



Verdadeira vigilância por vídeo em nuvem para aeroportos de Aviação Geral

Por Ken Francis



ÍNDICE

Introdução	2
Análises de vídeo de IA baseadas em nuvem para segurança da aviação	4
Análises de vídeo avançadas para câmeras analógicas e IP	5
Um Cloud VMS pode ajudar a recuperar os recursos de TI no local	5
Benefícios adicionais de nuvem	5
Software Cliente-Servidor versus True Cloud	6
Análises de vídeo de IA, baseadas em nuvem, para segurança da aviação	7
Vigilância por vídeo como um serviço	8
Forte proteção de segurança cibernética	8
Acessibilidade do Cloud VMS	8
Conclusão	9
Sobre a Ken Francis e a Eagle Eye Networks	9

Introdução

O progresso tecnológico recente na Aviação Geral (GA) gerou interesse no futuro do setor. Ele também estimulou o Centro de Excelência para a Aviação Geral da Administração Federal de Aviação a patrocinar um projeto da Parceria para Melhorar a Segurança, Acessibilidade e Sustentabilidade da Aviação Geral (PEGASAS) para explorar esse futuro¹. Esse relatório, com base em especialistas no assunto da indústria de GA, da NASA e da FAA, revelou uma visão surpreendente: o mundo da aviação geral está prestes a mudar nos próximos seis anos mais do que já mudou em toda a sua história.

O relatório da PEGASAS identificou o alto nível de congestionamento em aeroportos como um fator importante que afeta os locais de GA, observando que as PMEs esperam que as operações de alta densidade “tenham um efeito cascata, onde grandes aeroportos movimentados atingem sua capacidade, sobrecarregando aeroportos menores, que necessitarão de infraestrutura atualizada para lidar com o tráfego adicional,”² e que “espera-se que os aeroportos de GA de alto tráfego se tornem o elo fraco na segurança do Sistema Nacional de Espaço Aéreo (NAS).”

Especialistas sugerem que a segurança pode ser melhorada ao se adotar a tecnologia de sensores comerciais para aeroportos de GA,³ onde a segurança física e a segurança cibernética ampliadas serão cruciais.

As diretrizes de segurança de 2021 da FAA para aeroportos de GA destacam uma mudança significativa na abordagem da segurança da aviação geral: “Historicamente, as regulamentações de segurança da aviação civil não se aplicaram a operadores e usuários de aeroportos de GA . . . No entanto, é frequente que muitos gerentes e usuários de aeroportos de GA implementem medidas de segurança semelhantes às encontradas em todos os aeroportos de serviços de comércio do país.”⁴ As diretrizes afirmam ainda que, “Essas ações voluntárias reconhecem que o endurecimento de um alvo (como a aviação comercial) pode causar que os maus atores busquem alvos mais suaves”.

As diretrizes da FAA destinam-se a ajudar os gerentes de aeroportos de GA a identificar e adotar as medidas de segurança mais adequadas para mitigar suas vulnerabilidades. Por exemplo, muitos aeroportos comerciais usam sistemas de vigilância de alta resolução para alcançar um nível de consciência situacional sem exigir monitoramento de equipe em tempo integral. Essas câmeras podem usar IA para detectar possíveis problemas e notificar automaticamente o pessoal apropriado. Ambas características beneficiariam bastante os aeroportos de GA com níveis de pessoal muito mais baixos.

Muitos aeroportos comerciais usam sistemas de vigilância de alta resolução para alcançar um nível de consciência situacional sem exigir monitoramento de equipe em tempo integral.

¹ Briceno, S., Crossley, W., Harrison, E., Chakraborty, A., Bendarkar, M., Sells, B., Stickney, J., Gao, Z. & Lin, P. (2020, setembro) Parceria para aprimorar a segurança, a acessibilidade e a sustentabilidade da Aviação Geral. Extraído em 28 de dezembro de 2024 de <https://rosap.ntl.bts.gov/view/dot/57771>

² Ibid., p9.

³ Ibid., p12.

⁴ Administração de segurança de transportes (2021, 15 de junho). Diretrizes de segurança para operadores e usuários de aeroportos de Aviação Geral. Extraído em 28 de dezembro de 2024, de <https://www.tsa.gov/sites/default/files/2021-ga-security-guidelines-june-2021.pdf>



Além de baixo número de pessoas, as instalações de GA normalmente sofrem com limitadas fontes financeiras e de TI. No entanto, um sistema de gerenciamento de vídeo em nuvem bem projetado permite que os aeroportos de aviação geral tirem proveito do poder de processamento e de economias de escala que excedem os dos maiores aeroportos do mundo usando informática local.

Um sistema de gerenciamento de vídeo em nuvem bem projetado permite que os aeroportos de aviação geral tirem proveito da capacidade de processamento e de economias de escala que excedem as dos maiores aeroportos do mundo usando informática local.

No setor de segurança, algumas pessoas ainda consideram que os sistemas de gerenciamento de vídeo não são uma boa combinação para a nuvem, principalmente devido ao volume de dados de vídeo. No entanto, nos mundos de consumo e negócios, o vídeo vem sendo transferido predominantemente para a nuvem há mais de uma década. Além disso, os produtos de segurança proativos habilitados para IA são cada vez mais utilizados em todos os setores de negócios e de consumidores.



Análises de vídeo de IA, baseadas em nuvem, para segurança da aviação

Por meio do uso de inteligência artificial (IA), as câmeras de segurança podem fazer significativamente mais do que apenas observar de modo passivo. Aqui estão alguns usos principais das análises de vídeo de IA aplicáveis à aviação geral:



Segurança de perímetro e detecção de intrusão: monitoramento de perímetros de aeroportos em tempo real, detectando e alertando o pessoal de segurança para qualquer acesso não autorizado ou atividades suspeitas perto de cercas ou em outras áreas restritas.



Autenticação biométrica facial e controle de acesso: identificação de usuários aprovados para gerenciar o acesso em áreas restritas, para garantir que apenas pessoas autorizadas estejam acessando áreas confidenciais do aeroporto.



Monitoramento de conformidade: garantia de que as operações dentro do aeroporto sigam regulamentos, políticas e procedimentos.



Monitoramento de aeronaves: garantia de segurança da aeronave em terra e detecção de acesso não autorizado ou potencial adulteração.



Reconhecimento e rastreamento de veículos: identificação e rastreamento de veículos nos terrenos do aeroporto, de modo que apenas veículos autorizados estejam em áreas restritas e monitorem comportamentos suspeitos.



Detecção e resposta a incidentes: detecção de incidentes, como deslizamentos e quedas ou outras emergências, permitindo uma resposta mais rápida da equipe do aeroporto e dos serviços de emergência.



Inspeções de manutenção e segurança: identificação de possíveis perigos de segurança ou necessidades de manutenção dentro da infraestrutura do aeroporto, como danos às pistas, sinalização ou indicadores.



Detecção de bagagem abandonada: identificação e sinalização de malas ou pacotes abandonados, que podem representar um risco à segurança. O sistema pode alertar o pessoal do aeroporto para investigar esses itens imediatamente.



Reconhecimento de placas de carros: monitoramento e registro de veículos entrando e saindo do aeroporto, o que é útil para fins de segurança e administrativos.



Detecção de comportamento ocioso e anômalo: identificação de indivíduos que exibem comportamento incomum ou potencialmente ameaçador, permitindo uma intervenção precoce.

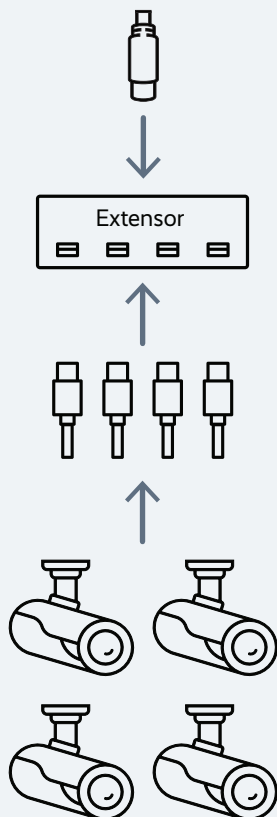


Gerenciamento de público e análise de fluxo: análise do fluxo de pessoas para otimizar a equipe e aprimorar a logística de negócios e a experiência do passageiro.



Detecção de vida selvagem e drones: detecção de animais que podem representar um risco para as aeronaves, bem como atividade de drones não autorizados dentro e ao redor do aeroporto.

Um único cabo coaxial muitas vezes pode dar suporte a até quatro câmeras PoE.



Análises de vídeo avançadas para câmeras analógicas e IP

Em um VMS em nuvem bem projetado, análises avançadas podem ser aplicadas uniformemente a feeds de vídeo de câmeras analógicas e IP, aumentando de modo significativo a eficácia de toda a configuração de vigilância por vídeo. Isso permite uma substituição acessível e em fases de câmeras analógicas. A adoção da tecnologia de Long Reach Power over Ethernet (LRPoE) baseada em padrões permite a reutilização econômica do cabeamento coaxial existente de câmeras analógicas. Esta abordagem simplifica as atualizações e mitiga o impacto e a despesa ambientais. Um único cabo coaxial muitas vezes pode dar suporte a até quatro câmeras PoE, para que os aeroportos possam alcançar um impacto ambiental positivo ao mesmo tempo em que reduzem os gastos.

Um Cloud VMS pode ajudar a recuperar os recursos de TI no local

Alguns aeroportos regionais são pressionados para manter sistemas computadorizados no local e têm necessidades de TI mais urgentes do que o gerenciamento de armazenamento de vídeo. A manutenção dos servidores VMS inevitavelmente resulta em tempo de inatividade do sistema. Em contraste, um verdadeiro VMS em nuvem requer poucos recursos de TI locais. As atualizações do sistema são aplicadas em tempo real, normalmente sem tempo de inatividade do sistema.



Benefícios adicionais de nuvem

Um VMS em nuvem bem projetado traz benefícios práticos adicionais para os aeroportos de GA:

- **Vídeo em um único lugar.** O vídeo inteiro é armazenado centralmente, em vez de em gravadores por todo o aeroporto.
- **Acesso em qualquer lugar, a qualquer momento.** O pessoal do aeroporto autorizado pode acessar vídeo de onde quer que esteja trabalhando e até mesmo fora do local, a partir de qualquer computador ou celular autorizado.
- **Flexibilidade e escalabilidade.** Um verdadeiro VMS em nuvem permite que você adicione ou subtraia usuários e câmeras do sistema, a qualquer momento, para que o sistema de segurança possa crescer e atender aos novos requisitos e necessidades sem precisar ser substituído.
- **Confiabilidade.** Um verdadeiro VMS em nuvem fornece um nível de redundância de dados financeira e tecnicamente impossível de alcançar no local. Se as câmeras ficarem off-line, o VMS notificará automaticamente o pessoal designado.
- **Atualizações automáticas do sistema.** As atualizações de firmware e de software para o hardware do VMS em nuvem local são realizadas automaticamente pelo fornecedor do VMS em nuvem como parte da assinatura do VSaaS. Os clientes e integradores não precisam tomar nenhuma ação.
- **Investimento em tecnologia preparada para o futuro.** As tecnologias de software e hardware de informática em nuvem estão avançando continuamente e os data centers em nuvem são projetados para serem atualizados continuamente, com tempo de inatividade mínimo do usuário final.

Software Cliente-Servidor versus True Cloud

É importante observar que nem todos os produtos do VMS em nuvem se qualificam como verdadeiros sistemas de nuvem. Este termo requer uma definição clara para distingui-lo de outros tipos de VMS em nuvem.

As capacidades de um sistema baseado em cliente-servidor são fixas — a escalabilidade das capacidades do sistema requer atualizações de hardware físico. Em contraste, os verdadeiros aplicativos de nuvem (ou “aplicativos nativos de nuvem”) funcionam em um conjunto de recursos de computação e de rede localizados remotamente e podem expandir ou contrair de forma dinâmica seus recursos alocados. Como o acesso a um VMS em nuvem é baseado na Internet, não há limitações práticas sobre o número de conexões de usuário simultâneas que ele pode suportar.

No contexto da vigilância por vídeo, um verdadeiro VMS baseado em nuvem é um aplicativo nativo de nuvem compartilhado com segurança por seus assinantes, funcionando em recursos de computador e de rede, também compartilhados por todos os assinantes. O software VMS é acessível pela Internet e os clientes pagam pelo software com base em assinatura.

Um verdadeiro VMS baseado em nuvem é um aplicativo nativo de nuvem, compartilhado com segurança por seus assinantes, funcionando em recursos de computação e de rede, também compartilhados por todos os assinantes

Alguns usuários finais, consultores de projeto de segurança e integradores de sistemas permanecem cautelosos sobre aplicativos de segurança baseados em nuvem. O setor de segurança física não tem um histórico de adoção oportuna e sem falhas de práticas de tecnologia da informação e de TI. Isso deu origem a suspeitas (e, em alguns casos, descobertas) de que nem todas as soluções promovidas como “baseadas em nuvem” são verdadeiras ofertas de nuvem.



Análises de vídeo de IA, baseadas em nuvem, para segurança da aviação

Por meio do uso de inteligência artificial (IA), as câmeras de segurança podem fazer significativamente mais do que apenas observar de modo passivo. Aqui estão alguns usos principais das análises de vídeo de IA aplicáveis à aviação geral:



As características de uma verdadeira plataforma VMS em nuvem asseguram aos CIOs e CSOs de pequenos aeroportos internacionais e regionais que alto desempenho, alta disponibilidade e alta segurança de dados são alcançáveis e acessíveis.



Acesso amplo à rede. As capacidades do Cloud VMS são fornecidas por meio de rede e acessadas por meio de mecanismos padrão, permitindo o uso de dispositivos de clientes, como telefones e computadores. Ele foi projetado para detectar e respeitar a largura de banda disponível, tolerar condições de baixa largura de banda, suportar breves interrupções de rede e continuar a fornecer uma experiência de usuário consistentemente boa.



Serviço medido. O uso de recursos de nuvem pode ser monitorado, controlado e relatado centralmente, fornecendo transparência para o provedor de serviços de nuvem e seus assinantes, permitindo o controle e a otimização automáticos de recursos e permitindo a implementação de funcionalidades de “pagar apenas pelo que você usa”.



Elasticidade e escalabilidade rápidas. Os recursos físicos ou virtuais podem ser ajustados de forma rápida e elástica, em alguns casos de modo automático, para aumentar ou diminuir rapidamente. Assim, o número de câmeras suportadas e a quantidade de armazenamento de vídeo disponível na nuvem são efetivamente ilimitados.



Autoatendimento sob demanda. Um usuário final pode configurar o sistema de nuvem ou selecionar opções do sistema, alimentando o uso sob demanda de análises de vídeo, entre outras funcionalidades. O sistema provisiona automaticamente as capacidades de computação necessárias, como tempo de processamento e armazenamento do servidor, sem exigir interação humana complexa com provedores de serviços de nuvem.

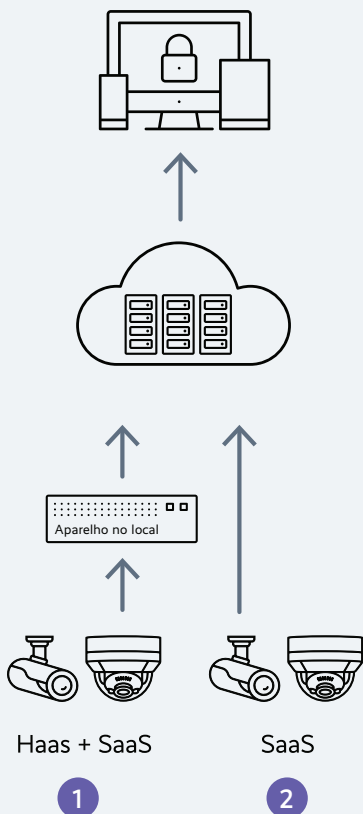


Agrupamento de recursos. Os recursos de processamento de um data center em nuvem (como Microsoft Azure, Amazon AWS, Google Cloud ou um data center personalizado de fornecedor) são agrupados para atender a vários assinantes, com diferentes recursos físicos e virtuais (como armazenamento, memória e poder de processamento) designados dinamicamente, de acordo com a demanda do assinante, tornando acessível a informática avançada em nuvem.



Multilocação. O modelo multilocatário é uma arquitetura de software na qual uma única instância de software atende a vários assinantes (ou subgrupos sob um assinante específico), referidos como locatários. Cada locatário compreende um grupo de usuários que compartilham um acesso comum com privilégios específicos do usuário para o aplicativo de software e seus dados armazenados.

Existem duas arquiteturas para vigilância por vídeo como um serviço (VSaaS).



Vigilância por vídeo como um serviço

Existem duas arquiteturas para vigilância por vídeo como um serviço (VSaaS). Uma é um modelo puramente de SaaS, onde as câmeras se conectam diretamente ao Cloud VMS. A outra combina SaaS com Hardware como um Serviço (HaaS) para dispositivos de buffer de vídeo no local e gravação local.

Um dispositivo de buffer de vídeo inteligente serve como um local de armazenamento temporário, com armazenamento em cache de vídeo durante períodos de alto uso da Internet no local. Normalmente, ele criptografa e transfere esses dados para o VMS baseado em nuvem durante períodos de uso inferior da Internet, normalmente após o horário de funcionamento normal, com base em programações ou regras predefinidas. Este dispositivo também pode realizar processamento analítico de vídeo ou criar metadados associados para upload para a nuvem. Idealmente, este dispositivo inclui a funcionalidade de firewall para isolar a LAN da câmera de vídeo de outras redes, incluindo a Internet.

Forte proteção de segurança cibernética

Além disso, à medida que os sistemas de TI dos aeroportos se tornam mais conectados, há maior preocupação em garantir a segurança cibernética nos aeroportos de GA.⁵ As câmeras de vídeo inteligentes em rede tornaram-se um alvo frequente de ataques cibernéticos.

Com o software Cloud VMS e a HaaS, o ônus da segurança cibernética para os aplicativos e o armazenamento VMS muda do usuário final para o provedor de VMS. As economias de escala permitem e incentivam os provedores de dados em nuvem a investir continuamente em medidas de segurança. Além disso, algumas medidas de segurança em nuvem — como armazenamento de dados persistente fora do local e servidores de aplicativos fisicamente inacessíveis — são impossíveis de alcançar com um sistema de segurança no local.

Os fornecedores de serviços de nuvem tomam suas próprias decisões de segurança cibernética e nem todos os aplicativos têm o mesmo nível de segurança. Observe que, se um fornecedor de Cloud VMS for membro da Aliança de Segurança de Nuvem (CSA), informações detalhadas sobre sua segurança de VMS em nuvem podem ser baixadas do registro CSA STAR.



Acessibilidade do Cloud VMS

de muitas ofertas de VMS em nuvem estão disponíveis como uma assinatura para vários anos, com montante único, semelhante aos investimentos periódicos de Despesas de Capital (CapEx) ou como uma assinatura mensal de Despesas Operacionais (OpEx) com custos iniciais mínimos. Este modelo baseado em assinatura se alinha com as estratégias da OpEx e facilita para as empresas a troca de provedores de serviços, se necessário.

⁵ Briceno, S. et alia, 7.

Conclusão

No âmbito da segurança física, a informática em nuvem é transformadora. Ela elimina efetivamente o ciclo de vida tradicional de 5 a 10 anos de sistemas de segurança porque os sistemas podem ser continuamente atualizados e melhorados “no local”, tornando as substituições periódicas obsoletas. Ele permite a integração de análises de vídeo habilitadas para IA e fornece acesso móvel flexível.

Uma atualização para um verdadeiro VMS em nuvem não apenas reforça as medidas de segurança, mas pode agregar valor às operações do aeroporto por meio de uma análise de atividades orientada por IA, oferecendo um retorno significativo sobre o investimento.

SOBRE KEN FRANCIS

Ken Francis tem mais de 30 anos no setor de segurança e ingressou na Eagle Eye Networks como Presidente da Eagle Eye Networks em 2016. Antes disso, Francis lançou os Serviços de Segurança ADT no mercado de negócios após o spin-off e o IPO da ADT pela Tyco International plc em 2012. Ele atuou como Vice-Presidente de Vendas e Marketing para a Segurança Global da UTC. Ele também é cofundador da AMAG Technology, Inc. Nos três papéis, Francis foi responsável pelo crescimento do controle de acesso e das tecnologias de vídeo baseadas em software por meio da liderança de equipes de gerenciamento de produtos internacionais e da expansão de canais globais. Atualmente, ele atua como presidente do Conselho Consultivo Executivo da Associação do Setor de Segurança.

SOBRE A EAGLE EYE NETWORKS

A Eagle Eye Networks é a líder global em vigilância por vídeo em nuvem, fornecendo vídeo ciberseguro e baseado em nuvem, com inteligência artificial (IA) e análises para tornar as empresas mais eficientes e o mundo um lugar mais seguro. Criado especificamente para a nuvem e a IA, o Eagle Eye Cloud VMS atende às necessidades de segurança e operacionais dos clientes, com escalabilidade ilimitada, preços de assinatura simples com base no uso, análises avançadas, IA integrada e uma plataforma de API RESTful aberta, fornecendo flexibilidade. A Eagle Eye vende por meio de uma rede global de revendedores e integradores. Fundada em 2012, a Eagle Eye está sediada em Austin, Texas, com escritórios em Amsterdã, Bangalore e Tóquio. Saiba mais em www.een.com.

