使用 VMware AppDefense 保护在虚拟化环境和云环境中运行的应用

虽然全球范围内的 IT 安全性开支不断攀升，但企业成为数据泄露受害者的几率已经上升到了四分之一[1]。尽管市场上存在数千种安全产品，而且此类产品的购买预算相当庞大，但数据却并不比以前安全。这就给首席信息安全官（CISO）带来一项巨大的挑战，他们必须保护日趋动态化的分布式 IT 环境中的应用和数据的安全。随着越来越多的企业采用现代化且敏捷的应用开发模式，根据业务发展速度实施相应的安全保护便成了一个更棘手的问题，安全性往往被视为业务发展的障碍。

CISO 及其团队在保护其数据和应用的工作中面临两大难题：

检测不到威胁和虚假警报

现有的端点安全解决方案会触发大量虚假警报，导致安全运维团队浪费大量时间来手动调查一些并不存在的威胁。更糟的是，他们可能会完全漏掉真正的威胁。

快节奏的动态化环境

现有安全解决方案并不能跟上现代应用开发和部署的速度，这意味着在新的应用推出和更新时，安全保护无法保持同步。

概览

VMware AppDefense™ 是一款数据中心端点安全产品，可保护在虚拟化环境中运行的应用。与追踪威胁的现有端点安全解决方案不同，AppDefense 侧重于根据应用的预期状态（即它们本该有的行为）来监控各种应用，并在它们偏离预期状态（表明存在威胁）时自动做出响应。这便最大限度地提高了安全运维的效率和有效性，同时简化了应用安全性就绪审查流程。

关键要点

- 简化数据中心端点安全性
- 改善 SOC 中的威胁检测
- 自动响应突发事件
- 简化应用安全性就绪审查

通过虚拟化实现安全转型

VMware AppDefense 具有得天独厚的优势，可同时解决这些难题。AppDefense 是一种数据中心端点安全产品，可将威胁检测和响应嵌入到应用和数据所在的虚拟化层中。AppDefense 借助 VMware vSphere® 提供了优于现有端点安全解决方案的三项关键优势：

对应用预期状态有着权威性的了解 – 知道什么是好的状态，便能检测到不好的状态

在 vSphere Hypervisor 中，AppDefense 对数据中心端点的预期行为有着权威性的了解，并在第一时间获悉发生的更改。这种切合实际情境的信息处理能力更加精确，不必再为哪些更改合规、哪些更改的确是威胁这样的问题猜来猜去。

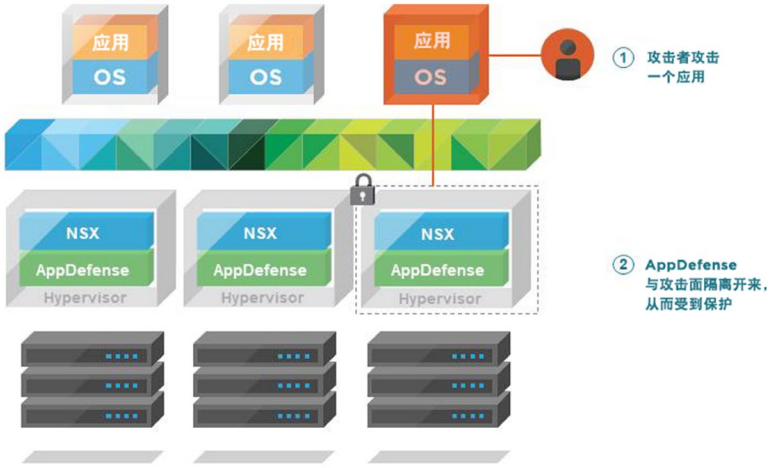
自动准确的威胁响应 – 即刻触发响应动作

当检测到威胁时，AppDefense 可以触发 vSphere 和 VMware NSX® 去编排正确的威胁响应流程，而无需手动干预。例如，AppDefense 可以自动：

- 阻止进程通信
- 给端点拍摄快照以便进行取证分析
- 挂起端点
- 关闭端点

与攻击面隔离开来 – 对保护者提供保护

多数恶意软件变体在到达端点时要做的第一件事是，禁用防病毒和其他基于代理的端点安全解决方案。Hypervisor 提供了一个受保护位置，让 AppDefense 可在该处运行，从而确保即使在端点受到攻击时，AppDefense 自身也能受到保护。



AppDefense 的实际应用

AppDefense 是一项基础安全产品，对企业的安全战略具有深远的影响。

针对安全运维中心 (SOC) 的以应用为中心的警报

AppDefense 不会生成大量警报，但当它真的发出警报时，务必要加以重视。AppDefense 生成的权威性警报以及自动响应功能使安全管理员能够专注于捕捉和消除其环境中的威胁，而不是在混乱的数据中艰难地筛选并调查并不存在的威胁。

应用安全性就绪审查转型

在现代应用开发领域，应用发布、变更以及淘汰的速度都非常快。等安全团队了解到新应用的存在时，它往往已经变化了。AppDefense 可在应用团队与安全团队之间创建一个公用可信来源，从而简化安全审查流程。

通过 VMware 实现以应用为中心的安全性

我们凭借自己的网络虚拟化平台 VMware NSX 及其跨整个数据中心实现微分段的能力，改变了网络安全的局面。NSX 将网络和安全性服务（如防火墙保护）直接设计到了 hypervisor 中，从而为网络实现最小权限模型。最终结果是，网络安全团队可以防止威胁在其环境中横向移动。

了解更多

有关更多信息或者想要购买 VMware AppDefense，可访问 http://www.vmware.com/cn/appdefense 并在我们的动手练习中试用该产品。

AppDefense 将威胁检测和响应功能分层到基础架构的另一个核心区域中，从而为数据中心端点实现最小权限模型。如果威胁进入端点，AppDefense 将立即检测到它并自动准确地响应。NSX 和 AppDefense 共同为保护应用基础架构（从而保护其中的应用和数据）提供了一个强大的解决方案。

[1]Ponemon Institute，2017 年 6 月，“2017 Cost of a Data Breach Study: Global Overview”

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京办公室北京朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：+86-10-5976-6300 传真：86-10-5976-6302
中国上海办公室 上海市淮海中路 333 号瑞安大厦 804-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真 852-3696 6101 www.vmware.com/cn