



# Considerações de TI para projetar um sistema de vídeo IP

Nove preocupações críticas de TI ao projetar um sistema de vídeo IP

## Índice

Introdução .....	3
1. O papel da experiência de TI para os sistemas de vídeo.....	4
2. Redimensionando equipamentos para atender às necessidades de videovigilância.....	5
3. O papel crítico da rede.....	6
4. Enfatizando o valor acima do preço .....	7
5. Ameaças e soluções de cibersegurança.....	7
6. Limitações de uma abordagem de “rede isolada” .....	8
7. Garantindo que não haja perda de dados de vídeo .....	9
8. Gerenciando ciclos de vida em sistemas de vigilância IP .....	10
9. O ecossistema de TI em sistemas de vídeo .....	10

A Alcatel-Lucent Enterprise contratou a SourceSecurity.com para produzir este documento.



## Introdução

Um sistema de videovigilância tem necessidades específicas quando se trata de tecnologia da informação (TI). Embora um sistema de vídeo digital possa usar as mesmas tecnologias que outros sistemas de TI, eles são configurados de maneira diferente tendo as necessidades específicas de videovigilância em mente.

O vídeo é um ambiente mais exigente, e coloca uma carga de trabalho mais pesada em cada parte de um sistema de TI. Considerando o estresse, especialmente no caso de um sistema corporativo maior, as coisas podem começar a falhar. A escolha do equipamento correto para o trabalho garante maior confiabilidade ao longo do tempo.

A Alcatel-Lucent Enterprise trabalhou com os especialistas SourceSecurity.com e Stone Security para identificar as nove preocupações críticas de TI ao projetar um sistema de vídeo IP. Neste whitepaper, exploramos como as necessidades específicas de um sistema de vigilância por vídeo impactam, quais tecnologias de TI são implantadas e como elas são usadas.

### Whitepaper

Considerações de TI para projetar um sistema de vídeo IP



## 1. O papel da experiência de TI para os sistemas de vídeo

Projetar e criar um sistema de videovigilância baseado no Protocolo de Internet (IP) requer um alto nível de conhecimento em TI para a comunidade de integradores.

Alguns integradores têm habilidades suficientes para lançar habilmente um sistema de vídeo IP, enquanto outros podem ter dificuldades.

Os treinamentos e certificações extras, familiares à maioria do mundo de TI, podem permitir que os integradores forneçam o alto nível de serviço exigido. Para começar, os instaladores devem ter a aptidão adequada, um conhecimento básico de redes e habilidades de solução de problemas.

Os integradores podem garantir uma equipe qualificada, limitando sua gama de escolhas tecnológicas e assegurando que cada funcionário seja bem treinado nas poucas tecnologias selecionadas. Selecionar soluções de alta qualidade e garantir que os funcionários sejam especialistas nesses produtos permite que um integrador entregue um sistema de alta qualidade aos clientes.

Limitar a combinação de produtos também permite que um integrador compreenda melhor a amplitude de recursos oferecidos por qualquer produto específico. Muitas vezes, o cliente compra um sistema que oferece uma variedade de recursos e, em seguida, utiliza apenas um número limitado desses recursos na sua operação diária, minando assim o valor do sistema pelo qual pagou.

Os integradores podem ajudar os clientes, instruindo-os a utilizar o valor total de qualquer sistema que comprem.

Os integradores também podem depender dos serviços de pré-consultoria dos fabricantes de equipamentos para orientá-los. Em alguns casos, os fabricantes de equipamentos possuem conhecimentos específicos sobre diversos mercados verticais, acumulados ao longo de uma história de atendimento a esses mercados.

Os fabricantes que levam a sério os mercados verticais específicos contratarão especialistas do setor para garantir o suporte especializado às necessidades de cada cliente. A sua orientação pode ajudar os integradores a terem sucesso em novos mercados e/ou a simplificar as melhores práticas para os mercados em que operam.

Os fabricantes também oferecem treinamentos e certificações, para garantir que os integradores estejam bem preparados para instalar seus sistemas. Um treinamento eficiente e substancial deve ser apresentado em sessões mais curtas, que respeitem o valor do tempo de cada participante.

## 2. Redimensionando equipamentos para atender às necessidades de videovigilância

Questões como requisitos de largura de banda e Power over Ethernet (PoE) são variáveis importantes em um sistema de vídeo. E o servidor de vídeo deve suportar uma carga maior, principalmente quando se trata de vídeos de transmissão ao vivo. Cada bit de dados chega ao servidor, mesmo os dados que não estão sendo registrados.

O vídeo é armazenado em buffer, o que garante que haja pelo menos alguns segundos de vídeo que possam ser preservados antes de uma gravação de vídeo com acionamento de alarme. Períodos mais longos de buffer podem ser necessários no caso de identificação de uma imagem que se aproxima, vinda de alguma distância. Todas as entradas e saídas passam pelo servidor, mesmo que uma quantidade limitada de dados seja gravada no armazenamento de longo prazo.

Há uma diferença fundamental entre como os integradores de sistemas de segurança veem o tamanho do sistema e como os profissionais de TI o veem. Os integradores de sistemas são mais propensos a falar em termos de contagem de câmeras, enquanto os profissionais de TI são mais propensos a falar em termos de gerenciamento de dados do sistema. Os dois estão intrinsecamente ligados, é claro, mas a relação não é linear. Em geral, uma contagem maior de câmeras equivale a mais dados a serem gerenciados pelo departamento de TI. Entretanto, há outros fatores envolvidos que impactam as necessidades de dados, como contagem de quadros, requisitos de qualidade de imagem, necessidades de armazenamento, aplicações diurnas/noturnas e uso de análise de vídeo.

Uma habilidade fundamental ao especificar um sistema de segurança IP é traduzir os requisitos de equipamentos e funcionalidades do sistema nos dados necessários para atender a essas necessidades. Para um sistema local, isso equivale à necessidade de especificar um servidor de computador que maximize o desempenho do sistema e reduza os custos. Questões como virtualização e sistemas em nuvem podem complicar a equação e proporcionar nova flexibilidade.

Outra variável relacionada ao projeto do sistema é o uso de câmeras na borda da rede para gravar vídeo usando cartões SD. Existem ainda sistemas que são “sem servidor”; por exemplo, onde toda a gravação ocorre na borda. Tal abordagem, na verdade, alivia a carga computacional do servidor para a borda, com a conseqüente diminuição da necessidade de capacidade do servidor. As câmeras atuais fornecem dados além do fluxo de vídeo, como metadados e áudio, que também impactam o projeto do sistema.

Os profissionais de TI devem ter uma visão completa de todo o sistema, como o que será conectado, taxas de quadros, resolução e codecs de vídeo das câmeras. Com essas informações, eles podem calcular os requisitos de rede, energia, servidores, capacidade de disco, memória, armazenamento, e se devem usar sistemas locais ou em nuvem. Isso garante uma abordagem completa e cuidadosa para design e implantação.

Os fabricantes fornecem “calculadoras” de software para ajudar os integradores a projetar sistemas, traduzindo os requisitos do sistema em especificações de equipamentos. Tenha em mente que os cálculos devem atender ou superar as expectativas e permitir o crescimento futuro.

A implementação de sistemas em nuvem é outra variável quando se trata do projeto de sistemas de videovigilância. Uma tendência clara é o uso de mais sistemas em nuvem para vigilância por vídeo. No entanto, a escolha das soluções em nuvem versus soluções locais deve ser feita caso a caso. Os arquitetos de sistemas e os usuários finais devem resistir à aparente inevitabilidade da nuvem e, em vez disso, tomar decisões com base nas necessidades do cliente.

Muitos fabricantes estão sob pressão para fazer a transição dos seus sistemas para a nuvem, mas o ideal é que forneçam aos seus clientes a possibilidade de escolha do sistema, e não uma solução única para todos.

Os fabricantes estão em uma boa posição para aconselhar os clientes sobre a conveniência de uma configuração em nuvem em vez de um design local. Os integradores também devem estar bem familiarizados com as vantagens de qualquer abordagem ou facilitar a decisão do cliente de qualquer maneira. O mercado não deveria empurrar aplicações para a nuvem, a menos que essa seja a abordagem ideal para cada cliente individual.

### 3. O papel crítico da rede

Um sistema de vídeo é tão forte quanto o seu elo mais fraco. Os switches de rede podem não ser tão visíveis quanto as câmeras e os VMSs, mas não são menos críticos.

O que tende a acontecer, porém, é que os clientes consideram o funcionamento de uma rede algo garantido, prestando pouca atenção ao seu funcionamento ou à forma de maximizar a sua utilidade. Na verdade, alguns clientes desejam instalar seu sistema de vídeo utilizando a infraestrutura de rede existente. Isso é possível, mas a capacidade de otimizar a rede de um sistema de vídeo pode ser limitada.

Idealmente, o cliente optará pelos melhores switches para vigilância por vídeo, o que garantirá um sistema que funcione de forma confiável e eficaz.

Cada sistema de vídeo é diferente, e portanto, dar atenção especial aos seus requisitos individualizados garante que ele atinja sua missão específica. Ao comissionar um sistema, a rede não deve ser vista como algo secundário. Em vez disso, deve ser cuidadosamente implementada utilizando os melhores componentes para aprimorar as operações em todo o sistema.

Switches que funcionam em “wire speed”, o que significa que têm poder de processamento suficiente para lidar com velocidade Ethernet total em tamanhos mínimos de pacotes, agora são padrão na indústria. Um novo ponto de diferenciação entre switches é a capacidade de entender e gerenciar seu tráfego.

Switches não gerenciados estão disponíveis no mercado, mas não são normalmente utilizados para aplicações comerciais e/ou empresariais. Eles são projetados para uso em redes pequenas com necessidades básicas, não há configurações para ajustar.

Por outro lado, switches gerenciados possibilitam a detecção e diagnóstico de problemas de desempenho e garantem uma performance confiável dos sistemas de videovigilância. Eles permitem que os usuários visualizem detalhadamente o que pode estar causando problemas no sistema e forneçam uma análise de como essas informações se apresentam.

O valor dos switches gerenciados, que são totalmente configuráveis, personalizáveis e fornecem uma variedade de dados sobre o desempenho, será evidente ao longo da vida útil do sistema, fornecendo insights importantes sobre a operação do sistema e facilitando a identificação de problemas.

Os switches devem ser projetados para atender às necessidades dos sistemas de vídeo IP. Como exemplo, no caso de um switch de 16 portas, é um consumo estimado de energia suficiente para operar todas as câmeras de vídeo conectadas ao switch. As câmeras PoE de hoje consomem mais energia do que as gerações anteriores. Os integradores precisam saber se o switch fornece energia suficiente para lidar com o número de câmeras e o crescimento futuro.

**“Quando estamos fazendo nossa seleção de hardware, queremos que cada switch tenha os recursos de largura de banda, o consumo estimado de energia e seja um switch gerenciado que nos poupe muito tempo na solução de problemas. Eles poupam o nosso dinheiro, e também poupam o dinheiro do cliente. É um investimento maior no início, mas que se pagará em longo prazo com a criação de um sistema mais fácil de ser reparado.”**

**Aaron H. Simpson, Presidente e CTO da Stone Security**

## 4. Enfatizando o valor acima do preço

A confiabilidade é fundamental na vigilância por vídeo, e começa com a escolha do equipamento.

Especificar componentes de menor qualidade pode parecer uma necessidade econômica no momento. No longo prazo, porém, a operação do sistema será prejudicada. O custo de escolher uma operação abaixo do ideal pode não ser óbvio ao projetar um sistema, mas ficará bastante claro com o tempo.

Por outro lado, escolher um equipamento melhor – mesmo que seja mais caro – compensará o investimento.

É fundamental pesar os custos (tais como o preço de melhores equipamentos) em relação aos riscos de inadequação ou falha do sistema. Adotar uma abordagem de custo total de propriedade (TCO) ao avaliar custos e riscos é a melhor estratégia. Outro elemento de custo a longo prazo a considerar é o valor dos sistemas abertos, que podem garantir flexibilidade ao expandir ou alterar um sistema no futuro.

É sempre melhor trabalhar com um fornecedor que ofereça produtos nos quais se tenha confiança e que possa oferecer suporte por um longo período.

## 5. Ameaças e soluções de cibersegurança

Historicamente, uma ironia na indústria da segurança física tem sido a falta de atenção à cibersegurança dos sistemas IP.

Felizmente, os envolvidos na segurança física estão agora dando mais atenção às preocupações de cibersegurança, em todos os níveis e em toda a cadeia de suprimentos de segurança física. Na verdade, a segurança cibernética tornou-se um dos principais pilares do processo de tomada de decisão para sistemas de segurança por vídeo de maior porte.

O mínimo para se proteger contra ameaças cibernéticas e restringir o acesso a um sistema é evitar o uso de senhas padrão. Elas são menos seguras e podem ser descobertas mais facilmente por um hacker ou bot. Na verdade, as senhas padrão foram proibidas na Califórnia.

Os riscos de cibersegurança começam na cadeia de suprimentos, onde os ataques podem comprometer um produto antes mesmo dele ser entregue. Analisar um produto em busca de possíveis ataques de “backdoor” ou “buffer overflow” antes da entrega pode mitigar a ameaça. Os clientes também podem optar por instalar virtualmente o “código bom” após a entrega dos produtos de hardware, garantindo assim a cibersegurança e substituindo qualquer código malicioso que possa ter sido instalado durante o envio.

Há também uma série de medidas de cibersegurança a serem abordadas durante a instalação e nos vários estágios de implementação do sistema. Por exemplo, a “segurança de porta aprendida” garante que uma porta seja acessada apenas por um dispositivo autorizado. Se um dispositivo não autorizado tentar se conectar ao sistema – por exemplo, para conectar uma nova câmera – um alerta será acionado e o acesso à porta será negado até que seja autorizado por uma pessoa.

A tecnologia Shortest Path Bridging (SPB) pode impedir que atividades maliciosas passem de um sistema para outro. As regras são configuradas para que uma câmera só possa transmitir para o gravador, e outras tecnologias de segmentação poderosas são implantadas em redes multi-IoT.

Os sistemas devem desativar protocolos inseguros, como FTP e Telnet, que facilitam a comunicação através de uma rede, mas podem fornecer oportunidades adicionais para hackers. Estas funcionalidades devem ser “seguras por padrão” para não permitir uma conexão à rede, a menos que seja intencional.

A cibersegurança eficaz também requer a restrição do acesso físico a um sistema. Se um switch for instalado no armário do zelador onde o acesso físico é aberto a todos, ele não estará bem protegido. Permitir o acesso físico a um sistema torna mais fácil para qualquer pessoa – incluindo um funcionário que representa uma ameaça interna – conectar um laptop e acessar todo o sistema.

As câmeras devem registrar o acesso aos equipamentos de rede como uma abordagem de “defesa em profundidade”.



## 6. Limitações de uma abordagem de “rede isolada”

Quando se trata de proteger sistemas de vídeo contra ataques de cibersegurança através da Internet, uma abordagem historicamente comum tem sido a criação de sistemas isolados (air-gapped).

Um sistema isolado envolve restringir um computador ou rede e impedir que ele estabeleça uma conexão externa. Como um computador isolado é fisicamente segregado e incapaz de se conectar fisicamente ou sem fio a outros computadores ou dispositivos de rede, a abordagem é vista como panaceia para garantir a cibersegurança do sistema de vídeo.

No entanto, é uma proposta arriscada depender de um air-gap como única proteção de cibersegurança. Há diversas situações em que um sistema isolado pode ser exposto à Internet, mesmo que por um curto período. Quando isso acontece, o sistema depende de quaisquer outras medidas de cibersegurança (se existirem) para protegê-lo contra desastres.

Presumir que um sistema ficará isolado para sempre não é uma solução de cibersegurança. Ao contrário, é um desastre esperando para acontecer.

Os sistemas isolados também não são capazes de tirar proveito da inteligência artificial (IA) e de outros recursos que dependem do acesso de muitos usuários e da análise de experiências compartilhadas. Os dados de um único cliente não são tão úteis quanto os dados de centenas de clientes, disponíveis na nuvem. Os sistemas isolados não permitem que os clientes aproveitem o valor agregado de análises mais inteligentes. Desistir de alguns dados (que vêm com considerações de privacidade) é um preço que os clientes pagam para gerar maior valor.

Devido aos requisitos atuais dos clientes para se conectarem e terem acesso contínuo aos seus sistemas, o uso de sistemas isolados está se tornando cada vez mais limitado.

As organizações também tendem a recuar diante da perspectiva de criar uma infra-estrutura de rede totalmente separada para a videovigilância. Não existe uma rede “separada e segura”.

## 7. Garantindo que não haja perda de dados de vídeo

A perda de dados é um problema para qualquer sistema de TI, mas ainda mais para sistemas de TI que fornecem vigilância por vídeo. Um sistema de vigilância por vídeo é de importância crítica e deve operar 24 horas por dia, 7 dias por semana. Não há tempo de inatividade para permitir que os administradores diagnostiquem e resolvam problemas de perda de dados; pelo contrário, os problemas devem ser abordados constantemente e em tempo real.

É aqui que os switches gerenciados podem ajudar. Os switches gerenciados podem permitir que os administradores do sistema diagnostiquem e resolvam rapidamente qualquer problema de perda de dados. Também podem identificar facilmente a(s) origem(s) da perda de dados. Não há acusação sobre qual componente do sistema está com defeito.

Os pacotes podem ser descartados devido à conversão de dados da transmissão de fibra para cobre e Ethernet. Transceptores elétricos são usados para traduzir dados de transmissão de fibra para transmissão elétrica, e os dispositivos podem ser uma fonte de pacotes de dados descartados.

Na videovigilância, um pacote de dados perdido equivale a comprometer uma imagem de vídeo – fazendo com que ela seja, na verdade, perdida para sempre. Não há como restaurar imagens de vídeo perdidas durante interrupções no tempo de inatividade. Consideremos uma aplicação de cassino, por exemplo, onde a consequência de uma falha no sistema de vídeo é a perda de cobertura de uma mesa de jogo, o que, por sua vez, também pode significar perda de receitas.

Na ampla variedade de aplicações de vigilância por vídeo, a redundância é necessária para garantir a operação contínua 24 horas por dia, 7 dias por semana.

A necessidade de confiabilidade deve ser ponderada no contexto do risco versus benefício. Um sistema pode ser menos caro, menos complexo e/ou menos tolerante a falhas, mas tal sistema pode não funcionar conforme o previsto — o que tem seus próprios custos.

Outra variável que pode causar problemas de desempenho em sistemas de vídeo gira em torno da distinção entre unicast e multicast, que são dois métodos para enviar dados por uma rede. O unicast fornece um modelo de comunicação “um para um”, no qual um único remetente entrega dados a um único receptor. Por outro lado, o multicast é um modelo “um para muitos”, no qual um único remetente entrega dados a vários destinatários.

Muitas aplicações de vigilância por vídeo operam no modo unicast. Isso significa que uma câmera é monitorada em tempo real por um indivíduo — um único fluxo de vídeo está envolvido.

Entretanto, algumas aplicações requerem multicast, no qual um único fluxo de vídeo é visualizado por vários usuários. Os problemas surgem quando um sistema faz a transição de unicast para multicast. Fazer a transição envolve mais do que apenas “apertar um botão”. Nuances e detalhes da transição podem causar problemas no desempenho do sistema. Os problemas aparecem se as partes de um sistema são configuradas para unicast quando deveriam ser multicast, ou vice-versa. A configuração adequada neste ponto, em todo o sistema, é crucial.

Os recursos inteligentes do network advisor permitem que um usuário final entenda o que é normal em termos de desempenho da rede, e então detecte quando algo está anormal ou fora dos limites das expectativas habituais. Quaisquer desvios são relatados automaticamente, e os humanos podem intervir conforme necessário para resolver os problemas.



## 8. Gerenciando ciclos de vida em sistemas de vigilância IP

No mundo da TI, os ciclos de vida dos produtos podem ser de três a 10 anos dependendo do setor e do produto. Existem protocolos existentes para lidar com questões como tempo médio entre falhas (MTBF), firmware e patches de segurança.

No campo da vigilância por vídeo, os ciclos de vida dos produtos historicamente têm sido mais longos — há câmeras de vídeo com décadas de idade ainda operando em campo. Adaptar as estratégias de gerenciamento de TI aos sistemas de vídeo IP pode revelar uma desconexão.

O suporte de TI fornecido pelo fabricante oferece um valor imenso ao integrador e ao usuário final. Historicamente, ciclos de vida mais longos na segurança física resultaram em sistemas que continuam a operar além do período esperado e em um ambiente não suportado.

Existem riscos inerentes ao continuar usando equipamentos que não são suportados pelo fabricante. Por exemplo, não atualizar o firmware pode abrir a porta para ameaças à cibersegurança.

A maioria dos equipamentos atuais tem uma garantia de cinco anos e, realisticamente, poderia continuar funcionando por mais cinco anos. Entretanto, com o cenário tecnológico em rápida mudança, a maioria dos clientes deseja utilizar funcionalidades mais atuais. De fato, a aceleração da tecnologia equivale a ciclos de vida mais curtos em segurança, assim como acontece no ambiente mais amplo de TI e de rede.

## 9. O ecossistema de TI nos sistemas de vídeo

Um ecossistema de TI unificado é a melhor abordagem para garantir o sucesso de um sistema de vídeo IP. O sucesso de qualquer nova tecnologia depende de um ecossistema de TI que lhe dê suporte. Questões como a interoperabilidade de hardware e software garantem a operação tranquila do sistema.

Os padrões abertos garantem a máxima flexibilidade para os clientes, no presente e no futuro. As operações simplificadas também são bastante úteis. Por exemplo, a [Alcatel-Lucent Enterprise](#) tem um único sistema operacional que funciona com todos os switches Ethernet vendidos pela empresa.

Para garantir o sucesso, mantenha uma estratégia de adoção de produtos que “funcionem bem” em seu ambiente e com outros produtos do ecossistema.

Um ecossistema de TI bem-sucedido não acontece por acaso. Em vez disso, ele é alimentado por parceiros do setor que trabalham juntos para garantir o sucesso. Princípios como abertura e interoperabilidade contribuem para o ecossistema de TI. O sucesso aumenta o desempenho de cada componente de um sistema, e do sistema como um todo.

**Saiba mais sobre as [Soluções de Videovigilância da Alcatel-Lucent Enterprise](#).**