竞争格局

当今中型企业的 6 项保护措施

行业领先的网络安全性

通过技术手段获得竞争优势对当今的中型企业至关重要。不幸的是，可以创造商业机会的技术也会带来新的攻击面和漏洞，从而对企业造成威胁。如果没有适当的保护，您的网络可能就会变成设备、数据等安全威胁的主要入口。Aruba 深谙安全对企业的重要性。了解 Aruba 方案的独到之处，旨在保护网络安全的创新型安全功能：

功能	Aruba	竞争优势	其他供应商	它们的弱点
全时段安全监控	支持 	Aruba 方案采用专用双频接入点作为传感器，支持对两个频段同时进行安全扫描，提供有效的网络攻击检测和规避。	有限	其他领先的云方案供应商采用专门用于扫描的第三个射频模块，从设计上看，只能在每个频段提供 50% 时间的安全扫描。第三个射频模块通常为 1×1 MIMO，只能检测部分威胁，识别攻击（如果有）需要更长时间。
嵌入式策略实施防火墙 (PEF)	支持 	Aruba 的多层策略防火墙可将安全、流量转发和网络性能策略应用于无线客户端和应用程序，以实现安全的高质量通信。	不支持 	其他方案不提供内置策略防火墙。它们需要专门的硬件、许可和支持。
内置 Web 内容过滤功能	支持 	Aruba 提供订阅式 Web 内容过滤功能，无需购买额外设备即可应用。	不支持 	Web 内容过滤解决方案驻留在硬件设备上，而硬件设备需要花费额外成本。
板载无线入侵和恶意设备规避方案	支持 	Aruba 的内置无线入侵防护功能经过测试，可以大规模执行，可持续快速识别恶意设备并规避威胁。	有限	标准的无线入侵产品识别恶意设备速度慢，无法控制威胁。适用的无线入侵防护需要额外的硬件和许可。
支持 WPA3 和 Enhanced Open	支持 	Aruba 安全专家在开发 WPA3 和 Enhanced Open 中使用的这些全新加密协议时提供了指导意见。Aruba 是首家出货的供应商（2018 年 11 月）	较少	虽然该标准早在 2018 年 10 月就已发布，但仍仅有少数供应商实施该标准并获得 Wi-Fi 认证。
用户/设备可见性和策略实施	支持 	Aruba 屡获大奖的 ClearPass 策略管理平台是业界针对用户和设备的身份验证和授权、策略实施和漏洞响应的最佳解决方案。	不支持 	虽然有其他高级的安全平台，但这些平台部署起来通常会很复杂，而且需要额外的许可和/或订阅基础服务，而且对多供应商方案的支持也比较有限。

想进一步了解 Aruba 中型企业解决方案？请点击此处。

© 版权所有 2019 Hewlett Packard Enterprise Development LP. 此处所含信息可能会在未经通知的情况下更改。对于 Hewlett Packard Enterprise 提供的产品和服务，仅在随产品和服务提供了明示担保声明时，Hewlett Packard Enterprise 方按照其中规定的条款提供担保，此处所述任何内容均不可理解为构成额外担保。对于此处所含的技术或编辑错误或疏漏，Hewlett Packard Enterprise 不承担任何责任。

CL_6PointProtection_072419