公有云能否演变为机密云

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Can the public cloud become confidential?		
原文作者	阿亚尔·约格夫（Ayal Yogev）	原文发布日期	2021年8月6日
作者简介	阿亚尔·约格夫是Anjuna Security公司的首席执行官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/08/06/public-cloud-confidential/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	机密云是由一个或多个公有云提供商组成的安全机密计算环境。机密云中的应用程序、数据和工作负载受到底层主机中硬件级加密、内存隔离等服务的保护。云的规模和经济性是不可否认的。现在，机密云消除了最后的安全问题。企业不需要在安全性与云基础架构的优势之间进行权衡了。强大的机密云将会席卷全球。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

公有云能否演变为机密云

阿亚尔·约格夫

2021 年 8 月 6 日

人们常说，人生有两件事情不可避免：一是死亡；二是税收。在过去的十年中，数据泄露似乎也可以添加到此行列中了。企业真得能够实现完全的安全，不用担心丢失保密/受监管数据、公司机密以及专有算法和 AI 代码吗？

现实情况是，完全保护数据或其他数字资产是极其困难的。本地、私有云和公有云数据都容易受到内部人员和恶意软件的攻击。在检测和防御攻击时，防御者只要失败一次，就会导致灾难。我们可以讨论每种环境的相对安全性，但是没有什么环境是绝对安全的。

根据 451 Research 的数据，近 70%的首席信息安全官（CISO）表示不信任公有云能够保护敏感数据和工作负载的机密性。他们知道，只要有足够的时间，任何类型的数据泄露（包括无意的数据泄露）都有可能发生。不仅 CISO 了解公有云的漏洞，公有云提供商也了解。

CISO 继续将最敏感的工作负载保存在私有数据中心，而公有云供应商则开始部署安全计算技术，旨在将存在漏洞的公有计算资源转变为完全机密的资源。

举例来说，AWS 最近发布了 AWS Nitro Enclaves，这是现有 AWS 主机的一种硬件卡附件，支持“使用中的数据”隔离——这是安全执行环境的基础。Microsoft Azure 机密计算也部署了类似的功能，部署了支持 Intel SGX 和 AMD SEV 技术的主机。谷歌宣布了类似的功能，该功能利用 AMD 的 SEV 专有安全计算技术。

不幸的是，在实践中，这些芯片级技术存在可用性限制，阻碍了 IT 企业的广泛采用。这主要是因为，它们专注于保护未加密的内存和使用中的数据——这是当今几乎所有运行主机的致命安全弱点。存储的数据和网络通信需要通过单点技术进行补救，而这些技术会造成复杂的孤岛和潜在的安全漏洞。

虽然这些技术非常强大，但对于拥有数千个老旧应用程序的企业来说仍然不可行。即使其中一些应用程序可以进行修改，但是代价高昂，因此很少有首席信息官（CIO）愿意进行这些修改。此外，这些修改还会导致企业最重要的应用程序锁定到单个云供应商和机密计算技术堆栈。

好消息是，这些机密计算技术为新的、基于软件的计算结构奠定了基础，使 IT 企业更容易采用安全计算，而不必考虑底层技术和公有云如何。它们还能够提供一个强大的平台，企业可以在该平台上构建新型安全计算应用程序——“机密云”。

机密云是什么？

机密云是由一个或多个公有云提供商组成的安全机密计算环境。机密云中的应用程序、数据和工作负载受到底层主机中硬件级加密、内存隔离等服务的保护。

与微分段和主机虚拟化一样，机密云中的资源以默认的零信任状态与所有进程和用户隔离。但机密云不仅仅隔离网络通信，它还隔离工作负载使用的整个 IT 环境，包括计算、存储和网络。因此，机密云几乎可以支持所有应用程序。

由于机密云保护是数据不可分割的一部分，因此保护服务可以扩展到数据所在的任何地方。传统企业边界由物理设备定义，但机密云的边界由硬件隔离、加密和最低权限访问策略等定义。最重要的是，即使在物理主机遭到破坏的情况下，工作负载和数据的处理也完全不受内部人员、不良行为者和恶意进程的影响，能够确保工作负载和数据的安全性。

机密云的前景

听起来很复杂是吗？其实，在实践中，机密云并不复杂。

机密云软件结构的另一个特点是，它对用户和应用程序都是透明的。机密云与服务器虚拟化技术非常相似，使现有工作负载能够以与现在完全相同的方式进行部署。

数据安全成为底层硬件/软件堆栈的固有服务，而非单个应用程序或附加安全功能（例如存储/网络加密和密钥管理）的责任。

通过这种方式，几乎所有应用程序都可以在机密云中运行，无需对开发或运行执行任何更改。由于保护服务伴随着数据本身，因此将机密云用于分布式云原生应用程序可以显著降低复杂性和成本，同时消除应用程序的大部分攻击面。

机密云即将上市？

机密云的基础和软件现已上市。几乎所有主要公有云提供商都在部署了某种形式的机密计算硬件，作为其当前主机产品的可选项。构成机密云的软件也可以直接通过云提供商获得。

运行预打包应用程序（包括市场领先的数据库、AI 引擎等）的概念验证环境，可快速实现实例化并进行测试。相关组件都已存在，已形成了完整的解决方案，企业可以在不中断运行的情况下轻松部署。

云的规模和经济性是不可否认的。现在，机密云消除了最后的安全问题。企业不需要在安全性与云基础架构的优势之间进行权衡了。强大的机密云将会席卷全球。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com