云计算为您的安全防护功能提供技术支持的六大方式

采用云计算使企业不得不做出选择，是选择使用云环境所带来的成本效益、可扩展性和便利性，还是选择将数据和应用安全地托管在自己服务器上所带来的安心。但是，本地就真的比云计算更安全吗？许多专家都表示并非如此。以下六大因素将向您展示为什么您可以放心地向云计算迁移。

1 安全防护价格昂贵

安全防护需要花钱。问问自己：我的公司实际能负担得起多少钱？事实上，给您的本地数据中心部署必要的安全防护成本过高，特别是对于中小型企业。为客户提供接近超大规模企业所能提供的安全级别是不切实际的。

2 安全防护需要大量人力资源

同样，安全防护也需要更多的人力资源。大规模云提供商采用全天候安全团队和完整的安全防护运维中心对 IT 基础架构和物理硬件进行持续监控。例如，Microsoft Azure 就由一支 3,500 多名网络安全专家组成的团队提供保护。大多数企业没有足够的员工队伍来提供媲美超大规模企业的安全防护。

3 云提供商本身就从事安全业务

您关心安全防护，但这并不是您的业务。虽然安全性是您关注的众多问题之一，但它却是云提供商的最高优先事项之一。为了业务存续并保持竞争力，云提供商必须为其客户提供尽可能高的安全防护级别。例如，Google Cloud 提供的“安全设计基础架构”在默认情况下具有内置保护和加密功能。[1]

Microsoft Azure“通过分析大量来源来帮助识别威胁，其中包括 180 亿个必应网页、4000 亿封电子邮件、10 亿次 Windows 设备更新和 4500 亿次使用机器学习、行为分析和基于应用智能的月度身份验证，并将其作为微软智能安全图的一部分。”[2]

云提供商还必须符合最高标准，包括通过一系列严格的计划，对安全防护人员、流程和技术进行独立的、国际公认的认证和审核。例如，Amazon Web Services（AWS）定期针对数千项全球合规性要求进行第三方验证。大多数企业既没有时间和资源，也没有足够的预算达到该级别的安全保证。[3]

1 *“信任与安全防护”，Google，2022 年 4 月 29 日发布。*
2 “借助 Azure 巩固安全态势”，*Azure，2022 年 4 月 29 日发布。*
3 *“AWS 云安全”，Amazon，2022 年 4 月 29 日发布。*

4 高级安全防护工具

云提供商部署了一系列高级安全防护工具来保护客户应用和数据。AWS 提供细粒度的身份和访问控制、持续监控、威胁检测、网络和应用保护、多个加密层、自动化事件响应和恢复功能等。超大规模企业对合作伙伴市场中可用的数百种其他安全解决方案提供访问权限。在您自己的网络和数据中心复制这套广泛的高级安全防护工具几乎是不可能的。对于一家非专攻安全防护的公司来说，其所需要的成本、人力、时间和精力都花销巨大。

5 网络分段

云环境固有的安全优势是从用户工作站进行分段。常见的网络攻击方法之一就是通过电子邮件和网站针对系统上的特定用户发起攻击。在这些情况下需要通过用户工作站进入系统。然而，在云环境中，用户工作站仅拥有足够的连接性使其用户完成自己的工作。工作站不能直接访问企业网络。因此，即使工作站遭到入侵，攻击者也无法访问公司及其应用和数据。

6 物理安全

物理安全仍然是一个关键因素。可直接亲自接触到硬件的人员可能是一个严重的潜在安全风险。但是，如果数据和应用位于云环境中，心怀不满的员工（以及其他有能力造成意外伤害的现场工作人员）则无法再近距离接触这些资产。因为在云环境中定位数据要困难得多。

此外，超大规模企业拥有防止数据真正被盗的资源，包括安全防护装置、服务器外箱上锁以及其他最先进的物理安全控制，而大多数企业不具备这些资源。

阅读更多

阅读“通过云服务为开发人员提供支持”，更深入地了解红帽 ® 云服务如何领航您的云原生应用之旅。