安全硬件是否会被SaaS式安全取代 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/0/2021_2022__E5_AE_89_E5_85_A8_E7_A1_AC_E4_c99_432.htm 随着云端运算逐渐迈向主流，采用软件服务化(简称 SaaS)模式的云端式信息安全，也恰巧搭上顺风车乘势而起。根据Infonetics Research的调查，该市场2009年成长率达到70%，同时，根据IDC 2009至2013年全球信息安全服务预测 (Worldwide Security as a Service 2009-13 Forecast)，该市场今年将成长到20亿美元的规模。去年9月，Oracle的Larry Ellison还曾经对云端运算嗤之以鼻。我想，除非观念发生彻底转变，否则传统软件厂商很难完全拥抱这项新模式。 这让我想起大约五、六年前安全硬件设备开始在市场上出现时，防火墙已经开始普遍采用硬件形式，并成为电子邮件和网络的实际网关，迅速取代原有的软件解决方案。现在，我相信当SaaS式的信息安全服务成为主流时，硬件装置也将面临相同的命运。另一个可能影响硬件设备的因素是应用程序都正在逐渐虚拟化，那安全应用又怎能例外？我们已经看到客户将网关安全解决方案部署在虚拟化环境。 一个的新型态，也就是混用SaaS的模式，已经开始在企业客户间流行。这是一种鱼与熊掌兼得的最佳办法：将应用程序的某些部分放在云端，其它需要与数据库密切整合或是有遵规要求的部分，则留在企业内部。企业再透过整合式网页主控台来同时设定并管理这两部分的政策。云端的效益包括大规模部署与易用性，而企业内的解决方案则提供更多的本地端控管。 小型企业会逐渐被一次购足的网关安全、端点安全与网络安全等整合式SaaS入口网站所吸引，其简易性让小型企业

拥有三年前所无法享有的信息安全技术。从最近的一些数据窃盗恶意程序事件来看，小型企业也如同大型企业一样，是网络犯罪者经常锁定的目标。事实上，根据我们最近一次针对趋势科技使用者所做的调查发现，小型企业与大型企业遭遇资料盗窃的比率没有太大差异。 虽然硬件装置可以大幅简化信息安全应用程序的部署，但是他们在某些信息安全领域的应用却即将面临淘汰。还有什么比登入因特网控制台更简单的事？SaaS式信息安全的未来是光明的，但安全设备的未来我就不敢确定了。 编辑特别推荐: #0000ff>教你选择安全合适的服务器机柜 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com