服务器托管危险隔离技术，沙箱、蜜罐以及欺骗防御有何区别

服务器托管用户在日常维护中需要预防各类恶意软件的入侵，而沙箱、蜜罐以及欺骗防御则是常见的手段。那么三者有何区别呢？

沙箱

几乎自网络和第三方程序出现起，对网络流量和程序的分析需求就一直存在。上世纪 70 年代，为测试人工智能应用程序而引入的沙箱技术，能令恶意软件在一个封闭的环境中安装并执行，令研究人员得以观测恶意软件的行为，识别潜在风险，开发应对措施。

沙箱、蜜罐和欺骗防御的区别

当前的有效沙箱基本都是在专用虚拟机上执行。这么做可以在与网络隔离的主机上用多种操作系统安全地测试恶意软件。安全研究人员会在分析恶意软件时采用沙箱技术，很多高级反恶意软件产品也用沙箱来根据可疑文件的行为确定其是否真的是恶意软件。因为现代恶意软件大多经过模糊处理以规避基于特征码的杀软，此类基于行为分析的反恶意软件解决方案就变得越来越重要了。

大多数公司企业无法像专业研究人员或供应商一样以一定的专业技术水平执行恶意软件分析。小公司通常会选择部署沙箱即服务，从已经实现了自动化整个沙箱检测过程的供应商那里收获沙箱技术的各种益处。

蜜罐

蜜罐和蜜网就是为诱捕攻击者而专门设置的脆弱系统。蜜罐是诱使攻击者盗取有价值数据或进一步探测目标网络的单个主机。

沙箱、蜜罐和欺骗防御的区别

1999 年开始出现的蜜网，则是为了探清攻击者所用攻击过程和策略。蜜网由多个蜜罐构成，常被配置成模拟一个实际的网络——有文件服务器、Web服务器等等，目的是让攻击者误以为自己成功渗透进了网络。但实际上，他们进入的是一个隔离环境，头上还高悬着研究人员的显微镜。

蜜罐可以让研究人员观测真实的攻击者是怎么动作的，而沙箱仅揭示恶意软件的行为。安全研究人员和分析师通常就是出于观测攻击者行动的目的而使用蜜罐和蜜网。关注防御的研究人员和 IT 及安全人员可以运用此信息，通过注意新攻击方法和实现新防御加以应对，来改善自家企业或组织机构的安全状况。蜜网还能浪费攻击者的时间，让他们因毫无所获而放弃攻击。

经常受到黑客攻击的政府机构和金融公司可以从蜜网中收获良多，但蜜网技术同样适用于中大型公司企业。根据业务模型和安全状况，一些中小型企业也可以从中获益，但今天的大多数中小企业尚不具备能够设置或维护蜜罐蜜网的安全专家。

网络欺骗 (Cyber Deception)

网络欺骗的核心概念最早是普渡大学的 Gene Spafford 于 1989 年提出的。有些人认为这一概念或多或少指的就是现代动态蜜罐和蜜网，基本上，他们的理解是正确的。

沙箱、蜜罐和欺骗防御的区别

欺骗防御则是一个新的术语，其定义尚未定型，但基本指的是一系列更高级的蜜罐和蜜网产品，能够基于所捕获的数据为检测和防御实现提供更高的自动化程度。

需要指出的是，欺骗技术分不同层次。有些类似高级版的蜜罐，有些具备真实网络的所有特征，包括真正的数据和设备。这种欺骗技术可以模仿并分析不同类型的流量，提供对账户和文件的虚假访问，更为神似模仿内部网络。有些安全欺骗产品还可以自动部署，让攻击者被耍得团团转，陷入无穷无尽地追逐更多信息的循环中，令用户能更具体更真实地响应攻击者。欺骗防御产品按既定意图运作时，黑客会真的相信自己已经渗透到受限网络中，正在收集关键数据。没错，他们确实在访问数据，但这些数据只是用户想要他们看到的那部分。

欺骗防御尚处于发展初期，与大多数新生安全技术一样，其初始用例是大企业才用的小众工具，随后才会逐渐在市场上铺开。目前，这些工具对政府设施、金融机构和研究公司之类引人注目的目标尤其有用。公司企业仍需安全分析师来解析安全欺骗工具收集的数据，所以没有专业安全员工的小公司通常无法享受到欺骗防御工具的好处。尽管如此，中小企业可以签约提供分析与防护即服务的安全供应商，以委托的方式从这种新兴技术中获益。

以上三种安全技术在预防与分析领域各司其职。从较高层次上看，沙箱允许恶意软件安装并运行以供观察其恶意行为；蜜罐和蜜网关注分析黑客会在自以为已被渗透的网络上干些什么；欺骗防御则是更新的高级入侵检测及预防设想。欺骗技术提供更为真实的蜜网，易于部署且能给用户提供更多信息，但需要更多的预算和更高的专业技能要求，通常只能在大企业中应用，至少现在其用例还仅限制在大企业里。

浦东数据中心为服务器托管用户提供专业技术支持。