安全的应用基础架构基础知识

安全性是所有行业的头等大事

随着用户、设备和物联网元素之间的连接越来越紧密，保护所有这些连接和环境就变得比以往更加重要。与此同时，这也成为 IT 当前面临的最大挑战之一。原因何在？因为无论在哪里、以何种方式连接，各行各业的 IT 组织都必须保护用户、应用和数据之间的所有交互。此外，还必须在瞬息万变、越发动态的环境中为这些交互提供保护。

那么，如何在 IT 复杂性和“随时随地”数字交互呈指数级增长的世界中降低风险呢？对于正在转向云环境和虚拟化环境的组织而言，最大的可见性和控制力是减轻这种风险的关键。

不断变化的威胁需要新的安全模式

近年来，几乎每个行业的企业都经历过窃取敏感企业数据和客户数据的严重数据泄漏事件，在修复成本、品牌形象损害、信誉受损以及销售损失方面造成的损失高达数十亿美元。尽管攻击方式各不相同，但大多数泄漏事件利用了（并揭露了）以边界为中心的网络安全措施的固有弱点，此类传统安全措施通常专注于通过边界防火墙来保护北南向流量。但如果威胁成功越过了边界防火墙呢？这时，数据中心内部署的控制措施不足以阻止威胁在东西向（即服务器到服务器）流量间扩散。非常不幸的是，在当今新型威胁日趋复杂的情况下，这中情况已屡见不鲜。

为了解决这一问题，许多组织部署了各种针对性产品，不同的系统构成了庞杂而又互不相干的网络，这些系统不够灵活、难以调配并且很大程度上并不适用于要保护的应用。更糟糕的是，可用于执行恶意攻击的工具功能强大且易于使用，从而使更多攻击者能够成功侵入各自的目标。

IT 需要安全性和敏捷性

为了满足业务主管和相关人员的期望，IT 组织必须能够既快速又安全地交付关键服务和应用。不过，在 IT 团队全力保护业务时，他们面临着诸多障碍，包括：

- 应用体系结构正在发生变化，从本地部署的整体应用转向分布式应用和微服务
- 缺少网络流量的可见性和情境信息
- 僵化的以边界为中心的安全模式和策略
- 难以实现、保持和证明合规性

业务需要敏捷性来推动增长

随着组织寻求为业务线和内部其他相关人员缩短销售就绪时间和价值实现时间，他们还需要更有效地管控安全性和风险。这意味着不仅要降低数据泄漏的风险，还要降低在发生泄漏时造成的影响。在这一方面，面临的挑战是：使用常规工具大幅改善安全性和合规性状况往往会对业务敏捷性造成负面影响。那么，如何向 IT 团队提供所需的解决方案和资源，以跟上业务运维团队的速度，同时保持基础架构安全？

将应用抽离基础架构可带来优势

要应对这一挑战，组织需要从根本上转变保护应用基础架构的方式。VMware 可提供一整套解决方案，使 IT 团队能够部署一个虚拟化平台，该平台可将基础架构抽离在其上运行的应用 - 无论该基础架构是本地部署还是位于公有云中。借助 VMware vSphere® 和 VMware NSX®，组织可充分利用灵活且可靠的虚拟化平台来支持新的和现有应用，而不会影响安全性和合规性。VMware vRealize® Network Insight™ 可通过企业级云计算管理增强其能力，以提供额外的可见性和保护。

保护应用基础架构安全的三点基本知识

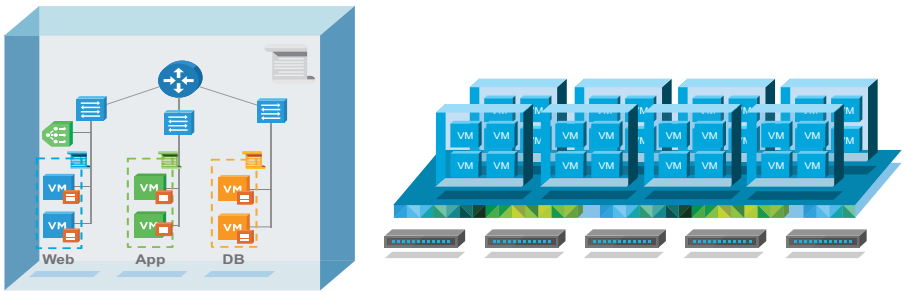
采用全新方法来保护应用基础架构安全使 IT 组织可充分利用以下几项强大功能：

将应用抽离基础架构

将应用抽离基础架构可实现对应用数据路径的全面可见性，以便更好地了解流量模式。这使 IT 大幅提高了基于情境理解基础架构、应用以及数据之间的交互的能力。借助完整且统一的数据、应用和基础架构视图，组织可更有效地创建策略并响应威胁。

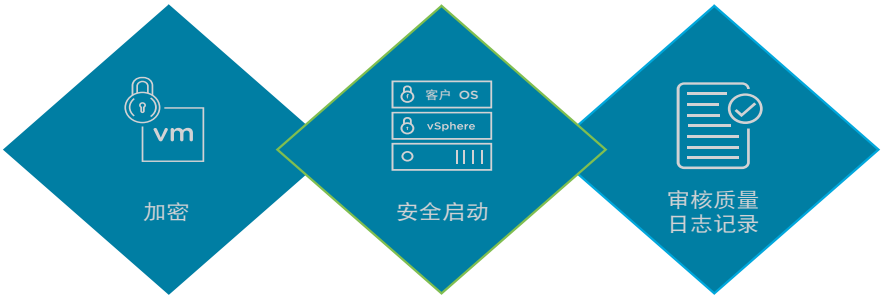
与应用一致的精细安全策略

虚拟化方法使组织能够将安全策略与其要保护的应用密切配合，并在应用跨公有云和私有云移动时跟随其一同移动。它使网络微分段能够阻止威胁在工作负载和应用之间进行横向（东西向）扩散。此外，通过它，更易于在需要新的功能时，智能地将第三方安全服务插入平台。



基于 hypervisor 的基础架构保护

将应用抽离底层基础架构的模式还在基础架构中提供了一个理想位置，可防范对基础架构本身的入侵。组织可通过每个 hypervisor 主机上的工作负载级加密保护静态数据。他们可加密传输中的数据，以缓解路由器和交换机等网络连接组件遭受侵袭的风险。



一系列保护应用基础架构安全的功能

不管组织的虚拟化之旅到了何种程度，VMware 都可提供业界领先的技术来增强应用安全环境。

VMware vSphere
为了在虚拟化环境中保护关键业务资源，组织需要管理精简且操作简便的策略驱动型安全功能。

VMware vSphere 是业界领先的虚拟化平台，为实现业务敏捷性奠定了强大、灵活、安全的基础，可帮助组织加快向云计算发展的数字化转型。借助解决方案的以下特性，可同时支持现有应用和新一代应用：简化的客户体验，用于实现自动化和大规模管理；全面的内置安全性，用于保护数据、基础架构和访问；通用应用平台，用于在任何地方运行任何应用。借助 vSphere，组织可以在常见运维环境中，跨云不同环境和设备运行、管理、连接以及保护其应用。

VMware vSphere 提供了丰富的安全功能特性，可帮助组织在发生数据泄漏时保护其环境并减轻问题：

- 大规模安全性 – 策略驱动型安全性可简化基础架构保护操作。
- 加密 – 虚拟机级别的加密可保护对静态数据和动态数据的未授权访问。
- 审核质量日志记录 – 增强的日志记录可提供有关用户操作的取证信息。

VMware NSX
为了针对当今的复杂威胁提供保护，组织需要使他们能够将数据中心划分为逻辑分段的虚拟网络环境。

如果攻击者突破数据中心边界防御，务必要阻止威胁在数据中心内横向移动。虚拟化方法使 IT 团队能够基于动态安全组为每个工作负载定义安全策略，以便他们可以立即对数据中心内的威胁作出响应。VMware NSX 是网络虚拟化平台，它为数据中心网络提供了类似于虚拟机的运维模式。借助 VMware NSX，组织能够以编程方式对整个网络执行创建、快照拍摄、存储、移动、删除和还原操作，就像运行虚拟机一样具有点击简便性和较快的速度，从而提供以硬件为中心或传统运维方式无法提供的安全性、敏捷性和可用性级别。该解决方案使组织能够将安全策略向下强制到单个虚拟机级别。

VMware NSX 可对想要发挥虚拟化的安全性和性能优势的组织提供支持。关键功能包括：

- 安全性 – hypervisor 中的嵌入式安全功能可针对各个工作负载提供微分段和精细安全性。
- 自动化 – 使用策略驱动型方法将网络和安全性服务附加到工作负载，从而实现自动化并提高性能。
- 应用连续性 – 将网络连接抽离底层硬件，从而将网络连接和安全策略附加到其关联的工作负载。

vRealize Network Insight

为了管理异构的混合云环境，组织需要一个专为该环境构建的企业级云计算管理平台。

vRealize Network Insight 借助跨虚拟和物理网络的融合可见性为软件定义的数据中心 (SDDC) 网络连接和安全性实现智能运维，并为 VMware NSX 提供微分段规划建议和运维管理。vRealize Network Insight 可提供帮助组织优化安全性的多种功能特性：

- 可见性 – 通过虚拟层与物理层的集成，跨叠加层和底层、虚拟层和物理层以及私有云和公有云提供融合可见性。
- 微分段建模应用行为 – 使用户能够轻松了解哪些人在相互通信，以及需要允许或阻止哪些流量。
- 审核和合规性 – 跟踪所有变更，以实现审核和合规性目的。

立即借助 VMware 保护您的应用基础架构

当今的 IT 组织面临着数字化转型和快速变化的威胁形势带来的前所未有的挑战。在这一动态环境中，与口碑良好的技术供应商合作以帮助确保业务运维安全比以往任何时候都更加重要。VMware 通过一个跨应用基础架构的遍布式软件层，来帮助组织转变其实现安全性的方法。通过将基础架构抽离其所支持的应用，VMware 使 IT 能够深入了解数据路径，以提高洞察力和控制力。通过结合使用微分段，该解决方案可帮助组织简化安全策略并提供更好的保护，以满足特定应用的需求。VMware 通过由广泛的合作伙伴生态系统提供支持的多种安全性和虚拟化解决方案选择做到这一切。通过部署可靠的安全性和合规性解决方案，组织可使 IT 团队安心地专注于推动业务增长和创新。

立即开始行动

保护您的应用基础架构 **了解更多 >**

在线加入我们：

关注 VMware中国

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
中国北京海淀区科学院南路 2 号融科资讯中心 C 座南楼 1 层 邮编：100190 电话：+86-10-5993-4200
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