WHITE PAPER

Aprimorando a segurança física por meio da unificação do sistema

Genetec™

genetec.com/br

Sumário Executivo

Embora as organizações procurem incorporar sistemas de videomonitoramento e controle de acesso que forneçam maior interoperabilidade como parte de sua estratégia de segurança, a maioria dos fabricantes de segurança continuou a fornecer sistemas diferentes, com comunicação limitada entre os sistemas.

Com os recentes avanços nas tecnologias de software e as parcerias contínuas entre fabricantes de segurança, a integração tornou-se um substituto popular para a interface tradicional. No entanto, mesmo a integração tem seus limites. A resposta pode ser encontrada em uma plataforma de software única que pode gerenciar dispositivos de controle de acesso, intercomunicador, intrusão e vídeo, oferecendo uma interface unificada para monitorar todo o sistema. Esse sistema vai além das funcionalidades básicas de interface e integração, oferecendo aos usuários finais uma opção eficiente, flexível e econômica para unificação de sistemas não disponível com soluções altamente customizadas e caras, como PSIMs.

Construindo Soluções de Segurança Que os Usuários Finais Desejam

Ainda hoje, com todas as tecnologias disponíveis, o setor está lutando para ter sucesso total na construção de soluções de segurança que atendam às verdadeiras necessidades dos usuários – um sistema coeso de controle de acesso e vídeo que seja eficiente, não proprietário e econômico. É importante reconhecer que sem esses critérios básicos, um sistema unificado de vídeo e controle de acesso pode não parecer vantajoso para os clientes e, portanto, não gerar demanda suficiente para os fabricantes justificarem o desenvolvimento de tal produto.

Os Ganhos em Eficiência São Importantes

A prioridade de qualquer equipe de segurança será dedicar tempo à execução de suas principais tarefas, como monitorar, investigar e responder a incidentes para garantir a segurança da organização. Sua capacidade de executar essas tarefas críticas não deve ser prejudicada pelo tempo gasto no gerenciamento da tecnologia. Em outras palavras, as tecnologias de segurança que eles usam devem ajudá-los a ser mais eficientes e eficazes, sem retardá-los.

Em um de seus artigos, Rich Anderson, CTO da Razberi Technologies, e anteriormente VP de Marketing da GE Security e VP de Engenharia da CASI-RUSCO, ilustra o problema comum com os sistemas díspares de hoje com a seguinte declaração: "Sistemas de controle de acesso em particular geram alarmes para crachás inválidos, eventos de porta forçada e travada. Esses eventos precisam ser investigados, mas fazer isso com um sistema de vigilância autônomo é uma tarefa penosa. O alarme é recebido em um sistema e seu operador terá que passar para outro sistema completamente diferente para investigar. Este sistema de vigilância tem uma interface de usuário diferente e, portanto, ele/ela precisa "mudar de estratégia". Então, qual câmera você aciona para ver a cena? Um operador experiente saberá, mas essa "experiência" custa muito em termos de treinamento." [2]

Misturando e combinando as melhores tecnologias

A indústria de PCs conseguiu construir produtos interoperáveis. Qualquer um pode comprar um PC hoje e, no futuro, adicionar novo hardware, como impressora, webcam, dispositivos de jogos, ou até mesmo instalar um novo disco rígido que processa informações duas vezes mais rápido que o anterior. Quase tudo pode ser feito sem alterar o PC inteiro ou o sistema operacional.

No entanto, o mesmo não pode ser dito ou feito no setor de segurança. Um usuário não pode simplesmente decidir comprar o mais recente controlador de porta sem fio de alta tecnologia e adicioná-lo a um sistema de controle

[2] Integração de Vídeo e Controle de Acesso, SecurityInfoWatch.com, Rich Anderson, 25-03-2009

de acesso existente. Ou comprar as melhores e mais recentes câmeras IP e conectá-las a um sistema de gerenciamento de vídeo (VMS) sem primeiro verificar se o modelo específico é compatível. Por essas e muitas outras razões, o setor de segurança está muito atrás do setor de PCs.

Na verdade, talvez nunca seja possível chegar ao que a indústria de PCs tem em termos de interoperabilidade. Assumir um compromisso com a tecnologia proprietária pode ser uma decisão dispendiosa. Quando surge uma nova tecnologia, a opção de incorporá-la torna-se mais uma questão de abrir mão ou não dos investimentos existentes e recomeçar do zero com um novo investimento.

Por outro lado, ter a capacidade de misturar e combinar os melhores produtos de diferentes fabricantes e ter a opção de incorporar os mais recentes avanços em tecnologia em um sistema de segurança oferece mais flexibilidade e a garantia adicional de que seu investimento é à prova do futuro.

Gerenciando Investimentos

Uma solução totalmente personalizada para se adequar a todos os sistemas e infraestruturas de negócios existentes pode ser muito eficiente e atraente, mas, como acontece com qualquer abordagem personalizada, provavelmente também será cara. Tomemos, por exemplo, sistemas ERP (planejamento de recursos empresariais) implantados por muitas empresas. Um sistema ERP pode ser personalizado para se adaptar a praticamente qualquer modelo e ambiente de negócios através de integradores de sistemas ERP especializados. Embora o custo de customização de tal sistema seja muito alto, geralmente há um ganho significativo de produtividade realizado após a implantação para justificar esse investimento.

Em aspectos semelhantes, os investimentos em departamentos e equipamentos de segurança são sempre considerados uma despesa e é improvável que os sistemas de segurança possam ser adaptados a todos os processos internos. Como esses sistemas raramente geram receita, os orçamentos são tradicionalmente rigidamente controlados. A completa reformulação de um sistema, independentemente da tecnologia

empregada, depende inteiramente da disponibilidade do orçamento e que a administração esteja de acordo. Muitas vezes, até mesmo as discussões de upgrade ou substituição de um sistema ocorrem por pura necessidade (por exemplo, sistema antigo ou falha de segurança) e o processo de aquisição e implementação de um sistema pode durar meses, quando não, anos.

Portanto, é crucial, mais do que qualquer outro fator, que o custo total de propriedade de um sistema coeso de vídeo e controle de acesso seja justificado.

Sistemas Integrados

Com os recentes avanços nas tecnologias e o aumento da colaboração entre os fabricantes, a integração tornou-se um substituto popular para a interface tradicional.

"Na tecnologia da informação, a integração de sistemas é o processo de conectar diferentes sistemas de computação e aplicativos de software física ou funcionalmente."[3]

Especificamente no setor de segurança, os métodos de integração mais populares envolvem protocolos de rede e kits de desenvolvimento de software (SDK).

Os protocolos de rede são muito poderosos, pois suportam uma combinação de sistemas operacionais e permitem que você gerencie suas aplicações em tempo real. No entanto, integrar dois sistemas por meio de um protocolo de rede requer mais tempo do que um SDK ou pode exigir um banco de dados compartilhado entre dois sistemas. Os protocolos de rede são populares para integrações de dispositivos de borda, como câmeras IP ou controladores de porta, mas são ainda mais usados entre dois aplicativos de software. Os protocolos de rede são simplesmente considerados mais eficazes.

Um SDK, também conhecido como interface de programação de aplicativos (API), consiste em um pacote DLL criado e distribuído por fabricantes de software para permitir que outros desenvolvedores de software se integrem ao seu sistema.

Os SDKs simplificam a integração ocultando mecanismos complexos dos desenvolvedores, como autenticação, decodificação de vídeo, protocolos de rede complexos e assim por diante. Como eles simplificam a tarefa de um integrador de software, a maioria dos fabricantes de DVR, NVR e controle de acesso oferece um SDK ou API em vez de um protocolo de rede.

A maioria dos fabricantes de videomonitoramento oferece um SDK que pode ser usado para integrar vídeo ao vivo e de reprodução em qualquer aplicação. Por exemplo, alguns fabricantes de controle de acesso usam o SDK dos fornecedores de DVR para linkar um alarme de controle de acesso ao vídeo associado para obter reprodução rápida. A maioria dos fabricantes de software de controle de acesso também oferece um SDK para que os sistemas VMS possam receber eventos de controle de acesso de seu sistema.

[3] Curso de Integração de Sistemas Syllabus, Georgia State University, página da web, reproduzido em 27 de junho de 2007

Alguns fornecedores de controle de acesso até permitem que os fabricantes de vídeo integrem algumas de suas funcionalidades na interface do usuário do sistema de controle de acesso.

Independentemente do método de integração escolhido, os sistemas integrados definitivamente começam a dar aos usuários as ferramentas para se tornarem mais eficientes. É muito comum que uma solução integrada de controle de acesso e vídeo exiba vídeo ao vivo ou gravado, associado a um evento de controle de acesso a partir da interface do usuário para controle de acesso.

Além disso, as soluções integradas oferecem outra vantagem para os usuários: não precisar depender de um único fabricante para todo o sistema de segurança. Em alguns casos, pode ser vantajoso trabalhar com dois fornecedores independentes, cada um com vários parceiros de tecnologia próprios. Nesse caso, os usuários que não gostarem de sua solução de videomonitoramento atual poderão mudar para outro fabricante, desde que seja compatível com o sistema de controle de acesso.

Embora a redução dos custos de troca do usuário final e o uso de um SDK ou API para obter um nível mais detalhado de integração entre produtos tenham seus benefícios, a integração também pode trazer algumas armadilhas.

A maioria dessas integrações ainda exige que as operadoras usem dois sistemas em paralelo porque nem o vídeo nem o sistema de controle de acesso oferecem todas as funcionalidades necessárias em uma interface de usuário.

Algumas limitações podem incluir:

- O sistema de controle de acesso não suporta sequências de câmeras
- Não ser algo fácil pesquisar todos os registros em vídeo gravados através de controle de acesso
- Falta recursos de pesquisa de movimento no sistema de controle de acesso

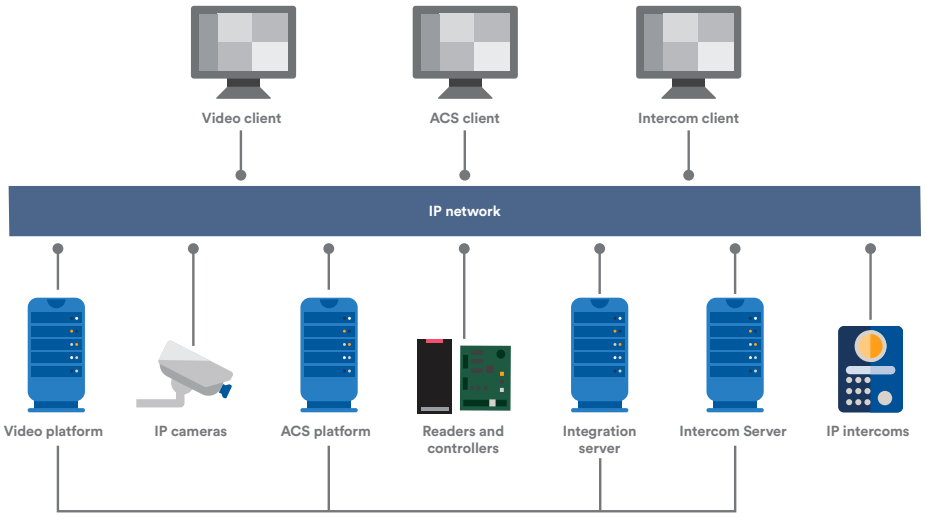

Figura 1 - Soluções integradas

- As funcionalidades de pan-tilt e zoom (PTZ) são limitadas no controle de acesso em comparação com o sistema de vídeo

Outra desvantagem comum a considerar com um sistema integrado surge da futura manutenção e configuração do referido sistema. Como o administrador tem dois ou três sistemas independentes para configurar e manter sincronizados, a manutenção de vários sistemas exigirá mais tempo.

Além disso, muitas das configurações necessárias são redundantes, forçando o administrador a repetir o mesmo trabalho em todos os sistemas.

Aqui estão alguns exemplos:

- Configurações de gerenciamento de alarmes independentes
- Gerenciamento de usuários: para cada operador, o gerente de segurança deve criar duas contas e especificar privilégios em dois sistemas
- Cada nova câmera requer configuração em dois sistemas independentes

Por fim, realizar upgrades e obter suporte para um sistema integrado pode ser um desafio. À medida que uma versão mais recente de uma aplicação é lançada, as alterações no software podem quebrar a compatibilidade

de uma integração entre dois sistemas, atrasando a capacidade de uma organização de realizar upgrades em seu sistema ou exigindo que ela invista em trabalho customizado para reintegrar os dois sistemas.

Os fabricantes alteram constantemente seus softwares para suportar novas funcionalidades e, com isso, também podem alterar a forma como as integrações existentes funcionam, principalmente quando alteram seu SDK ou API.

Considerando que um upgrade para a versão de software mais recente de um sistema que faz parte de uma solução integrada pode afetar a integração, o instalador é responsável por garantir que o software VMS mais recente ainda seja totalmente compatível com o software de controle de acesso. Antes de desativar o sistema de um usuário final e seguir com o upgrade, muitos integradores preferem construir um sistema de testes em seu laboratório para validar a integração.

Buscar suporte para uma solução integrada também pode se tornar um assunto complicado. Como há dois sistemas separados envolvidos, cada um sendo provavelmente de dois fornecedores diferentes, quando ocorre um problema, leva mais tempo para ser resolvido. Ambos os fabricantes, e muitas vezes o integrador, precisam investigar e descobrir qual sistema não está se comportando adequadamente. O tempo necessário para resolver o problema em questão também depende da relação entre os dois fabricantes de software.

Assim, embora existam muitas vantagens derivadas de um sistema integrado em comparação com a interface tradicional, ainda há muitos problemas que surgem com esse nível de integração.

Sistemas de plataforma aberta

Os produtos de plataforma aberta, conforme referido no setor de segurança, integram-se a diferentes fabricantes de hardware sem necessariamente usar padrões do setor, como sistemas de arquitetura aberta.

Os fabricantes de plataforma aberta desenvolvem, testam e mantêm a integração com cada dispositivo suportado pelo produto. Os produtos de plataforma aberta tendem a fornecer suporte a uma ampla variedade de fabricantes que oferecem funcionalidades semelhantes e produtos que são comoditizados. Os fabricantes desses sistemas fazem isso 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. Essa estratégia funciona bem para dispositivos especializados porque possuem funcionalidades fixas e bem definidas.

O conceito VMS de plataforma aberta, por exemplo, está bem estabelecido no mercado porque câmeras IP ou codificadores IP oferecem recursos comuns.

Esses tipos de sistemas oferecem enormes benefícios aos usuários finais porque agora eles têm a liberdade de mudar de fornecedor de software ou hardware sem ter que descartar todo o equipamento investido.

A indústria de controle de acesso, no entanto, tem sido tradicionalmente construída com base em soluções proprietárias, incluindo fabricantes únicos para os controladores de porta e o software de gerenciamento. Hoje, é mais fácil para os fornecedores construir sistemas de controle de acesso fechados. As razões são que oferecer um sistema fechado reduz a complexidade, simplifica os esforços de teste e aumenta a receita por cliente com a venda de hardware e software. Mas essa arquitetura fechada elimina muita flexibilidade para o usuário final.

Devido ao sucesso em videomonitoramento e porque os usuários finais estão exigindo mais liberdade, produtos semelhantes de plataforma aberta estão começando a surgir no setor de controle de acesso. Hoje, controladores de porta baseados em IP são oferecidos por fabricantes que nem sequer oferecem software de controle de acesso. Esses fabricantes de hardware disponibilizam seu protocolo com fio ou fornecem um SDK para se comunicar com seus controladores. Outras empresas de hardware também estão oferecendo cada vez mais travas de IP sem fio empacotados com leitores que reduzem os custos de instalação.

Melhor que o Restante: A Plataforma Aberta Unificada

Com o conceito de plataforma aberta já estabelecido no setor de videomonitoramento, a nova tendência de controladores de porta não proprietários na indústria de controle de acesso e os padrões de segurança emergentes, uma plataforma de segurança unificada agora é algo possível.

Uma plataforma unificada é uma solução de software abrangente que gerencia o controle de acesso, interfone, intrusão e funcionalidades de vídeo por meio de dispositivos de segurança não proprietários.

Uma plataforma unificada vai além de marcar ou destacar vídeos quando ocorre um evento de controle de acesso ou liberação de uma porta de acesso controlado a partir da interface do usuário de videomonitoramento. É uma interface de usuário unificada que oferece integração perfeita entre vídeo, intercomunicador, sistemas de acesso e intrusão com relatórios integrados e funcionalidades de gerenciamento de alarmes.

Com esse tipo de solução, é possível configurar e gerenciar câmeras de vídeo, portas de acesso controlado, imprimir crachás, monitorar painéis de intrusão e ter tudo à disposição do pessoal de segurança para garantir o nível de segurança de uma instalação dentro de um único e consistente pacote de software.

Uma solução unificada aberta protege o investimento do usuário final por meio da interoperabilidade, atende às necessidades de segurança do usuário e é acessível para comprar e manter.

Uma plataforma unificada aberta é um produto que visa o mercado de massa, fornecendo suporte integrado para produtos de segurança comodificados, como câmeras IP, DVRs, controladores de porta, painéis de alarme, intercomunicadores, impressoras de crachás, diretório ativo para autenticação e gerenciamento de cartões sem exigir customização para cada instalação.

Esse tipo de solução visa o mercado de massa, oferece interoperabilidade pronta para uso e tende a ser mais barato do que uma solução customizada integrada.

Sendo que uma plataforma unificada oferece suporte a produtos comoditizados, os investimentos em hardware também são protegidos. Portanto, se o usuário final não estiver satisfeito com a solução de software unificada, ele poderá alterar os componentes do software sem precisar reinvestir em dispositivos especializados.

No entanto, algo a ter em mente é que, mesmo que a customização não seja obrigatória para implantar uma plataforma unificada, ela ainda deve permitir integração e customizações de terceiros por meio de um SDK ou API. Essas ferramentas devem estar disponíveis para permitir que os usuários finais projetem e mantenham as integrações personalizadas além de seus aplicativos de vídeo e controle de acesso, e não dependam apenas do fabricante da plataforma unificada para essas iniciativas no futuro.

A Infraestrutura de Servidor Unificado

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

Esse tipo de arquitetura é mais fácil de instalar e gerenciar porque consiste em um único conjunto de software para conhecer, configurar, fazer upgrade e backup, diferente do sistema integrado, onde essas tarefas devem ser executadas para todos os sistemas envolvidos.

Uma infraestrutura de servidor centralizada também simplifica a vida do usuário final porque ele só precisa se conectar a um único servidor usando um único login. A partir dessa conexão, eles têm acesso a todos os serviços oferecidos pela plataforma unificada. Eles não precisam mais se conectar a servidores diferentes enquanto realizam investigações de controle de acesso e vídeo.

A unificação do servidor até a interface oferece vantagens além das necessidades iniciais do usuário final, como:

- Maior eficiência através do uso de uma única interface
- Correlação automatizada de eventos entre sistemas

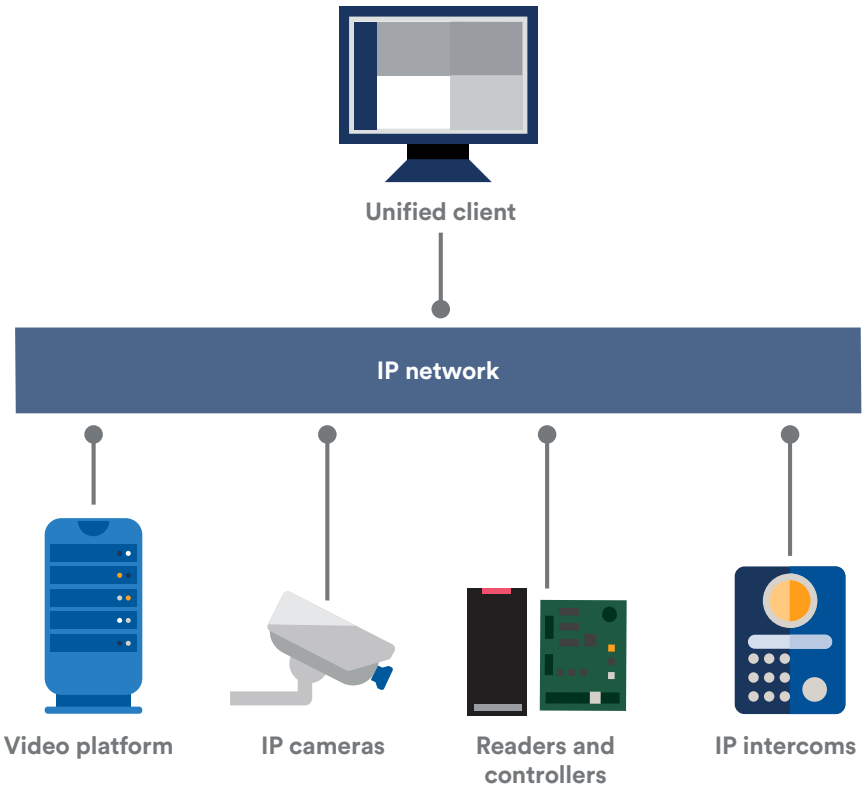

Figura 2 - Arquitetura de plataforma unificada

- Custo-benefício da configuração e manutenção compartilhadas

A Experiência do Usuário

Uma única interface de usuário para várias aplicações de segurança permite que os operadores passem de uma tarefa de segurança para outra com facilidade e eficiência dentro da mesma interface, evitando fluxos de trabalho complicados e manipulações de interface para chegar até a janela necessária.

Os fluxos de trabalho do usuário são consistentes entre o vídeo e as tarefas de controle de acesso para que o usuário se familiarize mais com o sistema, experimente o autoaprendizado e ganhe mais confiança em sua capacidade de usar o sistema.

Mais ainda, o número total de fluxos de trabalho para entender é reduzido por ter funções centrais comuns. Por exemplo, gerenciamento de alarmes, do evento para a ação, relatórios, investigações e fluxos de trabalho relacionados a incidentes são todos iguais, independentemente de serem para vídeo, controle de acesso ou comunicações de voz.

Como os sistemas unificados compartilham uma interface de usuário comum, é possível alternar de uma aplicação para outra de modo perfeito e é necessário menos tempo para treinar novos operadores em sistemas individuais.

Correlação de Eventos

Um sistema unificado é projetado para oferecer correlação de eventos porque eventos e alarmes são gerenciados por uma única infraestrutura de servidor. Os eventos de acesso e vídeo são correlacionados para permitir que os operadores analisem rapidamente os alarmes no sistema. Por exemplo, um operador pode validar rapidamente a identidade de um portador de cartão quando ocorre um evento de acesso, para garantir a autenticidade de uma credencial.

Uma plataforma unificada com boa correlação de eventos pode reduzir significativamente o tempo de investigação filtrando alarmes falsos.

Facilidade de Manutenção e Suporte

Com um sistema unificado, uma única plataforma de software precisa passar por upgrade e manutenção, ao contrário de uma solução integrada em que vários sistemas individuais precisam ser cuidados. Essa maior conveniência permite aos integradores
economizar tempo ao fazer upgrade do sistema de segurança e também possibilita que lidem com um único fabricante, caso precisem de suporte. Isso também permite que os usuários finais minimizem o tempo de inatividade do sistema durante upgrades e garante um tempo de resposta mais rápido para atender aos requisitos de seu sistema.

E quanto ao PSIM?

O gerenciamento de informações de segurança física (PSIM) é um produto de software capaz de supervisionar vários sistemas distintos. A principal função de um PSIM é gerenciar informações provenientes de diferentes sistemas e apresentá-las dentro de uma única interface de usuário.

Ao contrário de uma plataforma unificada, um PSIM geralmente não possui uma solução integrada de controle de acesso, intrusão ou videomonitoramento. Em vez disso, integra diferentes sistemas por meio de SDKs e APIs proprietários. Desafios de compatibilidade também podem surgir quando um dos subsistemas requer upgrade ou manutenção. Além disso, cada sistema integrado em um PSIM deve ser configurado separadamente e há um elevado grau de redundância e esforço duplicado (por exemplo, configuração de usuários em um PSIM e o controle de acesso subjacente, vídeo, comunicações de voz e sistemas de intrusão).

Por outro lado, um PSIM integra-se a uma gama mais ampla de produtos porque eles customizam o sistema em cima de vários sistemas de segurança dentro de uma corporação. No entanto, optar por um PSIM pode ser difícil e caro.

As desvantagens das integrações personalizadas em um PSIM e os custos de longo prazo associados para manter o suporte para uma variedade de produtos altamente customizados devem ser considerados objetivamente ao escolher a melhor tecnologia de segurança para as necessidades de uma organização.

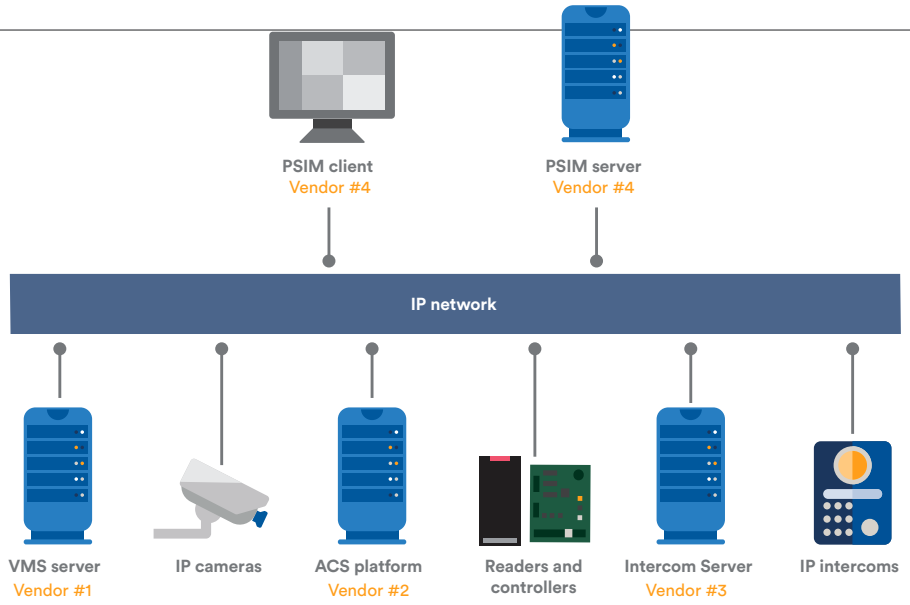

Figura 3 - Desvantagem de uma arquitetura PSIM versus uma arquitetura de plataforma unificada

Escolhendo uma Solução

Você está sendo eficiente, flexível e econômico na maneira como aborda a integração de vídeo e controle de acesso?

Como você leu nas páginas anteriores, há muitas maneiras de implantar um sistema de segurança física que inclui videomonitoramento e controle de acesso. Embora a interface e a integração sejam os métodos mais comumente implantados, a unificação de plataforma aberta oferece as aplicações de vídeo e controle de acesso mais eficientes, flexíveis e econômicas.

Por isso que é importante reservar um momento para analisar se você está empregando o método mais ideal de unificar seus sistemas de controle de acesso e vídeo. A resposta pode ajudá-lo a ganhar tempo e reduzir custos.

Sobre a Genetec

A Genetec™ desenvolve software de plataforma aberta, hardware e serviços baseados na nuvem para o setor de segurança física e segurança pública. Seu produto carro-chefe, o Security Center, unifica o videomonitoramento baseado em IP, controle de acesso e reconhecimento automático de placas de veículos (ALPR) em uma única plataforma. Um inovadora global desde 1997, a Genetec™ está sediada em Montreal, Canadá, e atende organizações empresariais e governamentais por meio de uma rede integrada de revendedores, integradores e consultores em mais de 80 países. A Genetec™ foi fundada com base no princípio da inovação e permanece na vanguarda das tecnologias emergentes que unificam os sistemas de segurança física. Para mais informações sobre a Genetec™, visite: genetec.com/br

Descubra por que a Genetec se encaixa.

genetec. com