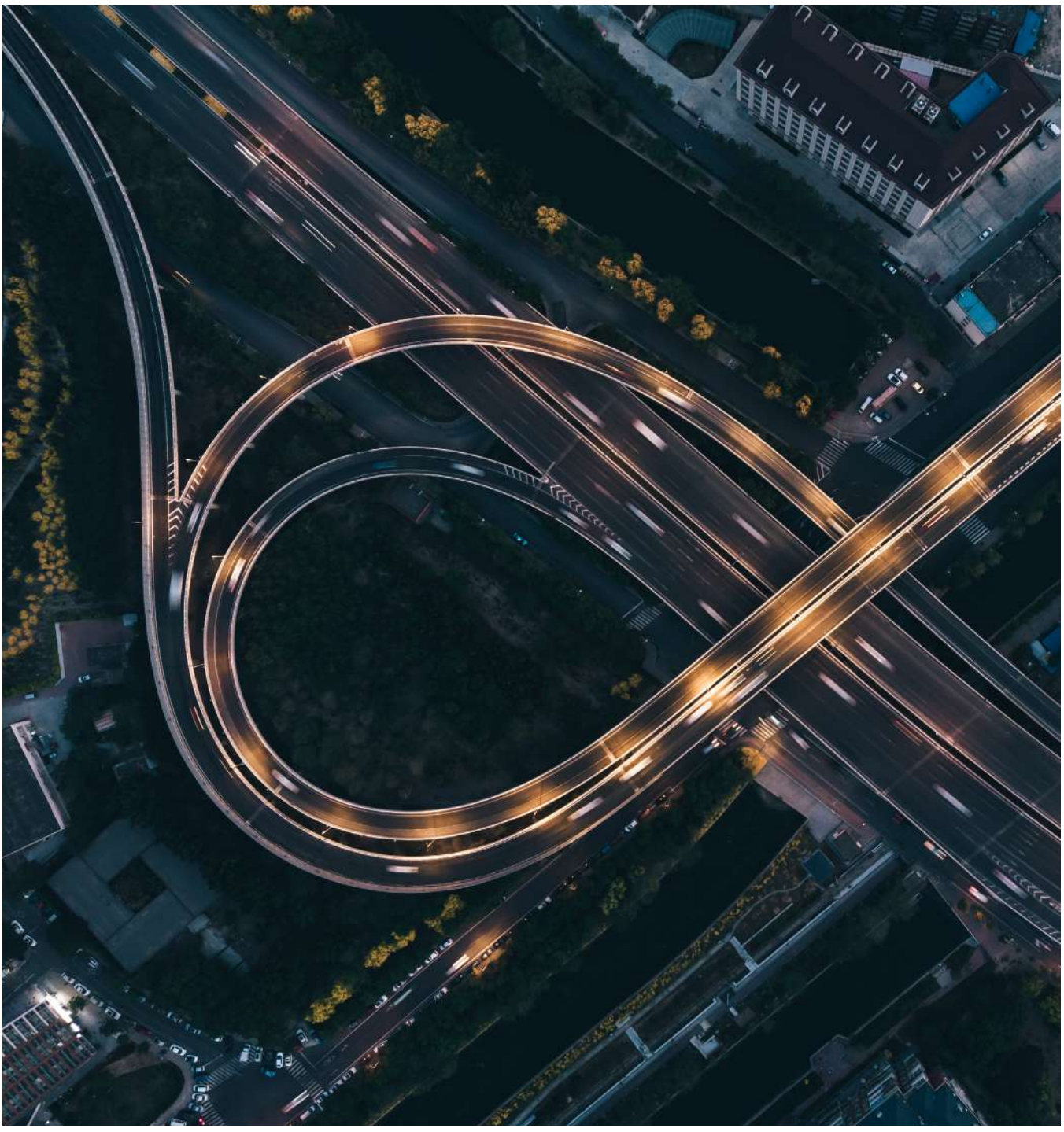
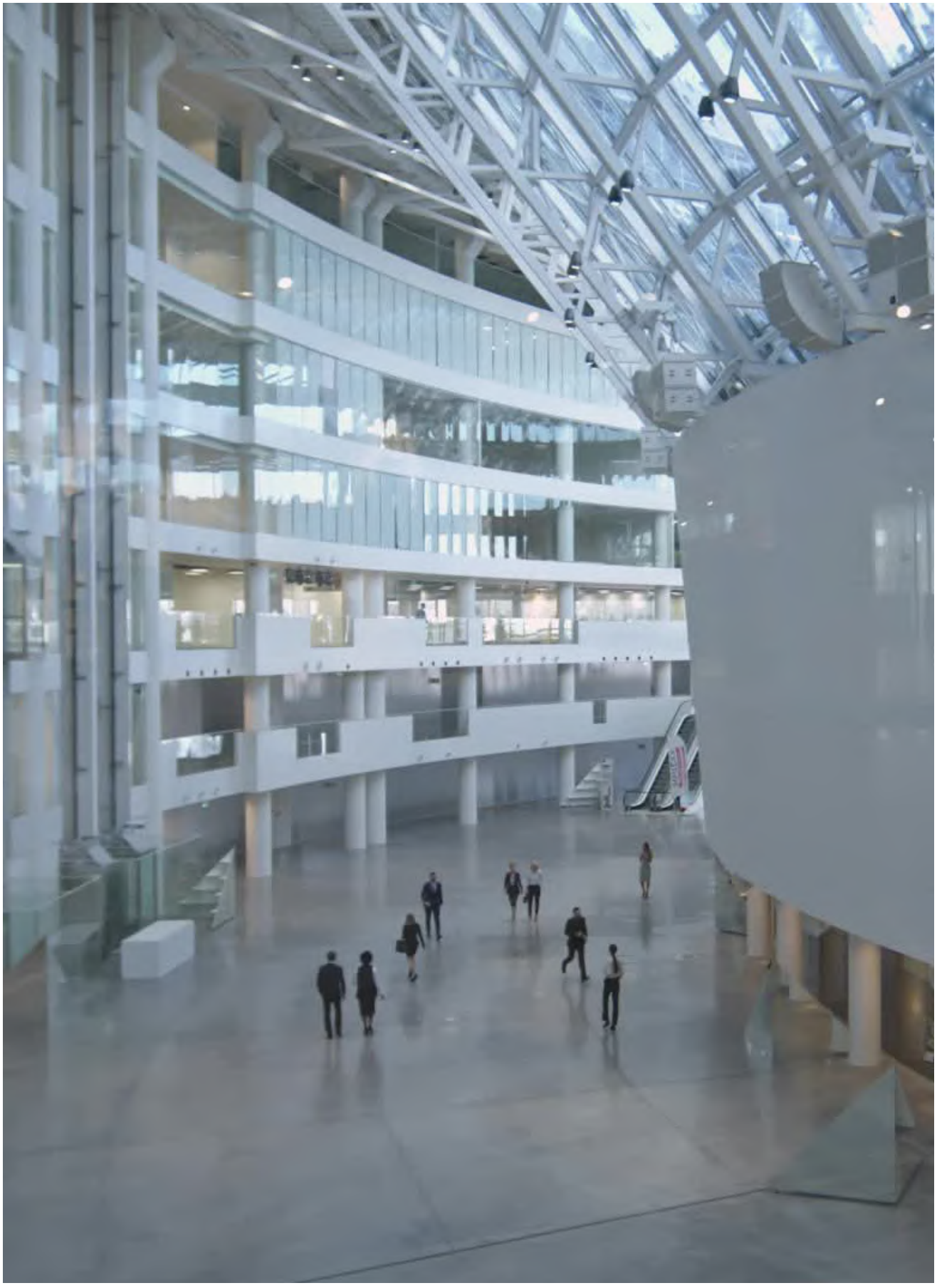
Whitepaper

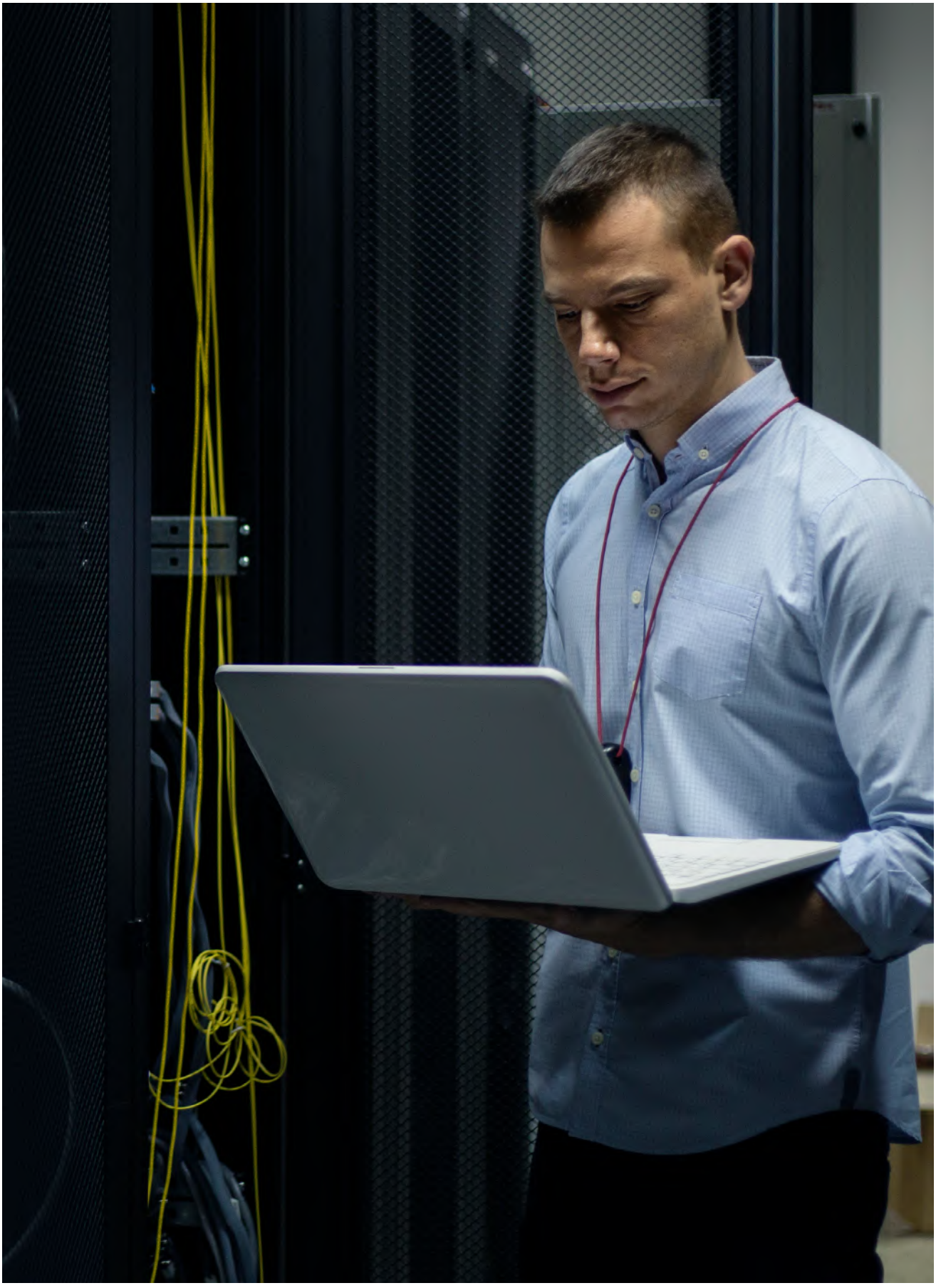
Prolongando a vida útil da segurança física através da unificação



Genetec™



Conteúdo



Sumário Executivo

Muitas organizações se deparam com soluções proprietárias que não atendem às suas necessidades de segurança em evolução.
Essas soluções podem ser uma séria responsabilidade, pois tentam responder a novas ameaças de segurança emergentes, um impacto crescente e uma pressão aumentada por descentralização.

Ao procurar modernizar seu sistema de segurança física existente, as organizações precisam decidir qual é a melhor base para sua nova infraestrutura de segurança. Existem duas opções disponíveis:

- Integração de sistemas
- Unificação

1

A jornada para a modernização

A decisão de modernizar um sistema de segurança física é o primeiro passo em uma jornada de vários estágios que pode melhorar drasticamente a segurança e as operações de negócios de uma organização. A jornada para a modernização pode ser dividida em quatro etapas: expansão, conexão, automação e entendimento.

Estágio 1: Expansão

O primeiro estágio é aumentar a cobertura do sensor por meio de uma aplicação de segurança independente. Depois de decidir se modernizar, uma organização começa a atualizar sua infraestrutura e aumentar a segurança, ampliando o alcance de seu sistema atual adicionando novos hardwares, incluindo câmeras de alta resolução e leitores biométricos.

Etapa 2: Conexão

Então, uma vez que uma organização atinge suas metas de maior cobertura de sensores, ela procura maneiras de aumentar a segurança com dados de outros sistemas. Nesse estágio, as organizações trabalham para conectar diferentes sistemas, por exemplo, conectando sistemas de videomonitoramento e controle de acesso para aumentar a velocidade de verificação e investigação de acesso.

Etapa 3: Automação

O aumento do número e variedade de sensores e a subsequente transmissão de todos esses dados por meio de um único painel faz com que uma aplicação no sistema de segurança seja bombardeada, muitas vezes de maneira não prioritária, com grandes quantidades de informações. Nesse estágio, a organização precisa automatizar tarefas repetitivas do dia a dia para ajudar os operadores a se concentrarem no que realmente importa.

93% das organizações que migraram para uma plataforma unificada viram constataram uma diminuição nos problemas de compatibilidade em seu sistema de segurança.

Estágio 4: Entendimento

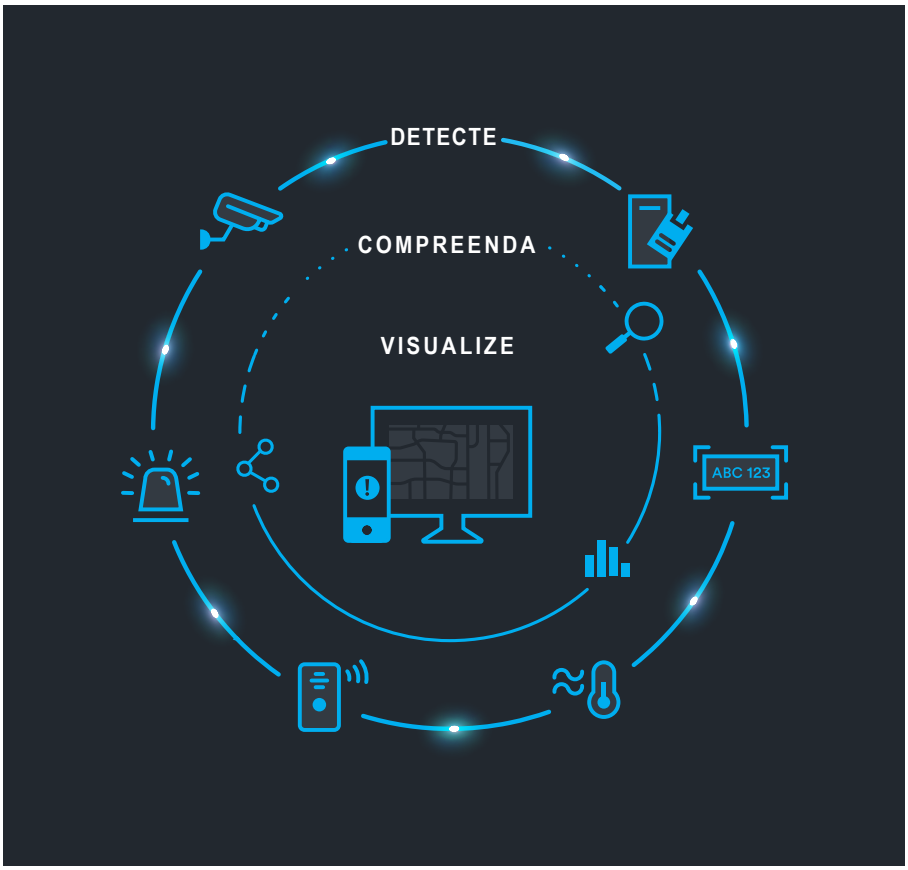
Este estágio de modernização não é mais apenas sobre segurança, mas também para melhorar a inteligência e as operações de negócios. O objetivo é utilizar os dados coletados em sistemas de segurança como um potencial diferencial competitivo.

Para a maioria das organizações, a jornada para a modernização termina entre os estágios 2 e 3. Depois de aumentar a cobertura de sensores com seu novo sistema e integrar parcialmente alguns de seus sensores legados, a manutenção desse amontoado de tecnologia complexa e precária sobrecarrega seus administradores de sistemas. Mas, ao adotar uma visão de longo prazo e usar essa oportunidade de modernização para implantar uma plataforma unificada e resolver problemas maiores relacionados à escalabilidade e falta de eficiência operacional, as organizações podem chegar ao estágio final e começar a usar dados para impulsionar as operações de negócios.

A principal razão pela qual a jornada termina entre o segundo e o terceiro estágio para muitos remonta à fundação de seu sistema de segurança física. Quando as organizações começam a se modernizar, geralmente adotam uma abordagem de integração de sistemas em vez de optar pela unificação. Embora a integração de sistemas permita que as organizações resolvam preocupações imediatas, bem como alguns desafios de segurança de curto prazo, não é uma visão de longo prazo. Como resultado da sobrecarga envolvida na manutenção de uma solução criada usando essa abordagem, as organizações se veem presas em um ciclo contínuo de lançamento, interrupção, validação e upgrade. Essas soluções não são capazes de entregar maior inteligência de negócios porque precisam gastar tempo e dinheiro com manutenção, pois seus componentes principais precisam ser atualizados constantemente em diferentes ciclos de lançamento.

De acordo com uma recente pesquisa de impacto da unificação da Genetec, 93% das organizações que migraram para uma plataforma unificada constataram uma diminuição nos problemas de compatibilidade em seu sistema de segurança. Ao permitir o fluxo de dados em todas as atividades operacionais e de segurança, a unificação capacita as organizações a enfrentar os desafios exclusivos em cada estágio de sua jornada. A implementação de uma única plataforma de software que oferece uma interface única para gerenciar os principais sistemas de segurança, como controle de acesso, intercomunicadores, intrusão e dispositivos de vídeo, é crucial. Mas, com a aceleração do ritmo de inovação no setor, a capacidade incluir sensores e dados externos, mantendo uma experiência de usuário coerente e intuitiva, é necessária para uma verdadeira sustentabilidade no longo prazo.

Além de proteger as organizações de possíveis obstáculos no curto prazo, a unificação também as ajuda a expandir seus negócios, dando suporte ao crescimento e a evolução no longo prazo. Como uma plataforma aberta e unificada facilita o fluxo e o gerenciamento de dados entre as atividades, as organizações podem ir além das atividades tradicionais de segurança física reativa e melhorar suas operações comerciais.



A maioria das soluções integradas exigirá que as operadoras usem vários sistemas porque nenhum oferece as funcionalidades necessárias em uma interface de usuário.

2

Integração de sistemas

A integração de sistemas tornou-se um substituto popular para a interface tradicional como resultado dos avanços na tecnologia e do aumento da colaboração entre os fabricantes. No setor de segurança, os protocolos padrão e os kits de desenvolvimento de software (SDK) são usados com mais frequência para conectar física ou funcionalmente diferentes sistemas de computação e aplicações de software.

Os protocolos padrão são poderosos e geralmente considerados mais eficazes do que um SDK. Eles suportam uma combinação de sistemas operacionais e permitem que os usuários gerenciem suas aplicações em tempo real. Os protocolos padrão são populares para integrações de dispositivos de borda, como câmeras IP ou controladores de porta, mas são mais comumente usados entre duas aplicações de software. No entanto, ao contrário de usar um SDK, integrar dois sistemas por meio de um protocolo padrão é demorado e pode exigir um banco de dados compartilhado entre os sistemas.

Um SDK, também conhecido como interface de programação de aplicativos (API), consiste em um pacote DLL criado e distribuído por fabricantes de software que permite que outros fabricantes integrem seus sistemas. Os SDKs simplificam a integração ocultando mecanismos complexos de outros desenvolvedores de software, incluindo autenticação, decodificação de vídeo e protocolos padrão complexos.

2.1 Benefícios da integração de sistemas

Independentemente do método de integração, os sistemas integrados fornecem aos usuários as ferramentas necessárias para se tornarem mais eficientes. Por exemplo, uma solução integrada de controle de acesso e gerenciamento de vídeo pode exibir vídeo ao vivo ou gravado, associado a um evento de controle de acesso a partir da interface do usuário de controle de acesso.

Outra vantagem da integração de sistemas é que as organizações não precisam mais depender de um único fabricante para todo o seu sistema de segurança. Trabalhar com soluções integradas permite que eles trabalhem com vários fornecedores independentes, cada um com seu próprio ecossistema de parceiros de tecnologia. Isso reduz custos porque, por exemplo, se uma organização não estiver satisfeita com seu sistema de gerenciamento de vídeo (VMS) atual, ela poderá mudar para outro fabricante sem começar do zero, desde que o novo VMS seja compatível com os demais componentes em seu sistema de segurança.

2.2 Problemas com integração de sistemas

Embora a integração de sistemas possa atingir um nível mais profundo de integração de produtos, há algumas desvantagens nessa abordagem.

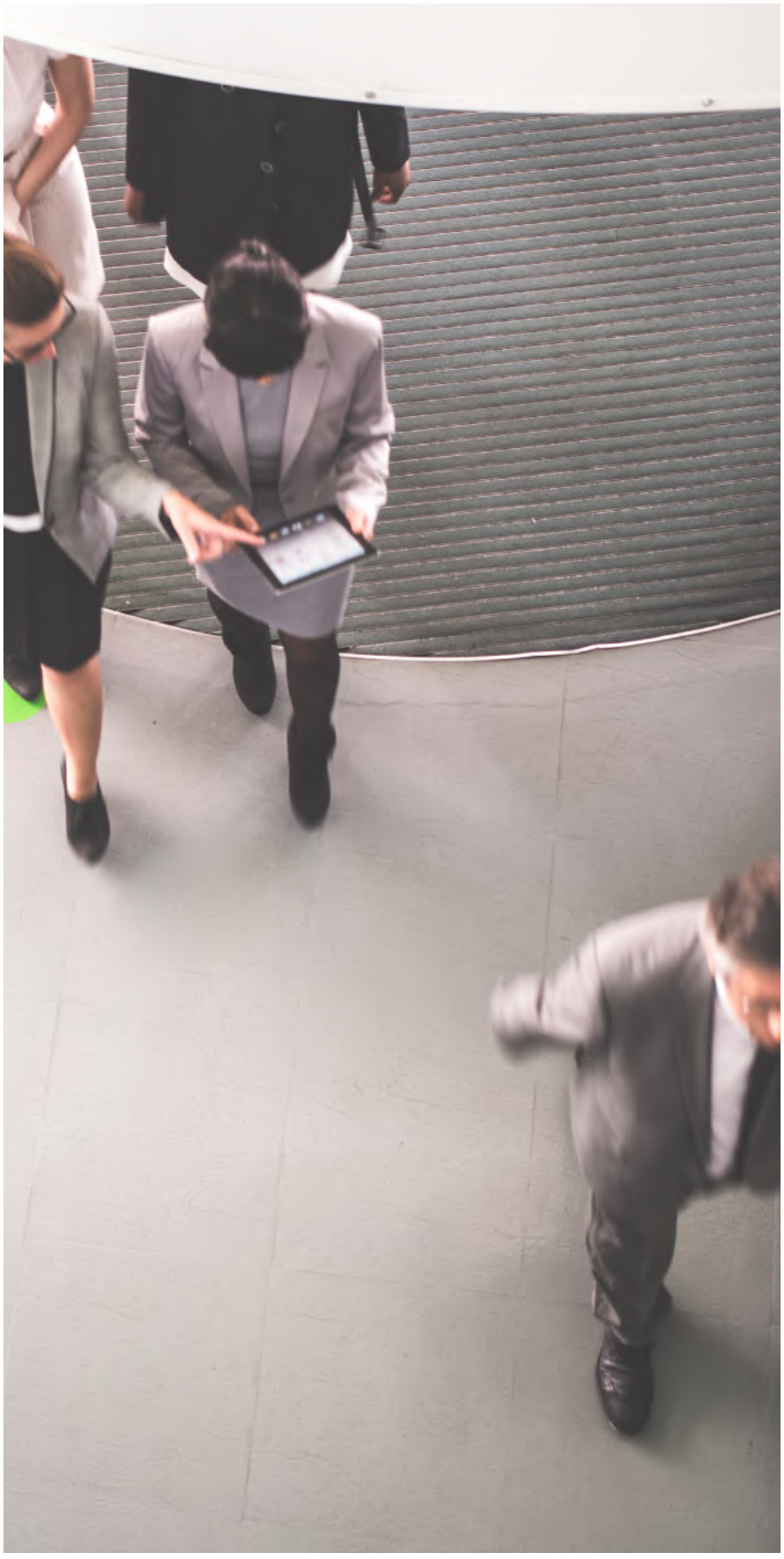
A maioria das soluções de integração ainda exige que os operadores usem vários sistemas porque nenhum deles oferece de forma independente as funcionalidades necessárias em uma interface de usuário. Mesmo quando as funcionalidades avançadas são suportadas no momento da instalação, novos recursos introduzidos por diferentes fornecedores não serão utilizáveis no sistema primário, impedindo que as organizações modernizem seus processos gradualmente para superar novas ameaças.

Isso significa que há casos em que um operador precisa ficar pulando de um sistema para outro. Por exemplo, um operador pode ser obrigado a executar pan-tilt-zoom (PTZ) no VMS porque essa funcionalidade é limitada dentro do sistema de controle de acesso (ACS) da organização. Outras limitações do ACS que podem forçar os operadores a alternar entre os sistemas inclui não oferecer suporte a sequências de câmeras, dificuldade de pesquisa em gravações de vídeo e falta de recursos de pesquisa de movimentos.

A manutenção e configuração futuras são desvantagens adicionais a ser consideradas com um sistema integrado. Como o administrador tem dois ou três sistemas independentes para configurar e manter sincronizados, a manutenção exige mais tempo. A ineficiência de um sistema integrado aumenta ainda mais porque muitas das configurações necessárias são redundantes, o que significa que os administradores precisam executar as mesmas tarefas em vários sistemas. Exemplos disso incluem gerentes de segurança que precisam criar contas e especificar privilégios para usuários em vários sistemas e operadores de segurança que precisam configurar cada nova câmera em vários sistemas.

As organizações também podem achar desafiador realizar upgrades e obter suporte para seus sistemas integrados. Como os fabricantes alteram constantemente seus softwares para oferecer suporte a novas funcionalidades, essas alterações podem afetar a maneira como as integrações existentes funcionam e podem até fazer com que os sistemas integrados percam a compatibilidade, especialmente quando alteram seu SDK ou API. Isso tem o potencial para retardar upgrades ou forçar uma organização a investir na reintegração dos sistemas afetados.

Buscar suporte para uma solução integrada também pode ser complicado. Como uma solução integrada é composta por diferentes sistemas de diferentes fornecedores, pode levar tempo para resolver os problemas. Os fabricantes, e muitas vezes o integrador, primeiro precisam investigar o problema e descobrir qual sistema não está se comportando adequadamente. Em seguida, precisam corrigir o problema, o que pode resultar em mais atrasos, dependendo do relacionamento entre os fabricantes.



3

E quanto ao PSIM?

Conforme mencionado anteriormente, a maioria das organizações que decidem modernizar seus sistemas de segurança física não passa do segundo estágio em sua jornada como resultado do aumento da complexidade e do aumento dos custos de manutenção.

As soluções de gerenciamento de informações de segurança física (PSIM) podem ajudar as organizações a passar para o terceiro estágio de sua jornada de modernização. Um PSIM é um produto de software que pode supervisionar vários sistemas distintos. Sua principal função é gerenciar informações de diferentes sistemas e apresentar esses dados em uma única interface de usuário.

Um PSIM geralmente não possui uma solução integrada de controle de acesso, intrusão ou videomonitoramento. Em vez disso, geralmente é customizado para uma organização com base em vários sistemas de segurança preexistentes e os integra por meio de SDKs e APIs proprietários.

Essa solução também ajuda a garantir que os operadores possam gerenciar todos os dados que chegam ao sistema de maneira escalável. Ao instalar um PSIM, uma organização pode projetar fluxos de trabalho para orientar as respostas do operador e criar processos automatizados que não requerem intervenção humana.

3.1 Problemas com soluções PSIM

As organizações que pensam em instalar um PSIM devem estar atentas aos possíveis problemas de compatibilidade, bem como aos custos de longo prazo associados à manutenção do suporte para uma variedade de produtos altamente customizados.

Como um PSIM se baseia na mesma abordagem das integrações tradicionais, uma organização pode enfrentar desafios de compatibilidade quando um dos subsistemas requer manutenção ou upgrade. Além disso, cada sistema integrado em um PSIM deve ser configurado separadamente. Isso leva a um alto grau de redundância e esforço duplicado. Por exemplo, ao usar um PSIM, uma organização teria que configurar usuários no PSIM, bem como em cada um dos sistemas subjacentes de controle de acesso, vídeo, comunicações por voz e intrusão. As soluções PSIM também são estáticas, o que torna muito difícil melhorar os processos e o fluxo de trabalho após a implantação da solução.

4

Unificação: plataforma aberta e unificada

Uma plataforma aberta e unificada é uma solução de software abrangente que ajuda as organizações atender às suas necessidades de segurança imediatas e de longo prazo. Ao oferecer interconectividade perfeita entre vários sistemas, incluindo vídeo, acesso, intercomunicadores e intrusão, ele oferece tudo o que a equipe de segurança precisa em um único conjunto de software unificado.

4.1 Conheça os fatos

A unificação também é econômica. De acordo com a pesquisa de impacto da unificação da Genetec, 77% dos entrevistados disseram que a unificação reduziu seu impacto em infraestrutura, 78% disseram que melhorou os custos de manutenção e 89% disseram que reduziu o tempo de manutenção.

Uma plataforma aberta e unificada custa menos para comprar e manter do que soluções integradas customizadas e também protege o investimento em segurança de uma organização por meio da interoperabilidade. Com interoperabilidade pronta para uso, esta solução visa o mercado de massa, fornecendo suporte integrado para produtos de segurança comoditizados sem exigir customização para cada instalação. Esses produtos comoditizados incluem câmeras IP, DVRs, controladores de portas, painéis de alarme, intercomunicadores, impressoras de crachás, diretório ativo para autenticação e gerenciamento de cartões.

Sendo que uma plataforma unificada oferece suporte a produtos comoditizados, os investimentos em hardware também são protegidos. Se uma organização não estiver satisfeita com a solução de software unificada, ela poderá alterar os componentes do software sem precisar reinvestir em dispositivos especializados.

Uma solução unificada significa que os usuários só precisam conhecer, configurar, fazer upgrade e backup de um único pacote de software.

Embora a customização não seja necessária ao implantar uma plataforma aberta e unificada, a plataforma ainda permite integração e customizações de terceiros por meio de um SDK ou API. Sendo que uma plataforma unificada é construída em torno de atividades como monitoramento e geração de relatórios e não é projetada para uma única tecnologia, sua interface suporta perfeitamente novas integrações. Com esses tipos de ferramentas, as organizações podem aproveitar as integrações existentes e também projetar e manter integrações customizadas por conta própria, em vez de depender do fabricante da plataforma unificada.

4.2 A infraestrutura unificada do servidor

Uma plataforma verdadeiramente unificada otimiza recursos compartilhando servidores e bancos de dados comuns para:

- autenticação e permissões
- licenciamento
- definições de configuração
- alarmes e eventos
- auditoria e registro de atividades
- gravação de vídeo
- registros de acesso
- agendamentos

A implantação de uma infraestrutura de servidor unificada significa que os usuários só precisam conhecer, configurar, fazer upgrade e backup de um único conjunto de software. Isso torna a instalação e o gerenciamento de uma plataforma aberta e unificada mais fácil do que um sistema integrado. O acesso também é mais fácil, pois os administradores podem gerenciar o sistema por meio de uma única aplicação, independentemente do número de servidores ou tecnologias. Então, com esta conexão, eles podem acessar todos os serviços oferecidos pelo sistema, pois os dados são armazenados em um local central.

A unificação do servidor para a interface oferece benefícios distintos para as organizações, incluindo:

- maior eficiência através do uso de uma única interface
- maior inteligência situacional por meio da correlação automatizada de eventos entre sistemas
- custos reduzidos com configuração/manutenção compartilhadas

4.3 A experiência do usuário

Uma plataforma aberta e unificada também oferece uma interface de usuário única para várias aplicações de segurança. Como resultado, alternar de uma aplicação para outra acontece de forma perfeita. Significa que os operadores podem passar de uma tarefa de segurança para outra com facilidade e eficiência, economizando tempo e energia e melhorando a segurança. De acordo com a pesquisa da Genetec com clientes que implantaram plataformas unificadas:

- 63% disseram que viram uma grande melhoria na detecção de eventos
- 59% disseram que viram grandes melhorias nos tempos de resposta
- 70% viram grandes melhorias no tempo necessário para coletar evidências e outras informações relevantes

A interface de usuário comum também reduz o tempo necessário para treinar novos operadores em sistemas individuais dentro da infraestrutura de segurança. De acordo com a pesquisa sobre impacto da unificação Genetec, 86% dos entrevistados observaram uma redução no tempo gasto com treinamento de novos operadores e 88% relataram uma redução no número de erros do operador.

Todos os sistemas construídos em uma plataforma aberta e unificada também compartilham funções básicas comuns. Isso significa que o gerenciamento de alarmes, do evento à ação, relatórios, investigação e fluxos de trabalho relacionados a incidentes são todos iguais, independentemente de serem para vídeo, controle de acesso ou comunicações de voz. Isso reduz significativamente o número total de fluxos de trabalho que os operadores precisam aprender e usar.

4.3.1 Correlação de eventos

Como os eventos e alarmes são gerenciados por uma única infraestrutura de servidor, um sistema unificado oferece correlação de eventos por design. Ao correlacionar eventos de acesso e vídeo, por exemplo, uma plataforma unificada permite que as operadoras validem rapidamente a identidade de um portador de cartão quando ocorre um evento de acesso, para garantir a autenticidade de suas credenciais. A correlação de eventos também pode reduzir significativamente o tempo de resposta filtrando alarmes falsos.

4.3.2 Facilidade de manutenção e suporte

Um sistema unificado é mais fácil para fazer upgrade e manter do que uma solução integrada porque possui uma única plataforma de software. Em vez de fazer upgrade em vários sistemas, o integrador só precisa fazer upgrade da plataforma, economizando tempo e simplificando a manutenção caso o suporte do fabricante for necessário. Também minimiza o tempo de inatividade do sistema durante upgrades. De acordo com a pesquisa de impacto da unificação Genetec, 83% dos entrevistados relataram uma diminuição no tempo gasto em questões técnicas individuais e 53% disseram que a unificação teve um grande impacto na manutenção.

4.3.3 A importância da integração

No setor de segurança, os sistemas de plataforma aberta e unificada, ao contrário dos sistemas de arquitetura aberta, não usam padrões do setor para integração com hardware de diferentes fabricantes. Esse método de integração é realizado primeiro construindo uma camada de integração genérica que fornece as funcionalidades mais comuns e, em seguida, desenvolvendo um driver para cada produto específico com o qual o sistema se integra.

Nesses sistemas, os fabricantes de plataformas abertas e unificadas são responsáveis por desenvolver, testar e manter a integração com todos os dispositivos suportados por seus produtos. Os sistemas de plataforma aberta e unificada tendem a fornecer suporte a uma ampla variedade de fabricantes que oferecem funcionalidades semelhantes e produtos que são comoditizados. Essa estratégia funciona bem para dispositivos especializados porque possuem funcionalidades fixas e bem definidas. Com esses tipos de sistemas, as organizações também têm a liberdade de trocar os fornecedores de software ou hardware sem precisar substituir todos os equipamentos de segurança existentes.

5

Escolher uma solução

Antes de iniciar o processo de modernização, as organizações precisam decidir sobre a base ideal para seu novo sistema de segurança física. Embora a maioria das organizações invista na integração de sistemas, a unificação é uma opção melhor.
Além de oferecer as aplicações mais eficientes, flexíveis e econômicas, a unificação também dá às organizações a confiança de que precisam para empreender a jornada de vários estágios em direção a operações de negócios aprimoradas e crescimento sustentado no longo prazo.


25
56

A Genetec Inc. é uma empresa de tecnologia inovadora com um amplo portfólio de soluções que abrange segurança, inteligência e operações. O produto carro-chefe da empresa, o Genetec™ Security Center é uma plataforma de segurança física que unifica videomonitoramento IP, controle de acesso, reconhecimento automático de placas de veículos (ALPR), comunicações e analíticos. A Genetec também desenvolve soluções baseadas na nuvem e serviços projetados para melhorar a segurança e contribuir com novos níveis de inteligência operacional para governos, empresas, transporte e as comunidades em que vivemos. Fundada em 1997 e sediada em Montreal, 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.

Videomonitoramento: Obtenha uma maior consciência situacional e aumente a segurança em sua cidade com a capacidade de compartilhar câmeras entre agências e organizações, fornecendo uma imagem operacional em comum e melhorando o tempo de resposta a incidentes.

Controle de acesso: Aumente a segurança da sua organização, responda com eficiência às ameaças e tome decisões mais claras e em tempo hábil usando uma plataforma unificada e pronta para IP, seja implantando um novo sistema de controle de acesso ou atualizando uma instalação existente.

Reconhecimento automático de placas de veículos: Automatize a detecção de veículos de interesse, aumente a eficiência da fiscalização em estacionamentos e acelere as investigações de segurança pública por meio da capacidade de compartilhar informações de placas de veículos com agências selecionadas e organizações parceiras, sem violar propriedade e privacidade.

Suporte à decisão operacional: Gere mais eficiência no tratamento de incidentes e tomada de decisões através de fluxos de trabalho avançados que guiam os operadores durante alertas de situação por meio de procedimentos baseados em políticas para exportação de compilação detalhada de casos.

Gerenciamento de caso investigativo: Simplifique o gerenciamento de casos e acelere as investigações com uma plataforma que permite centralizar evidências digitais e colaborar de forma segura com investigadores, agências externas e o público.

Serviços na nuvem: Estenda os recursos do seu sistema de segurança in loco e reduza os custos de TI com serviços na nuvem altamente escalável, sob demanda que capacitam sua cidade a lidar facilmente com os requisitos de segurança em rápida mudança e operar com maior eficiência.

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

ATUALIZADO: 22-JUN-2023