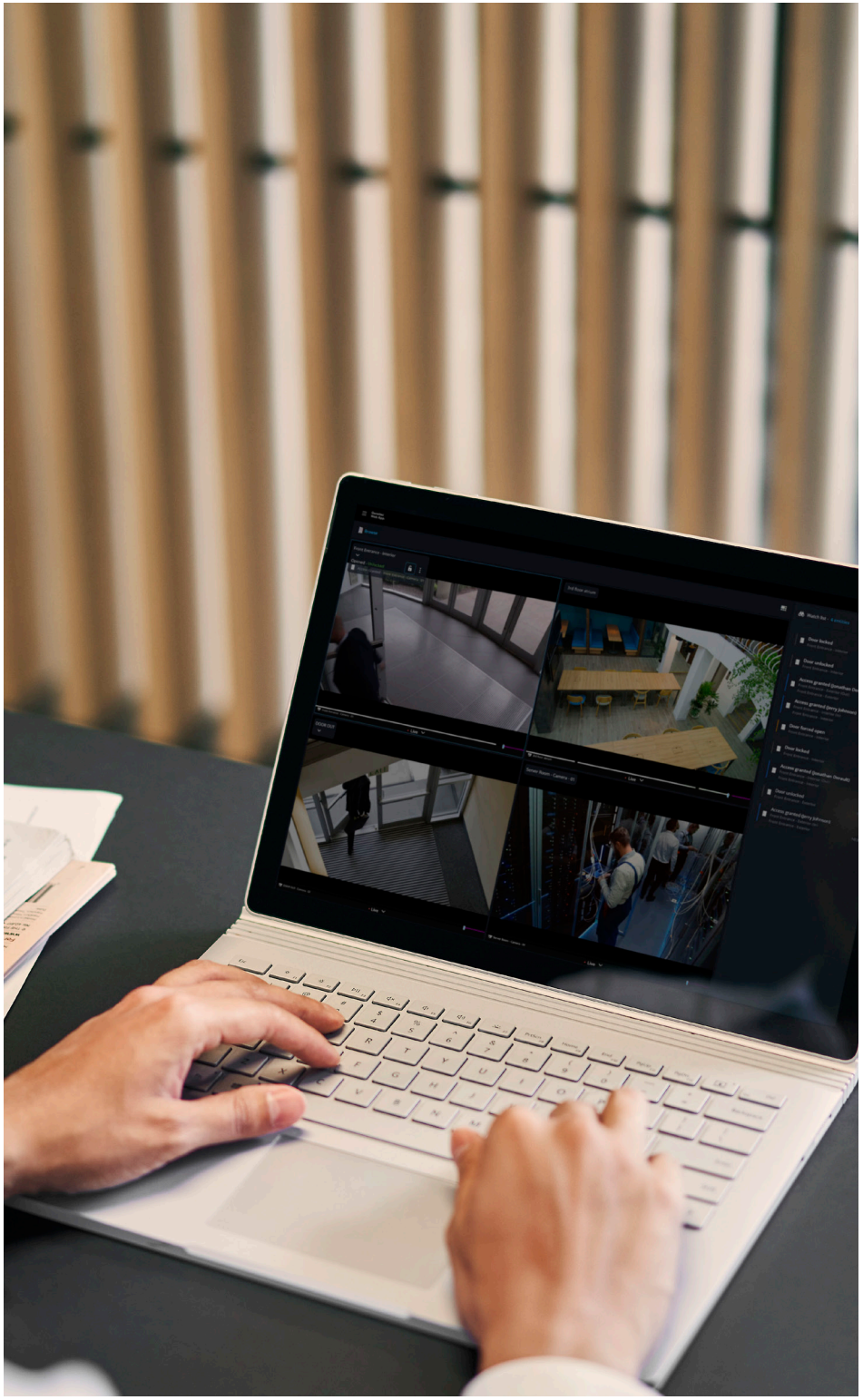
Como implementar uma estratégia de segurança física com privacidade em mente

Seu guia para proteger colaboradores, ativos e dados com Privacidade por Design

Genetec™



Um olhar por dentro

"As organizações jamais devem ter que escolher entre proteger a privacidade dos indivíduos e sua segurança física"

–Pierre Racz
Presidente da Genetec

O papel da privacidade na segurança física

As pessoas se preocupam imensamente com a privacidade de suas informações pessoais. Uma pesquisa de 2021 encomendada pelo Office of the Privacy Commissioner of Canada constatou que nove em cada dez pessoas estavam preocupadas em proteger sua privacidade, enquanto quatro em cada dez encerraram a relação comercial com alguma empresa devido a questões de privacidade.

Embora possa parecer que a segurança pública e a privacidade pessoal estão inerentemente em desacordo, não precisa ser assim. Ao dar mais controle sobre a coleta de dados pessoais às pessoas, os especialistas em privacidade dizem que elas ficam mais dispostas a aceitar.
Os consumidores também são mais propensos a confiar em empresas que limitam o uso de seus dados e respondem de forma rápida, pública e proativa a ameaças como violações ou hacks.

Neste e-book, descreveremos as etapas práticas que você pode seguir para diminuir as preocupações com a privacidade, incluindo:

Garantir que seus dados de segurança física gerenciados, transmitidos e armazenados por seus sistemas de segurança estejam em compliance com os padrões da indústria e do governo

Escolher produtos de segurança que oferecem total controle e visibilidade sobre quem pode e tem acesso aos seus dados

Implementar medidas e ferramentas de anonimização em vídeo para compartilhar dados digitais de forma segura

75%

dos clientes associam fortemente privacidade com confiança

Fonte: Salesforce

137

países já têm legislação para garantir a proteção de dados e privacidade

Fonte: UNCTAD

Manter-se atualizado com as regulamentações de privacidade

A maioria dos sistemas de segurança de hoje pode não atender aos requisitos de privacidade de amanhã - é com essa mesma frequência que eles mudam.

Nos últimos anos, os governos em todo o mundo introduziram novos regulamentos para priorizar os direitos de privacidade e garantir que os dados pessoais sejam coletados e gerenciados com a privacidade em mente.

Dependendo de onde você faz negócios e da confidencialidade das informações privadas que está coletando, pode ser necessário nomear um especialista de proteção de dados (DPO) para garantir compliance com as leis de privacidade.

Um DPO também vai supervisionar processos, procedimentos e políticas internas para proteger dados, anonimizar informações e responder a violações e solicitações dos cidadãos. Por fim, um DPO criará e manterá a documentação de todas essas etapas.

"No meu universo, quando se trata de, digamos, privacidade versus segurança pública, posso garantir que nunca é a privacidade que vence, nem deveria ser. Mas o que eu rejeito é a proposição de que a privacidade deve ser sacrificada."

– Dra. Ann Cavoukian
Autora e ex-Comissária de Privacidade e Informação da província de Ontário

Privacidade por Design

O futuro da privacidade não é apenas cumprir a legislação governamental. Deve vir no modo de operação padrão de uma organização. Se estiver adquirindo uma nova solução de segurança física, considere aquelas que vêm com privacidade incorporada desde o início.

Na década de 1990, a Dra. Ann Cavoukian desenvolveu a estrutura Privacy by Design para orientar os desenvolvedores de aplicações a colocar a privacidade no centro de suas operações. Desde então, isso se tornou um guia básico de melhores práticas para organizações de todos os tipos e tamanhos.

As metodologias Privacidade por Design foram inicialmente desenvolvidas de modo a fornecer um roteiro essencial para desenvolvedores éticos e com visão de futuro para incorporar esses princípios em seus produtos. Isso envolveu a inclusão proativa de privacidade no design e operação de sistemas de TI, infraestrutura de rede e práticas de negócios desde a primeira linha de código até os fornecedores terceirizados selecionados para parceria e integração.

Mas isso não é apenas uma ideia importante para pessoas que escrevem código de software. Com a tecnologia agora incorporada em quase todos os aspectos da vida, a estrutura Privacidade por Design é relevante para organizações de todos os tipos e tamanhos.

Quando a proteção da privacidade passa a ser um dos valores fundamentais da sua organização, ela se torna perfeitamente incorporada a todas as suas operações, desde como seu software é codificado até hábitos e rotinas diárias de seus colaboradores.

> Respeitar o direito à privacidade é um ganha-ganha. Isso gera confiança entre as pessoas que você serve, aumentando as chances de que elas aceitem as políticas de permissão para acessar dados quando houver necessidade de coletar informações pessoais.

Avaliando sua infraestrutura de segurança física atual

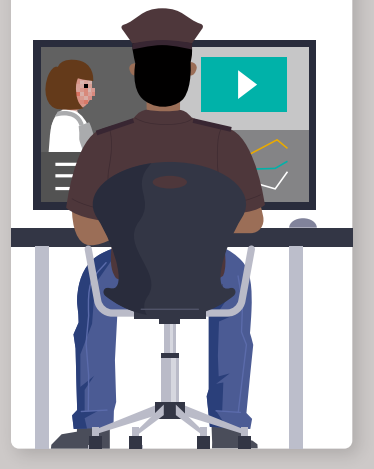
Equipamentos de segurança legados ou sistemas proprietários mais antigos podem não oferecer suporte total aos fundamentos da Privacidade por Design. As capacidades e integrações limitadas de um sistema criam situações em que você pode não obter total compliance com a privacidade.

Escolher uma solução criada com Privacidade por Design é um passo em direção a um compliance legislativo mais forte. Uma solução específica e voltada para a privacidade permite que as empresas evoluam suas operações de segurança para adicionar camadas de privacidade e proteção de dados.

Como a privacidade e cybersecurity estão inter-relacionadas, aqui estão 5 perguntas importantes a se fazer:

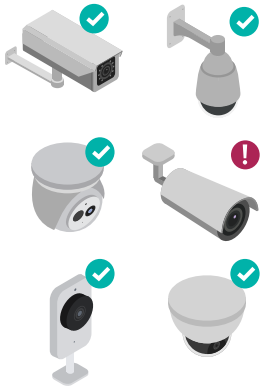
1

Como posso compartilhar vídeos e proteger a privacidade individual?



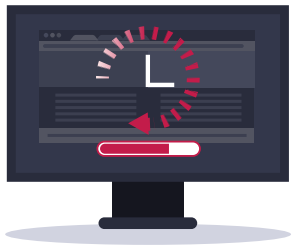
2

Posso proteger várias câmeras interconectadas para reduzir as ameaças cibernéticas?



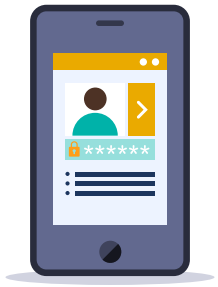
3

Como faço para minimizar o tempo gasto com atualizações de software em várias plataformas?



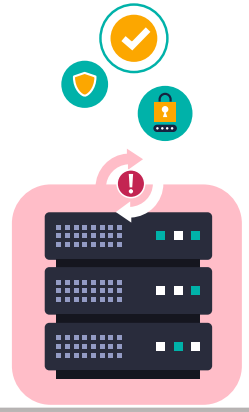
4

As políticas de higiene cibernética são mantidas com várias camadas de autorização, tornando o login eficiente para todos os meus usuários?



5

Meus sistemas estão muito desatualizados para suportar as políticas de criptografia e cybersecurity mais recentes?



Construindo uma abordagem holística para a privacidade

Quando se trata de proteger nossos dados, não podemos nos concentrar apenas nas ameaças externas. Com a maior integração entre sistemas e colaboração em equipe, mais entidades do que nunca interagem com nossos sistemas de segurança e acessam dados confidenciais.

Além de proteger o acesso por meio de mecanismos de autenticação adequados, devemos garantir que as políticas internas de negócios limitem quem vê dados confidenciais e restringe o que podem fazer com eles.

"Como sociedade, a invasão de privacidade oferece muito pouco e nos custa muito. Na Genetec, fazemos nosso trabalho criando ferramentas que a sociedade precisa, mas o mais importante, criamos essas ferramentas com base no contrato social das sociedades em que atuamos".

–Pierre Racz
Presidente da Genetec

Colete e armazene apenas os dados necessários

Com a variedade estonteante de sensores, câmeras e outros dispositivos disponíveis, é possível coletar uma quantidade considerável de dados. Mas você precisa de todas essas informações ao seu alcance? Limitar os dados que você coleta e armazena apenas ao necessário reduz sua exposição ao risco em caso de violação de dados e facilita o monitoramento do que é mais importante.

Por exemplo, se considerar ajustar o campo de visão de uma câmera para que não registre as workstations dos colaboradores? Implementando máscaras de privacidade estáticas ou dinâmicas, permitirá capturar as imagens necessárias enquanto anonimiza partes dessas imagens.

Ao armazenar imagens de videomonitoramento, considere quanto tempo você precisa manter as informações pessoais em arquivo. Defina protocolos para arquivar ou excluir dados automaticamente com base em sua relevância.

Para proteger os dados, os administradores devem ser capazes de implementar privilégios de acesso de usuário detalhados, selecionar as informações que podem ser compartilhadas com parceiros e autoridades e controlar por quanto tempo os dados ficam guardados.

Limite o acesso a dados confidenciais com base na necessidade de conhecimento

O acesso aos dados pessoais só deve ser concedido a quem deles necessite para fazer seu trabalho, tendo em mente que seu acesso e atividades também devem ser monitorados de perto para garantir que os dados sejam usados conforme intencionado. Isso envolve a autenticação adequada de usuários, grupos de usuários e a limitação dos direitos de acesso a servidores, workstations, sites ou aplicações específicas combase na necessidade.

Permissões e privilégios precisarão mudar à medida que as funções e responsabilidades evoluírem. É importante revisar+ os direitos de acesso periodicamente para se manter alinhado com os requisitos do usuário. Isso reduzirá efetivamente o risco de acesso não autorizado a informação privada.

Para eliminar ainda mais o erro humano, as organizações podem usar um provedor de identidade, como o Microsoft Active Directory, para adicionar e remover automaticamente contas de usuário de segurança, conceder direitos de acesso ou remover usuários quando eles não estiverem mais trabalhando com a organização.

Anonimização automática da coleta de dados

Proteger pessoas e ativos no setor de segurança física geralmente exige que as organizações coletem dados pessoais. Mas para atender às expectativas de privacidade do público e cumprir os regulamentos globais, o acesso a esses dados ou imagens precisa ser restrito e protegido.

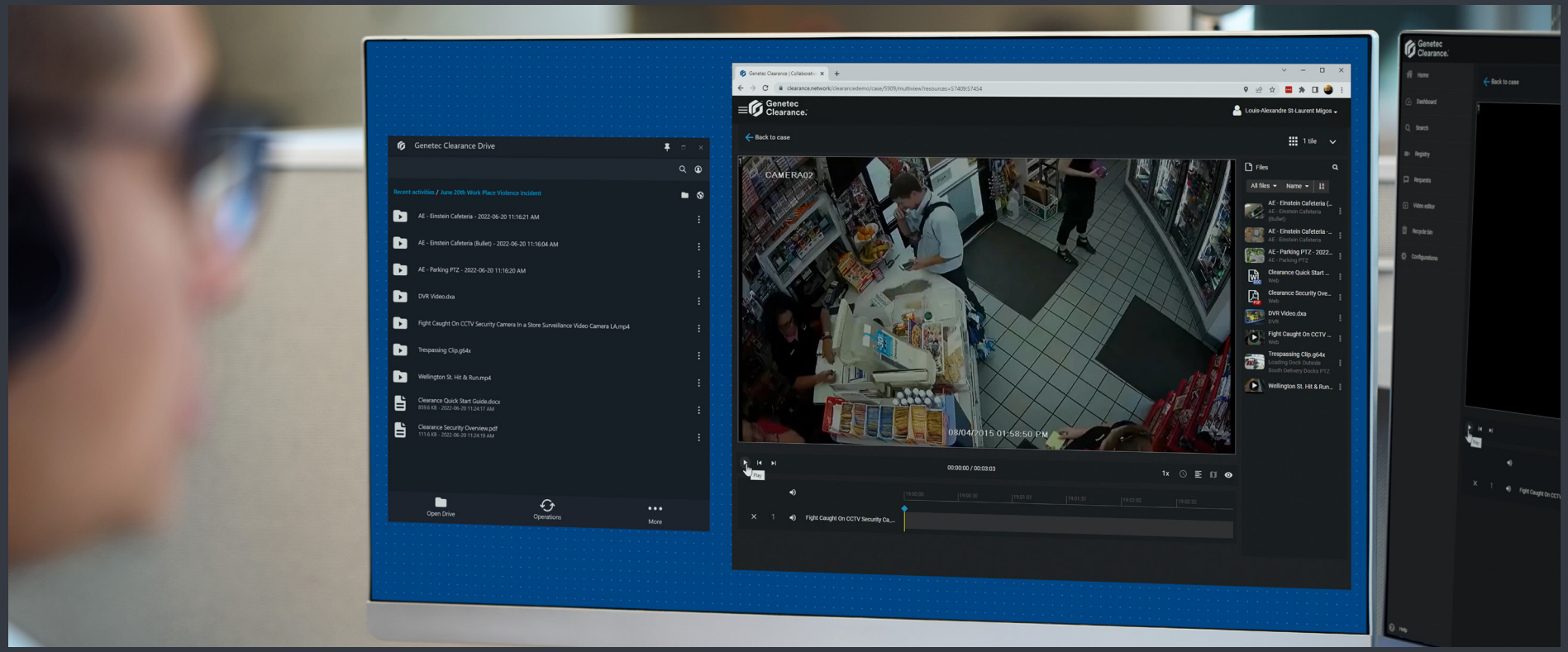
Com a ajuda de novas tecnologias que anonimizam os dados coletados, agora é possível coletar dados granulares desta forma, sem comprometer a privacidade individual.

Especificamente para aplicações de videomonitoramento, uma dessas camadas que deve considerar é a máscara de privacidade para ocultar ou anonimizar uma parte do vídeo, seja ao vivo ou gravado. Também pode encobrir parte de uma área. Isso permite a seus operadores inspecionar ativamente o ambiente, respeitando a privacidade individual.

On-demand para a plataforma unificada Genetec™ Security Center, o Proteção de Privacidade KiwiVision™ oculta automaticamente os rostos dos indivíduos captados no campo de visão de uma câmera para que os operadores de segurança vejam apenas o que precisam ver. O acesso a imagens não ocultas requer uma camada adicional de permissões de acesso que é usada apenas quando um evento justifica tal investigação. Uma trilha de auditoria é mantida, mostrando quem acessou as informações adicionais e por quê.

"Proteger a identidade das pessoas registradas em vídeo é essencial para proteger sua privacidade. O fato do Proteção de Privacidade KiwiVision ter sido certificado pelo EuroPriSe por mais de uma década é uma prova da criatividade dos engenheiros em fornecer tecnologia avançada de segurança física que pode atender aos principais padrões de privacidade de operação, permitindo que os usuários cumpram as regulamentações."

–Florian Matusek
Diretor do Grupo de Produtos Genetec



Proteja a privacidade ao compartilhar informações

Assim como garantir o anonimato de pessoas captadas em vídeos de segurança é essencial para proteger sua privacidade, a capacidade de compartilhar com segurança informações durante as investigações também é fundamental para proteger a integridade dos dados e a privacidade dos indivíduos.

O sistema de gerenciamento de evidências digitais Genetec Clearance™, permite que as organizações reúnam e compartilhem evidências confiáveis que protegem a privacidade de todos. Com a edição de vídeo integrada e o gerenciamento seguro de usuário, a identidade de vítimas, transeuntes, testemunhas e policiais permanecerá protegida.

O Genetec Clearance ajuda os usuários finais a definir quem tem acesso a dados e filmagens confidenciais sem retardar as investigações e a resposta a incidentes. Dessa forma, os usuários finais têm controle sobre esses dados para que possam adequar métodos e processos de proteção para cumprir a legislação de privacidade em todo o mundo.

Unificação: uma estratégia bem-sucedida de proteção de dados e privacidade

Uma abordagem de segurança física unificada pode ser um divisor de águas para sua estratégia de proteção de dados. Veja como:

Proteção de privacidade centralizada poupa tempo

Quando todos os seus sistemas estiverem em uma única plataforma, não precisará perder tempo alternando entre diferentes fontes para garantir a higiene cibernética ou acompanhar o status de integridade de todos os seus sistemas e dispositivos. Em vez disso, poderá manter o controle dos dados de todos os seus sistemas por meio de uma única interface.

Medidas de privacidade integradas agiliza processos

Ferramentas e serviços unificados alertam sobre vulnerabilidades em potencial e ajudam a agilizar as atualizações. Outros recursos ajudam a restringir o acesso ao sistema e os privilégios do usuário e fornecem pontuações de segurança para garantir que você obtenha a resiliência do sistema em escala total.

A flexibilidade ajuda a adaptar os dados métodos de proteção

As leis de privacidade estão em constante mudança e sua equipe precisa acompanhar a evolução das ameaças. Com uma plataforma de segurança flexível, você pode ajustar métodos e processos de proteção de dados para reforçar a confidencialidade e integridade do sistema para permanecer em compliance por muitos anos à frente.

TEXAS A&M UNIVERSITY

"Faço parte do comitê de Tecnologia de Vigilância Audiovisual (AVST). Somos responsáveis por estabelecer diretrizes para locais autorizados para câmeras, quem pode visualizá-las e os motivos pelos quais as câmeras podem ser autorizadas para uso. O Security Center fornece privilégios de usuário granulares, direitos de acesso e autorizações. Ele oferece muitas ferramentas integradas que dão suporte aos nossos esforços de privacidade, permitindo-nos manter facilmente o controle e o equilíbrio de nossas operações."

–Dell Hamilton
Gerente de Serviços de Transporte,
Texas A&M University

LEE HEALTH
Caring People. Inspiring Health.

"Uma coisa com a qual nos debatemos é 'o que fazemos com todos esses vídeos? E como fazer com que estes vídeos cheguem aos nossos parceiros de negócios relevantes?' O Genetec Clearance nos permite determinar o armazenamento para cada incidente que acontece dentro da organização. Portanto, se for um evento de queda por escorregão ou tropeço, definiremos um tempo mínimo de retenção para esse vídeo dentro do Clearance. Ele atua como nosso repositório central para todos os arquivos de vídeo de longo prazo. Podemos então compartilhar facilmente os vídeos com nossas equipes internas ou agências externas de forma segura e eficiente".

–Sean Owens
Diretor de Tecnologia de Segurança e Cuidados Não Agudos,
Lee Health

cytiva

"No passado, precisávamos conceder acesso aos nossos sistemas de segurança física a mais pessoas para atender a essas solicitações de acesso. Como os fluxos de trabalho de provisionamento são todos automatizados no ClearID agora, conseguimos restringir o acesso à aplicação a um grupo muito limitado de usuários do sistema. Isso torna nossas operações de segurança muito mais seguras e resilientes."

–Larry Allen
Administrador Técnico de Produto para Instalações, Segurança e Gerenciamento de Crises,
Cytiva

Mais de 42.500 clientes escolheram a Genetec para proteger seu dia a dia, saiba mais sobre suas histórias.

Por que selecionar os fornecedores certos é fundamental

O mais alto nível de proteção de privacidade e resiliência contra ameaças cibernéticas não se alcança sozinho. Acontece quando todos os envolvidos se comprometem com as melhores práticas. Isso requer a avaliação de sua supply chain, incluindo todos os fornecedores que compõem sua infraestrutura de segurança física, para entender em profundidade suas políticas de proteção de dados e privacidade.

Aqui estão cinco qualidades para buscar em seus fornecedores:

1. **Identificação e mitigação de riscos**
   O fornecedor monitora proativamente o surgimento de novas ameaças e seu impacto potencial nas operações, dados e pessoas? Eles possuem uma estratégia abrangente para eliminar brechas de segurança e vulnerabilidades? Que políticas eles aplicam em relação a cybersecurity?

2. **Soluções construídas com cybersecurity em mente**
   Suas soluções são desenvolvidas com várias camadas de segurança, como o emprego de tecnologias avançadas de autenticação e criptografia? Eles estão protegendo os dados da organização e a privacidade de seus clientes?

3. **Uma rede de confiança**
   Eles trabalham com parceiros que também têm em mente a segurança e a proteção de dados? Eles avaliam e selecionam cuidadosamente os parceiros para garantir os mais altos níveis de cybersecurity e compliance?

4. **Transparência e abertura**
   Quais medidas eles tomam para informar e dar suporte a seus clientes em relação às melhores práticas de cybersecurity? Eles são transparentes sobre vulnerabilidades conhecidas e compartilham estratégias e correções para rápida reparação?

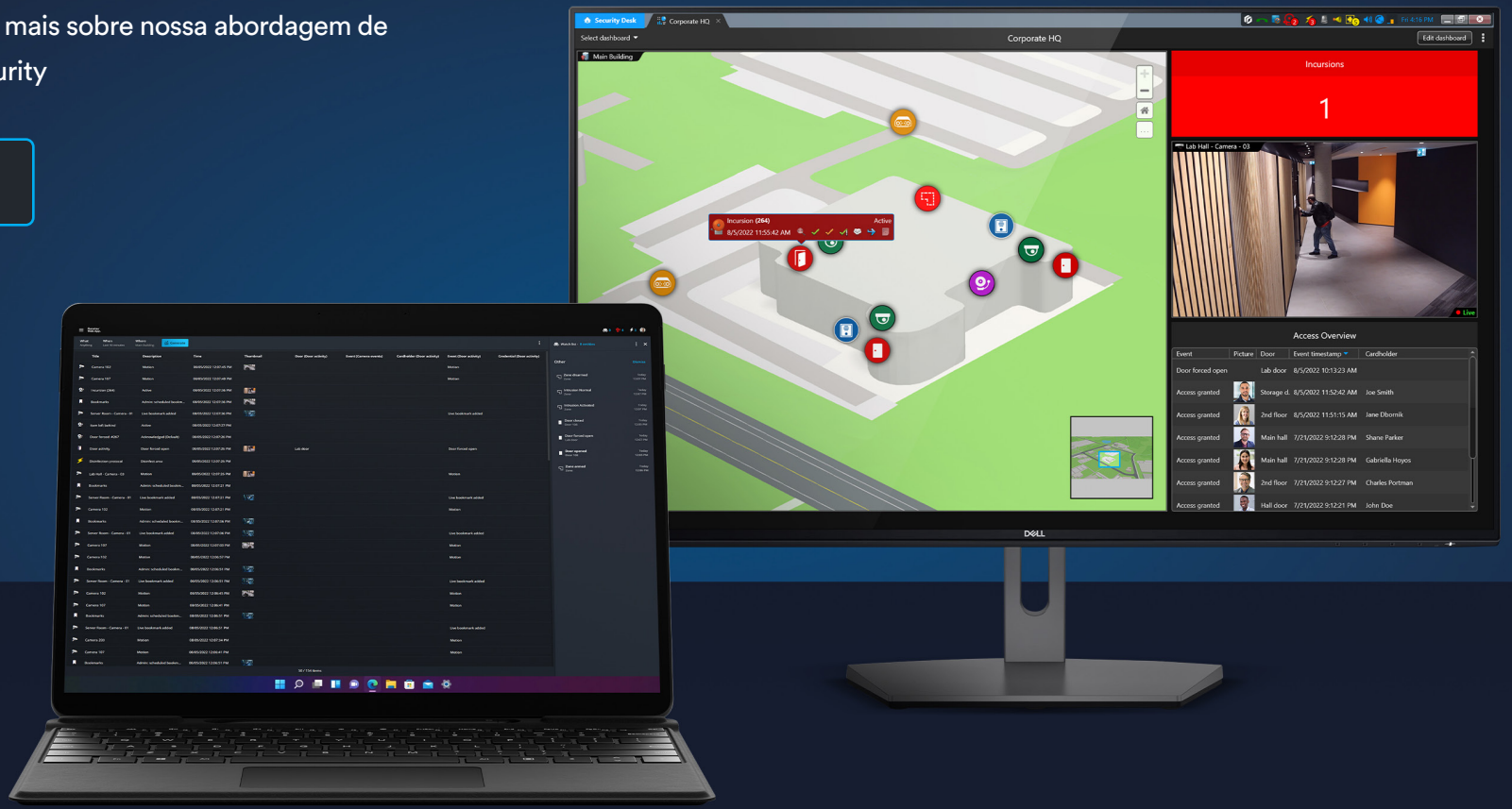
5. **Normas de segurança e privacidade de dados**
   Eles aderem a padrões de segurança da informação como o ISO 27001? Eles contratam auditores terceirizados e realizam testes de penetração para identificar e corrigir falhas de segurança? Eles possuem certificações de outros órgãos reguladores e associações internacionais?

Seu relacionamento com parceiros de tecnologia deve ser construído com base na confiança e na transparência. Ao fazer essas perguntas, você pode identificar colaboradores que realmente valorizam a segurança e a privacidade dos dados. Isso ajuda a fortalecer a segurança e evitar o acesso não autorizado para cada componente do sistema.

Escolher soluções que garantam a privacidade sem comprometer a segurança

Segurança e privacidade não são um jogo de soma zero. As soluções Genetec são construídas desde o início com várias camadas de cybersecurity em mente. Visite o Genetec Trust Center para saber mais sobre nossa abordagem de privacidade e cybersecurity

Visite o Trust Center



Genetec Inc.
Genetec.com/br
info@genetec.com
@genetec.com

UDPT: 20 DE JANEIRO DE 2023