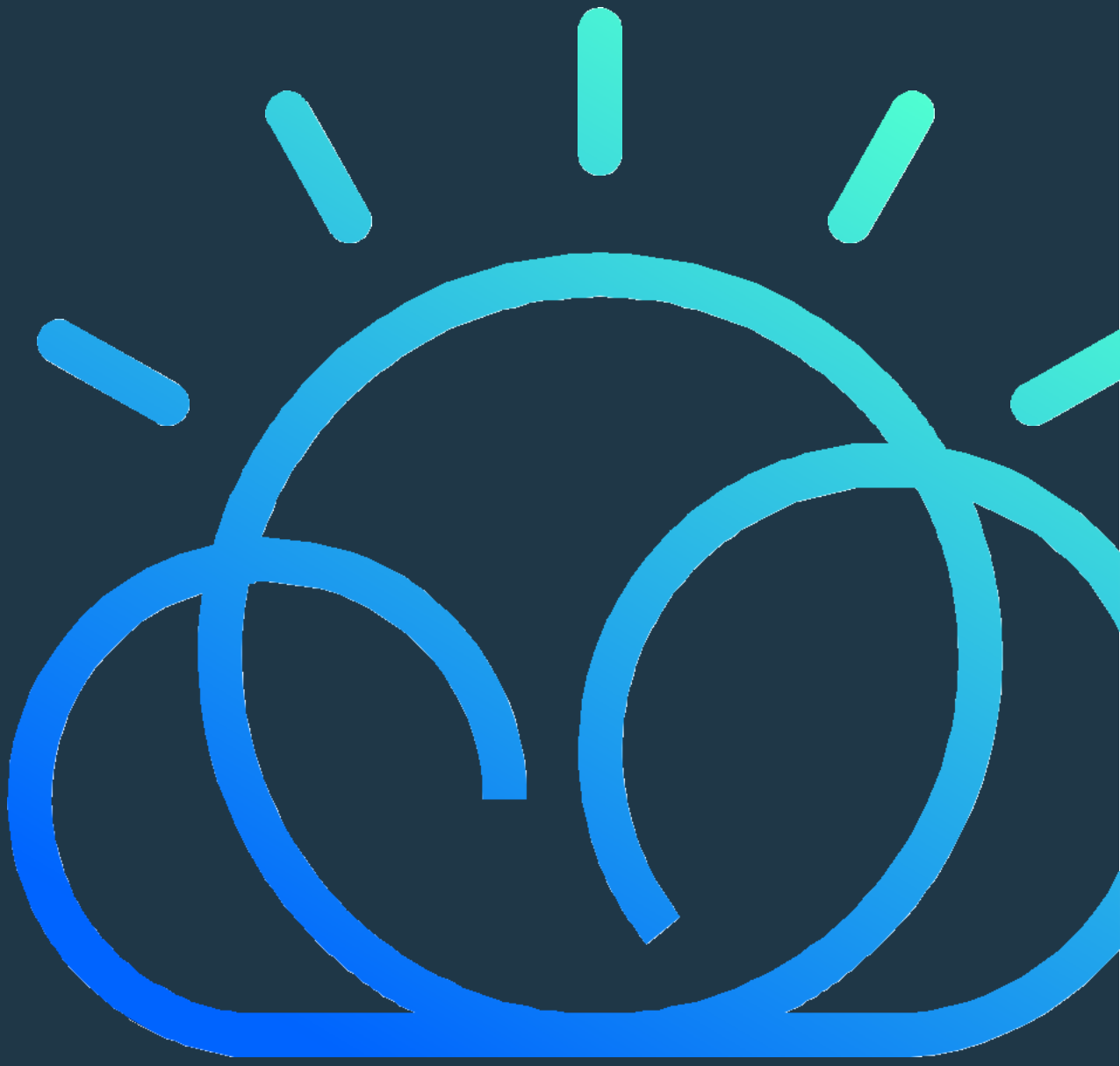
2018 年白皮书

确保核心安全：确保公有云安全的五大考虑事项

解决 IT 架构师在公有云安全方面所面临紧迫问题的良方



IBM **Cloud**

IBM

在当今的信息技术领域，有两大趋势在“争相交锋”。

第一个是规模化的云采用不断加速，而且这种趋势不可阻挡。另一个是全球数据威胁环境的敏感性和意识快速提升，这使得公有云的安全性遭到了质疑。

因此，IT 架构师就面临一个问题“如何在继续推进公有云计划的同时减缓安全风险？”

很多统计数据都表明，企业对公有云的兴趣有增无减。McKinsey & Co. 发布的一份报告[1]显示，“使用公有云会颠覆许多企业多年来所构建的传统网络安全模式。”McKinsey 在去年针对 90 家企业级组织进行的一项调研结果显示，80% 的受访者计划在 2020 年之前将 10% 或以上的关键工作负载部署到公有云，或者说他们对公有云服务的使用量会翻番。毫无疑问，研究和咨询公司迫切希望组织能够“大幅演变他们的网络安全实践，以使用公有云服务... 保护关键数据。”

低安全、高成本

与此同时，公有云安全的提升面临着一个极具动态性的全球威胁环境。毫无疑问，IT 架构师会非常担心面向互联网的应用、Web 站点和工作负载所面临威胁的规模和范围不断增加的问题。拥有高级技术及充足资金支持的攻击者想尽各种办法去利用公有云和公有应用编程接口 (API) 中所存在的漏洞，而且他们“深谙此道”。近期针对 1,000 多家组织进行的一项调研结果显示，76% 的受访者表示他们在去年遭受过两次或两次以上的分布式拒绝服务 (DDoS) 攻击。[2]在美国，每次数据泄露事件的平均成本已攀升到 700 万美元，而据预计，每次成功的 DDoS 攻击每小时的成本最高可达到 250,000 美元。

未来的安全方法

无论是公有云的业务优势，还是网络攻击者对敏感云数据的潜在威胁，都非常明显。以下所述是 IT 团队、CTO 及其他业务利益相关者在选择公有云安全解决方案时的五大关键考虑事项。

1. 选择裸机服务器会构建一个独立的环境。

单租户的裸机服务器是客户的专用服务器。在独立的环境中运行工作负载会额外增加工作负载的安全性，但并非所有的计算服务器都具有完全相同的安全水平。因此，必须确保所部署的是真正的单租户解决方案并专供您的组织所用，这样才能获得完全的独立性。一些提供商会在裸机服务器上放置一个管理程序，使其成为虚拟服务器，用于将工作负载分布到不同的用户。因此，寻找适用您需求的解决方案。

2. 并非所有的公有云防火墙都是相同的。

IT 架构师都已认识到，防火墙是云基础架构保护机制中不可或缺的一部分，不仅有助于防范外部网络威胁，还有助于确保合规性。随着组织从传统的内部设备转变到软件即服务模式，选择正确的防火墙可帮助您在这两个方面确保相同级别的安全性。因此，您应该选择可提供最广泛选项的解决方案，比如：实例级保护；通过可作为高可用性选项进行部署的防火墙实现网络级保护；部署专用的硬件防火墙，以保护单个公有虚拟 LAN 中所有服务器的入站流量；提供门户支持和 API 支持，以便更轻松地入门；提供下一代功能，例如侵入保护系统、杀毒系统和 Web 应用防火墙。我们要切记一点，尽管云原生防火墙解决方案具有广泛的可用性，但物理设备对企业来说也很关键。您并不希望在安全和性能方面作出艰难的抉择。

3. 安全组具有许多可变规则。

在云安全领域中，安全组由一系列 IP 过滤规则集构成，这些规则集旨在调节对网络资源的访问。它们会定义如何处理虚拟服务器实例公有接口和私有接口的入站和出站流量。值得注意的是，您可以将安全组分配到单个或多个虚拟服务器实例。确保安全组的可用性，有助于充分解决关键网络安全问题。举例来说，IT 架构师通常希望在虚拟服务器部署完毕后能够立即确保安全。因此，在订购虚拟服务器时，您要确保可以使用安全组，以便在服务器完成部署后，您能够完全控制流经服务器的流量。此外，您应选择不会对安全组功能的使用进行额外收费的解决方案，因为在解决方案部署之后，您可能会希望在必要时，针对解决方案提供商数据中心中的所有虚拟服务器使用安全组。

4. 加密密钥是成功安全保护的关键。

在前文提到的面向 1,000 名全球 IT 领导者进行的调研中，受访者被问及了推动他们使用公有云服务的主要因素。他们认为最主要的因素是"能够对组织的数据进行加密，同时能够在本地存储和管理加密密钥"。因此，您要选择配有防篡改硬件设备、能够安全存储加密密钥的云安全解决方案。您的密钥应始终保留在 FIPS 140-2 三级硬件上。此类安全模块应允许 IT 团队对其进行远程管理，而且应能够在多个应用或租户之间共享，以降低审计成本和合规成本。如果您的用例有高性能要求，比如 SSL/TLS 密钥保护、海量代码签署，则应确保您所选的硬件模块能够提供这些功能。

5. 易用性不应牺牲性能或安全。

会导致 IT 团队必须在安全与性能之间作出权衡抉择的云安全解决方案，通常都会引起 IT 团队的不满。因此，您应选择能够将低延迟安全服务与流量优化服务（如缓存服务、负载均衡服务等）完全集成到一起的解决方案。专注于易用性的解决方案应能使您在数分钟内完成 Web 应用和 Web 站点的安全保护部署，同时还能够避免可能的高成本误配置。

部署正确的公有云安全解决方案

在选择公有云提供商时，安全应该是第一优先事项。Forbes 的一份报告显示，在他们评选的云服务提供商三强中，有一家提供商"非常注重转型，而且已成功地将其广泛的软件专业知识和技术从内部系统迁移到云端"[3]，进而能够继续保持其竞争优势。该服务提供商就是 IBM，该提供商的公有云客户不仅能够访问所有的 IBM Cloud 安全服务，还可以通过 IBM 的全球安全团队获得广泛的全球支持。

IBM 的云安全方法专注于确保最优的可视性，主动监控公有云服务，使得用户能够更快地响应威胁、加速威胁调查和减缓流程。除了可提供非常易用的高级分析功能之外，IBM 的解决方案还能够让用户通过密钥管理服务对静态数据和动态数据进行加密。该解决方案还提供了身份与访问管理功能，可帮助客户强化合规管理、降低整体风险。

IBM 提供的一些主要公有云安全解决方案和服务包括：

裸机服务器解决方案：可通过独立环境交付安全，还可提供完全的可控性、灵活性等其他优势。借助 IBM Cloud 裸机服务器，客户不会共享任何计算资源。整个堆栈都归您所有，包括组件的配置和自定义。这意味着，您不需要担心"邻近噪音"共享您的资源、拖慢您的工作负载。

防火墙：可实现从传统环境到虚拟环境无缝过渡的防火墙。在此类 IBM 产品中，一款关键的产品就是 FortiGate Security Appliance，其运行速度可达到 FSA 10Gbps，是业内首款企业级经硬件加速的高吞吐量防火墙。

云安全组：可帮助用户在完成配备后立即实现虚拟服务器的安全保护，同时还可在实例级别实现对流程的精细化控制。

硬件安全模块：能够安全地管理和处理加密密钥并将其存储在防篡改设备中，进而锁定客户的加密基础架构。

云互联网服务：它是一款软件定义安全解决方案，可确保面向 Web 的应用的安全性、弹性和高性能。仅需在单个门户或 API 中进行数次简单的点击或使用数个命令，即可确保更安全的互联网体验。

结论

现在，充分利用规模化地公有云服务，同时确保敏感数据不会遭受不必要的风险。尽管市场上有许多服务提供商可提供各种各样的公有云服务，但您在投资公有云之前，您必须仔细考量并对比这些服务。作为所有顶级公有云提供商中企业安全领域经验最为丰富的全球领导者，IBM Cloud 可提供一流的服务且拥有一流的安全团队，可帮助企业实现他们的最大目标：确保基础架构的核心安全，真正做到完全放心。

有关更多信息，敬请访问：

https://www.ibm.com/cloud/security

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国印刷
2018 年

尾注

1 "Making a Secure Transition to the Public Cloud". McKinsey & Co. 2018 年 1 月

2 "IBM Cloud Internet Services: Optimizing Security to Protect Your Web Applications". IBM. 2018 年 2 月

3 "The Top 5 Cloud-Computing Vendors". Forbes. 2017 年 11 月 7 日

TechTarget | Custom Media