Whitepaper

CIBERSEGURANÇA EM SISTEMAS DE CFTV.

Protocolo ONVIF e Secure Streaming: Sistema Confiável

A3A® Engenharia de Sistemas

Sumário

Introdução

À medida que os sistemas de videomonitoramento evoluem e se tornam mais integrados à rede corporativa, a segurança das imagens capturadas já não depende apenas da qualidade das câmeras ou da infraestrutura física. Hoje, a proteção das informações transmitidas por um sistema de CFTV exige o mesmo nível de atenção dedicado a qualquer outro ativo digital.

Câmeras IP e servidores de gravação em rede são dispositivos conectados, que operam dentro da estrutura lógica da empresa e por isso, estão sujeitos aos mesmos riscos cibernéticos que afetam servidores, computadores e aplicações web. Vazamento de imagens, invasões remotas, sequestro de dispositivos e acesso indevido a gravações são apenas alguns dos cenários críticos que podem comprometer não apenas a operação, mas também a reputação e a conformidade legal da organização.

Diante desse cenário, torna-se fundamental tratar a cibersegurança como parte integrante do projeto de CFTV, não como um recurso adicional, mas como item obrigatório para garantir que o sistema esteja protegido contra ameaças externas. Isso envolve a adoção de padrões abertos e confiáveis, como os profiles do protocolo ONVIF, e o uso de tecnologias como secure streaming, que garantem a integridade e a confidencialidade dos dados desde a origem até o destino.

Nos próximos tópicos, este whitepaper apresenta os fundamentos técnicos da cibersegurança aplicada ao CFTV, explora os principais recursos utilizados nos planos avançados e demonstra como uma infraestrutura segura pode ser decisiva para a confiabilidade do sistema, a continuidade da operação e a proteção da empresa como um todo.

Por que a Segurança Digital deve ser prioridade no CFTV ?

Durante muitos anos, a preocupação com segurança nos projetos de CFTV esteve concentrada na proteção física para garantir a integridade das instalações, a continuidade da gravação e a cobertura adequada dos ambientes. No entanto, com a evolução dos sistemas e a consolidação das câmeras digitais e dos sistemas baseados em rede, o cenário mudou, e com ele, as ameaças começaram a ser frequentes.

Hoje, cada câmera conectada representa um ponto de entrada potencial para hackers. Câmeras de baixa qualidade e sem recursos de proteção podem ser utilizadas para acessar redes internas, capturar imagens, interromper operações críticas ou até mesmo coletar dados financeiros e operacionais de uma organização. Casos reais de invasões, inclusive transmitidas ao vivo sem consentimento, se tornaram mais comuns nos últimos anos.

Além do risco operacional, há o risco jurídico. Imagens vazadas, manipuladas ou acessadas sem autorização podem violar leis de proteção de dado como a LGPD e expor empresas a sanções legais, perda de credibilidade e danos à reputação.

A verdade é que um sistema de CFTV que não adota práticas de cibersegurança deixa de ser um recurso de proteção e passa a ser um ponto de vulnerabilidade. Proteger o perímetro digital é tão importante quanto proteger o perímetro físico.

Por isso, é fundamental que a segurança da informação seja parte central na escolha das tecnologias de monitoramento. E isso começa com a seleção de dispositivos que sigam padrões internacionais confiáveis, como o protocolo ONVIF, e se estende até a adoção de câmeras com recursos avançados como o secure streaming que vamos explicar melhor na sequencia, controle regulado

de acesso ao VMS e o gerenciamento seguro de senhas e atualizações.

Nos próximos tópicos, veremos como essas práticas são aplicadas de forma padronizada por meio do protocolo ONVIF.

O que é o Protocolo ONVIF ?

O ONVIF (Open Network Video Interface Forum) é um padrão global criado para garantir a interoperabilidade entre dispositivos de videomonitoramento IP — como câmeras, gravadores e sistemas de gerenciamento de vídeo (VMS) independentemente do fabricante. Ele estabelece uma linguagem comum de comunicação entre os equipamentos, permitindo que dispositivos compatíveis possam ser integrados de forma segura e padronizada.

Na prática, o ONVIF define um conjunto de regras (chamadas de profiles) que os fabricantes devem seguir para que seus dispositivos possam operar com sistemas de terceiros. Isso inclui protocolos de descoberta de dispositivos, autenticação, controle de PTZ, streaming de vídeo, gerenciamento de eventos, configuração de áudio e vídeo, e — mais recentemente — segurança cibernética e analíticos de vídeo.

Cada dispositivo que afirma ser compatível com ONVIF deve declarar quais profiles suporta. Os profiles são pacotes de funcionalidades, e cada um atende a necessidades específicas do sistema.

Como Verificar se um Dispositivo é Compatível com ONVIF ?

Para saber se uma câmera, NVR ou VMS é verdadeiramente compatível com ONVIF e com quais profiles, o caminho mais confiável é consultar diretamente o site oficial:

https://www.onvif.org/conformant-products/

Acessando o site é possível buscar por fabricante, modelo ou categoria e visualizar todos os profiles oficialmente certificados. A presença do selo “ONVIF conformant” deve ser validada com essa base de dados — muitas marcas afirmam ser compatíveis, mas não seguem totalmente o padrão.

Por que exigir equipamentos que atendam as exigências do protocolo ONVIF?

Exigir que os dispositivos utilizados em um sistema de CFTV sejam certificados e estejam em conformidade com o protocolo ONVIF é uma medida técnica e estratégica fundamental. Essa exigência garante que o sistema será compatível com os principais softwares e gravadores do mercado, evitará aprisionamento tecnológico (vendor lock-in), permitirá atualizações futuras com maior facilidade e, principalmente, assegura a adoção de práticas mínimas de segurança digital e integridade dos dados.

Entenda o que cada Profile ONVIF Significa

Profile S

Transmissão de vídeo via RTSP.
Descoberta e controle básico da câmera.
Autenticação padrão.
É o perfil mais comum e voltado para streaming de vídeo ao vivo.

Profile G

Gerenciamento e reprodução de gravações armazenadas em dispositivos (edge storage).
Aplicável a NVRs e câmeras com gravação local.
Permite acesso remoto seguro às gravações.

Profile T

Suporte a vídeo em H.264 e H.265.
Transmissão segura com criptografia TLS (secure streaming).
Melhoria nos controles de autenticação.
Indicado para projetos que priorizam segurança de transmissão e eficiência de banda.

Profile M

Integração com metadados e analíticos de vídeo.
Transporte seguro de eventos e classificações (ex: pessoa, carro, objeto).
Autenticação reforçada para analíticos baseados em IA.
Essencial em projetos que utilizam analíticos e precisam manter a integridade das informações.

Importante: Um sistema completo e seguro normalmente envolve câmeras com suporte ao Profile T ou M, gravadores com Profile G e um VMS compatível com múltiplos profiles para controle centralizado.

Principais benefícios de utilizar equipamentos em acordo com o protocolo Onvif

Interoperabilidade garantida: dispositivos de diferentes marcas podem ser integrados sem dependência de SDKs proprietários.

Padronização técnica: configurações de vídeo, controle de câmeras, áudio, eventos e até analíticos seguem uma linguagem comum.

Evolução tecnológica constante: novos profiles são desenvolvidos para acompanhar as tendências e garantir compatibilidade futura.

Transparência e conformidade: fabricantes precisam seguir regras específicas para obter e manter a certificação.

Base pública de validação: é possível verificar diretamente no site do ONVIF quais dispositivos são realmente conformes.

Segurança validada: os profiles mais recentes (como T e M) trazem melhorias importantes em criptografia, autenticação e proteção contra ataques.

E se o fabricante foi banido do ONVIF ?

É de amplo conhecimento público que recentemente alguns fabricantes de marcas amplamente conhecidas no varejo foram banidos do protocolo ONVIF por descumprirem requisitos essenciais de segurança cibernética. A decisão do fórum ONVIF não é arbitrária: ela ocorre após auditorias técnicas e reincidências de falhas graves relacionadas à proteção dos dispositivos e dos dados transmitidos.

Exemplos reais de problemas que levaram ao banimento:

Falhas de autenticação: acesso remoto possível mesmo com senhas definidas pelo usuário.

Backdoors (portas escondidas): funções ocultas nos dispositivos que permitem acesso direto por fabricantes ou terceiros.

Falta de criptografia nas transmissões de vídeo: permitindo interceptações e espionagem.

Má gestão de firmware: ausência de atualizações regulares ou envio de firmware sem verificação de integridade.

Casos confirmados de invasões massivas por redes de botnets e ransomware.

Nestes incidentes milhares de câmeras foram exploradas como vetores de ataque, seja para espionar empresas, minerar criptomoedas ilegalmente, propagar malware em redes locais ou capturar imagens sensíveis sem autorização.

Com a exclusão do ONVIF, essas marcas perdem credibilidade, suporte e interoperabilidade com os principais VMS e sistemas corporativos, tornando seus dispositivos um risco operacional e um passivo de segurança.

No contexto empresarial, institucional ou público, o uso de dispositivos em não conformidade pode resultar em sanções, perda de dados, falhas operacionais e exposição jurídica.

Secure Streaming - Proteção adicional

Proteger as imagens captadas pelas câmeras vai além de impedir acessos indevidos ao sistema. É necessário garantir que o conteúdo transmitido da câmera até o destino que pode ser um gravador, um servidor com VMS, uma central de monitoramento ou um servidor em nuvem esteja protegido contra interceptações, manipulações ou vazamentos. É exatamente esse o papel do secure streaming.

Secure streaming é o processo de transmitir vídeo criptografado em tempo real, utilizando protocolos seguros como TLS (Transport Layer Security). Isso garante que os dados transmitidos entre a câmera e o sistema de armazenamento ou visualização estejam embaralhados de forma que não possam ser acessados ou interpretados por terceiros, mesmo que capturados durante a transmissão.

Além da criptografia, o secure streaming também inclui mecanismos como:

Autenticação de dispositivos e usuários
Impede que sistemas não autorizados acessem ou recebam o fluxo de vídeo.

Integridade dos dados
Garante que o conteúdo transmitido não seja alterado, corrompido ou falsificado.

Proteção contra ataques man-in-the-middle
Bloqueia interceptações que tentam desviar o conteúdo da câmera para terceiros antes de chegar ao destino legítimo.

Por que isso é tão importante ?

Sem secure streaming, qualquer imagem transmitida pela câmera pode ser interceptada — principalmente se o sistema estiver em uma rede pública ou desprotegida. Isso significa que criminosos, concorrentes ou até mesmo agentes externos com conhecimento técnico podem:

Espionar ambientes internos em tempo real.

Mapear rotinas, fluxos e horários de operação.

Capturar imagens sigilosas ou estratégicas.

Utilizar as imagens como vetor para extorsão ou ataques futuros.

Esse tipo de exposição é inadmissível em ambientes corporativos, industriais, governamentais e de missão crítica.

Importância da Cibersegurança no sistema de CFTV

A inclusão de camadas de cibersegurança em projetos de CFTV vai além da proteção das imagens. Trata-se de uma estratégia de mitigação de riscos, valorização do investimento em tecnologia e blindagem da operação contra falhas que podem comprometer a empresa de forma profunda, tecnicamente, juridicamente e institucionalmente.

A Cibersegurança garante segurança operacional

Sistemas vulneráveis podem ser alvos de ataques que causam paralisações, perda de gravações, interrupção do monitoramento ou acesso indevido aos dados. Com camadas robustas de segurança — como criptografia, autenticação e dispositivos certificados — o risco de interrupções por ameaças cibernéticas é drasticamente reduzido.

Redução de ataques a reputação da empresa

Vazamentos de imagens, invasões remotas e exposições indevidas podem gerar repercussão pública negativa, afetando a confiança de clientes, parceiros e investidores. Um sistema seguro transmite profissionalismo e demonstra que a empresa valoriza a privacidade e a proteção de dados.

Conformidade com normas e regulamentações

A Lei Geral de Proteção de Dados (LGPD), normas técnicas da ABNT, diretrizes internas de compliance e exigências específicas de auditoria corporativa ou órgãos reguladores reforçam a necessidade de controle e proteção da informação. Sistemas de CFTV com segurança aplicada contribuem para manter a empresa em conformidade e evitar sanções.

Valorização da infraestrutura

Soluções seguras são mais duráveis, confiáveis e compatíveis com atualizações futuras. Isso significa reduzir a frequebcia de novos investimentos, mais escalabilidade e maior longevidade do sistema, preservando o retorno sobre o investimento.

Confiança técnica e institucional
Câmeras compatíveis com o protocolo ONVIF, transmissões criptografadas, gerenciamento seguro de acesso e suporte com SLA são elementos que aumentam a confiança na operação. Isso facilita a integração entre áreas, o envolvimento da TI e o apoio da alta gestão em novos projetos.

Ao considerar a cibersegurança como parte indissociável do sistema de CFTV, a empresa não apenas protege suas instalações — ela protege sua reputação, sua operação e seu futuro. Essa é a diferença entre um sistema de câmeras instalado e uma solução de monitoramento profissional.

Considerações finais

Em um cenário onde as ameaças cibernéticas aumentam exponencialmente, os sistemas de segurança física estão diretamente conectados às redes corporativas, a proteção das imagens, dos dados e da infraestrutura digital tornou-se um fator crítico em qualquer projeto de CFTV.

A escolha de dispositivos em conformidade com o protocolo ONVIF, o uso de secure streaming, a gestão segura de credenciais, atualizações de firmware e o controle de acesso ao sistema são tão importantes quanto a qualidade de imagem e a cobertura das câmeras.

A cibersegurança em sistemas de CFTV é uma exigência técnica, legal e estratégica, pois protege contra invasões, vazamentos de informações, interrupções operacionais e exposição pública. Ao mesmo tempo, contribui para o cumprimento da LGPD, aumenta a longevidade da infraestrutura e gera confiança no sistema implantado.

Certifique-se que os dispositivos de segurança ofertados são certificados com suporte a ONVIF Profile S, G, T e M, streaming criptografado, controle de acesso profissional, suporte técnico especializado e arquitetura preparada para crescer com segurança.

Investir em cibersegurança no CFTV é uma necessidade, e quando a segurança é a base, todo o sistema se torna mais confiável, escalável e preparado para os desafios reais do monitoramento moderno.