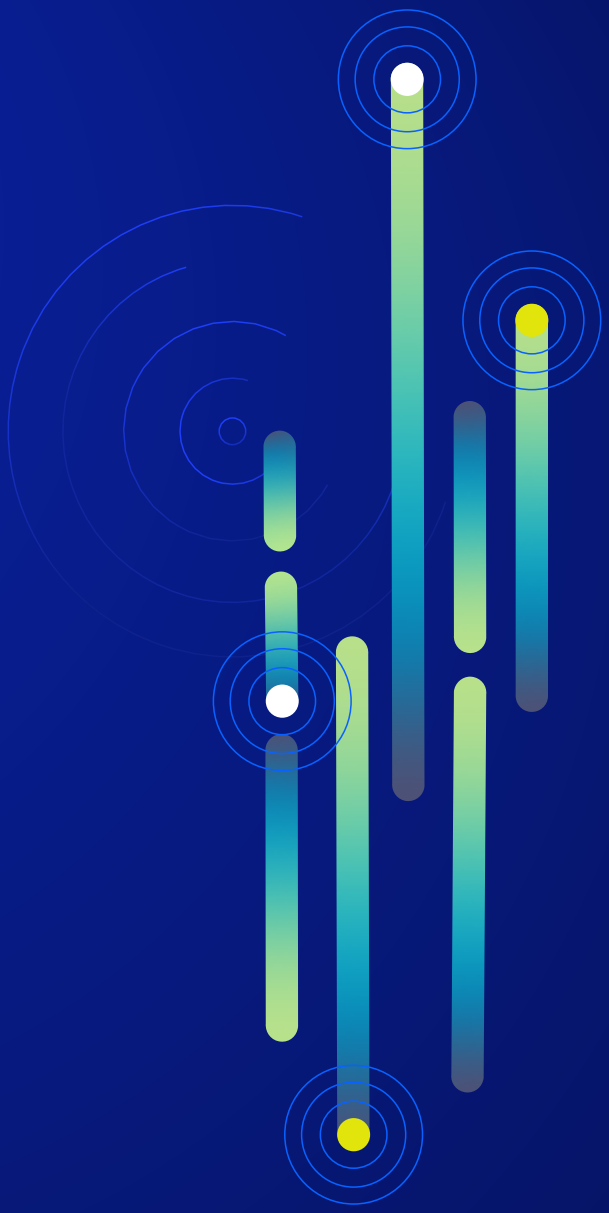
Estado da Segurança Física 2024:

Abraçando a tecnologia e novas formas de trabalhar

Insights da pesquisa com mais de 5.500 profissionais de segurança física



ESTADO DA SEGURANÇA FÍSICA 4ª EDIÇÃO 2024

Genetec™

Conteúdo

Sobre a pesquisa

A Genetec Inc. entrevistou profissionais de segurança física entre 21 de agosto a 15 de setembro de 2023. Após uma revisão das entrevistas e limpeza de dados, 5.554 entrevistados foram para análise.

Resumo da metodologia da pesquisa

O público-alvo da pesquisa se concentrou em dois grupos principais:

Usuários finais

Indivíduos que trabalham para organizações, participando na aquisição, gestão, manutenção e/ou uso de tecnologia de segurança física.

Parceiros de canal

Indivíduos que prestam consultoria, instalam, vendem ou fazem manutenção de soluções de segurança. Para melhor legibilidade, este relatório se referirá a parceiros de canal,instaladores, fabricantes, integradores de sistemas e fornecedores como parceiros de canal.

O público-alvo foi alcançado por meio de eventos presenciais e por terceiros através de suas listas de e-mail, listas de e-mail opt-in da Genetec, e promoções digitais.

Um conjunto de perguntas da pesquisa foi feito aos usuários finais e um conjunto diferente de perguntas foi feito aos parceiros de canal, instaladores, fabricantes, integradores de sistemas e fornecedores. No entanto, algumas perguntas foram feitas apenas para usuários finais e algumas apenas para parceiros de canal, instaladores, fabricantes, integradores de sistemas e fornecedores.

Insights

Pequenas diferenças foram encontradas em resultados entre usuários finais e respostas dos parceiros de canal.

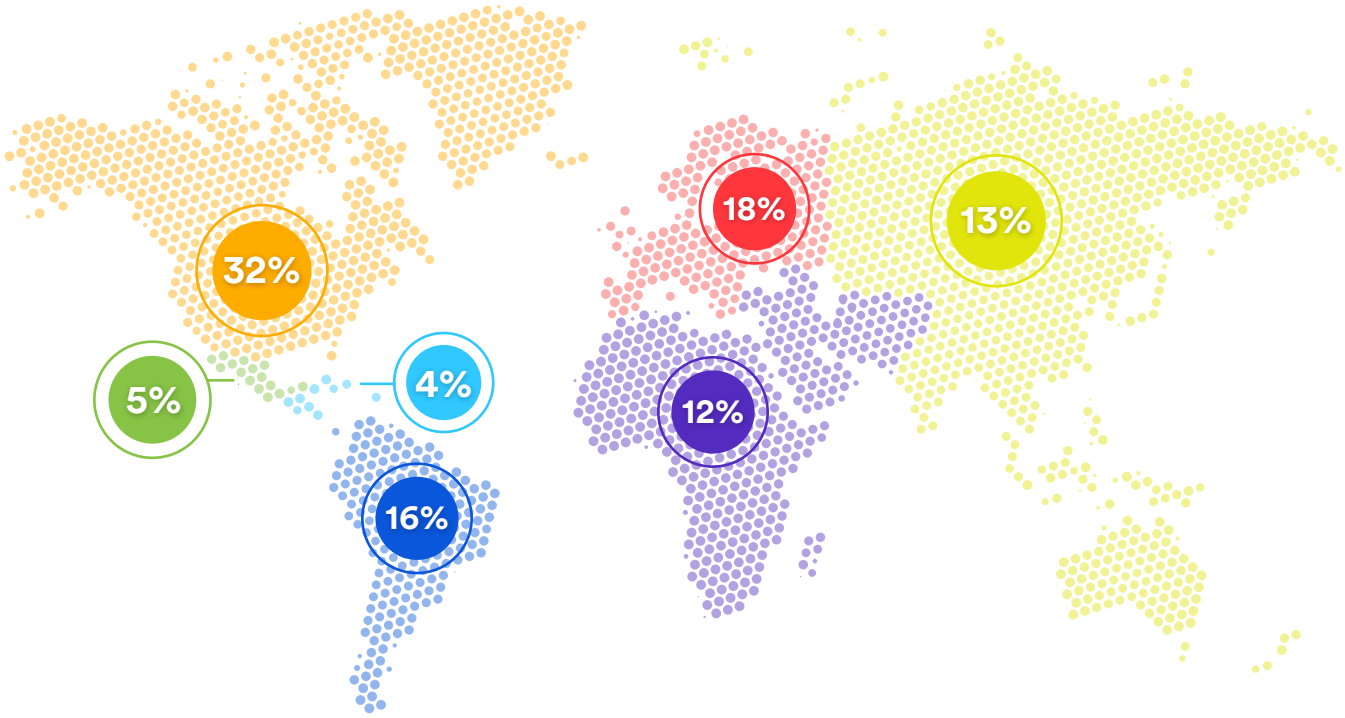
Na maioria dos casos, houve pouca diferença nos resultados. As respostas de “apenas usuários finais” estiveram em linha com as respostas de parceiros de canal, instaladores, fabricantes, integradores de sistemas e fornecedores.

Este relatório aponta se as respostas são de todos os entrevistados, dos usuários finais ou dos parceiros de canal, integradores, instaladores, fabricantes, integradores de sistemas e fornecedores.

Apenas pesquisas totalmente preenchidas por indivíduos dentro do público-alvo foram incluídas na análise final.

Para melhorar a legibilidade, este relatório se referirá a parceiros de canal, instaladores, fabricantes, integradores de sistemas e fornecedores como parceiros de canal.

Público-alvo-alvo em todas as regiões geográficas



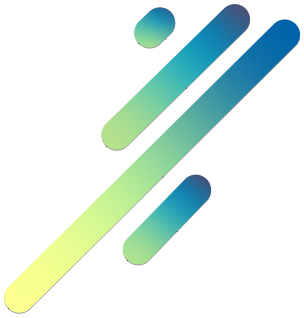
- **América do Norte: EUA e Canadá**
- **América do Norte: México**
- **América Central e Caribe**
- **América do Sul**
- **Europa e Reino Unido**
- **Oriente Médio e África**
- **Ásia-Pacífico**

Apenas pesquisas totalmente preenchidas por indivíduos dentro do público-alvo foram incluídas na análise final.

Para mais detalhes sobre a metodologia da pesquisa e dados demográficos dos participantes, consulte os Apêndices 1 e 2.

Sumário executivo

É um momento emocionante para a indústria de segurança física. Com base nos dados coletados em nossa pesquisa de 2022, ficamos surpresos com alguns dos resultados da pesquisa de 2023. Da crescente demanda por nuvem e tecnologia aos desafios que não melhoraram como esperado – está claro que a indústria está abraçando a mudança e se adaptando a novas formas de trabalhar.



Novas tecnologias estão sendo rapidamente adotadas

A integração de novas aplicações em ambientes de segurança física aumentou e não mostra sinais de desaceleração no próximo ano.

A conectividade na nuvem acelera

A adoção da nuvem no setor de segurança física tem sido gradual, mas agora está acelerando. O futuro para a maioria das soluções de segurança física parece ser uma mistura de soluções in loco e hospedadas na nuvem.

As preocupações com cybersecurity aumentam

Apesar da implementação de processos para enfrentar os desafios de cybersecurity, o nível de preocupação com as ameaças cibernéticas continua a subir.

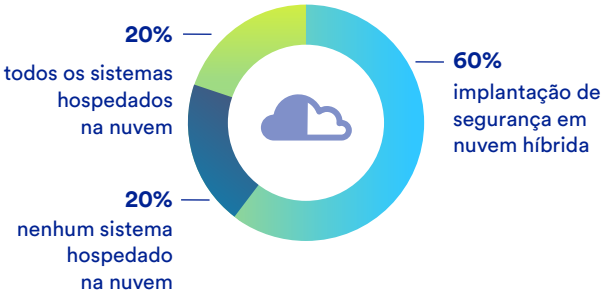
Os desafios da supply chain e de RH persistem

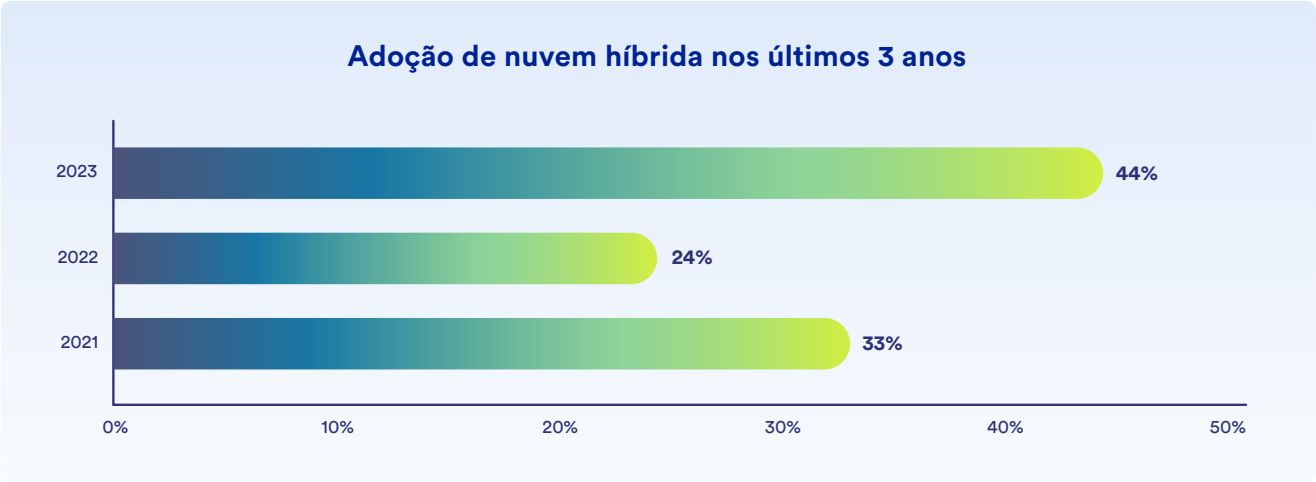
Esperava-se que as restrições da supply chain e questões de recursos humanos (RH) relacionadas com a pandemia já estivessem resolvidas a essa altura. No entanto, esses desafios continuam disruptivos para muitas organizações.

Principais descobertas globais

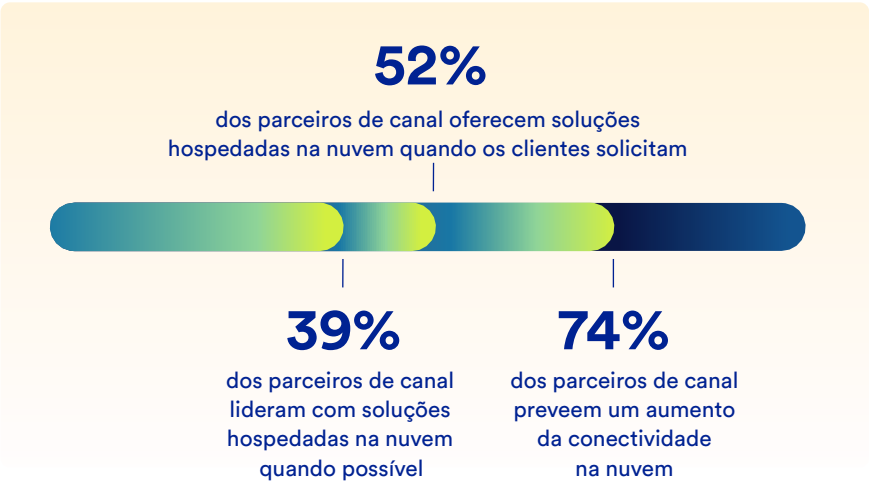
Acelerando em direção à nuvem

Durante última década, a adoção da nuvem para segurança física tem sido gradual.
No entanto, agora está acelerando. Na pesquisa de 2023, 44% dos usuários finais indicaram que mais de um quarto do seu ambiente de segurança física é nuvem ou nuvem híbrida em comparação com 24% da pesquisa de 2022.





Apesar da mudança para a nuvem, as arquiteturas híbridas se misturam no local e na nuvemsoluções baseadas em software serão adequadas para a maioria das organizações. Esta mudança para sistemas híbridos já está em andamento.



Insights

Dados da pesquisa de 2023 indicam 11% de aumento no armazenamento de vídeo em nuvem híbrida

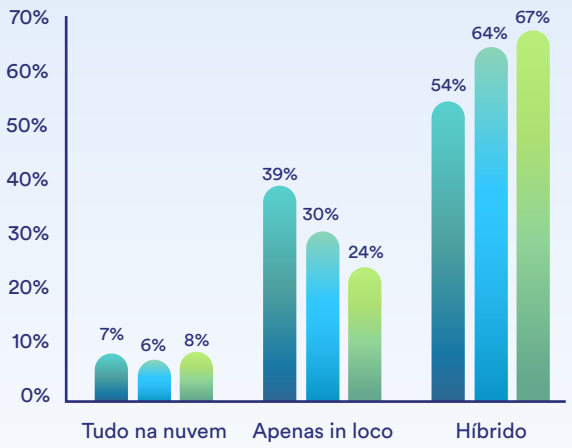
Adoção da nuvem por porte da organização

Sistemas de videomonitoramento hospedados na nuvem foram inicialmente adotados mais rápido por organizações pequenas e grandes que tinham sites de distribuição e um pequeno número de câmeras, como restaurantes de fast food e redes de bancos de varejo. Os resultados de 2023 indicaram que esta situação está mudando. Um número maior de grandes organizações empresariais que possuem mais de 100.000 colaboradores agora estão adotando sistemas de videomonitoramento hospedados na nuvem.

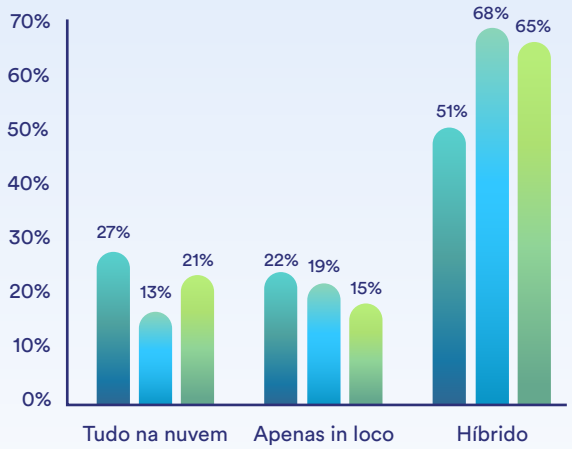
Insights

36% dos usuários finais do governo estadual e local e 29% da justiça e segurança pública informaram que nenhuma solução seria hospedada na nuvem.

Adoção da nuvem em 2023



Previsão para 5 anos de adoção da nuvem



1-200 colaboradores | 201-10.000 colaboradores | Mais de 10.001 colaboradores

A migração para a nuvem é híbrida

Em nossa pesquisa de 2022, os entrevistados relataram que 58% de seu sistema de segurança física era in loco e 42% na nuvem ou nuvem híbrida. Em nossa pesquisa de 2023, esses números saltaram para 33% dos entrevistados afirmando que seus sistemas de segurança física eram in loco e 67% eram nuvem ou nuvem híbrida. Esses resultados indicam que os usuários finais não querem ficar presos e estão buscando opções ao aproveitar a tecnologia na nuvem para otimizar sua infraestrutura.

"Ao utilizar soluções na nuvem, podemos aproveitar a experiência das equipes profissionais dos provedores de serviços na nuvem para monitorar e manter nossas aplicações de segurança física, aliviando assim a sobrecarrega para nossas equipes internas."

–Usuário final entrevistado

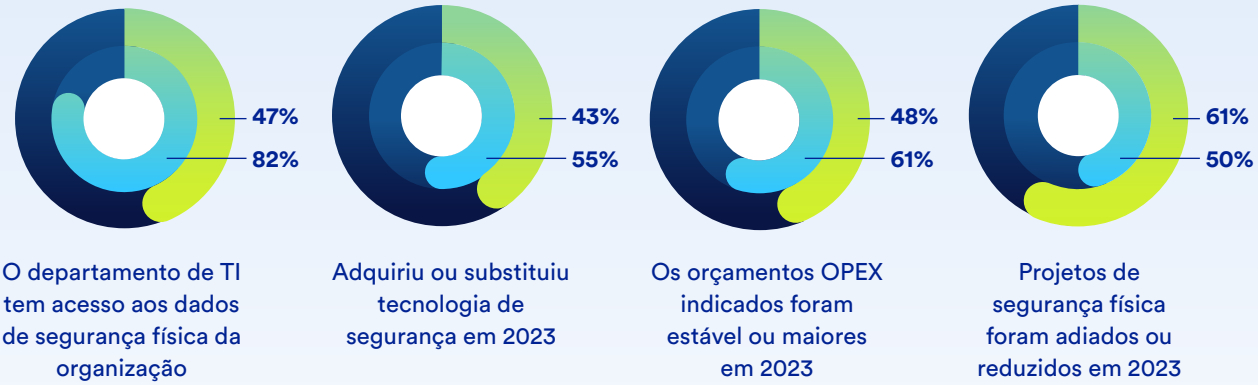
Especialistas em segurança e proteção comparados a especialistas em TI

Há uma década, a maioria dos sistemas de segurança física em organizações maiores eram gerenciados por equipes de departamentos de segurança especializados. A transição para sistemas de segurança física de rede significou que os departamentos de tecnologia da informação (TI) estão assumindo maior responsabilidade para gerenciar sistemas de segurança física como parte de sua governança tecnológica. Esses departamentos podem ter perspectivas e prioridades diferentes. Isso explica por que os entrevistados que indicaram sua profissão como “tecnologia da informação” muitas vezes tinham um ponto de vista diferente do que seus colegas que indicaram "segurança e proteção".

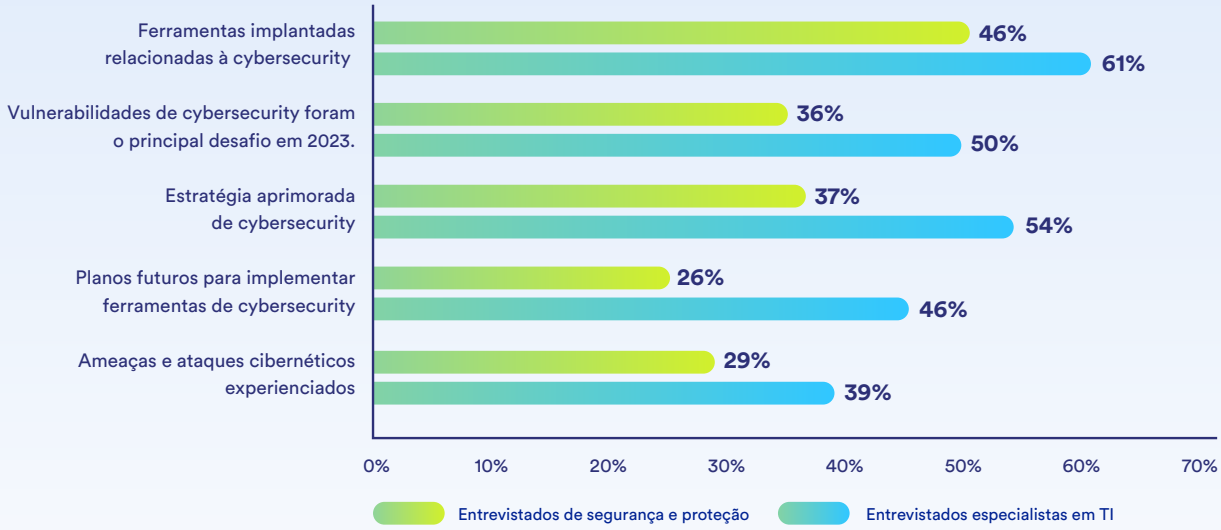
Insights

As questões de cybersecurity foram priorizadas nas respostas de entrevistados de "tecnologia da informação". Os dados da pesquisa também indicam que eles dispõem de orçamentos mais altos em comparação com outros departamentos que poderiam tornar mais fácil colocar foco em medidas de cybersecurity.

Segurança e proteção versus tecnologia da informação



Perspectiva de segurança e proteção em comparação com TI em cybersecurity



Ponto de vista

Muitas organizações ainda lidam com vídeo e controle de acesso separadamente. No entanto, há um forte impulso para modernização, incentivando essas organizações a eliminar a fragmentação em seus sistemas e tecnologia. Alguns possuem até departamentos diferentes, portanto também há uma questão de estrutura organizacional. Eliminar essas fragmentações requer uma liderança firme e gerenciamento eficaz.
Não se trata apenas de tecnologia; a forma como é administrado e conduzido é igualmente importante.

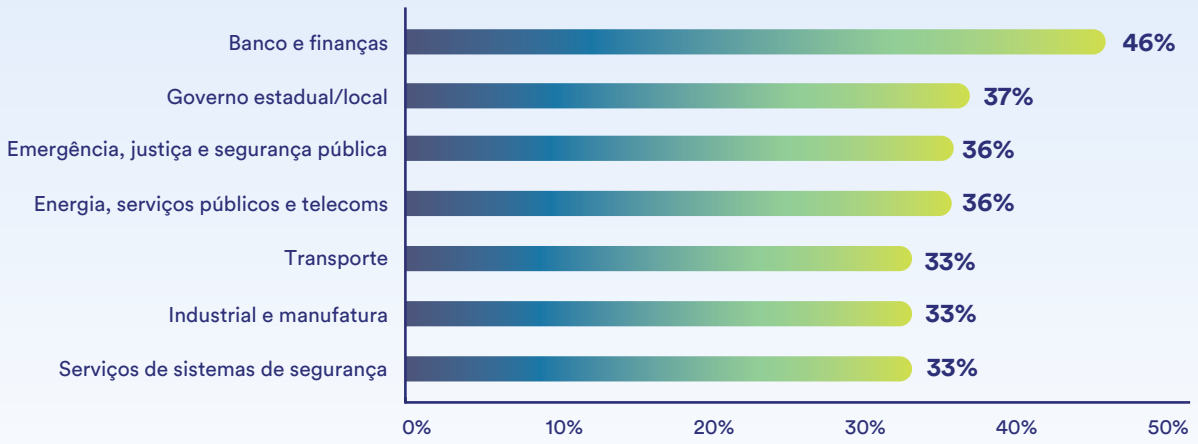
"A tecnologia muda rapidamente, mas as organizações mudam muito mais lentamente." – George Westermen

Pervez Siddiqui
Vice-presidente de Ofertas
e Transformação
Genetec Inc.

Aumentam as preocupações com ameaças cibernéticas

Preocupantes 31% dos usuários finais indicaram que a sua organização foi alvo de cibercriminosos em 2023.

Indústrias mais afetadas por ameaças cibernéticas



As organizações priorizam uma melhor estratégia de cybersecurity

Em resposta às ameaças cibernéticas, 42% das organizações aumentaram as implementações de ferramentas relacionadas com cybersecurity nos seus ambientes de segurança física em 2023, contra apenas 29% em 2022.

Preocupações cibernéticas sobre redução da nuvem

Na pesquisa de 2022, usuários finais classificaram os riscos de cybersecurity como a principal razão para dissuadir a sua organização de adotar soluções na nuvem. Na pesquisa de 2023, este número caiu para o 6.º lugar.

As 5 principais ações tomadas pelos parceiros de canal para melhorar a cybersecurity

61%
Educar os usuários sobre as melhores práticas de cybersecurity

47%
Fortalecimento da infraestrutura de segurança

42%
Ajustar as permissões e privilégios do usuário

42%
Proteger o sistema contra acesso não autorizado

41%
Proteger o armazenamento de dados

Ponto de vista

Com o aumento dos riscos cibernéticos nos sistemas de segurança física, as organizações estão demonstrando uma maior consciência sobre cybersecurity e adoção de melhores práticas para encarar estes desafios de frente.

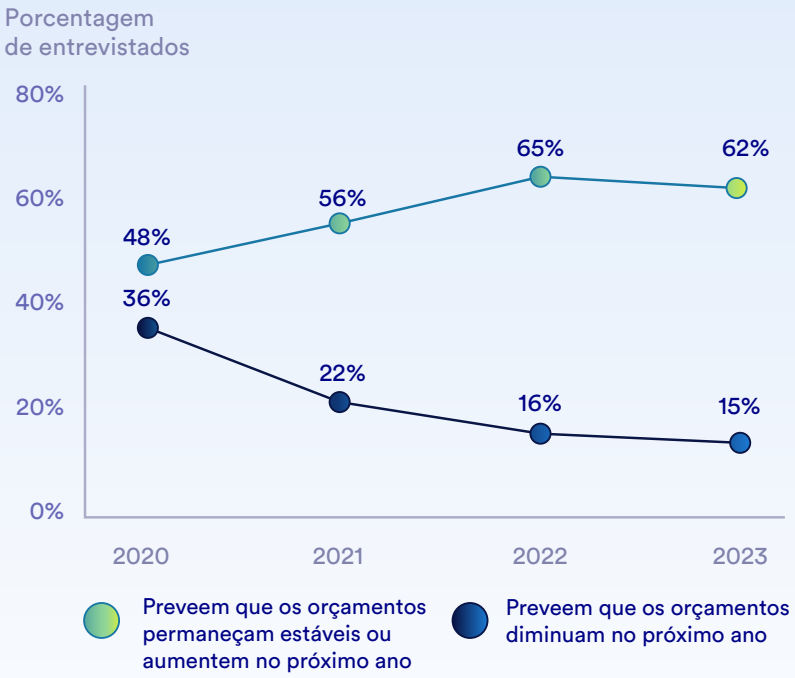
Isso reflete o padrão observado durante os estágios iniciais da integração da cybersecurity na indústria de TI. Como os profissionais de TI se envolvem cada vez mais em projetos de segurança física e seus conhecimentos estão enriquecendo a área. A indústria de segurança física está caminhando na direção certa, mas ainda há alguma distância a percorrer.

Mathieu Chevalier
Gerente e Arquiteto Chefe de Segurança,
Segurança da Informação
Genetec Inc.

Os orçamentos OPEX continuam a aumentar

A boa notícia para a indústria é que os orçamentos OPEX continuam a crescer. 62% dos usuários finais preveem que os orçamentos aumentem ou permaneçam estáveis em 2024 e apenas 15% esperam que os orçamentos diminuam. Trata-se de proporções muito semelhantes às esperadas pelos entrevistados para o ano seguinte na nossa pesquisa de 2022. Em 2022, o mercado de equipamentos de videomonitoramento explodiu em muitas regiões, com os analistas de mercado Novaira Insights relatando um crescimento de 19% nas Américas e 12% na EMEA.

Dados da pesquisa orçamentária OPEX ao longo de 4 anos



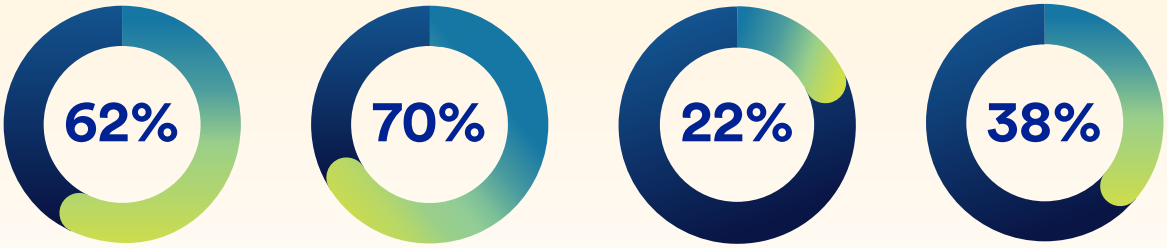
Insights

Muitas soluções são nuvem são cobradas de forma recorrente. Poderia-se gerar um caso para que o aumento nos orçamentos OPEX esteja parcialmente vinculado ao crescente interesse e adoção de soluções na nuvem e nuvem híbrida. Isso também pode refletir a contínua influência dos departamentos de TI na compra de soluções de segurança física.

Os desafios de RH ficaram piores

Em todas as indústrias, escassez de talentos, planos de retorno às empresas e expectativas dos colaboradores para novas formas de trabalho desafiou as organizações nos últimos anos. Infelizmente, os resultados da nossa pesquisa sugerem que, para os parceiros de canal, os desafios de RH estão piorando em vez de melhorar.

Distribuição dos desafios de RH de acordo com os parceiros de canal

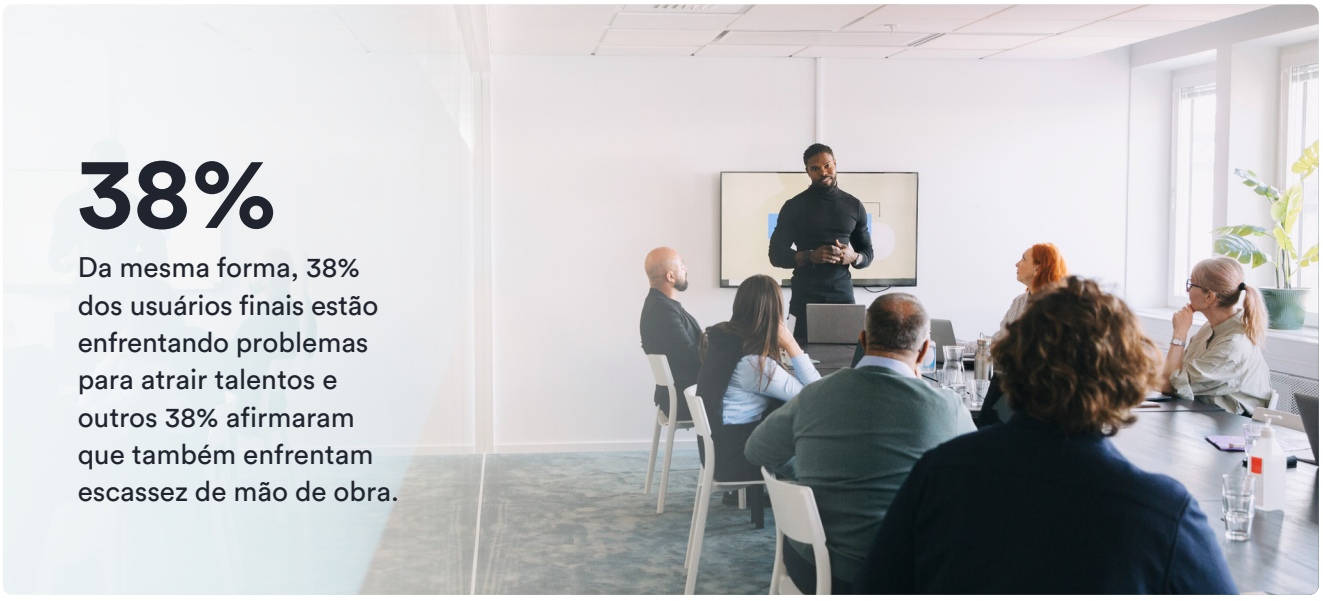


Problemas de RH aumentaram em 2023

Problemas de RH aumentarão em 2024

Os problemas de RH permanecerão os mesmos em 2024

Escassez de mão de obra causará atrasos em projetos em 2024



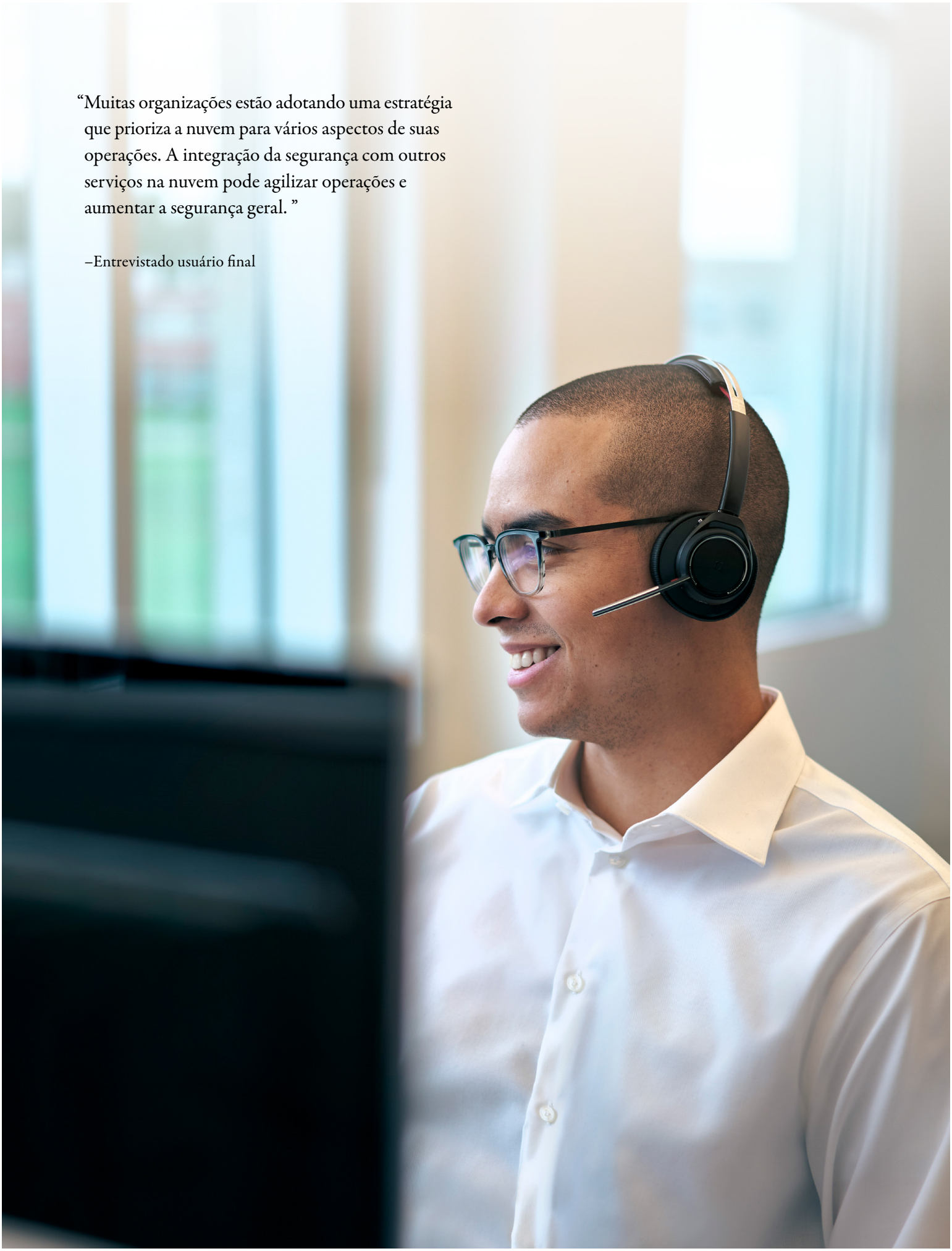
38%

Da mesma forma, 38% dos usuários finais estão enfrentando problemas para atrair talentos e outros 38% afirmaram que também enfrentam escassez de mão de obra.

Ponto de vista

À medida que a adoção da tecnologia evolui, abrem-se oportunidades para toda a indústria. Novas abordagens para trabalho e conjuntos de recursos impulsionados por maior conectividade e entrega de recursos híbridos na nuvem pode facilitar maior escalabilidade, segurança e agilidade nas implantações de segurança física nos próximos anos. Isso significa que os usuários finais podem trabalhar com seus parceiros para adaptar suas integrações visando atender às suas necessidades de forma exata e beneficiar-se da inovação.

Michel Chalouhi
Vice-presidente de Vendas Globais
Genetec Inc.



"Muitas organizações estão adotando uma estratégia que prioriza a nuvem para vários aspectos de suas operações. A integração da segurança com outros serviços na nuvem pode agilizar operações e aumentar a segurança geral. "

–Entrevistado usuário final

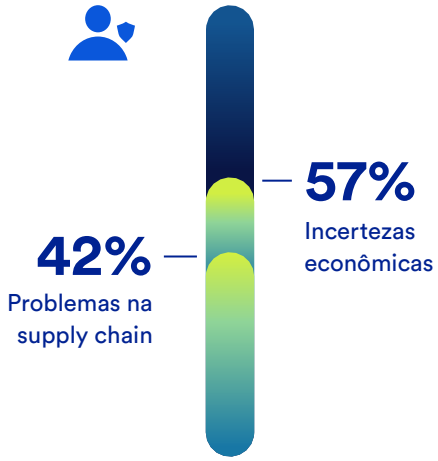
Os problemas da supply chain persistem

Muitos projetos de segurança física foram adiados em 2021 e 2022 devido a problemas sem precedentes na supply chain. Esses atrasos persistiram até 2023.

45% dos usuários finais responderam que seus projetos de segurança física foram adiados ou reduzidos em 2023. Outros 12% confirmaram que foram totalmente cancelados.

56% dos parceiros de canal responderam que tinham um backlog de implantação no início de 2022. 50% acreditam que os problemas da supply chain irão aumentar muito ou um pouco. Enquanto o restante acredita que permanecerá igual (28%) ou diminuirá um pouco ou bastante (22%).

Principais motivos para atrasos em projetos

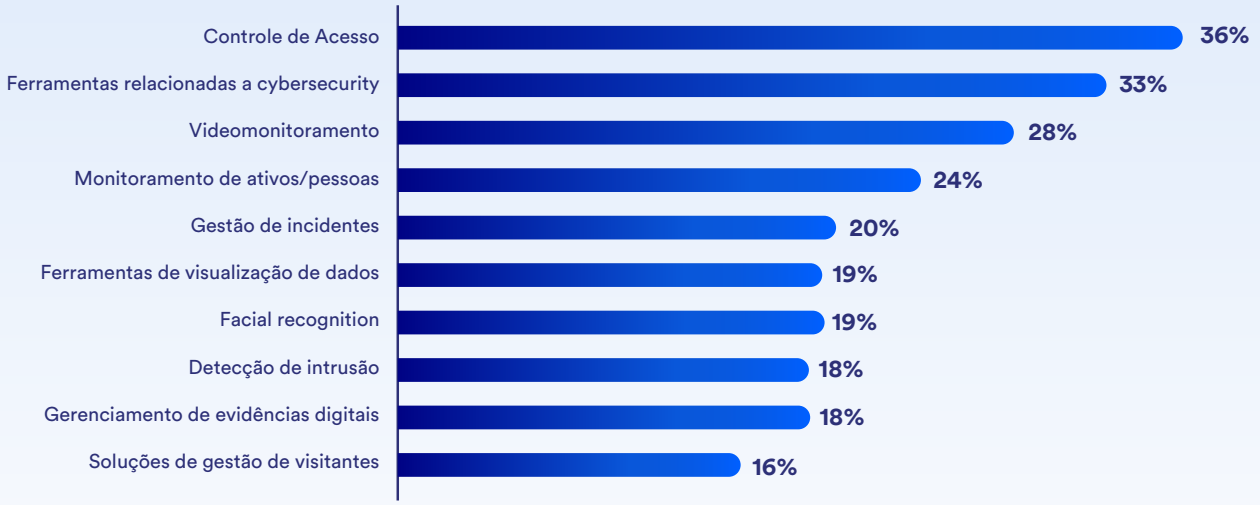


Observação: os entrevistados poderiam selecionar mais de um motivo

Nova tecnologia é adotada

Os avanços na tecnologia estão sendo aplicados a ambientes de segurança física para aprimorar as ofertas de segurança tradicionais. Em nossa pesquisa, os usuários finais foram questionados sobre que tipo de projetos planejam focar em 2024. Juntamente com projetos tradicionais de segurança física, como controle de acesso, videomonitoramento e detecção de intrusão, uma proporção relativamente alta de usuários finais também selecionou as seguintes tecnologias:

As 10 principais tecnologias nas quais os usuários finais planejam investir



Integrações de inteligência artificial em ascensão

22% dos usuários finais afirmaram que sua organização já havia integrado aplicações de aprendizado de máquina, inteligência artificial (IA) e/ou grande modelo de linguagem (LLM) em seu ambiente de segurança física. Isto variou de acordo com a indústria, com 46% dos entrevistados no setor de trânsito e estacionamento indicando que adotaram a IA, enquanto apenas 10% no setor de saúde o fizeram.

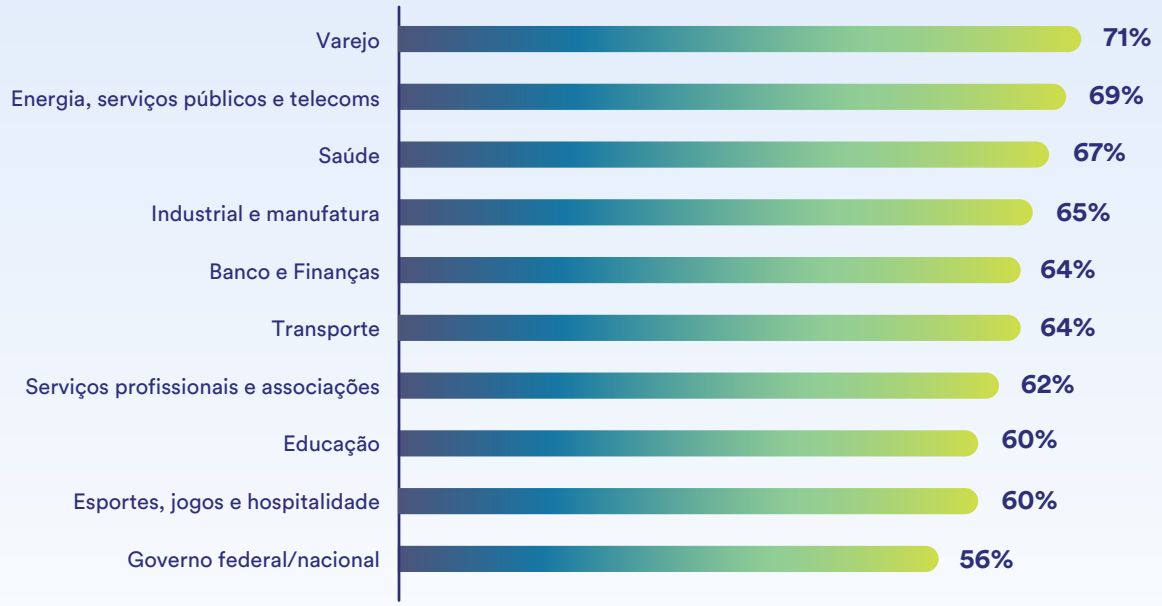
Insights

33% dos usuários finais planeja adicionar aplicações de IA em 2024.

Conectividade

64% dos usuários finais responderam que o atual sistema de segurança física de sua organização permite conectividade remota de fora de sua rede local (por exemplo, atualizações remotas de firmware, patches, monitoramento remoto etc.). Para as organizações onde este não é o caso, 31% dos usuários finais indicaram que no momento existe um plano para permitir a conectividade remota fora da sua rede local. Os dados da pesquisa variaram consideravelmente por setor.

Indústrias que permitem conectividade remota



55% dos usuários finais afirmaram que seu departamento de TI tem acesso a dados de segurança física. Considerando o aumento da tecnologia e adoção da nuvem, não é surpreendente que os departamentos de TI estão desempenhando um papel maior na segurança física. Suas habilidades são muitas vezes necessárias para integrar com segurança novos aplicações em redes organizacionais relevantes. A colaboração adicional tornou-se essencial para garantir a seleção, governança e resiliência cibernética adequadas das soluções de segurança física em rede.

Departamentos que têm acesso a dados de segurança física

Ponto de vista

Com 1) o atual movimento de trabalho híbrido mudando o panorama da força de trabalho, 2) uma supply chain que ainda enfrenta alguma instabilidade e incerteza,
3) um foco cada vez maior na transformação digital,
4) os grandes avanços no aprendizado de máquina e
5) a mudança para uma maior conectividade na nuvem,
a indústria de segurança física está num período de mudanças desafiadoras, mas emocionantes.
Estas mudanças estão se traduzindo em enormes oportunidades para os players da indústria que são capazes de agir rapidamente e adaptar-se a este ambiente em mudança para trazer soluções inovadoras baseadas em dados para a vanguarda, tanto para seus parceiros quanto para os clientes. A habilidade de adaptação das organizações está se tornando uma das capacidades mais importantes para o sucesso de qualquer empresa.

Nadia Boujenoui
Vice-presidente de Experiência do Cliente
Genetec Inc.

Principais conclusões

1

Nova confiança na nuvem

A indústria de segurança física está se equiparando a outras indústrias na adoção da nuvem. A partir das respostas recebidas às perguntas sobre nuvem na pesquisa deste ano, notamos que os usuários finais passaram a compreender o seu valor. Onde antes classificavam os riscos de cybersecurity como o principal obstáculo para a migração para a nuvem, agora há mais conhecimento e confiança.

As implantações de nuvem híbrida parecem ser a direção para a maioria das organizações, pois conseguem justificar os custos, as preocupações e as abordagens da migração para a nuvem.

2

Surgimento de equipes de TI e segurança física experientes em tecnologia

À medida que aumenta a adoção de sistemas de segurança física na nuvem, também aumentam as ameaças à cybersecurity, gerenciamento de dados e requisitos de compliance.

A pesquisa de 2023 indica um aumento nas integrações de novas tecnologias. Os usuários finais têm mais confiança ao usar essas aplicações para melhorar os insights em segurança física e operações. O resultado de maior envolvimento com TI.

À medida que mais tecnologia é adotada e a conectividade remota de redes locais externas aumenta, a relação entre TI e segurança física continuará a evoluir.

3

Tornando cybersecurity uma prioridade máxima

A resposta da indústria de segurança física às ameaças cibernéticas no passado era geralmente inadequada. Porém, as atitudes estão mudando. Várias perguntas da pesquisa revelaram um maior foco na cybersecurity tanto de usuários finais quanto parceiros de canal. Isto pode ser em resposta a um crescente número de entrevistados que admitem que a sua organização enfrentou ataques cibernéticos.

Os entrevistados de TI priorizaram a cybersecurity em várias de suas respostas. Também parecem ter orçamentos maiores, o que poderá facilitar colocar foco na manutenção e suporte financeiro a uma estratégia de cybersecurity.

44%

dos usuários finais indicaram que mais de um quarto de seus ambientes de segurança física ficam na nuvem ou nuvem híbrida na pesquisa de 2023 . Isso se compara com 24% da pesquisa de 2022.

55%

dos usuários finais indicaram que o departamento de TI tem acesso a dados de segurança física.

42%

dos usuários finais indicaram que sua organização implantou ferramentas relacionadas a cybersecurity em seu ambiente de segurança física em 2023.

Resumo das diferenças ao redor do mundo

Os dados da pesquisa não variaram estatisticamente em relação à média global e, principalmente, demonstraram uma visão, experiência e expectativa comuns na maioria dos casos.

A maior variação ocorreu frequentemente nas três regiões latino-americanas: México, América Central e Caribe e América do Sul. Para outras regiões, também registramos os raros casos em que constatamos diferenças significativas nas respostas em relação à média global.

Ásia-Pacífico

Backlog de implantação e foco em ferramentas de cybersecurity

Pendências de implantação: 41% dos parceiros de canal relatou ter enfrentado atrasos de implantação no início de 2023. Um contraste com a cifra global de 56%. Isto indica uma abordagem mais simplificada para implantações na região.

Conectividade e acesso remoto: 57% dos usuários finais indicaram que o sistema de segurança física de sua organização permite conectividade remota.
Um total de 65% dos parceiros de canal na APAC indicaram que mais de 25% dos novos sistemas de segurança física que implantarão serão na nuvem ou nuvem híbrida nos próximos cinco anos, em comparação com 69% dos parceiros de canal no mundo todo.

Foco na segurança cibernética: 42% dos utilizadores finais indicaram que os seus departamentos colocaram foco na implementação de ferramentas relacionadas a cybersecurity em 2024, em comparação com a média global de 33%. Esta ênfase na cybersecurity está alinhada com o fato de que 50% dos usuários finais identificaram vulnerabilidades de cybersecurity como um grande desafio pare suas organizações em 2023, em comparação com 36% globalmente.

América Central e Caribe

Foco na unificação de sistema e cybersecurity

Adoção mais lenta da nuvem: Adoção da nuvem nesta região parece estar crescendo em um ritmo mais lento do que em outros países. Uma porcentagem menor de parceiros de canal nesta região (37%) têm clientes que usam segurança na nuvem em comparação à média global (49%). Além disso, 55% dos parceiros de canal nesta região indicaram que 25% dos sistemas de segurança física que implantam será na nuvem ou nuvem híbrida em cinco anos, em comparação com 69% dos parceiros de canal em todo o mundo.

Desafios com colaboradores: A contratação de pessoal parece ser um grande problema na América Central e no Caribe, com 80% dos parceiros de canal na região prevendo desafios em 2024. Isso supera a média global de 70%.

Backlog de implantação: Em 2023, 71% dos parceiros de canal nessa região começaram o ano com atrasos de projetos em comparação com a média global de 56%. Além disso, uma porcentagem mais alta (84%) experinciou um aumento em seu backlog durante o ano, superando a cifra global (61%).

Atrasos e causas: As incertezas econômicas são menos frequentemente citadas como razão para atrasos nos projectos, com apenas 45% dos usuários finais nesta região escolhendo esta opção, em comparação com a média globalde 57%.

Combinando videomonitoramento e controle de acesso : Os usuários finais na América Central e Caribe estão mais entusiasmados com a unificação de videomonitoramento e controle de acesso do que outras regiões. Entre os usuários finais que possuem ambos os sistemas, 68% integram ou unificam essas soluções, enquanto globalmente, esse número é de 56%.

Foco na cybersecurity: Enquanto outras regiões priorizam o investimento em ferramentas relacionadas à cybersecurity, apenas 23% dos usuários finais nesta região indicaram que essas ferramentas serão um foco departamental em 2024, em comparação com a média global de 33%. No entanto, a região se destaca na educação dos usuários sobre as melhores práticas de cybersecurity, com 77% dos entrevistados relatando os esforços da sua organização nesta área, superando a média global de 61%.

Europa, Reino Unido, Oriente Médio e África (EMEA)

Migração mais lenta para a nuvem e atrasos em meio a conflitos globais

Transição para nuvem: Dados de pesquisa da EMEA indicaram que esta região é a mais lenta na migração para soluções hospedadas na nuvem. Um total de 62% dos parceiros de canal indicou que mais de ¼ dos novos sistemas que implantarão será nuvem ou nuvem híbrida nos próximos cinco anos, em comparação com a média global de 69%.

Retenção de talentos: Na EMEA, reter talentos é menos problemático que em outras regiões. Apenas 33% dos usuários finais afirmaram que a retenção de talentos foi um desafio em 2023, em oposição à média global de 39%.

Impacto dos conflitos globais: Mais usuários finais na EMEA (15%) citaram guerra ou conflito como a principal causa de atrasos nos projetos, excedendo significativamente a média global de 8%. Isto enfatiza a influência de fatores geopolíticos nos cronogramas dos projetos na região.

México

Resiliente aos problemas da supply chain e entusiasmado com a nuvem

Resiliência da supply chain: Os entrevistados do México demonstram uma resiliência notável na abordagem dos desafios da supply chain. Uma porcentagem mais baixa de usuários finais no México indicou que problemas na supply chain causaram atrasos de projetos em 2023 (27%) comparado à média global (42%). Isto sugere uma perspectiva mais otimista, apesar das preocupações globais.

Adoção da nuvem: Os entrevistados nesta região exibem um interesse mais acentuado em soluções de segurança hospedadas na nuvem do que outras regiões. 85% dos parceiros de canal antecipam um aumento no número de clientes usuários finais que adotam conectividade na nuvem para segurança em 2024, superando a média global de 74%.

Orçamentos operacionais estáveis: Menos usuários finais (15%) constataram aumento em seu orçamento OPEX em 2023 em comparação com a média global (29%). Adicionalmente, mais usuários finais desta região (47%) preveem um orçamento OPEX consistente em 2024, excedendo a taxa global (35%).

Prioridades de cybersecurity: Ao contrário de outras regiões que estão colocando foco em fortalecer sua estratégia de segurança, os entrevistados do México se destacam com uma porcentagem menor de usuários finais (19%) que priorizam ferramentas relacionadas à cybersecurity em seu foco departamental em 2024, em comparação com a média global (33%).

América do Sul

Crescimento da nuvem, contínuas incertezas econômicas e de RH

Crescimento da nuvem: Entrevistados da América do Sul têm uma visão otimista sobre a tecnologia de nuvem em sua região. Uma porcentagem maior dos parceiros de canal (83%) esperam um aumento na adoção de sistemas de segurança conectados à nuvem em 2024, superando a média global (72%). Quanto aos usuários finais, uma porcentagem mais baixa indicou que mais de 25% do ambiente de segurança física da sua organização é nuvem ou nuvem híbrida (29%) do que globalmente (44%).

Desafios de recursos humanos: Parceiros de canal estão particularmente preocupados com os desafios com pessoal , com 83% esperando que este problema aumente, em comparação com a média global de 70%.

Supply chain: Menos usuários finais na América do Sul (30%) enfrentaram atrasos em projetos devido a problemas na supply chain em 2023, em comparação com a média global (42%). Por outro lado, mais parceiros de canal na América do Sul (51%) esperam que os preços caiam um pouco à medida que os problemas da supply chain melhorarem em 2024, enquanto, globalmente, menos de 39% indicaram o mesmo.

Atrasos no orçamento e projetos: Apenas 15% dos usuários finais relataram orçamentos mais altos para 2023, isso é menos que a média global de 29%. Os atrasos nos projectos devem-se principalmente a incertezas econômicas (70%) e políticas (36%), que são superiores às médias globais (57% e 25%, respectivamente). Além disso, incertezas econômicas e inflação são percebidas como potenciais culpadas pelos atrasos nos projetos em 2024, com 59% dos parceiros de canal na América do Sul demonstrando preocupação em comparação com a média global de 48%.

Abordagem de cybersecurity: A América do Sul leva a cybersecurity a sério, mas surpreendentemente apenas 35% dos usuários finais identificaram o reforço da infraestrutura de segurança como uma abordagem específica adotada pelas suas organizações, em contraste com a média global de 47%.

EUA e Canadá

Adoção da nuvem e desafios da supply chain

Conectividade na nuvem: Parceiros de canal nos EUA e Canadá estão à frente da curva quando se trata da adoção da nuvem, com 61% deles relatando que mais de um quarto dos seus clientes usuários finais existentes permitem conectividade na nuvem para fins de segurança. Esse percentual supera a média global de 49%.

Desafios de RH: Ao contrário da tendência global onde desafios de RH, como treinamento e qualificação são comuns, apenas 36% dos usuários finais nos EUA e Canadá identificaram este tópico como problemas nos seus departamentos. Esse percentual é inferior à média global de 46%.

Problemas da supply chain: Atrasos em projetos devido a problemas na supply chain são uma questão maior nos EUA e Canadá, com 55% dos usuários finais envolvidos. Globalmente, uma porcentagem mais baixa (42%) enfrentou estes atrasos.

Apêndice

Apêndice 1 – Metodologia da pesquisa

A Genetec Inc. entrevistou profissionais de segurança física entre 21 de agosto a 15 de setembro de 2023.

O objetivo da pesquisa foi:

- obter uma visão das operações de segurança física e ambientes
- entender a resposta das organizações a desafios externos, como ameaças cibernéticas e dificuldades de RH
- entenda o foco global para 2024

Após uma análise das entrevistas e filtragem de dados, 5.554 entrevistados foram incluídos na amostra para análise.

Detalhes sobre a pesquisa e análise

- A população-alvo da pesquisa concentrou-se em indivíduos que trabalham para organizações que participam de aquisições, gerenciamento, serviços e/ou uso de tecnologia para segurança física. A população-alvo incluía usuários finais da Genetec, bem como participantes alcançados por meio de publicidade digital ou contactados diretamente por terceiros através de suas listas de e-mail opt-in.
- Os convites para responder à pesquisa on-line foram enviados aos potenciais participantes por e-mail em inglês, francês, alemão, holandês, italiano, espanhol, português, japonês e coreano.
- O formulário de pesquisa on-line estava disponível em inglês, francês, alemão, holandês, italiano, espanhol, português, japonês e coreano.
- Somente pesquisas totalmente preenchidas enviadas por indivíduos da população-alvo para a pesquisa foram incluídos na análise final.
- As amostras da pesquisa foram realizadas em todas as regiões, incluindo EUA e Canadá, México, América Central, Caribe, América do Sul, Europa, Reino Unido, Oriente Médio, África, Leste Asiático, Sul da Ásia, Sudeste Asiático, Ásia Central, Ásia Ocidental e Austrália-Nova Zelândia.
- As taxas de resposta e taxas de conclusão da pesquisa variaram por região e por tamanho da organização, potencialmente introduzindo erros de amostragem em conjuntos de subamostras.
- As respostas foram coletadas de duas populações-alvo principais: usuários finais de segurança física e parceiros de canal, instaladores, fabricantes, integradores de sistemas, fornecedores. A filtragem de dados foi realizada para validar a classificação do entrevistado em um desses dois públicos e limitar possíveis erros. Presume-se que quaisquer erros não relacionados com a amostragem resultam da recolha de dados fora da população-alvo (por exemplo, indivíduos que se identificam incorretamente como usuários finais quando, na verdade, são colaboradores tais como parceiros de canal).

Uma observação sobre cálculos de pesquisa

Devido ao arredondamento e estrutura da pesquisa (incluindo escala de classificação, selecione todas as opções aplicáveis e questões de múltipla escolha), nem todos os percentuais totais neste relatório serão iguais a 100%. Para todas as perguntas aplicáveis (onde os entrevistados podem escolher várias respostas), as porcentagens referem-se à proporção de entrevistados que escolheram a resposta individual.

Apêndice 2 – Informações demográficas da pesquisa

A Genetec Inc. entrevistou profissionais de segurança física entre 21 de agosto a 15 de setembro de 2023.

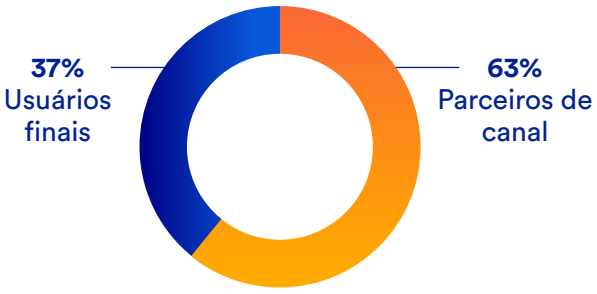
Indústrias

Parceiros de canal (Parceiros de canal, instaladores, fabricantes e consultores)	63%
Industrial e fabricação	6%
Energia, serviços públicos e telecomunicações	4%
Educação	4%
Transporte	3%
Saúde	3%
Outro	2%
Serviços Profissionais e Associações	2%
Banco e finanças	2%
Governo Federal/Nacional	2%
Esportes, jogos e hospitalidade	2%
Varejo	2%
Governo Estadual/Local	2%
Serviços de emergência, justiça e segurança pública	1%
Serviços de Sistemas de Segurança	1%
Trânsito e estacionamento	1%
Cannabis	0%

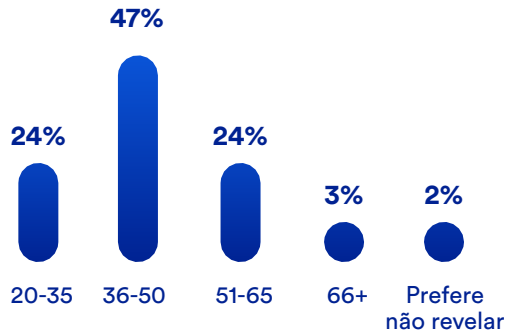
Funções de trabalho

Engenharia, P&D, Projeto de Sistema	15%
Segurança e Proteção	13%
Tecnologia da Informação (TI)	12%
Vendas	10%
Administração/Administração de Escritórios	8%
Gerenciamento de operações	7%
Gerenciamento de projetos/Gerenciamento de riscos	7%
Atendimento ao cliente ou suporte (suporte técnico)	6%
Gerenciamento de instalações/operações	6%
administrativo/jurídico	4%
Contabilidade/Finanças	4%
Marketing	3%
Gestão da Qualidade	2%
Estimativa	2%
Compras e aquisição	1%
Jurídico	1%

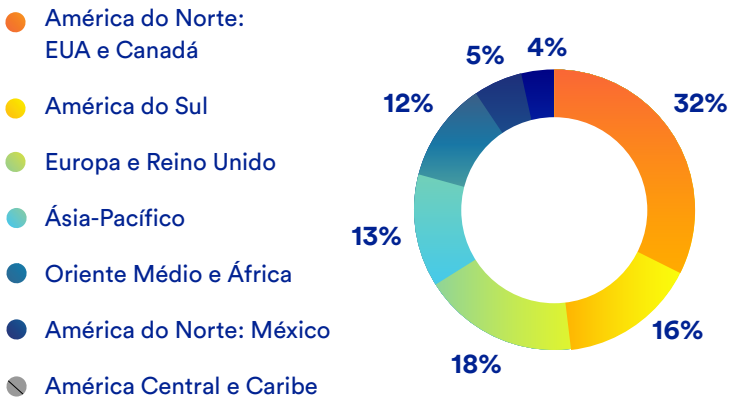
Tipo de entrevistado



Faixa etária do entrevistado



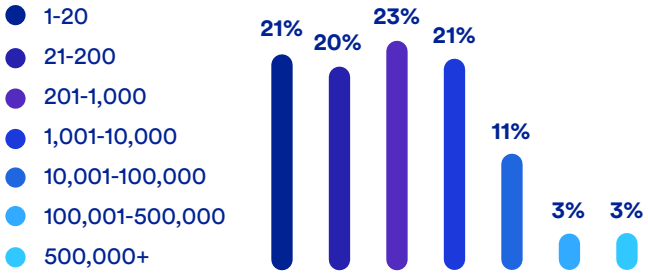
Regiões geográficas



Receita organizacional (usuários finais) (USD)

USD 500 mil a USD 4,9M	17%
USD 5M a 24,9M	10%
USD 25M a 199,9M	10%
USD 200M a 499,9M	8%
USD 500M a 999,9M	6%
USD 1B-10B	7%
USD 10B +	5%
Não é possível revelar	38%

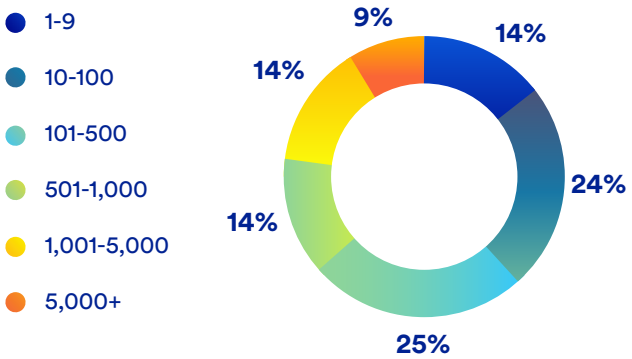
Organização global contagem de colaboradores (usuários finais)



Departamento de segurança física contagem de colaboradores

1-20 colab.	50%
21-200 colab.	32%
201-1.000 colab.	11%
1.001-10.000 colab.	5%
Mais de 10.000 colab.	2%

Implantação de videomonitoramento (nº de câmeras) (usuários finais)



Implantação de controle de acesso (# de crachás ou leitores de acesso sem atrito) (usuários finais)

20 port. cartão	13%
21-50 port. cartão	8%
51-100 port. cartão	6%
101-500 port. cartão	16%
501-1.000 port. cartão	10%
Acima 1.001 port. cartão	35%
Nenhuma das acima/NA	11%

Apêndice 3 – Comentários abertos

Os participantes da pesquisa puderam fornecer comentários adicionais associados a algumas perguntas da pesquisa. A seguir estão as respostas selecionadas que são representativas das impressões gerais:

Usuários finais: C02. Que tecnologia você implantou no ambiente de segurança física da sua organização? Outros, explique:

- Analíticos de áudio
- Recuperação de desastres e tecnologia de resposta a emergências
- Drones
- Detecção de disparos
- Câmeras térmicas portáteis
- Tecnologia de saúde e segurança
- Sistema de gerenciamento de chaves
- Magnetômetros
- Botões de pânico
- Sistema de gestão de consciência situacional
- Gerenciamento de ameaças
- Sistema de escaneamento por baixo de veículos
- Detecção de armas/explosivos
- Sistema meteorológico
- Triagem por raios X

Parceiros de canal: CA04. Que tipo de tecnologia de segurança física sua organização instala/implanta com mais frequência?

Outros, explique:

- Portões automáticos e sistema de estacionamento, raio X e sistema de detecção de metais
- Projeto de explosão e HVM
- Gestão de valores monetários em trânsito
- Escaneamento de itens enviados via correios, detecção de disparos, notificação de emergência em massa
- Infraestruturas de rádio profissionais
- Controle de temperatura através de câmeras térmicas

Usuários finais: C07. Como está estruturada a infraestrutura de segurança física da sua organização?

Outro (por favor, especifique:

- Monitoramento local no TOC - Centro de Operações de Tráfego
- Monitoramento local pela equipe de vigilância, alguma capacidade de monitoramento remoto
- Monitoramento local de todas as câmeras por departamento
- Monitoramento da vigilância pela polícia local
- Ninguém está no comando, as pessoas que perceberem uma intrusão poderão investigar se tiverem tempo para isso
- Botões de pânico
- Capacidade de reagir com pouco ou nenhum monitoramento
- Estamos explorando o monitoramento remoto através de uma empresa terceirizada de monitoramento de alarmes

Usuários finais H03. Que tipo de dados você está coletando em seu centro de operações de segurança (SOC) de outros sistemas?

Outros, explique:

- Atividades de jogos de cassino
- Dados relacionados ao crime são coletados
- Dados de crimes por local
- Gerenciamento de estacionamento
- Informações do paciente, resultados laboratoriais, imagens (ultrassom, raio-X, tomografia computadorizada etc.)
- Segurança em viagens - informações ao passageiro

Parceiros de canal: CE07. Outras operações serão impactadas pelo trabalho em sua lista de pendências para implantação?

- (A pergunta anterior mencionava as seguintes operações: Venda de novos sistemas, vendas de renovação de serviços, capacidade de se manter atualizado com a inovação da indústria)
- Faturamento e cobrança
- Correções de bugs
- Cybersecurity
- Tempos de entrega
- Nova contratação
- Treinamento de pessoal (Vendas e Parte Técnica)
- Teste e garantia de qualidade: pendências de implantação podem ter impacto nos processos de teste e garantia de qualidade
- Nuvem

Usuários finais: D09. Alguma outra coisa retardou a adoção de soluções hospedadas na nuvem para aplicações de segurança física por parte de sua empresa?

- Questões de clareza por parte do Governo
- Problemas de compliance relativas à nuvem na organização
- Instalação de fibra pelo prestador de serviço
- Falta de confiança na continuidade e qualidade dos serviços dos fornecedores de Internet
- Capacidade da infraestrutura de rede para suportar armazenamento na nuvem
- Não há desejo de transferir nada para a nuvem visando segurança física.
- A otimização de nossos protocolos de segurança com a nuvem às vezes leva mais tempo do que o esperado para parear e permanecer atualizado
- Cultura organizacional
- Nossa universidade é muito bem preparada e tende a não tomar decisões até que seja absolutamente necessário.
- Preferem segurança local
- Redundância em caso de falha ou perda de comunicação
- Estamos trabalhando ativamente para sair da nuvem e retornar a uma solução in loco

Parceiros de canal: CC08. Alguma coisa tem retardado a adoção de soluções hospedadas na nuvem?

- Atitudes em relação aos modelos de custo OpEx e custo fixo.
- Os benchmarks não são usados para equilibrar dados entre plataformas
- Políticas complexas de retenção de dados (propriedade e armazenamento de dados para Microsoft/Google/AWS etc.), sem compromissos rígidos, governos e objetos de alto risco ainda não migrarão para a nuvem em breve. Também as condições de infraestrutura (por exemplo, fibra) nos países locais desempenham um papel
- Profissionais de segurança pública com mentalidade conservadora e que desejam manter o controle de seus dados
- Cliente dependendo das variações de preço do hospedeiro. Cliente refém do aumento

progressivo de preços.

- Falta de conhecimento e educação na nuvem
- A maioria dos nossos clientes simplesmente não precisa dos recursos que ele oferece
- Despesas OpEX vs CapEX; falta de clareza sobre interrupções na Internet
- Algumas organizações possuem um grande número de sistemas e aplicações tradicionais, e integrá-los à nuvem pode ser complexo, o que pode retardar a adoção de soluções na nuvem.

Usuários finais: D13. Alguma outra coisa levou sua organização a começar a usar a nuvem para aplicações de segurança física?

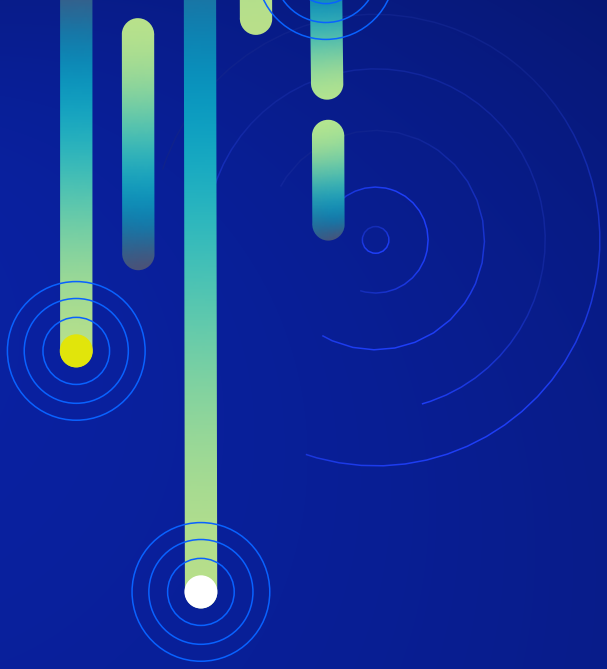
- Como os hackers manipulam os sistemas, nos deparamos com poucas intrusões as quais não conseguimos monitorar... como agora temos vigilância hospedada na nuvem, é mais fácil mantê-la a salvo e segura.
- Ao utilizar soluções na nuvem, podemos aproveitar a experiência das equipes profissionais dos provedores de serviços na nuvem para monitorar e manter nossos aplicações de segurança física, aliviando assim a carga sobre nossas equipes internas.
- As plataformas na nuvem facilitam a colaboração e o compartilhamento de informações, permitindo que as equipes de segurança colaborem de forma mais eficaz no tratamento de incidentes e ameaças de segurança.
- Os provedores de nuvem normalmente possuem equipes de segurança dedicadas, mais bem equipadas para lidar com possíveis riscos de segurança, reduzindo assim minha exposição a riscos.
- Economia de custos ao não precisar implantar redes corporativas em alguns sites de médio porte
- Elimine servidores físicos
- Em um ambiente de nuvem, você pode obter uma rápida recuperação de desastres, permitindo a rápida restauração das operações normais, mesmo em casos de falhas ou perda de dados.
- O restante da empresa está migrando para a nuvem
- O armazenamento na nuvem mais rápido!
- Atualização e escalabilidade
- Podemos aproveitar a experiência das equipes profissionais dos provedores de serviços na nuvem para monitorar e manter nossas aplicações de segurança física, aliviando assim a carga sobre nossas equipes internas.

Parceiros de canal: CC06. Existem outros fatores que fazem com que os usuários finais comecem a considerar o uso da nuvem?

- Capacidades adicionais que evoluem com o tempo
- Suporte de IA, aprendizado de máquina e velocidade de (novos) desenvolvimentos tecnológicos na nuvem
- Permanece sempre operacional. Nenhum dado de hardware inteligente que possa ser perdido.
- Cópias de backup para ransomware
- Consegue analisar informações de qualquer lugar e não apenas fisicamente como antes.
- Melhor ROI e baixo CAPEX
- Gerenciamento centralizado de casos e evidências
- A computação na nuvem permite que os usuários aumentem ou reduzam facilmente seus recursos conforme necessário. Isto é especialmente importante para empresas que enfrentam um rápido crescimento ou uma procura flutuante.
- Os provedores de nuvem oferecem serviços de IA e aprendizado de máquina que permitem aos

usuários desenvolver e implantar aplicações orientadas por IA sem a necessidade de amplo conhecimento nessas áreas.

- Provedores de segurança na nuvem podem oferecer ferramentas e recursos que ajudam as organizações a cumprir com regulamentos específicos do setor e requisitos de proteção de dados.
- Os provedores de segurança na nuvem geralmente possuem conhecimentos especializados e recursos dedicados à segurança, o que pode ser benéfico para organizações que não possuem conhecimentos internos de segurança.
- As soluções de segurança na nuvem podem ajudar a garantir a segurança do acesso remoto.
- As soluções de segurança na nuvem podem fornecer recursos robustos de continuidade de negócios e recuperação de desastres, garantindo a disponibilidade de dados e sistemas.
- As soluções de segurança na nuvem normalmente exibem um alto grau de escalabilidade, permitindo rápida expansão ou contração conforme os requisitos. Esta capacidade é particularmente vital para lidar com as flutuações dos negócios.
- Exagero com tecnologia na nuvem
- As plataformas de segurança na nuvem geralmente fornecem acesso à inteligência e análise de ameaças em tempo real, permitindo que as organizações permaneçam à frente de ameaças e vulnerabilidades emergentes.
- As soluções de segurança hospedadas na nuvem podem oferecer recursos robustos de recuperação de desastres, garantindo que os dados e os sistemas não dependam de HDs físicos que podem ser roubados
- Não querem manter servidores
- Mais verde
- No longo prazo você só paga pelo que usa e precisa
- Inovação e tempo de colocação no mercado: A computação na nuvem fornece uma plataforma para desenvolver e implementar rapidamente novas aplicações e serviços. Ela permite que as organizações experimentem, inovem e coloquem produtos no mercado com mais rapidez.
- IOT e dispositivo de hardware não são totalmente compatíveis com a nuvem
- A migração de um ambiente de escritório completo para a nuvem, os sistemas de recomendação devem então vir junto. Não há mais servidores in loco.
- Modelo OPEX preferido
- O roubo ou manipulação do gravador CCTV, permitindo ter o backup na nuvem e não local



Sobre a Genetec

A Genetec Inc. é uma empresa de tecnologia inovadora com um amplo portfólio de soluções de segurança física. O principal produto da empresa, Security Center, é uma plataforma de arquitetura aberta que unifica videomonitoramento IP, controle de acesso , reconhecimento automático de placas de veículos (ALPR), comunicações e analíticos. A Genetec também desenvolve soluções e serviços hospedados na nuvem projetados para melhorar a segurança e contribuir com novos níveis de inteligência operacional para governos, empresas, transportes e comunidades em que vivemos. Fundada em 1997 e sediada em Montreal, QC, Canadá, a Genetec atende seus clientes globais por meio de uma extensa rede de revendedores, integradores, parceiros de canal certificados e consultores em mais de 159 países.

Para saber mais sobre nós, acesse **genetec.com/br**

Para mais informações sobre este relatório,
entre em contato com Genetec-research@genetec.com

Genetec Inc.
genetec.com/br/fale-conosco
info@genetec.com
@genetec