中型企业 6 大安全忠告

如果您所在的企业属于中型企业，降低网络安全漏洞的风险就是安全工作的关键。了解这些百试不爽的忠告建议，帮助确保公司和网络的安全。

忠告 1 为用户提供恰当的访问权限

由于用户漫游和物联网设备的广泛使用，基于角色进行访问控制的 Wi-Fi 是一种行之有效的方法。您可以将所需使用的 SSID 的数量将至最低，同时保证无论是访客、打印机，甚至是有人带进工作场所的 Apple TV，仍然可以根据用户或设备类型对接入进行区分。

忠告 2 构建应用程序友好型策略

根据位置、使用的应用程序或流量类型应用额外的安全特性。策略实施的自动化可以让这一目标的实现变得简单。现在，无论在何时何地，您都不必担心访客流量会干扰员工的业务关键型应用程序。

忠告 3 使用最新的 WI-FI 安全标准

WPA2 Wi-Fi 安全方案已经无法确保安全性。最近已在 WPA2 中发现了安全漏洞，这些漏洞会使网络和客户端面临潜在的密码钓鱼攻击。确保您选择的无线设备经过认证，支持具有机会性无线加密 (OWE) 功能的 WPA3 和 Enhanced Open，避免不必要的风险。

忠告 4 选择内置入侵保护功能的 WI-FI 接入点

网络上安装的未知接入点会为 IT 部门带来沉重的工作负担。Wi-Fi 接入点需要包括无线入侵保护功能，以便帮助您发现并关闭流氓或干扰接入点，或可能构成威胁的其他设备。最好的功能是，网络会向 IT 管理员发出意外威胁警报。

忠告 5 通过内置内容过滤管理 WEB 访问

防止用户访问恶意内容十分困难，让不断增加的不安全网站列表始终保持最新状态几乎是不可能的。保证网络安全的一个好方法是选择一个可以通过简单的方式按 URL、位置或 IP 地址对内容进行过滤，保证安全浏览内容的 Wi-Fi 解决方案。

忠告 6 选择注重安全性的供应商

虽然保证健壮的网络安全性是一个明智的选择，但由于更多的用户往往会使用多个设备，从多个位置连接到网络，所以我们要考虑添加中心化的用户和设备级控制功能。外部策略服务器可能起到关键的作用。确保内置安全功能与高级安全解决方案无缝集成，这样就可以利用一整套 API 帮助您覆盖整个用户群。

智能安全，智能网络接入

aruba
a Hewlett Packard Enterprise company

SixSecurityTipsMidsizeBusiness_080519