tudo está diferente, porém, igual.

Os profissionais de segurança cibernética que contribuíram para a quarta edição do nosso Relatório global de informações sobre segurança estão em uma posição muito diferente em relação ao momento em que foram entrevistados em 2020. Após um ano da maior e mais rápida transformação nos padrões de trabalho da história, as equipes de segurança agora gerenciam o ecossistema mais distribuído e heterogêneo de todos os tempos.

Os programas de transformação digital avançaram rapidamente à medida que a superfície de ataque cibernético se expandia para incluir salas de estar, cozinhas, redes domésticas e dispositivos pessoais. A força de trabalho remota tem um comportamento muito diferente da força de trabalho do escritório, pois acessa a rede em horários imprevisíveis enquanto equilibra as demandas do trabalho e da família. Consequentemente, o tráfego da rede mudou drasticamente. Os defensores precisam adaptar os sistemas de monitoramento e os pontos de gatilho; caso contrário, correrão o risco de abrir brechas para que as fontes de ameaças usem padrões atípicos e mascarem tentativas de infiltração.

Nesse cenário de rápidas mudanças, alguns aspectos permanecem inalterados: Um dos setores que não foi interrompido pela COVID-19 é o crime cibernético.

A frequência dos ataques é alta, a sofisticação continua evoluindo e as violações são uma consequência inevitável.

Três quartos (76%) dos 3.542 entrevistados em nossa pesquisa disseram que o número de ataques que enfrentaram aumentou no ano passado. 78% desses três quartos afirmaram que os ataques aumentaram porque há mais funcionários trabalhando em casa. 79% alegaram que os ataques se tornaram mais sofisticados.

O resultado? O número de violações aumentou: os entrevistados que sofreram ataques cibernéticos relataram que **ocorreram, em média, 2,35 violações por ano**. E não foram incidentes sem importância. Em oito de cada 10 casos, a violação foi um incidente relevante que precisou ser informado aos reguladores ou encaminhado a uma equipe de resposta a incidentes (RI, pela sigla em inglês).

Claramente, as equipes de segurança estão sob pressão e há pouca complacência: 56% dos CISOs entrevistados temem que sua organização enfrente uma violação relevante no próximo ano.

Os CISOs não têm visão além do alcance

Os volumes de ataques cibernéticos aumentaram, mas a rápida transição para o trabalho remoto significa que as empresas ainda não estão tendo visão do panorama completo. O comportamento irregular dos funcionários, os dispositivos pessoais e o uso da rede doméstica reduzem a visibilidade, criando pontos cegos e cantos escuros nos quais os ataques passam despercebidos. Consequentemente:

78%

afirmaram que os ataques aumentaram porque há mais pessoas trabalhando em casa

2,35

violações foram relatadas por organização, em média

82%

relataram que sofreram uma violação relevante

Apps de terceiros e ransomware são as principais causas de violação

Quando questionados sobre o que está gerando as violações, três vetores quase empataram no topo da lista como causa do desenvolvimento de um cenário de ameaças externas e pontos fracos internos. Os aplicativos de terceiros foram as causas mais comuns, seguidos pelo ransomware e pela tecnologia de segurança desatualizada.

A rápida transição para o trabalho remoto expôs as organizações que deixaram lacunas na higiene da segurança e não conseguiram implementar a autenticação multifator. Além disso, os pontos fracos do processo e as vulnerabilidades do sistema operacional também foram causas comuns de violação.

Além dessas ameaças, a rápida intensificação do ransomware tornou o cenário ainda mais tenso. Campanhas realizadas em vários estágios envolvendo penetração, persistência, roubo de dados e extorsão estão aumentando a pressão à medida que os invasores aproveitam a disrupção enfrentada pelos trabalhadores remotos. Na maioria dos ataques de ransomware, o e-mail continua sendo usado como o vetor de ataque mais comum para obter acesso inicial.

Ressurgimento do ransomware

O ransomware retorna como uma das principais causas de violação à medida que os invasores lançam campanhas sofisticadas e lucrativas em vários estágios.

14% de todas as violações em todo o mundo foram causadas por ransomware.

O setor de saúde está refém

19% das violações do setor de saúde em todo o mundo foram ocasionadas por ransomware.

Apreensão em relação ao desenvolvimento e consumo de apps

Os apps de terceiros são as principais causas de violações, segundo os CISOs entrevistados. É natural que as equipes de segurança estejam se concentrando em aprimorar o enfoque de desenvolvimento e consumo de apps.

Quase dois terços dos entrevistados concordam[1] que precisam ter maior visibilidade dos dados e apps para evitar ataques. Um número semelhante concorda que é necessário ter maior segurança contextual para rastrear a segurança dos dados durante o ciclo de vida do aplicativo. O impacto da COVID-19 é considerável porque três em cada cinco entrevistados concordam que precisam abordar a segurança de forma diferente atualmente porque a superfície de ataque aumentou.

Os apps também estão no topo da lista como o ponto mais vulnerável na jornada de dados, mas eles não são a única área de preocupação.

As cargas de trabalho estão aumentando significativamente como uma fonte de vulnerabilidade reconhecida.

15% dos entrevistados disseram que as cargas de trabalho eram o ponto de violação mais vulnerável na jornada de dados em sua organização, mas vale a pena ressaltar que o cenário não era esse há 12 meses.

[1] O verbo "concordam" é a combinação de "concordo plenamente" e "concordo de certa forma"

Outros 4% afirmaram que esse é o ponto mais vulnerável há mais de 12 meses. As equipes admitem que os antivírus tradicionais não conseguem proteger as cargas de trabalho dos servidores e as configurações incorretas são um risco significativo de violação. Isso geralmente acontece devido à lacuna de conhecimento entre as equipes de segurança e de infraestrutura, em que as equipes de segurança não sabem como as cargas de trabalho de produção devem se comportar e as de infraestrutura não têm experiência no reconhecimento do comportamento do invasor. Neste ano, prevemos que as organizações procurarão resolver essas lacunas e fortalecer os métodos de defesa das cargas de trabalho na nuvem.

Em relação à nuvem, nossa pesquisa descobriu que uma mudança inexorável está em andamento. Quase todos os CISOs que entrevistamos já seguem uma estratégia de segurança que dá prioridade à nuvem ou planejam fazê-lo em breve. Essa é uma mudança considerável e mostra que as organizações estão acelerando seu plano de desenvolvimento de segurança de nuvem em resposta aos desafios da COVID-19. Possivelmente, eles já estavam percorrendo essa estrada, mas estão acelerando o processo de reconhecimento da necessidade de uma segurança abrangente que dá prioridade à nuvem em um mundo digital.

Esperamos que nosso quarto **Relatório global de informações sobre segurança da VMware** seja elucidativo e informativo.

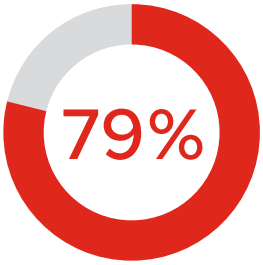
Principais descobertas

A frequência dos ataques e o risco de violação permanecem altos

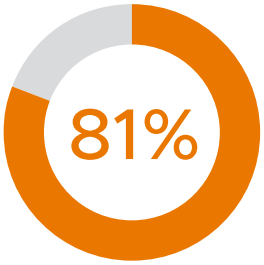
A frequência dos ataques é alta, sua sofisticação continua evoluindo e as violações são uma consequência inevitável.

76% afirmaram que os volumes dos ataques aumentaram nos últimos 12 meses, uma média de 52% em todas as organizações afetadas.

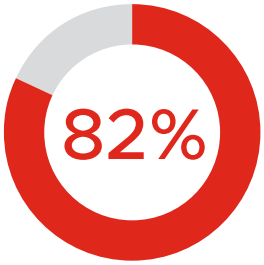
78% das organizações que foram vítimas de ataques cibernéticos alegaram que os ataques aumentaram porque há mais pessoas trabalhando em casa.



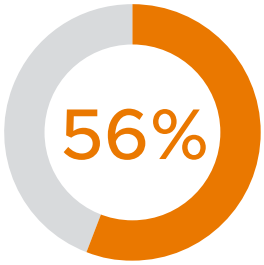
das organizações que foram vítimas de ataques cibernéticos alegaram que os ataques se tornaram mais sofisticados.



sofreram violações nos últimos 12 meses e, em média, foram vítimas de 2,35 violações durante esse período.



afirmaram que as violações que sofreram foram relevantes.



temem uma violação relevante nos próximos 12 meses.

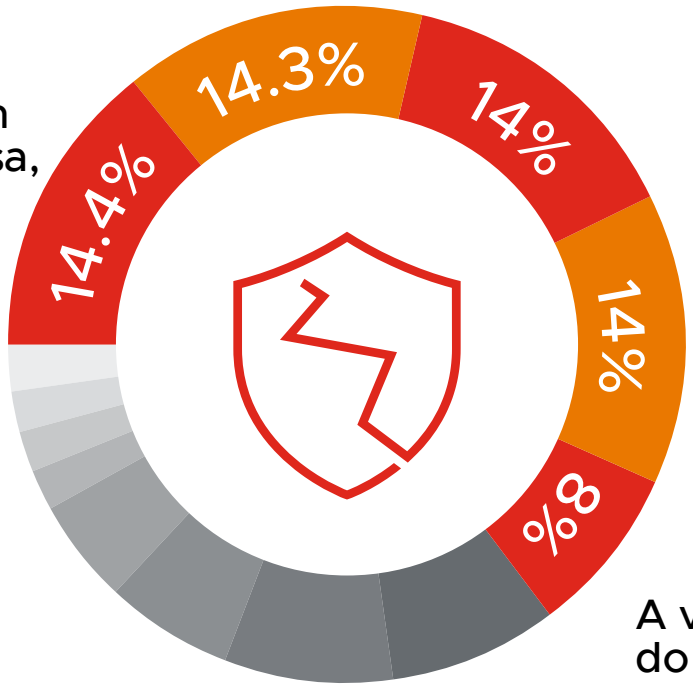
As principais preocupações dos CISOs com apps, cargas de trabalho e ransomware

Os três principais vetores que causam violações desenvolvem um cenário de ameaças externas e pontos fracos internos.

As principais causas de violação para os que foram vítimas de ataques cibernéticos:

O ransomware ficou em segundo lugar com 14,3%.

Os apps de terceiros foram a principal causa, com 14,4%.



A tecnologia de segurança desatualizada e os pontos fracos do processo empataram em terceiro lugar, com 14%.

A vulnerabilidade do sistema operacional (8%) compõe as cinco principais causas.

Os apps e as cargas de trabalho estão no topo da lista como o ponto mais vulnerável na jornada de dados, mas eles não são a única área de preocupação.

A expansão das superfícies de ataque faz com que os líderes repensem seu enfoque tradicional de segurança

A boa notícia é que já se reconhece a necessidade de uma mudança fundamental na segurança para uma era digital altamente conectada e com suporte ao trabalho remoto.

61% quase dois terços concordam que precisam abordar a segurança de maneira diferente à medida que a superfície de ataque aumenta.

63% concordam que precisam de maior segurança contextual para rastrear dados ao longo do ciclo de vida.

63% concordam que precisam de maior visibilidade dos dados e apps para evitar ataques.

Simplificação, consolidação e priorização da nuvem estão nos planos para 2021

Os CISOs entrevistados parecem estar seguindo um caminho de consolidação de tecnologias e adoção de um enfoque mais intrínseco à segurança, ao mesmo tempo que aumentam seu orçamento de segurança para atingir esses objetivos.

43% estão proporcionando mais segurança em sua infraestrutura e apps e reduzindo o número de soluções pontuais.

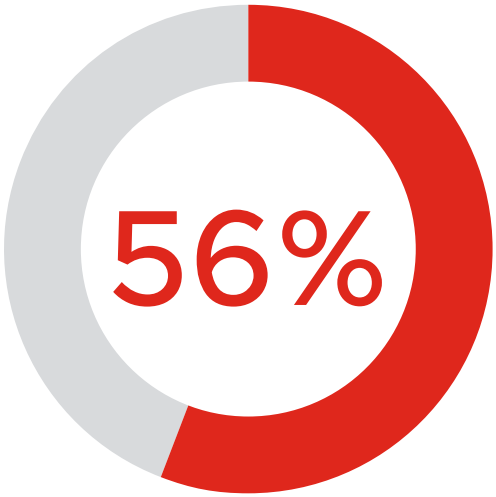
42% atualizaram sua tecnologia de segurança para reduzir os riscos.

41% atualizaram sua política e enfoque de segurança para reduzir os riscos.

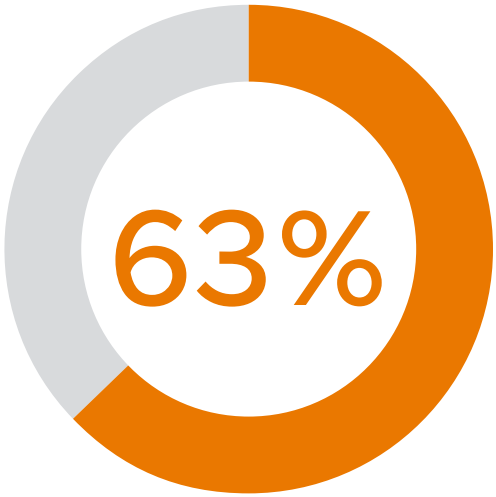
98% já usam ou planejam mudar para uma estratégia de segurança que dá prioridade à nuvem.

A IA é a próxima fronteira para a inovação empresarial, mas as preocupações com a segurança sufocam o progresso?

A próxima fronteira para a inovação empresarial é a IA, à medida que as empresas buscam uma vantagem para promover experiências digitais e serviços de atendimento ao cliente mais competitivos.

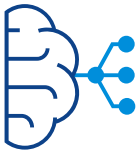


No entanto, mais da metade dos entrevistados em todo o mundo (56%) concorda que as preocupações com a segurança estão atrasando o processo de adoção de apps com base em IA/aprendizado de máquina (ML, pela sigla em inglês) para melhorar esses serviços.



63% dos entrevistados concordam que, para que possam inovar, é necessário que sejam desenvolvidos apps mais seguros para funcionários e clientes.

A IA é a próxima fronteira para a inovação empresarial, mas as preocupações com a segurança sufocam o progresso?



Muitos entrevistados estão preocupados por não conseguirem responder à oportunidade digital.

57%

concordam que há muita complexidade no setor de soluções de segurança para fazê-los mudar sua política de segurança, mesmo sabendo que a segurança de TI atual não está funcionando.

60%

concordam que sua diretoria/equipe de liderança sênior fica cada vez mais preocupada quando eles colocam novos apps/serviços no mercado devido à crescente ameaça e danos causados por ataques/violações de dados.

62%

concordam que gostariam de usar mais IA/ML em seus apps para melhorar a segurança e os serviços.

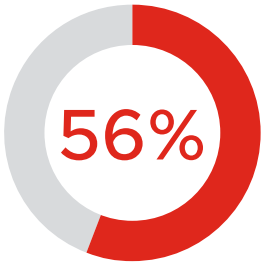
Proteção da marca e da reputação: isso torna a mudança mais urgente?

A marca e a reputação continuam sendo sagradas para as empresas, e são facilmente perdidas. No entanto, o impacto das violações de segurança na reputação supera o impacto financeiro.

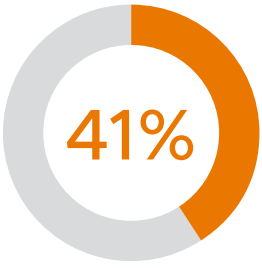
↗ 75% daqueles que sofreram um ataque cibernético dizem que sua reputação foi prejudicada de alguma forma, em comparação a 70% em junho de 2020.

↗ 82% dos entrevistados tiveram que enviar relatórios aos reguladores ou contratar uma empresa de RI para superar os problemas de reputação causados por violações relevantes nos últimos 12 meses.

Há, entre os entrevistados, o reconhecimento sobre a gravidade dessas violações e a falta de senso de urgência para mudanças, apesar do cenário de crescentes ameaças.



estão com medo de sofrer uma violação relevante no próximo ano.



atualizaram sua política e enfoque de segurança para reduzir os riscos.

Resultados completos da pesquisa

Você percebeu um aumento nos ataques cibernéticos em sua empresa nos últimos 12 meses? Em caso afirmativo, quanto?

76% dos CISOs entrevistados disseram que experimentaram um aumento no número de ataques cibernéticos em suas organizações nos últimos 12 meses. Esse aumento saltou para 89% no setor de serviços financeiros.

Regionalmente, mais entrevistados da Arábia Saudita estavam experimentando aumentos no volume de ataques (92% relataram o aumento). No outro extremo da escala, apenas 64% dos entrevistados de Cingapura experimentaram um aumento.

O aumento médio nos ataques experimentados foi de 52% (37% dos entrevistados disseram que os volumes de ataque aumentaram de 51% para 300%) A Espanha relatou o maior aumento médio: 69%.

O tamanho é importante quando se trata do volume de ataques enfrentados. Apenas 69% das empresas com 251 a 500 funcionários afirmam que o volume de ataques aumentou, em comparação com 93% das empresas com 5.001 a 10.000 funcionários.

Em geral, o número de ataques cibernéticos típicos a seu sistema mudou depois que os funcionários passaram a trabalhar em casa devido à pandemia da COVID-19?

78% dos entrevistados que sofreram ataques cibernéticos relataram um aumento na frequência dos ataques devido ao trabalho remoto.

A França experimentou o maior aumento de ataques devido ao trabalho remoto, com 96% dos entrevistados confirmando esse aumento, enquanto o Reino Unido (86%) e a Austrália (89%) também registraram aumento na frequência dos ataques. O trabalho remoto comprovou ser um problema um pouco menor nas regiões dos EUA e dos países nórdicos, com apenas 63% das organizações relatando aumento dos ataques.

Mais uma vez, o tamanho é um fator importante. 76% das organizações de pequeno porte (251 a 500 funcionários) dizem que o trabalho em casa resultou no aumento dos ataques, em comparação com 89% das empresas com 5.001 a 10.000 funcionários.

Os ataques cibernéticos contra sua empresa se tornaram mais ou menos sofisticados nos últimos 12 meses?

Quando se trata de sofisticação de ataque, **79% dos CISOs entrevistados que sofreram ataques cibernéticos relataram que perceberam uma maior sofisticação nos ataques.** Esses dados estão em conformidade com os 80% que sinalizaram o mesmo no Relatório de informações sobre segurança de 2020. 49% afirmam que são significativamente ou moderadamente mais sofisticados.

Os CISOs entrevistados na França apresentam maior probabilidade de terem percebido aumento na sofisticação (89% relataram ataques mais complexos). Apenas 66% dos entrevistados na Itália alegam o mesmo.

Os adversários estão direcionando suas táticas, técnicas e procedimentos (TTPs, pela sigla em inglês) mais sofisticados para organizações maiores. 90% das empresas com 5.001 a 10.000 funcionários que sofreram um ataque cibernético perceberam um aumento na sofisticação, em comparação com apenas 78% das empresas com 251 a 500 funcionários. Isso significa que, quanto maior a empresa, mais valiosos e volumosos serão os dados que ela contém, o que significa que há mais oportunidades para os criminosos cibernéticos monetizarem seu trabalho.

> 79% dos CISOs entrevistados que sofreram ataques cibernéticos relataram que perceberam uma maior sofisticação nos ataques.

Qual foi o tipo de ataque cibernético mais prolífico (ou seja, mais frequente) que sua empresa sofreu nos últimos 12 meses?

Os ataques com base em nuvem são os mais frequentes, mas a proporção de todos esses ataques caiu quase pela metade nos últimos 12 meses, de 18% para 10%. O ransomware está tomando o lugar desses ataques, com um aumento em relação a junho de 2020. Agora, ele representa 9% de todos os ataques, em comparação com apenas 4,5% em nosso último Relatório de informações sobre segurança. Isso reflete a experiência da VMware Threat Analysis Unit™, que observou um aumento de 900% em ransomware no primeiro semestre de 2020 e aponta para as táticas de extorsão dupla que ganharam destaque em 2020.

Na Alemanha, na França, nos Estados Unidos, no Reino Unido, nos países nórdicos e no Japão, o ransomware foi o tipo de ataque mais experimentado.

Os ataques a apps externos ficaram em terceiro lugar, representando menos de 9% dos ataques. Nos Países Baixos, eles foram mais comuns, representando 15% dos ataques; eles também foram os mais experimentados no Canadá e na Austrália.

Com que frequência sua empresa foi violada por um ataque cibernético nos últimos 12 meses?

Mais de oito em cada 10 organizações entrevistadas sofreram violações no ano passado. Isso representa uma queda em relação aos 94% que relataram terem sido vítimas de violações em junho de 2020.

A média estimada mascara qualquer variação regional significativa. 97% das organizações francesas e 93% das organizações do Reino da Arábia Saudita relataram ter sofrido violação. No outro extremo da escala, apenas dois terços (66%) dos entrevistados de Cingapura e 69% do Reino Unido sofreram violações.

> Mais de oito em cada 10 organizações entrevistadas sofreram violações no ano passado.

Aqueles que relataram terem sido vítimas de violações normalmente estão sofrendo ainda mais violações atualmente.

Em média, os CISOs entrevistados relataram que sofreram 2,35 vezes mais violações do que no ano passado, em comparação a 2,17 vezes em junho de 2020. 59% afirmaram que sofreram uma única violação, mas cerca de 14% sofreram cinco ou mais incidentes de violação.

Os EUA tiveram o maior número médio de violações (3,44), enquanto a Espanha se saiu melhor com apenas 1,6.

Qual foi a principal causa dessas violações?

Os aplicativos de terceiros são a principal causa de violações, representando 14% de todos os incidentes ocorridos, seguido pelo ransomware e pela tecnologia de segurança desatualizada (ambos um pouco inferiores a 14%).

Os Países Baixos estão vendo um problema específico com aplicativos de terceiros (36% das organizações relatam que eles são a causa mais comum de violações) Em termos de setor vertical, 16% dos entrevistados do governo e 21% das empresas de mídia e entretenimento disseram que apps de terceiros são a principal causa das violações.

O ransomware é a principal causa de violações na França, na Alemanha, nos países nórdicos, na Austrália e no Japão.

O setor de saúde é particularmente afetado pelo ransomware, com quase um quinto (19%) dos entrevistados no setor de saúde afirmando que essa foi a principal causa das violações.

A segurança desatualizada é o principal problema, segundo 19% dos entrevistados do setor de manufatura e automotivo.

Qual porcentagem das violações por um ataque cibernético nos últimos 12 meses você acredita ter sido uma violação relevante (ou seja, você precisou divulgá-las aos reguladores/ligar para uma equipe de resposta a incidentes para se recuperar etc.)?

Quando uma violação acontece, a questão é grave. **A maioria dos entrevistados (82%) precisou informar os reguladores ou contratar uma empresa de RI para corrigir os problemas causados pelas violações.**

A maioria dos entrevistados (82%) precisou informar os reguladores ou contratar uma empresa de RI para corrigir os problemas causados pelas violações.

A porcentagem de entrevistados que experimentaram violações relevantes foi mais alta no Reino da Arábia Saudita (94%), seguida pela Espanha e pelos EUA, onde 92% e 90% foram consideradas relevantes, respectivamente. A Cingapura se saiu melhor, com apenas 68% das organizações relatando incidentes relevantes.

Quais foram as consequências dessas violações nas finanças e na reputação da sua empresa?

Menos de um quarto (24%) dos entrevistados que sofreram ataques cibernéticos afirmaram que as finanças da sua organização foram prejudicadas devido a uma violação de dados. Essa estimativa caiu 30% para as organizações que alegaram o mesmo em junho de 2020. No entanto, a porcentagem que afirma não ter percebido nenhum impacto financeiro negativo caiu de 56% para 51%. Houve um grande aumento na proporção dos entrevistados que simplesmente não sabem o impacto financeiro causado pelas violações. 20% disseram que não tinham ideia, em comparação com 9% em junho de 2020.

Mais uma vez, houve grandes variações regionais. As penalidades financeiras das violações foram mais sentidas nos Emirados Árabes Unidos, em que 47% relataram um impacto negativo, e nos Países Baixos, em 40% dos entrevistados disseram o mesmo. No outro extremo da escala, apenas 6% no Canadá, 9% na Itália e 10% no Reino Unido disseram que seus negócios foram afetados financeiramente devido a uma violação.

As empresas de serviços profissionais têm maior probabilidade de relatarem um impacto financeiro devido a uma violação, com 32% registrando perdas. 83% nesse setor afirmaram que também sofreram danos à reputação.

Em geral, o efeito sobre a reputação da marca foi maior. Três quartos dos entrevistados disseram que sua marca foi afetada negativamente por uma violação de dados, aumentando para 89% no Japão e 83% na França e na Cingapura.

Apenas 19% disseram que a reputação não foi prejudicada após uma violação, uma queda de quase um quarto em relação aos mesmos entrevistados que disseram isso em 2020.

Até que ponto você tem medo das violações relevantes que sua organização pode sofrer nos próximos 12 meses?

Existe um certo medo associado à possibilidade de violações relevantes no próximo ano. Maisxda metade (56%) tem muito ou pouco medo de que uma violação atinja seus negócios. Isso aumenta para 74% na França e é menor nos Países Baixos (37%).

O setor de serviços financeiros e o setor de varejo estão mais preocupados, com 67% dos entrevistados em ambas as áreas afirmando que temem uma violação relevante. Apenas metade das organizações governamentais e de saúde estão preocupadas com uma violação.

Como você está lidando com a probabilidade de violações (se é que está lidando com isso)?

Quando questionados sobre seus planos para mitigar os riscos de violações, os entrevistados priorizaram a simplificação e a consolidação das soluções de segurança, tornando a segurança intrínseca. A atualização da tecnologia e da política e a utilização do orçamento para o fim proposto também foram fatores importantes.

43% dos entrevistados disseram que planejam **proporcionar mais segurança em sua infraestrutura e apps e reduzir o número de soluções pontuais**. Isso aumentou para 48% nos setores de varejo e alimentos e bebidas.

Mais da metade dos entrevistados na Itália, na Alemanha, na Cingapura e no Japão planejam adotar a segurança intrínseca e reduzir o número de soluções pontuais utilizadas, embora haja uma adesão menor a esse enfoque nos Países Baixos (32%), no Canadá (34%) e nos Emirados Árabes Unidos (37%).

42% disseram que **atualizaram sua tecnologia de segurança para mitigar os riscos**. Os entrevistados do setor de viagens e transporte têm mais probabilidade de aderir a esse enfoque (54%).

As atualizações de tecnologia são mais comuns em Cingapura (51%), Japão (50%) e Austrália (48%). Menos propensos a adotarem esse enfoque são os entrevistados do Canadá (30%), dos Emirados Árabes Unidos (33%) e da Espanha (35%).

41% afirmaram que **atualizaram a política de segurança para mitigar os riscos**, uma tática importante, dadas as mudanças significativas no cenário de segurança no ano passado. As empresas de mídia e entretenimento preferiram essa tática (44%).

O Japão (50%), os países nórdicos (49%) e a Alemanha (47%) têm maior probabilidade de atualizar as políticas de segurança para facilitar o gerenciamento dos riscos de violação.

40% **adaptaram a segurança para mitigar os riscos**, enquanto 39% **aumentaram o orçamento da segurança**. Os setores de varejo (44%), saúde (42%) e serviços financeiros (41%) têm maior probabilidade de aumentar seus orçamentos.

Os entrevistados no Japão (48%) são os que têm maior probabilidade de aumentar o orçamento, enquanto a Itália apresenta a menor probabilidade (32%).

É interessante que as organizações estejam priorizando a estratégia em detrimento do investimento em dinheiro para solucionar o problema, o que torna o aumento do orçamento uma prioridade geral mais baixa do que outras áreas.

Até que ponto você concorda ou discorda das seguintes declarações relacionadas ao desenvolvimento e consumo de apps em sua organização?

Quando questionados sobre a mudança na maneira como estão vendo os desafios de segurança em torno do desenvolvimento e consumo de apps em sua organização, nossos entrevistados nos deram informações sobre os problemas que estão enfrentando.

A visibilidade é uma preocupação inegável. 63% concordam que **precisam de maior visibilidade de seus dados e apps para evitar ataques**. Essa estimativa aumenta para 73% nos setores de **viagens e transporte** e **serviços de utilidade pública**, além de ser uma preocupação primordial na França, onde 84% dos entrevistados concordaram ou concordaram plenamente.

61% dos entrevistados em todo o mundo concordaram que as mudanças no cenário de ataque ocasionadas pela COVID-19 exigem que a segurança seja repensada e acordaram que **precisam tratar a segurança de forma diferente à medida que a superfície de ataque aumenta**. Mais uma vez, os setores de **viagens e transporte** e **serviços de utilidade pública** estão mais propensos a aderirem a essa visão.

Quase dois terços (63%) concordam que **precisam de maior segurança contextual para conseguirem rastrear dados/segurança ao longo do ciclo de vida**. Isso aponta para um ambiente determinante em que a segurança tende a ser reativa e centrada em ameaças. Os CISOs estão reconhecendo que ambientes dinâmicos exigem um enfoque centrado em contexto.

Os CISOs entrevistados não se iludem quanto à natureza essencial da segurança dos apps para a continuidade das operações. 63% concordaram que sua **capacidade de inovação como empresa depende de sua capacidade de desenvolver, gerenciar e distribuir apps com mais segurança**. Naturalmente, isso é mais sentido nos setores voltados para o consumidor, com os entrevistados dos setores de varejo (74%) e de viagens e transporte (75%) mais propensos a concordar com essa afirmação.

62% dos entrevistados **têm confiança em colocar novos apps no mercado porque sabem que eles estarão protegidos**. Os entrevistados nos Emirados Árabes Unidos e na Arábia Saudita têm mais confiança para lançar apps no mercado, com 82% e 83% confirmando essa estatística, respectivamente. Em contrapartida, os CISOs na Espanha estão menos confiantes, com apenas 39% afirmando que se sentem confiantes e 23% dizendo que não estão confiantes para lançar apps seguros.

Questionados sobre seu ponto de vista quanto à IA no desenvolvimento de apps seguros, há divergências entre os entrevistados. 56% concordam **que as preocupações com a segurança os impedem de adotar apps com base em IA/ML para melhorar os serviços**, mas 62% concordam **que gostariam de usar mais IA e ML em seus apps para melhorar a segurança e os serviços**.

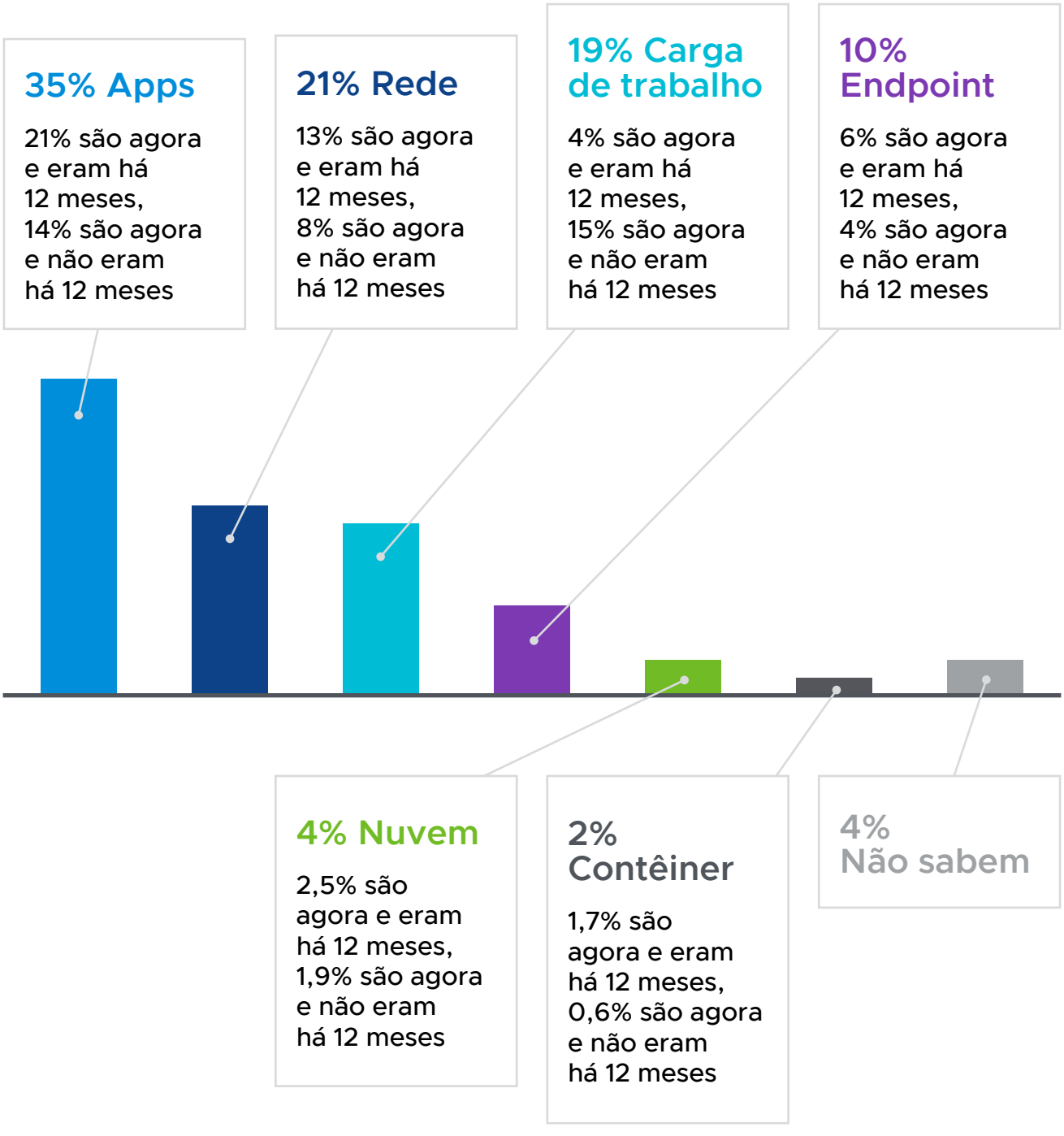
Mais da metade dos entrevistados (57%) concordou que **o mercado de soluções de segurança é muito complicado para fazê-los mudar sua política de segurança, embora saibam que a segurança de TI atualmente não está funcionando**, indicando que os fornecedores terão trabalho para simplificar sua proposta em um enfoque unificado.

Por fim, 60% concordaram que a segurança dos apps está sendo alvo da atenção da diretoria e que sua **equipe de liderança sênior fica cada vez mais preocupada quando eles colocam novos apps/serviços no mercado devido à crescente ameaça e danos causados por ataques/violações de dados**. A diretoria é mais propensa a se preocupar em empresas de serviços de utilidade pública, com três quartos dos CISOs afirmando que a diretoria está preocupada. Mais uma vez, os setores de varejo e de viagens e transporte voltados para o consumidor acompanham essa tendência.

Os diretores na Arábia Saudita e nos Emirados Árabes Unidos têm mais probabilidade de se preocupar com o lançamento de apps e serviços, com 83% e 74% concordando com essa estatística, respectivamente.

Na sua opinião, qual é o ponto de violação mais vulnerável da jornada de dados em sua infraestrutura de segurança? Isso mudou nos últimos 12 meses?

Os apps lideram essa área, que tem sido claramente uma preocupação há algum tempo. O mais interessante é que as cargas de trabalho estão cada vez mais se tornando uma fonte de vulnerabilidade presumível.



Como as organizações enfrentaram os desafios da mudança para o trabalho remoto?

Solicitamos os CISOs entrevistados que avaliassem seu sucesso na mudança da força de trabalho para o trabalho remoto e se um enfoque que dá prioridade à segurança teria ajudado a fazer a transição com mais eficiência.

54% concordam que conseguiram colocar sua força de trabalho em funcionamento remotamente, e a segurança não tem sido uma barreira. Esse é um testemunho do trabalho das equipes de segurança que, mais do que nunca, estiveram no centro das operações. No entanto, existem variações regionais significativas, com apenas 33% dos entrevistados no Reino Unido concordando que colocaram sua força de trabalho em funcionamento sem problemas; 22% discordam. Por outro lado, 76% dos CISOs entrevistados na França tiveram poucos problemas.

Os entrevistados reconhecem que sempre há espaço para melhorias, 60% concordam que um enfoque que dá prioridade à segurança aumentaria sua capacidade de preparar os funcionários para trabalhar em locais alternativos e continuar produtivos. Isso também foi confirmado em uma pesquisa anterior da VMware, que descobriu que a incapacidade de implementar a autenticação multifator foi a maior preocupação dos profissionais de TI em sua resposta à migração para o trabalho remoto. Agora que o perfil de segurança aumentou, deve ser mais fácil para os CISOs garantir o suporte da diretoria em um enfoque que dá prioridade à segurança.

Você usa ou planeja usar uma estratégia de segurança que dá prioridade à nuvem?

> Em geral, 98% já usam ou planejam adotar um enfoque que dá prioridade à nuvem para proteger a organização.

Os entrevistados declararam quase que universalmente que planejam mudar para uma estratégia de segurança que dá prioridade à nuvem, se não imediatamente, isso está decididamente no plano de desenvolvimento. **Em geral, 98% já usam ou planejam adotar um enfoque que dá prioridade à nuvem para proteger a organização.**

100% dos entrevistados nos EUA estão recorrendo à nuvem, mas apenas 87% dos que estão nos Países Baixos dizem o mesmo.

Em geral, 46% afirmam que estão usando um enfoque que dá prioridade à nuvem há mais de um ano, enquanto 30% declaram que priorizam a nuvem há menos de 12 meses. Outros 11% planejam dar prioridade à nuvem no próximo ano, embora a mudança esteja logo ali para esses 11%.

A maturidade da prioridade à nuvem é mais alta na Austrália, onde 63% priorizam a nuvem por mais de 12 meses. Ela é mais baixa no Canadá, onde apenas 25% dizem o mesmo.

Principais informações e ações

Nosso quarto Relatório global de informações sobre segurança mostra que os profissionais de segurança cibernética sênior e as organizações a quem eles atendem continuam a enfrentar ameaças sofisticadas de alto volume. Isso é exacerbado pela transição para uma força de trabalho altamente distribuída e, embora a maioria das organizações tenha conseguido migrar para o trabalho remoto, os CISOs reconhecem que um enfoque que dá prioridade à segurança teria tornado a transição mais fácil.

Sem dúvida, a COVID-19 mudou significativamente o ambiente de segurança cibernética e continuará a influenciar a estratégia de segurança. Por sua vez, o setor de segurança cibernética deve se concentrar em fornecer soluções que reduzam a complexidade operacional e, ao mesmo tempo, protejam de maneira robusta os ambientes de trabalho distribuídos que se tornarão o estado futuro padrão da maioria das organizações.

A análise das respostas da pesquisa revela áreas importantes que precisam ser consideradas pela segurança cibernética no próximo ano.

Priorize a melhoria da visibilidade

As organizações têm um problema de visibilidade resultante da rápida mudança para o trabalho remoto. É difícil identificar a verdadeira escala dos ataques porque os defensores não conseguem ver os cantos em que os dispositivos móveis pessoais e as redes domésticas foram inseridos no ecossistema corporativo. Sem contar o aumento dos desafios de monitoramento de fornecedores e apps de terceiros, bem como do número de pontos cegos.

Em suma, os defensores não sabem o que não é do seu domínio e as empresas acabam ficando expostas. Essa informação contextual limitada dos riscos coloca os defensores em desvantagem ao proteger a superfície de ataque estendida. As organizações devem priorizar a melhoria da visibilidade em todos os endpoints e cargas de trabalho para proteger o ambiente de trabalho remoto. A inteligência situacional robusta que fornece o contexto das ameaças ajudará os defensores a priorizar e corrigir os riscos com confiança.

Responda ao ressurgimento do ransomware

Os ataques cibernéticos continuaram a aumentar a sofisticação e o ransomware não é exceção. Os invasores estão obtendo acesso não detectado às redes, transferindo, de forma não autorizada, dados e estabelecendo backdoors antes de solicitar resgate e/ou monetizar diretamente os dados roubados. Para evitar se tornarem vítimas de ataques repetidos, as organizações precisam combinar proteção avançada de ransomware com correção pós-ataque robusta que detecta a presença contínua de adversários em seu ambiente.

Continue abordando a ineficiência da tecnologia de segurança legada e os pontos fracos do processo

Os pontos fracos do processo e a segurança desatualizada continuam representando um risco significativo para as organizações, e a mudança para o trabalho remoto as deixou ainda mais expostas. À medida que emergimos da fase de resposta imediata e começamos a ver o formato do futuro a longo prazo, as organizações devem identificar as mudanças essenciais nos processos e na tecnologia necessárias para dar suporte a funcionários remotos e híbridos para trabalhar com segurança e reduzir os riscos.

Proporcione segurança como um serviço distribuído

Houve um tempo em que as equipes de segurança protegiam desktops corporativos para funcionários que trabalhavam em campo, conectando-se a aplicativos corporativos executados em servidores em um data center de propriedade da empresa. O mundo é um lugar mais complicado hoje, com trabalhadores remotos conectando-se a aplicativos executados em uma infraestrutura que pode ou não ser gerenciada, adquirida ou controlada pela empresa. Com tantas novas superfícies e diferentes tipos de ambientes a serem protegidos, a segurança não pode ser fornecida como uma série de produtos pontuais e pontos de estrangulamento de rede. Em vez disso, os controles de endpoint e rede devem ser fornecidos como um serviço distribuído. Isso significa oferecer segurança que acompanha os ativos protegidos, independentemente do tipo de ambiente que você possua.

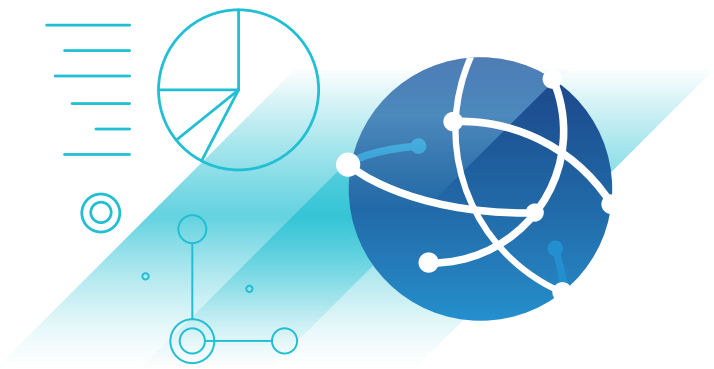
Adote um enfoque intrínseco à segurança que dá prioridade à nuvem

A maior mudança descoberta por nossa pesquisa é a transição para uma estratégia de segurança que dá prioridade à nuvem. É difícil superestimar a magnitude da mudança que ocorreu em tão curto espaço de tempo; antes de 2020, muito poucos CISOs descreveram sua estratégia de segurança como um recurso que dá prioridade à nuvem. Esse é o resultado lógico de as organizações precisarem responder às repentinas práticas de trabalho altamente distribuídas causadas pela COVID-19.

Mas, migrar para a nuvem não é a panaceia para a segurança. Nem todas as nuvens são iguais, e os controles precisam ser examinados por organizações de consumidores, pois se os adversários quiserem atacar em grande escala, a nuvem será o lugar para isso. À medida que essa mudança ganha impulso, o investimento em segurança de nuvem pública será essencial. Quando você migrar para uma nuvem pública, estará se mudando para um bairro muito difícil, onde a segurança dependerá de suas próprias ações e das de seus vizinhos. Você possivelmente conseguirá proteger seus próprios recursos, mas não terá controle sobre aqueles que compartilham esse ambiente com você. As organizações devem priorizar a proteção das cargas de trabalho de nuvem em cada ponto do ciclo de vida da segurança, enquanto a grande mudança na nuvem continua.

Por fim, o Relatório global de informações sobre segurança da VMware de 2021 mostra um setor que está focado em basear-se nos sucessos do ano passado e responder ao ambiente de ameaças em constante mudança. Os CISOs têm um forte senso da direção que precisam tomar e das ferramentas que precisam usar para anteciparem-se aos invasores.

Metodologia



A VMware encomendou uma pesquisa a uma organização de pesquisa independente, a Opinion Matters, em dezembro de 2020. **3.542 CIOs, CTOs e CISOs** de empresas de diversos setores foram entrevistados, incluindo finanças, saúde, governo e autoridades locais, varejo, manufatura e engenharia, alimentos e bebidas, serviços públicos, serviços profissionais, e mídia e entretenimento. Este é o quarto Relatório global de informações sobre segurança da VMware, com base nas pesquisas anteriores realizadas em fevereiro de 2019, outubro de 2019 e junho de 2020. Isso compõe parte de um projeto global de pesquisa em **14 países**, incluindo Austrália, Canadá, Arábia Saudita, Oriente Médio, Reino Unido, França, Alemanha, Espanha, Países Baixos, países nórdicos, Itália, Japão, Cingapura e Estados Unidos.

Sobre a VMware

O software VMware viabiliza a complexa infraestrutura digital global. As ofertas de nuvem, modernização de aplicativos, rede, segurança e espaço de trabalho digital da empresa ajudam os clientes a fornecer qualquer aplicativo em qualquer nuvem e dispositivo. Sediada em Palo Alto, Califórnia, a VMware tem o compromisso de ser uma força do bem, desde suas inovações tecnológicas até seu impacto global. Para obter mais informações, acesse vmware.com/br/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel: 877-486-9273 Fax: 650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP 04571-050 Cidade Monções – São Paulo – SP Tel.: (+55) 11 5509-7200 www.vmware.com/br