WHITE PAPER

Proteção do perímetro com monitoramento inteligente

Um estudo das opções de sensores, aplicativos e importantes considerações para garantir uma solução de segurança preparada para o futuro e uma variedade de setores.

Julho 2021

AXIS COMMUNICATIONS

Sumário

1 Resumo

Uma cerca é muitas vezes um componente fundamental da "camada externa" da segurança de um site e pode atuar como uma barreira, uma tela ou um impedimento para pessoas e animais. Outros recursos podem ser incorporados para melhorar a eficácia da cerca, já que qualquer barreira física só pode atrasar ou impedir uma intrusão.

Vários tipos de detectores são usados juntamente com as cercas. Os detectores baseados em cabos podem seguir a rota da cerca, e sensores de radar (micro-ondas), barreiras infravermelhas ou lasers podem ser posicionados em locais estratégicos.

Todos os tipos de detectores podem produzir alarmes falsos, causados, por exemplo, por animais, plantas e árvores em movimento e clima severo. Também pode haver outros fatores de restrição, como choques de frequência ao usar sensores de micro-ondas ou limitações físicas no ambiente de instalação.

As câmeras fornecem um benefício óbvio aos que desejam monitorar grandes áreas ou vários locais. As soluções modernas de vídeo em rede combinam processamento do computador na câmera e inteligência artificial. A escalabilidade, eficácia e natureza dissuasiva inerentes da tecnologia significam que as câmeras de vídeo são potencialmente uma adição altamente econômica a um sistema de segurança.

Embora as câmeras e o software de detecção de movimento tenham expandido o alcance e os recursos de proteção de perímetro, essas soluções podem ser limitadas pela incapacidade de detectar em condições climáticas adversas. Câmeras térmicas, quando apropriadamente calibradas e acopladas à análise de vídeo, oferecem monitoramento eficaz, não afetado pelas condições de iluminação e virtualmente desimpedidas pelas condições climáticas extremas.

A análise de vídeo evoluiu significativamente ao longo do tempo e agora é comum, mesmo em câmeras destinadas ao mercado de segurança residencial. A análise pode reduzir os requisitos de armazenamento gravando apenas o vídeo que contém a atividade de interesse. Ao processar grande parte do vídeo gravado na própria câmera, a carga na rede é significativamente reduzida, pois apenas vídeo relevante é transmitido através de stream das câmeras. Isso tem benefícios óbvios em um cenário de sala de controle.

Como com qualquer medida de segurança, a avaliação de uma solução de proteção de perímetro deve ser apropriada e proporcional. Como sempre, a ameaça deve ser a principal consideração.

Uma abordagem convergente de segurança que inclui entradas e considerações de outros departamentos, tais como TI e operações, está se tornando prática recomendada rapidamente. Isso inclui a necessidade de incluir as pessoas que lidam com a engenharia o mais cedo possível.

Demonstrar o retorno do investimento (ROI) de uma solução de segurança projetada para evitar um incidente é notoriamente difícil. Isso se deve principalmente à falta de receita potencial para comparar ao custo. É possível demonstrar um ROI mais tangível; os exemplos incluem soluções que não apenas alertam a equipe sobre comportamento suspeito ou intrusão, mas também produzem respostas automatizadas.

2 Introdução

As soluções eletrônicas de proteção de perímetro têm sido tradicionalmente o domínio de sites governamentais e comerciais de alta segurança ou dos muito ricos. Com avanços na tecnologia, um mercado mais competitivo e a redução consequente nos custos, soluções relativamente de alta tecnologia agora estão disponíveis para muitos mais.

Então em que uma solução de proteção de perímetro moderna consiste? Qual é a tecnologia em ação e como ela pode fornecer tanto segurança quanto proteção genuína?

Este white paper analisa algumas das opções atuais baseadas em sensor para proteger um perímetro e fornece uma visão sobre a tecnologia por trás das soluções.

3 Soluções de proteção de perímetro

3.1 Soluções físicas

As soluções físicas normalmente são um componente fundamental da "camada externa" de uma abordagem compartimentalizada para proteger um site, que normalmente compreende uma cerca de perímetro, muitas vezes construída de arame ou malha soldada, em painéis soldados ou concretos. Uma cerca de perímetro serve muitas finalidades, uma das principais sendo apresentar uma barreira física que atrasará ou prevenirá invasões. Uma cerca pode também impedir o monitoramento ao rastrear um ativo e serve como um impedimento e detém a entrada de animais. Recursos como dispositivos antiescalada, rotas designadas de acesso de veículo, dispositivos anticruzamento e telas de cerca também podem ser incorporados para aprimorar a eficácia de uma cerca de perímetro.

No entanto, qualquer barreira física invariavelmente apenas atrasarão uma intrusão. Consequentemente, o perímetro deve também ser equipado com tecnologia de detecção de intrusão automática, que é capaz de fornecer alertas verificáveis em tempo real, dados de localização, rastreamento de alvos e a capacidade de juntar evidências e dados para investigação pós-incidente.

3.2 Detecção de intrusão no perímetro físico

Vários tipos de "detectores" de cabo são frequentemente usados para proteger perímetros estendidos. Estes detectores com base em cabos são usualmente enterrados no solo ou montados na cerca. Eles seguem a rota da cerca e não precisam estar em linha reta. Eles também fornecem cobertura em torno de esquinas e em **áreas mortas**. Alguns fornecedores oferecem cercas equipadas com soluções de detecção automática.

Como acontece com qualquer solução de detecção, os detectores baseados em cabos podem produzir alarmes falsos, chamados de "falsos positivos". As causas comuns de falsos positivos incluem animais, plantas e árvores em movimento e clima severo. As soluções baseadas em cabo trabalham melhor quando aumentadas com videomonitoramento. O vídeo pode ser usado não somente para verificar uma intrusão, mas também para determinar a causa de um alarme. Uma solução baseada em cabo apenas será capaz de fornecer um alerta para a própria intrusão. Ela não poderá fornecer informações sobre o número de invasores ou quaisquer outros detalhes necessários para preparar uma resposta.

3.3 Outros sensores de detecção de intrusão

Outros detectores de intrusão, tais como sensores de radar (micro-ondas), barreiras infravermelhas ou lasers, podem ser posicionados em locais estratégicos ao redor do perímetro. Novamente, essas tecnologias podem ser restringidas por questões como falsos positivos e recursos de detecção limitados com relação à distância e altura se as regras de instalação não forem seguidas corretamente.

O uso do radar no perímetro pode ser particularmente problemático em um ambiente que usa outros dispositivos eletrônicos. Estes podem operar na mesma frequência e espectro e, embora uma escolha cuidadosa de frequência ou redução na potência possa reduzir a interferência, também prejudicará o alcance eficaz do dispositivo.

4 Soluções baseadas em vídeo

4.1 A aplicação das câmeras de vídeo

As tecnologias autônomas de CFTV do passado têm pouca semelhança às soluções de câmera em rede de alta tecnologia disponíveis hoje. As soluções em rede modernas são capazes de combinar o processamento do computador na câmera e inteligência artificial. Este nível de tecnologia, no entanto, apenas foi disponibilizado recentemente e ainda está em sua infância.

As câmeras fornecem um benefício óbvio aos que desejam monitorar grandes áreas ou vários locais. A escalabilidade, eficácia e natureza dissuasiva inerentes da tecnologia significam que as câmeras de vídeo são potencialmente uma adição altamente econômica a um sistema de segurança.

Dependendo da legislação local, a tecnologia de câmera pode ser usada para monitorar além do perímetro físico, fornecendo um buffer de monitoramento adicional e potencialmente permitindo ao operador tempo extra para responder. As soluções que aproveitam a análise de vídeo tornam possível acionar um alarme de acordo com regras estabelecidas. Por exemplo, um alarme soa se uma pessoa se aproxima a 50 metros de uma cerca. Um nível mais alto de alarme pode ser acionado se a mesma pessoa continuar a perambular ou entrar na zona de 10 metros.

4.2 Soluções termográficas de videomonitoramento

A combinação de câmeras de videomonitoramento e software de detecção de movimento expandiu a faixa e as capacidades das soluções de proteção de perímetro, de simples detecção a análises de intrusão complexas. No entanto, a eficácia do vídeo pode ser severamente limitada por sua incapacidade de detectar em condições climáticas adversas.

O aumento da disponibilidade da tecnologia de câmera térmica levou ao destaque do seu uso no perímetro. Câmeras térmicas (ou termográficas), quando apropriadamente calibradas e acopladas à análise de vídeo, podem oferecer monitoramento eficaz, não afetadas pelas condições de iluminação e virtualmente desimpedidas pelo mau tempo. Sensores que usam tecnologia térmica fornecem contraste superior comparados a uma câmera comum de luz visível e são consequentemente benéficas para proteção do perímetro, devido aos recursos de detecção de intrusão amplamente aprimorados.

Sensores térmico criam uma imagem, usando radiação infravermelha emitida por objetos, tais como veículos ou pessoas. Quando combinadas com análise de vídeo, as câmeras térmicas modernas com poder de processamento suficiente podem distinguir entre tipos diferentes de alvo de intrusão e podem alertar o operador com base em uma lista predefinida de condições. Elas podem incluir a direção e a velocidade de uma pessoa ou veículo. Câmeras tradicionais também são capazes de fazer isso, mas precisam fazê-lo usando luz visível. Estas câmeras são exploradas na próxima seção.

4.3 Câmeras de luz visível

Todas as câmeras de monitoramento de luz visível padrões precisam de iluminação natural ou aumentada para fornecer imagens. A iluminação para apoiar o videomonitoramento é uma área de especialização por direito próprio e documentos separados foram escritos sobre este assunto importante. No entanto, ainda precisamos reiterar o ponto óbvio, mas crítico, que as câmeras padrão precisam de luz visível. A luz pode ser um desafio em qualquer ambiente, com efeitos óbvios conforme muda a qualidade da luz. Algo nem sempre considerado ou compreendido, particularmente por aqueles que especificam a solução, são os efeitos do clima.

As câmeras térmicas têm seus benefícios, mas isso não quer dizer que as câmeras térmicas devem ou podem ser uma substituição direta para a câmera de luz visível — longe disso. Estas duas tecnologias trabalham melhor quando integradas na mesma solução. As câmeras tradicionais não podem detectar objetos no alcance das câmeras térmicas, mas as câmeras térmicas não podem fornecer os detalhes forenses fornecidos pelas câmeras de luz visível. As duas tecnologias são frequentemente combinadas com a câmera térmica, oferecendo o alarme de detecção e o benefício forense da câmera de luz visível e fornecendo rastreamento de evidências e alvo.

4.4 Análise de conteúdo de vídeo

O videomonitoramento em rede trouxe uma escala sem precedentes para as operações de segurança. Uma hierarquia de permissão eficaz permite o acesso controlado por vídeo, distribuição e armazenamento em um número teoricamente ilimitado de partes interessadas. Um avanço tecnológico em particular está trazendo níveis ainda maiores de escalabilidade - análise de vídeo.

A análise de vídeo evoluiu significativamente ao longo do tempo, principalmente devido ao desenvolvimento da tecnologia de câmera IP. Isso pode ser evidenciado em câmeras destinadas ao mercado de segurança residencial, muitas das quais agora incorporam algum nível de função analítica, permitindo, por exemplo, detectar movimento na cena. Funcionalidades adicionais podem vir "embaladas" com a câmera, incluindo detecção de cruzamento de linha, objetos movidos ou até mesmo contagem de pessoas.

A análise de vídeo pode remover a necessidade de espaço de armazenamento, gravando apenas o vídeo que contém atividade. Além disso, ao processar o máximo de vídeo gravado na própria câmera (conhecida como "inteligência na borda"), a carga na rede é significativamente reduzida, pois apenas vídeo relevante é transmitido através de stream das câmeras. Isso traz benefícios óbvios em um cenário de sala de controle, com um operador de segurança apenas tendo que examinar o vídeo quando um alerta é recebido, uma grande melhoria para o operador de segurança e a eficiência operacional da organização.

Há duas amplas categorias de arquitetura de sistema para implementação de análise de vídeo: centralizada e distribuída. Em arquiteturas centralizadas, informações de vídeo e de outros dados são coletadas por câmeras e sensores e enviadas para um servidor central para análise. Em arquiteturas distribuídas, os próprios dispositivos periféricos (câmeras de rede e codificadores de vídeo) podem processar o vídeo e extrair as informações relevantes. A análise na borda remove o requisito para servidores de análise dedicados e, como a compactação é apenas utilizada para transferir dados de vídeo para um servidor central, a análise agora pode ser realizada no feed de vídeo descompactado. O resultado é uma arquitetura muito mais econômica e flexível. Na verdade, os mesmos servidores, que poderiam normalmente processar apenas alguns poucos streams de vídeo devido ao poder de processamento necessário, podem agora lidar com centenas de streams de vídeo quando grande parte do processamento é realizada nas câmeras.

4.4.1 Velocidades de processamento e GPUs

Embora a previsão precisa de Gordon E. Moore (também conhecida como Lei de Moore) de melhoria exponencial nas velocidades de processamento e capacidade tenha sido prevista por algumas empresas líderes de tecnologia para desacelerar em um futuro próximo, o atual aumento na potência, combinada com a redução no tamanho, significou que fabricantes e desenvolvedores podem mudar a maneira como o poder de processamento é aproveitado.

Até recentemente, qualquer capacidade de processamento adicional foi utilizada para melhorar a qualidade de imagem, trazendo maior resolução e compactação de vídeo mais eficiente. Por enquanto, porém, o mercado parece ter quase atingido um patamar em sua demanda por uma resolução de imagem cada vez maior. Consequentemente, os fabricantes agora estão usando o poder de processamento para fornecer níveis de inteligência nunca antes vistos na borda. Em muitos casos, isso significa que a poderosa análise de vídeo baseada em servidor agora pode se beneficiar do processamento na câmera.

As características menores e mais rápidas dos processadores modernos significam que as câmeras são capazes de acomodar unidades de processamento gráfico (GPUs), fornecendo recursos de processamento paralelo e abrindo novas oportunidades e possibilidades analíticas. Esse novo recurso resultou com que os desenvolvedores de software mudassem sua atenção para fornecer versões mais recentes de análises baseadas em servidor existentes e comprovadas em variantes baseadas na borda, ajudando a impulsionar a demanda por câmeras mais inteligentes, capazes de agregar valor muito além de apenas segurança e videomonitoramento.

4.4.2 Aprendizado profundo e inteligência artificial (IA)

As GPUs possibilitaram um salto no desempenho analítico na borda, mas a demanda está crescendo por outros tipos de tecnologia a serem aplicadas em ambientes de monitoramento, fornecendo recursos como contagem de pessoas e gerenciamento de ocupação. Desenvolvimentos em IA e aprendizagem de máquina levaram às Unidades de Processamento de Aprendizado Profundo (DLPU) a serem integradas em câmeras, o que está provando ser uma virada de jogo.

Uma DLPU é criada para uma aplicação mais ampla de análise de aprendizado profundo. Análises com base em aprendizado profundo podem fornecer precisão superior para detecção e classificação, já que o algoritmo é treinado com eficácia na aparência de um conjunto de objetos prescritos. Isso significa que uma solução de detecção de intrusão em um perímetro pode ser configurada para gerar alertas apenas para objetos e cenários muito específicos; uma versão avançada do If-this-then-this (ITTT, Se-isso-então-isso).

Em alguns casos, apenas parte de um objeto pode estar visível, como o para-choque traseiro de um carro, mas o sistema de análise do sistema ainda o reconhecerá e identificará. No momento em que este artigo foi escrito, e apesar de algumas afirmações, a maioria das soluções comprovadas no mercado se limitava a identificar e discriminar entre pessoas e tipos de veículos. No entanto, exemplos de modelos de análise baseados em câmera capazes de discriminação mais detalhada, tais como a cor das roupas que uma pessoa está vestindo, estão em um estágio avançado de testes.

Esses avanços em tecnologia poderiam potencialmente levar a sistemas de detecção altamente direcionados, capazes de identificar e diferenciar entre funcionários, clientes, público ou ameaças potenciais. De uma perspectiva de segurança, análises avançadas em um ambiente com segurança física bem aplicada podem resultar em um sistema ainda mais eficiente e preciso para detectar e prevenir crimes. A evolução para o próximo estágio de capacidade pode não demorar muito.

5 Custos

5.1 Avaliação e medição de um retorno do investimento

Como com qualquer medida de segurança, seja do ponto de vista de vulnerabilidade ou resiliência, a avaliação de uma solução de proteção de perímetro deve ser apropriada e proporcional. Como sempre, a ameaça deve ser a consideração principal, que para quase qualquer empresa de tamanho considerável ou site do governo nos tempos modernos pode variar de invasores acidentais a manifestantes ou até terroristas.

Uma abordagem convergente de segurança que inclui entradas e considerações de outros departamentos, tais como TI e operações, está se tornando prática recomendada rapidamente. Isso inclui a necessidade de envolver aqueles com experiência em requisitos de engenharia e eles devem ser envolvidos o mais cedo possível. Ao considerar as medidas a serem aplicadas, historicamente, um bom ponto de partida para o perímetro teria sido as medidas mais tradicionais, que normalmente detêm e atrasam um invasor em potencial. Só então o projetista de segurança passaria para os sistemas de detecção técnica extras'.

Mas com muitas medidas e sistemas agora se integrando entre si, uma abordagem mais considerada e holística é necessária.

Demonstrar o retorno do investimento (ROI) de uma solução de segurança projetada para evitar um incidente é notoriamente difícil. Isso se deve principalmente à falta de receita potencial para comparar ao custo. Normalmente, o pessoal de segurança trabalhará com seus colegas no departamento de finanças para ilustrar o custo de diferentes tipos de incidente de segurança, sejam eles custos diretos devidos à perda ou destruição de ativos ou custos menos imediatos, mas igualmente prejudiciais, associados com a perda da reputação.

No entanto, é possível demonstrar um ROI mais tangível, especialmente com certas tecnologias capazes de reduzir a atividade manual específica ou permitir que a equipe de segurança seja redirecionada para outras tarefas. Exemplos podem ser encontrados em soluções que não apenas alertam a equipe sobre comportamento suspeito ou intrusão, mas também podem produzir uma resposta suave automatizada. Isso pode incluir sistemas de áudio IP que podem fornecer anúncios pré-gravados ou sinalização iluminada informando a um possível intruso que ele foi detectado e instruindo-o a deixar a área.

Se câmeras de monitoramento forem incorporadas à solução, pode-se obter maior eficácia mostrando ao invasor algumas evidências de sua identificação, como uma tela mostrando que a placa do seu carro foi capturada ou até mesmo uma imagem do invasor. Apenas quando isso não tiver o resultado desejado, é necessário que a equipe de segurança seja implantada para investigar ou tomar uma ação mais direta. Essa abordagem em fases em resposta a alertas pode ser mais adequada para uso além do perímetro, mas ajudará a minimizar a necessidade da equipe de segurança se envolver em um estágio inicial, liberando horas-homem para um claro benefício de eficiência.

5.2 Avaliação do custo

A estimativa de custo deve se basear no cálculo do custo total de propriedade (TCO). O TCO inclui todos os custos associados com uma solução por todo o seu ciclo de vida; os custos materiais e humanos, os custos dos estudos, os custos de instalação do sistema, os custos operacionais, os custos de manutenção, os custos de desativação e de reciclagem. Isso pode exigir uma mudança de abordagem pelos departamentos de finança e compras, pois pode haver a necessidade de realocar capital entre os orçamentos operacionais e de despesas de capital.

Como acontece com qualquer ativo tangível, a organização precisará saber a vida útil da solução de detecção de perímetro. Os gerentes de segurança e de TI podem ajudar seus colegas de finanças explicando e demonstrando como a aquisição da tecnologia certa como plataforma para soluções futuras economizará dinheiro. Uma característica dos dispositivos avançados de monitoramento inteligente é que eles são, até certo ponto, inerentemente à prova de futuro. Ou seja, dispositivos com poder de processamento adequado são capazes de aproveitar repetidamente as vantagens dos avanços tecnológicos ao longo do tempo, principalmente por meio de análises de processamento baseadas em IA e aprendizado de máquina.

6 Proposta da Axis Communications

A abordagem aberta da Axis para se integrar com soluções de parceiros significa que seus sensores em rede, combinada com análise comprovada de vídeo e aproveitamento de IA, permite que os clientes implementem soluções de proteção de perímetro integradas de alto desempenho que são ciberseguras e econômicas em toda a empresa e por toda a vida útil do sistema.

Onde os sensores térmicos podem não ser apropriados, a tecnologia de micro-ondas (radar) é uma grande alternativa, capaz de oferecer muitos dos mesmos benefícios que a tecnologia térmica, potencialmente com menos falsos positivos. A tecnologia de radar da Axis se beneficia dos mesmos aprendizado de máquina e

aprendizado profundo que as mais avançadas câmeras de monitoramento. As unidades de radar da Axis podem detectar, classificar e rastrear pessoas e veículos com precisão com taxas de alarme falso quase zero.

A tecnologia de radar funciona 24 horas por dia, 7 dias por semanas, e virtualmente não é afetada por acionadores comuns, como sombras em movimento ou feixes de luz, pequenos animais e insetos ou condições climáticas adversas. Isso resulta em uma operação altamente econômica, assegurando que a equipe de segurança possa focar em ameaças confirmadas genuínas. O radar também pode fornecer a velocidade de um objetivo, permitindo o cálculo preciso do ponto de contato ou até mesmo para impor limites de velocidade.

O desempenho de uma solução frequentemente é a primeira parte de qualquer solicitação de informação (RFI) ou questionário de análise de mercado. As câmeras Axis possuem seus próprios processadores ARTPEC da Axis, com capacidade líder do setor, permitindo que algumas das mais avançadas soluções de análise de vídeo de proteção de perímetro sejam incorporadas à câmera (na borda). Decisivamente, isso também fornece garantia de que a solução está aproveitando o poder da tecnologia interna e não de componentes de terceiros.

Esta inteligência "na borda" significa que várias câmeras podem então rastrear vários eventos que ocorrem simultaneamente em diferentes locais. A chamada arquitetura técnica distribuída permite estender a solução para quantas câmeras forem necessárias, ao mesmo tempo que elimina investimentos em tecnologia de servidor centralizado.

Com o AXIS Perimeter Defender (APD) aprovado pelo governo do Reino Unido, quatros tipos diferentes de eventos são detectados, para um ou mais indivíduos ou veículos:

- Invasão em uma área predefinida
- Zonas de passagem em ordem e direção predeterminadas
- Passagem de zona condicional
- A presença de pessoas perambulando

O APD pode fornecer mais do que apenas um alarme de intrusão e vídeo correspondente. Ele também fornece metadados que podem ser utilizados para exibir uma sobreposição no vídeo, mostrando os limites e trajetórias de pessoas e veículos em movimento. Para uma abordagem mais integrada, as câmeras Axis (luz visível ou térmica) também trabalham com alto-falantes IP para transmitir mensagens automáticas após a detecção, potencialmente como uma solução autônoma. Este tipo de aviso automatizado permitirá uma "escalada" de medidas e contramedidas, importantes para determinar a intenção de um invasor e qualquer resposta subsequente necessária.

O APD pode ser integrado diretamente ao software normalmente usado nas plataformas corporativas (ex.: Genetec, Milestone, Seetec, Prysm, Qognify e outras mais).

A Axis fornece ferramentas de desenho complementares para ajudar com planejamento pós-pesquisa e suporte em cada fase de um projeto, desde encontrar os produtos certos baseados em critérios específicos para calcular, com precisão, os requisitos de armazenamento, instalar a tecnologia e gerenciar os sistemas. Aproveitar as ferramentas Axis ajudará os consultores a planejar e estimar, e o integrador a gerenciar projetos de forma mais suave e eficiente. Estas ferramentas facilitam ainda mais garantir a segurança do sistema instalado porque o software incluído torna mais simples a instalação de atualizações e patches de segurança.

Conforme as ameaças e contramedidas evoluem, uma coisa crítica permanece constante: a integridade e a segurança do perímetro. O perímetro é uma consideração fundamental para aqueles que implementam o dever de uma organização para oferecer um ambiente seguro e protegido para a equipe, visitantes e público. Este documento se destina a promover os benefícios para organizações de uma abordagem

de tecnologia integrada ao planejar a segurança do perímetro. Ele também destaca o fato de que o investimento em tecnologia de segurança deve ser apoiado por um ROI comprovável. Em todos os casos, entender os recursos de tecnologia atuais relevantes, bem como uma avaliação das tendências futuras, é uma abordagem sólida de segurança operacional e de aquisição para qualquer profissional de segurança, independentemente do seu departamento, cargo ou setor.

Referências de produto

Câmeras IP térmicas:

AXIS Q19 e mais www.axis.com/pt-br/products/thermal-cameras

Software de análise:

AXIS Perimeter Defender

https://www.axis.com/pt-br/products/axis-perimeter-defender

Alto-falantes IP externos:

AXIS C1310-E www.axis.com/pt-br/products/axis-c1310-e

Radar de segurança IP:

D2110-VE www.axis.com/pt-br/products/axis-d2110-ve

T10169467/PT/M1.3/2107

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções para melhorar a segurança e o desempenho dos negócios. Como empresa de tecnologia de rede e líder do setor, a Axis oferece soluções em vigilância por vídeo, controle de acesso, intercomunicação e áudio. Nossas soluções são aprimoradas por aplicativos de análise inteligentes e apoiados por treinamento de alta qualidade.

A Axis tem cerca de 4.000 funcionários dedicados em mais de 50 países e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e tem sede em Lund, Suécia