TeamViewer

远程 IT
安全检查清单

投资合适的远程技术颇费功夫。为此，我们精心准备了一份检查清单，
其中列出了提供安全远程 IT 支持的关键要素。请根据情况进行逐一核对，具体包括：

实施严格的密码规则
制定基于单点登录 (SSO) 的员工安全操作规范，
让所有人员只需使用一个密码，即可完成安全登录。
此举可省去因创建（和遗忘）多个弱密码而带来的麻烦。

构建多层次验证防护
运用多重身份验证 (MFA)，防止遭到未经授权的访问。
在授予帐号、设备和系统的访问权限前，
务必确保用户已提供多种形式的身份验证。

禁用远程输入
禁用远程输入，可保障远程会话安全无虞、顺畅无阻。
同时，所支持的最终用户也不会影响或干扰流程，可安心进行远程连接。

防止他人窥视屏幕内容
没有黑屏功能，远程支持解决方案就谈不上完善。黑屏功能可在远程访问时，
将设备屏幕设置为黑屏状态，确保操作的安全性和私密性。

坚守安全标准不松懈
实施自带证书 (BYOC) 策略，
利用数字证书保障云服务和应用程序的安全。
通过加大控制权，更好地满足安全标准和合规性要求。

授予、限制和撤销访问权限（自主掌控）
作为一种基于规则的功能，条件访问可根据用户凭据、
位置、时间和设备等条件执行相应操作，
从而大幅提升远程安全性。

选择性授予访问权限
构建精细的访问权限控制，全面掌控组织内
特定设备的访问权限分配。针对不同的团队、个人和设备，
应用特别设立的权限、许可证和策略。

希望提供更贴心的安全 IT 支持？
请单击右边按钮了解更多信息。

了解详情