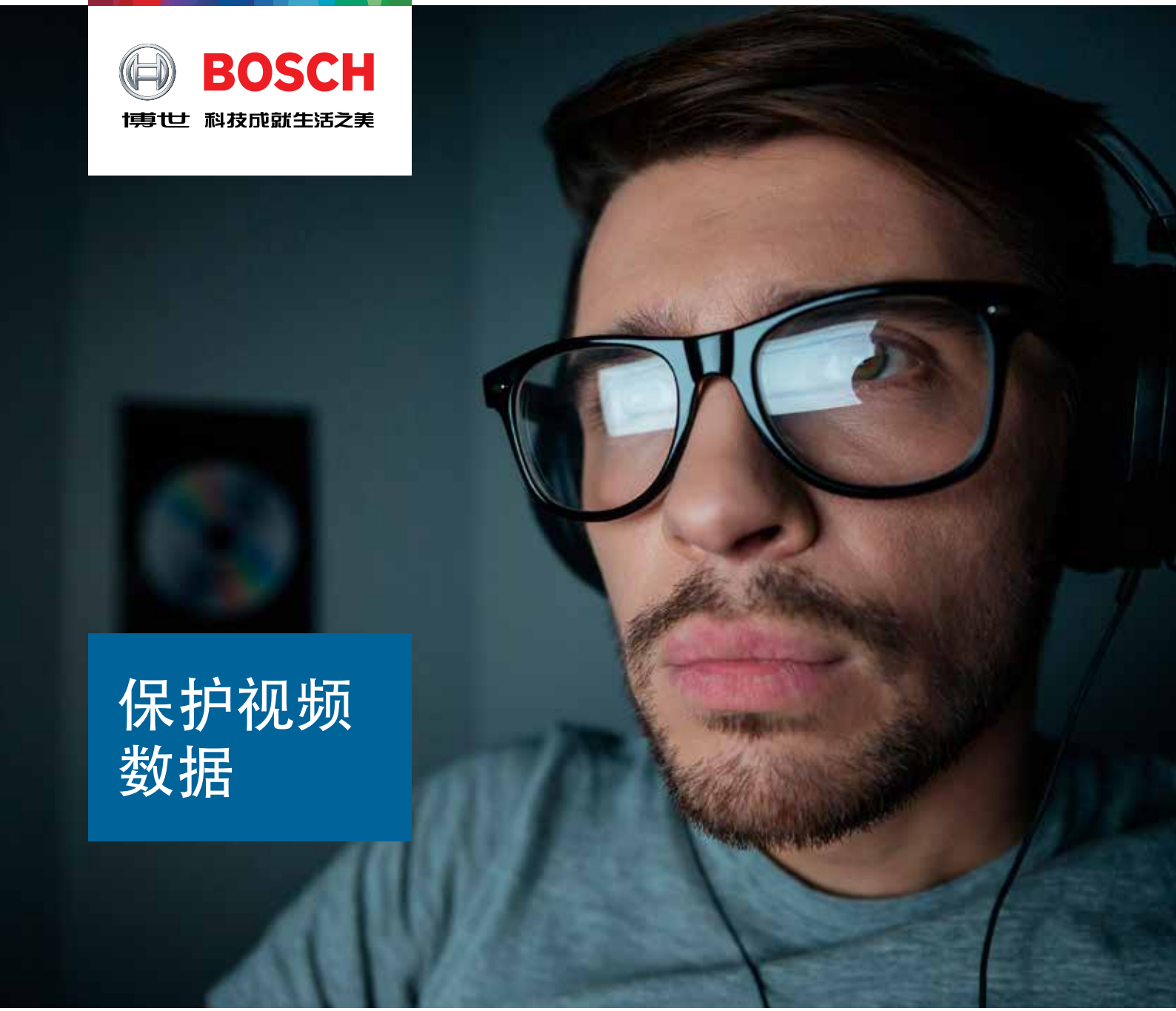
BOSCH

博世 科技成就生活之美



保护视频数据

视频安全数据在本地和全球网络中的互联程度日益加深。越来越多的前端组件（摄像机）将数据通过Internet发送到核心组件（服务器），而Internet上的数字入侵者和黑客在蠢蠢欲动。

风险

视频安全设置中的一个薄弱环节就会危及到整个系统。例如，技术娴熟的黑客可以发起所谓的中间人攻击，劫持摄像机和视频管理系统(VMS)之间的通信。在黑客获得访问权之后，他们可以注入替代视频源来遮掩非法活动，或者操纵实况摄像机画面以便有选择地移除场景中的某些细节或人物。

覆盖各个角度

我们采用一个方法建立了最高标准，该方法考虑到整个视频安全基础架构，分为四个步骤。我们通过为网络中的每个组件分配一个身份验证密钥来建立信任。我们通过在硬件级别使用安全地存放在独特内置可信平台模块(TPM)中的加密密钥对数据进行加密，从而防范黑客窃取数据。我们还提供简单的方法来管理用户访问权限，从而确保只有授权用户才可以访问您的数据。最后，我们支持搭建公钥基础架构。因此，利用博世产品，您完全可以做到安全无忧。

由于视频数据通常具有极高的重要性和敏感度，因此博世推出了一种系统化的方法，通过同时考虑物理安全和网络安全来最大程度地提高数据的安全性。博世的系统方法是实现端到端数据安全方面的最高标准的关键所在。

博世考虑了视频安全基础架构的所有主要因素：

我们如何确保摄像机的安全

- 支持使用安全连接 (HTTPS)
- 在初次设置时强制提供密码
- “禁用”第三方软件的执行
- 仅通过制造商签名的文件进行固件更新
- 针对验证和加密的加密操作仅在独特的内置可信平台模块(TPM)中执行

我们如何确保核心设备的安全

- 针对验证和加密的加密操作仅在独特的内置可信平台模块(TPM)中执行
- 支持Microsoft Active Directory以实现用户访问权限的安全管理
- 仅允许摘要式访问验证
- 通过安全补丁进行定期更新

我们如何确保网络通信的安全

- 默认情况下禁用不安全的端口
- 在初次设置时强制提供密码
- 使用802.1x协议进行网络验证
- 支持高级加密标准（最高256位的加密密钥）

我们如何支持公钥基础架构(PKI)

- 所有摄像机出厂时均附带唯一的博世签名证书
- 在独特的内置可信平台模块(TPM)执行高度安全的加密操作
- 内部证书认证机构(Escrypt)
- 支持客户的特定证书
- 支持第三方PKI解决方案

有关更多信息，请下载我们的：
数据安全指南
网络验证技术说明
VS-EH-zh-CN-06_F01U561107_02