VMware NSX Data Center

帮助 IT 实现与业务同步发展

“技术以惊人的速度不断发展，定能给掌握主动权的企业带来丰厚的回报。”

BART VAN ARK 博士
世界大型企业联合会执行副总裁、
总经济师兼战略官

VMware NSX® Data Center 是一款支持虚拟云网络的网络虚拟化和安全性平台，能够以软件定义的方式实现可跨数据中心、云环境和应用框架进行延展的网络连接。借助 NSX Data Center，可以使网络和安全性更贴近应用，而无论应用在何处（包括虚拟机 [VM]、容器和裸机）运行。与虚拟机的运维模式类似，可独立于底层硬件对网络进行调配和管理。NSX Data Center 通过软件方式重现整个网络模型，从而实现在几秒钟内创建和调配从简单网络到复杂多层网络的任何网络拓扑。用户可以创建多个具有不同要求的虚拟网络，利用由 NSX 或范围广泛的第三方集成（从新一代防火墙到高性能管理解决方案）生态系统提供的服务组合构建本质上更敏捷、更安全的环境。然后，可以将这些服务延展至同一云环境内部或跨多个云环境的各种端点。

相互矛盾的需求导致妥协

速度和敏捷性、可靠的安全性以及应用的高可用性都是 IT 企业得以发展的至关重要的优先事项。企业在很大程度上依赖于可靠的应用基础架构，因此，IT 越来越成为企业在数字化转型过程中实现创新并取得成功的基础。但是，IT 领域极快的变化速度及不断转变的预期导致需要不断调整优先事项，而这常常会影响交付效率。

IT 强烈意识到，他们常常为满足多个相关人员的需求而处于紧张状态，从而不得不经常权衡考虑，将一项 IT 事务优先于其他事务进行处理。例如，由于安全性方面的操作极不灵活且非常复杂，时常会为保护应用安全而牺牲其部署速度。跨环境应用的可用性经常会有此类牺牲，导致 IT 与整个企业之间出现相互矛盾。

这种持续的紧张和妥协最终会对 IT 造成巨大影响。实际上，这会导致多个职责领域出现严重问题：企业无法快速满足需求、数据中心和云环境中到处都是漏洞，并且缺乏总体敏捷性。

发挥基础架构的全部潜力

大多数企业都已将数据中心内的计算组件虚拟化。此外，许多企业也已经决定将存储虚拟化，这些企业中有 70% 以上已经采用或计划采用软件定义的存储。

这种将硬件功能抽象化为软件形式的技术使企业能够快速调配应用组件、在数据中心内部以及多个数据中心之间移动虚拟系统，并自动执行关键流程。

主要优势

精细级安全性 – 借助工作负载级微分段安全策略，防止威胁在环境中横向扩散

速度和敏捷性 – 通过自动化将网络调配时间从数天缩短至数秒并提高运维效率

一致的运维 – 跨数据中心、公有云和私有云，以及应用框架以独立于物理网络拓扑的方式实现对网络和安全性策略的一致管理

遗憾的是，其中许多优势仍仅在发展缓慢的数据中心组件上得以体现，还没有应用到数据中心基础架构的其中一个尚未完全虚拟化的部分，即网络部分。如果不将网络虚拟化，软件定义数据中心将难以实现全部价值。

事实上，在速度、敏捷性或安全性方面，采用植根于硬件的网络体系架构的企业根本无法与部署虚拟化网络的企业相匹敌。企业的状态受限于网络的状态。

数据中心网络连接需要一种全新方法，不再需要在速度与安全性或安全性与敏捷性之间做出选择，让其中一个有所牺牲。需要重新编写阻碍企业发挥全部潜力的数据中心规则，以使 IT 部门能够在不做出任何牺牲的情况下顺利执行任务。数千家企业现在已经认识到，这种新方法就是网络虚拟化。

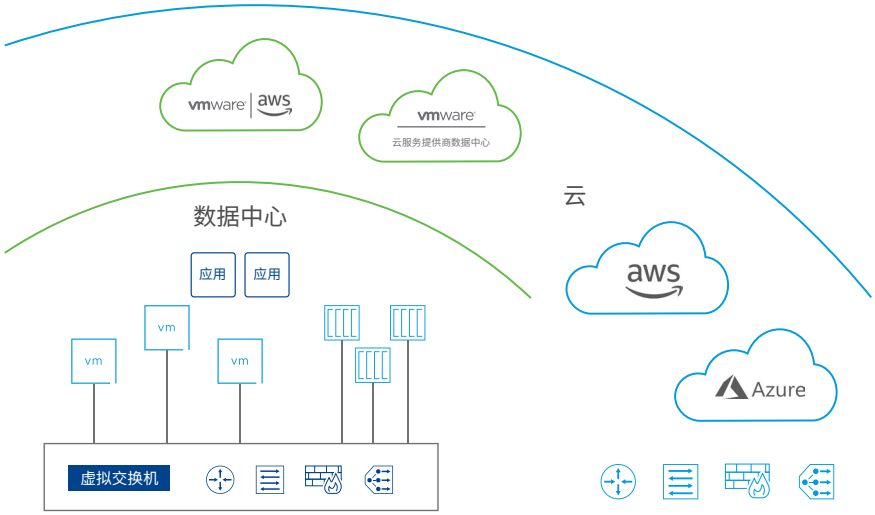

图 1：通过 NSX DATA CENTER 提供一致的网络和安全性。

网络虚拟化将网络和安全性服务移至数据中心虚拟化层，使 IT 部门能够对整个应用环境执行创建、快照拍摄、存储、移动、删除和还原操作，并且就像他们现在启动虚拟机一样简单快速。NSX Data Center 跨异构环境和应用框架延展通用网络和安全性策略，使这些优势可以跨数据中心、私有云和公有云、传统应用及新的容器化云原生应用而实现。这进而能够实现以前在操作上和经济上均不可行的安全性与效率水平。

VMware NSX 是适用于软件定义数据中心的网络虚拟化平台，可以延展多云环境。它具有先前嵌入到网络硬件中的功能（例如交换、路由和防火墙保护），并将这些功能抽象到软件中。

借助 NSX，IT 部门能够推动企业创新，即时有效满足多个相关人员的要求，而不是将这些要求视为相互矛盾和排斥。现在，IT 部门不仅能提供前所未有的安全水平，还能与业务发展速度保持同步。

主要功能特性

分布式有状态防火墙保护 – 启用最高运用到第 7 层的有状态防火墙保护，该保护嵌入在 hypervisor 内核中、跨整个环境而分布，并且直接集成到云原生环境、原生公有云和裸机主机中

环境感知微分段 – 动态创建安全组和策略，并根据许多属性和第 7 层应用信息自动更新它们，以启用自适应微分段策略

云计算管理 – 与 vRealize Suite、OpenStack 等工具原生集成，并且完全支持 Terraform Provider、Ansible 模块和 PowerShell 集成

第三方集成 – 通过由领先的第三方供应商构成的生态系统增强安全性和高级网络服务

云原生支持 – 跨容器平台、虚拟机和裸机主机为企业级高级网络和安全性提供支持，同时提供容器网络可见性

NSX Intelligence™ – 缩短用于发现、分析和执行应用分段策略的时间，且无需部署任何新工具或代理；内置在基础架构中的固有安全性可简化安全操作

固有的安全性

NSX Data Center 提供了独有的可见性，让您能够了解应用组合（从网络通信到针对单个工作负载的进程级行为），这要归功于它在 hypervisor 中的内置位置以及作为应用构建基础的其他原生控制点。这种可见性有助于基于应用的预期安全状况自动创建网络安全策略。这可以减少 IT/信息安全和应用开发团队在安全性审查周期中花费的时间。

利用它，还可以跨多数据中心和混合云环境延展和强制实施安全策略，并对基于虚拟机、容器和裸机服务器构建的应用进行全面控制。NSX Data Center 还会将可见性和控制延展到第三方安全服务（如新一代防火墙、入侵防御系统 [IPS]/入侵检测系统 [IDS] 解决方案，以及防病毒工具），从而提高这些服务的效用。

安全保护曾是应用开发生命周期中被动的额外流程，NSX Data Center 将其转换成了生命周期中主动、集成并且自动化的步骤。新调配的工作负载会自动继承安全策略，这些策略将在工作负载的整个生命周期内跟随着这些工作负载。当弃用工作负载时，其安全策略也将一并弃用，这可以防止策略随时间推移而越积越多并可简化管理。

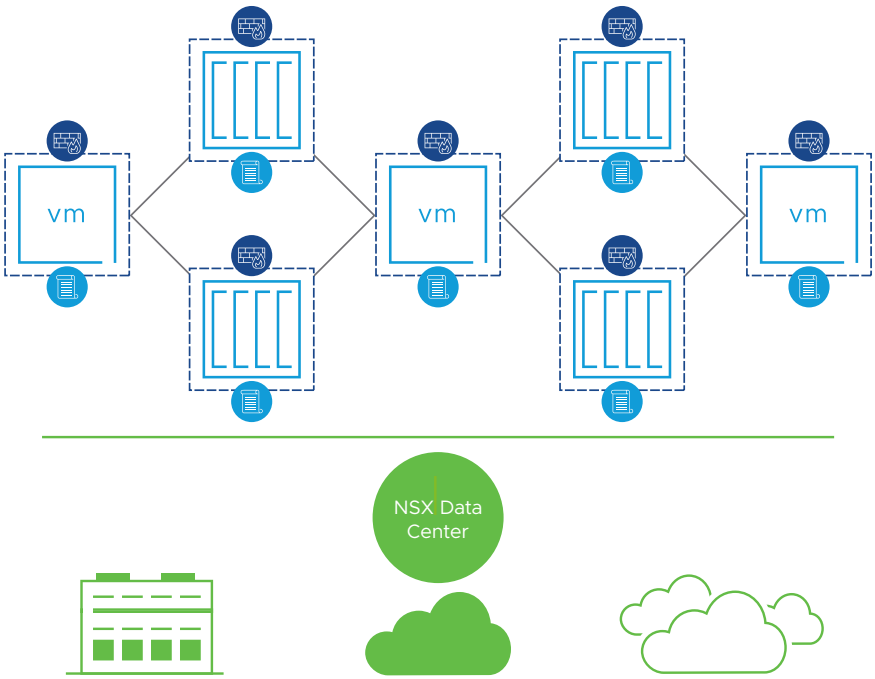

图 2：对数据中心强制实施最精细的安全保护。

自动化

随着企业的业务范围不断扩展，发展速度不断加快，自动实施虚拟化网络和安全性可确保根据业务发展速度创建和部署服务和应用。通过利用自动化移除易于出错的手动网络调配任务，大幅加快应用部署速度。

与云计算管理软件（例如 VMware vRealize® Automation Cloud™）配对使用的 NSX Data Center 可以从中央控制平面管理网络和安全性基础架构及应用的调配、部署、运维和停用。通过将网络和安全性生命周期集成到流程中，VMware 可自动执行所有基础架构操作，并消除应用生命周期中的网络和安全性瓶颈。

通过跨两个框架延展通用网络和安全性策略，可以使传统（基于虚拟机）和新（基于容器）应用的网络和安全性实现自动化。此外，这样可以跨本地部署数据中心、私有云和公有云自动部署、移动和停用应用。

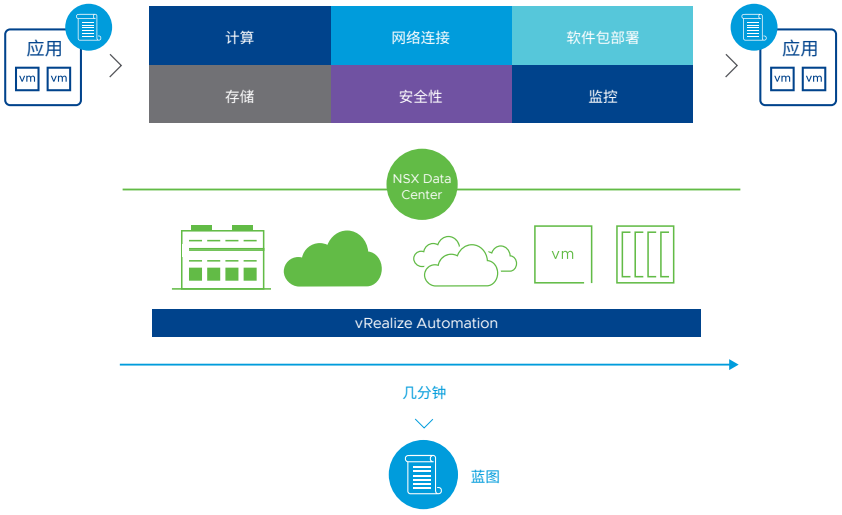

图 3：具有自动化网络和安全性的快速且可重复的部署。

多云环境网络

NSX Data Center 和 NSX Cloud 可提供跨站点的统一网络和安全性模型，使您无需再手动进行网络配置，而是通过网络自动化实现高效运维。网络和安全性策略在各工作负载的整个生命周期内都跟随该工作负载，这简化了混合云和多云环境中的策略和管理。

这还使企业能够在极少停止甚至不停止运行应用的情况下，将虚拟机或整个数据中心从一个位置迁移到另一个位置。因此，企业能够在计划内迁移和意外故障期间加快恢复速度。由于网络和安全性跨异构站点，企业还可以利用其各个物理数据中心内的资源来作为单一私有云运行。双活数据中心的这种资源池化形式称为“多数据中心池化”或“城域池化”。

所有这些可以帮助实现安全、无缝的应用移动性，从而轻松向云或从云进行迁移或者在物理站点之间迁移。NSX Data Center 和 NSX Cloud 可将 IT 企业在其基础架构上使用的同一虚拟化网络和安全性平台延展到云环境或其他站点中，从而实现低干预度的快速迁移流程。

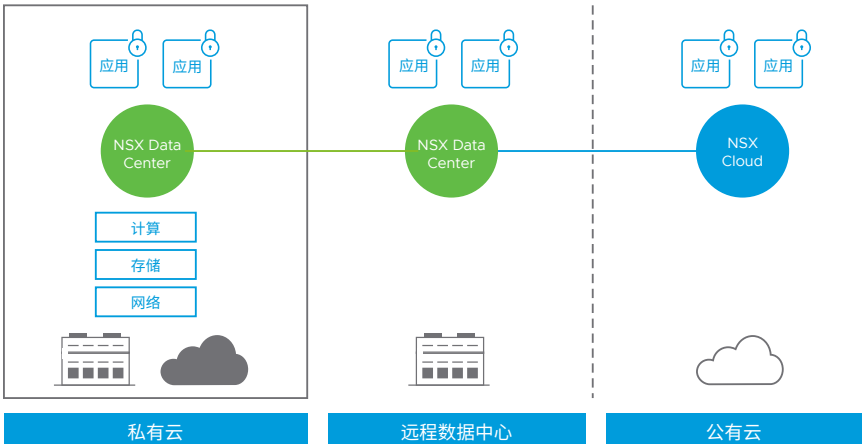

图 4：跨站点和云环境实现一致的网络和安全性，同时降低故障影响。

云原生

VMware NSX Data Center 与新应用平台集成，以提供网络和安全性功能（如负载均衡、防火墙保护、交换和路由），这些功能完全在软件中构建，可通过 API 驱动的、基础架构即代码形式使用。

随着应用越来越多地基于容器和微服务体系架构，我们需要能够连接和保护这些新应用，乃至单个工作负载。NSX Data Center 将容器和微服务视为“一等公民”，与任何其他工作负载或端点一样，它也能够建立 L3 网络。它能够以原生方式建立容器间网络，以及向下微分段至单个容器级别，从而为微服务启用微分段，并且在调配、更改、移动和停用工作负载期间让策略始终跟随工作负载。

NSX Data Center 可与多个应用和容器编排平台、hypervisor 和公有云环境集成。此外，还可以跨应用平台进行集成，以便在开发新应用时为这些应用提供固有的敏捷网络和安全性。

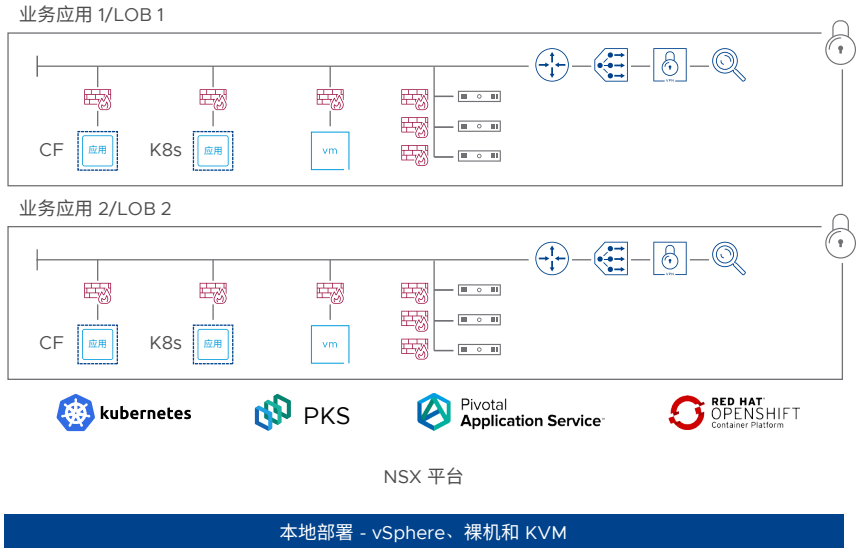

图 5：将高级网络和安全性纳入到跨应用框架、平台、站点和云环境的容器化工作负载中。

了解更多

有关更多信息，请访问 https://www.vmware.com/cn/products/nsx。

VMware NSX Intelligence

NSX Intelligence 是以原生方式内置在 NSX Data Center 中的分布式分析引擎，可提供持续的数据中心级可见性，从根本上将使用 NSX Service 定义的防火墙实施微分段的过程简化和自动化。它首先构建列有全部虚拟机的清单，记录每个流量并直观显示详细的应用依赖关系图。NSX Intelligence 通过与 vRealize Network Insight™ 紧密集成来丰富分组，并可摄取所有当前的清单元数据、配置管理数据库 (CMDB) 标记或任何应用模型。

创建策略很简单；系统会自动推荐用于防火墙保护的应用组和分段策略。NSX Intelligence UI 嵌入在 NSX Manager™ 中，提供了无缝的工作流来迭代您的策略。所做的任何更改都会立即反映在拓扑图中，即时提供直观的反馈，并让您能够快速看到新策略。

在当前加快实现业务价值，为未来奠定坚实基础

那些部署了 NSX Data Center 的企业发现，NSX Data Center 正迅速成为 IT 企业成功与否的决定性因素，而且是数据中心基础架构和多云战略的基础部分。如今，数以千计的 NSX Data Center 客户正在加速为企业提供价值，他们基于快速、敏捷且安全的虚拟网络交付一些最敏感且最关键的应用，而且采用的是在基于硬件的传统网络上根本无法实现的交付方式。

网络和安全性方面的这种发展不仅使 NSX Data Center 客户获得了显著、即时的优势，还消除了之前占用大量企业带宽且耗时费力的任务。这进而又给这些企业带来了更大的选择自由，让他们能够在规划企业未来以及 IT 支持该愿景所需具备的功能时考虑采用更具组织性的战略。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com
威睿信息技术（中国）有限公司
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
中国上海办公室 上海市淮海中路 333 号瑞安大厦 805B-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