

**BOSCH**

Tecnologia para a vida

Proteja dados de vídeos

Os dados de segurança por vídeo estão cada vez mais conectados em redes locais e globais. Um número crescente de componentes de borda (câmeras) enviam seus dados para componentes centrais (servidores) via Internet, onde invasores digitais e hackers estão à espreita.

Os riscos

Até mesmo um único elo fraco no ambiente de segurança por vídeo pode comprometer um sistema inteiro. Por exemplo, hackers habilidosos podem praticar os conhecidos ataques man-in-the-middle, capturando as comunicações entre a câmera e o sistema de gerenciamento de vídeo (VMS). Uma vez conquistado o acesso, os hackers podem injetar um feed de vídeo alternativo para disfarçar atividades ilícitas ou manipular os vídeos de câmeras em tempo real para remover detalhes ou até mesmo pessoas da cena.

Cobrimo todos os ângulos

Atingimos os padrões mais elevados com uma abordagem em quatro etapas que leva em consideração a infraestrutura inteira de segurança por vídeo. Garantimos segurança ao atribuir uma chave de autenticação para cada um dos componentes de rede. Oferecemos proteção contra hackers ao criptografar dados em nível de hardware com o auxílio de uma chave criptográfica que é armazenada com segurança em um exclusivo módulo de plataforma confiável (TPM) integrado. Garantimos formas simples de gerenciar os direitos de acesso dos usuários, para que somente as pessoas certas tenham acesso aos seus dados. E, finalmente, podemos dar suporte à configuração de uma infraestrutura de chave pública. Com a Bosch, você não poderia ficar mais seguro.



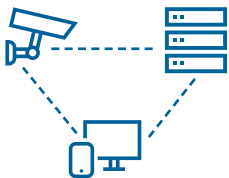
Como os dados de vídeo costumam ser altamente importantes e confidenciais, a Bosch está adotando uma abordagem sistemática para maximizar a segurança deles, levando em consideração tanto a segurança física quanto a cibernética. A abordagem do sistema da Bosch é a chave para a obtenção dos mais altos padrões em segurança de dados fim a fim.

A Bosch aborda todos os principais elementos da infraestrutura de segurança por vídeo:



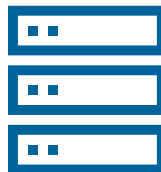
Como protegemos nossas câmeras

- ▶ Há suporte para conexões protegidas (HTTPS)
- ▶ Aplicação de senha na configuração inicial
- ▶ Execução de software de terceiros “desativada”
- ▶ Atualizações de firmware somente via arquivos assinados pelo fabricante
- ▶ As operações criptográficas, para autenticação e criptografia, são executadas somente dentro do exclusivo módulo de plataforma confiável (TPM) integrado



Como protegemos as comunicações de rede

- ▶ Portas não seguras são desativadas por padrão
- ▶ Aplicação de senha na configuração inicial
- ▶ Autenticação de rede usando o protocolo 802.1x
- ▶ Suporte do Advanced Encryption Standard (chaves de até 256 bits para criptografia)



Como protegemos nossos dispositivos centrais

- ▶ As operações criptográficas, para autenticação e criptografia, são executadas somente dentro do exclusivo módulo de plataforma confiável (TPM) integrado
- ▶ Suporte ao Microsoft Active Directory para gerenciar com segurança os direitos de acesso dos usuários
- ▶ Somente acesso autenticado conforme modelo Digest
- ▶ Atualizações regulares via patches de segurança



Como oferecemos suporte a infraestruturas de chaves públicas (PKI)

- ▶ Certificados assinados pela Bosch exclusivos carregados na fábrica em todas as câmeras
- ▶ Exclusivo módulo de plataforma confiável (TPM) integrado para operações criptográficas de alta segurança
- ▶ Autoridade de certificação interna (Escrypt)
- ▶ Suporte de certificados específicos do cliente
- ▶ Suporte de soluções de PKI de terceiros

Para obter mais informações, você pode baixar os seguintes documentos:

[Guia de segurança de dados](#)

[Nota técnica sobre autenticação de rede](#)

VS-EH-pt-BR-06_F01U561111_02