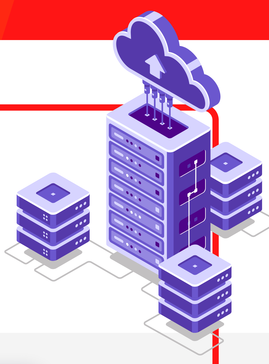
ivanti

您的网络安全之旅

随着企业快速转向远程工作方式，许多安全漏洞在无处不在的工作空间中浮现出来，这就需要有一个全面和可扩展的网络安全战略来尽量减少潜在的威胁。

以下 6 个关键领域需要您予以考虑，帮助您实现坚实的网络安全战略之旅。

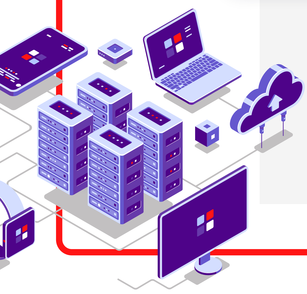


1. 全面掌握资产状况

原因：
您无法管理自己都不了解的东西。
如果资产清单（云、软件、硬件）不明，那么您的组织很容易遭受安全风险。

方式：
实时全面洞察所有连接设备，从而更好地管理、组织和优化您的 IT 基础设施。

2. 设备管理现代化



原因：
监控各类远程用户及设备是否合规对安全运营至关重要，例如保持软件为最新状态和快速排除问题。

方式：
将 UEM 部署纳入您的战略。

3. 确定设备健康状况

原因：
对所有设备设立通用安全要求，这使问题的诊断更快捷、更容易。

方式：
使用自动化手段主动检测和管理任何与设备健康有关的安全问题。

4. 保护您的用户

原因：
密码缺乏全局背景信息（设备、应用、网络、威胁），所以无法区分授权和非授权用户。

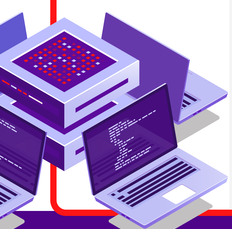
方式：
零登录：不用密码，也就不会有登录凭证或密码被盗的风险。

5. 提供正确的访问权限

原因：
限制用户仅可访问所需业务资源，这能最大限度地减少基于访问权限的安全威胁。

方式：
利用零信任网络访问来跟踪、监控并全面掌握用户对公司数据的访问情况。

6. 自动执行合规及风险管理



原因：
手动管理费时费力，效率低下，而且会引入更多的安全风险。

方式：
主动出击，而不是被动应付：部署一个通用性自动化的合规和风险管理战略。

想了解更多如何建立一个坚实的网络安全战略？立即获取“实现对网络完全旅程的管理、自动化与编排 (M.A.P)”：

下载电子书

ivanti