vmware®

VMware 金融行业解决方案手册

业务创新推动金融行业数字化转型

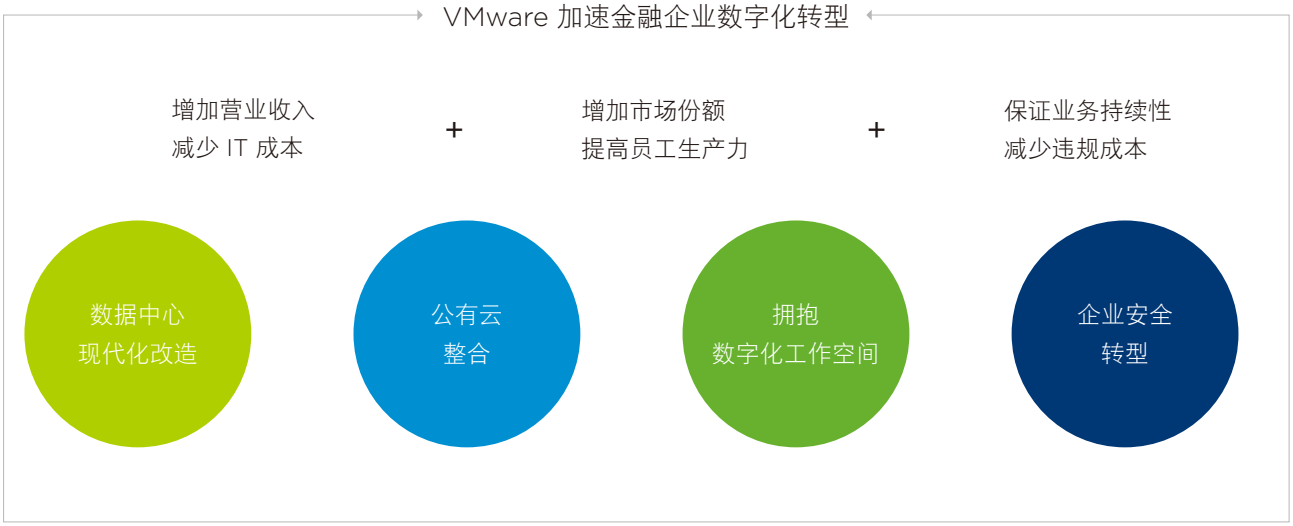
随着信息技术的飞速发展，金融行业也在不断利用信息技术进行业务创新，新的业务模式不断涌现。金融行业的 CIO 们期望在未来更多的业务收入来自于数字化销售和服务，希望数字化新业务的收入相对于传统业务的比例逐渐提高，甚至在将来能超够出传统业务。

另一方面，金融行业也在面临着来自于更多的竞争，这些竞争或者来自于国外的同外，或者来自于新兴的互联网行业，所有的这些竞争都要求金融企业通过优化管理来提高服务水平，降低运营成本，提高企业竞争力。

在这些背景下，数字化转型已经成为金融企业业务创新、提高运营水平的必由之路。应对金融企业的数字化转型需求，VMware 提供了一系列的解决方案，从各个维度全面助力企业数字化转型，加速企业实现收入增长、成本降低的目标。

VMware 可以从以下几个方面来帮助金融企业向数字化转型：

- 数据中心现代化改造：把传统的数据中心改造成软件定义的数据中心。
- 公有云整合：整合企业私有云和公有云服务，助力企业IT基础架构向混合云转型。
- 拥抱数字化工作空间：利用数字化工作空间提高员工生产力，通过移动营销实现业务创新。
- 企业安全转型：全面防范企业安全威胁，确保金融业务应用和数据安全。



数据中心现代化改造

从 UNIX 迁移到虚拟化的 Linux (U2VL)

因为历史原因，很多金融企业的一些关键应用还运行在传统的 UNIX 服务器平台上，从市场发展趋势来看，UNIX 服务器的市场份额正在逐渐萎缩，而让位于 x86 服务器，“去小机化”逐渐演变成当前技术改造的一个趋势。传统的 UNIX 服务器价格昂贵，软硬件技术封闭，运维成本高；而 x86 服务器经过多年的发展，从性能和可靠性上都不逊色于 UNIX 服务器，但采购价格和运维成本却要便宜得多。

经过多年的运营，很多企业的 UNIX 服务器也逐渐到了退役的年龄。针对这种情况，VMware 提供了 U2VL (UNIX To Virtualized Linux) 解决方案来将原来运行于 UNIX 平台上的关键应用迁移到基于 x86 服务器的虚拟化环境。VMware 已经为国内的众多客户成功实施了从 UNIX 迁移到虚拟化 Linux 的项目，拥有丰富的实践经验，可以充分保证关键应用的平滑迁移，把对于金融业务的影响降到最低。

x86 服务器 vSphere 虚拟化环境的优点：

- 计算资源池化，灵活应对突发计算需求，快速应对业务变化。
- 虚拟化集群提供原生高可用环境，为应用提供高可用保护。
- 计算资源整合，减少服务器的数量，进而降低能耗和节省机房空间。
- 系统架构易于扩展，增加服务器就可以增加整个数据中心的计算和存储容理。
- 完善的数据中心运维、数据备份和灾备解决方案，提升数据中心运维水平。

改造基础架构

传统的数据中心基础架构是分别采购服务器、存储和网络设备，再把它们组装在一起，整个过程比较费时费力，往往需要几周的时间才能投入使用。而且不同的设备和软件分属不同的厂商，遇到问题时容易出现推诿责任的现象。现在越来越多的用户选择超融合系统来搭建私有云环境，超融合系统整合了服务器和存储（或者也包括了网络），在交货前已经由厂商负责整合和测试，可以做到开箱即用，大大缩短了 IT 基础设施的交付时间。

针对这种需求，VMware 专门推出了超融合软件堆栈 HSS (HCI Software Stack)，其中包括：虚拟化操作系统 vSphere、集群管理软件 vCenter、存储虚拟化软件 vSAN。 现在，大部分硬件厂商都推出了基于 VMware 超融合软件堆栈的系统，如 Dell-EMC 的 VxRail 等等，凡是标识为 vSAN ReadyNode 的硬件系统都可以作为 VMware 超融合软件堆栈运行平台。

在上面的架构中，vSAN 是整个超融合系统的关键，它通过高速网络把多台服务器上的直连硬盘整合成一个虚拟的存储，并且利用 SSD 作为读写的高速缓存，具有低成本、高性能的特点。vSAN 会在多台服务器上保存数据副本，任何单台服务器的硬件故障，都不会造成数据丢失。vSAN 也很容易扩展，将来只需要增加服务器和硬盘就可以扩展 vSAN 的存储容量。

高可靠解决方案 (High Availability)

为了保证业务的持续性，金融行业对于 IT 基础架构的可靠性要求都比较高，VMware 提供了多种高可靠解决方案来满足这一业务需求。

- vSphere 集群 (Cluster)：vSphere 虚拟化环境把物理服务器组成一个集群，任何一台服务器发生硬件故障，上面的虚机会被迁移到其他服务器上继续运行。 vSphere 集群只能防止单机故障，而不能防止站点级故障。
- 跨数据中心灾备：VMware Site Recovery Manager (SRM) 可以提供跨数据中心站点的灾备方案，当一个站发生故障时，SRM 可以把受保护的虚机迁移到另一个站点继续运行。两个站点也可以设计成互为灾备，从而形成双活数据中心。
- vSAN 延伸集群 (Stretched Cluster)：当两个数据中心距离较近，它们之间光纤网络延迟较低时，也可以采用 vSAN 延伸集群来保护虚机，相当于把两个数据中心的服务器放在一个大的 vSphere 集群中进行保护。跟 SRM 方案相比，vSAN 延伸集群是一种低成本的跨数据中心灾备方案。
- Fault Tolerance 容错方案：以上三种方案都有一个服务中断恢复的过程，如果某个关键应用不能中断地话，VMware 提供了一种容错方案 Fault Tolerance，利用一台备份服务器完全同步主服务器上的受保护虚机，来实现完全无中断的高可靠方案。

软件定义数据中心 (Software Defined Data Center)

IT 自动化 (vRealize Automation)

在虚拟化的基础上，VMware 提出了软件定义数据中心 (SDDC – Software Defined Data Center) 的建议，利用数据中心自动化工具 vRealize Automation 来自动创建 IT 基础架构，如创建虚拟服务器、分配存储空间、创建虚拟化的网络设备等等，把数据中心完全变成软件定义的。这样所有的IT基础设施都可以由软件工具自动调配而成，利用 vRealize Automation，虚拟资源的调配可以从几个星期缩短到几个小时，甚至是数十分钟，从而大大提高数据中心的运营效率，更好地应对金融业务快速变化带来的挑战。

当项目结束之后，不再使用的资源可以退还到资源池中；如果有项目组没有主动退还所申请的计算资源，vRealize Automation 工具可以自动发现长时间无人使用虚机，并且提醒相关责任人采取必要的动作，如果超过规定时间还没有动作，可以强制释放资源。有企业利用这一功能，节省了 30% 以上的硬件资源投资，通过及时释放不再使用的资源来满足新的业务需求，而不再需要采购新的硬件。仅此一项所产生的经济效益，就远远超出了在自动化工具上的投入。

SDDC 平台 (VMware Cloud Foundation)

针对软件定义数据中心的建设需求，VMware 推出了 SDDC 平台 VMware Cloud Foundation，其中整合了计算虚拟化软件 vSphere、存储虚拟化软件 vSAN 和网络虚拟化软件 NSX 的全部功能，通过一个产品来支持新一代云平台的建设。Cloud Foundation 中包括了全自动的部署工具 SDDC Manager，来帮助用户快速地构建私有云平台，可以用几个小时就完成整个软件定义数据中心的部署。同样的工作由传统的手工部署方式来个做的话，需要几个星期的时间。SDDC Manager 也负责管理维护整个私有云的生命周期，它可以全自动地完成整个软件堆栈的升级和维护操作。

VMware Cloud Foundation 不仅是一个私有云平台，它也可以以公有云服务的形式来交付，VMware 已经分别与两大公有云供应商 AWS 和 IBM SoftLayer 宣布合作，基于他们的公有云平台来提供 Cloud Foundation 服务。随着云计算技术的发展，越来越多的金融企业计划把部分工作负载迁移到公有云平台上去，但是他们不知道如何迈出这一步。VMware 提出了基于 Cloud Founation 的跨云架构 (Cross-Cloud Architecture)，这是一个面向公有云迁移的技术方案，用户可以利用 Cloud Foundation 从私有云平滑地迁移到公有云，因为私有云和公有云上的运行平台是完全一致的，而且这种迁移不仅仅是从私有云到公有云，也包括在不同的公有云平台之间迁移工作负载，为用户选择不同的云服务供应商提供了灵活性。

部署新一代应用

除了传统业务之外，几乎每家金融企业都在借助移动互联网技术开拓新业务，相关的应用架构也在不断创新，很多应用引入了云原生 (Cloud Native) 应用的架构，即运行在容器上。VMware 的虚拟化环境也完全支持容器技术，VMware 在 vSphere 中内置了 VIC (vSphere Integrated Containers) 技术，来提供对于容器技术的支持。利用 vSphere 独门的即时克隆 (Instant Clone) 和 Photon OS (虚机镜像可以小至几十兆) 技术，VIC 技术做到了跟容器技术同等水平的资源消耗，但是在安全性、高可靠、运维管理、容灾等方面提供了更完善的运行环境和解决方案。对于已经是 vSphere 的金融行业用户来说，VIC 是尝试容器技术的最佳选择，它远比开源的容器技术更为成熟可靠。

公有云整合

基于安全方面的考虑，大部分金融企业的核心业务还是运行在企业自己的私有云中，但是也有部分企业已经或计划把部分的非核心业务放到公有云上去，或者直接使用基于云端的软件服务。VMware 为金融企业向混合云转型提供了多种选择。

VMware 的云服务

目前 VMware 提供有以下标准的云服务：

- VMware Cloud on AWS：基于 AWS 公有云提供的 Cloud Foundation 服务，为基于 Cloud Foundation 私有云的用户迁移到公有云提供无缝对接。
- Horizon Cloud Service：基于 Horizon 平台的虚拟桌面和应用服务，提供云端虚拟桌面和应用托管服务。
- Workspace ONE / AirWatch：提供数字化工作空间和移动设备管理服务。

目前，这些服务只在境外提供，如果金融企业向海外拓展业务的话，可以考虑选择这些云端服务。

VCP 云服务

在国内，VMware 是通过 VCP (VMware Cloud Provider) 合作伙伴来提供云服务的，可以提供以下几类云服务：

- 基础架构：多租户的 IaaS 服务，提供虚拟机和网络的自助服务；借助于云管平台和网络虚拟化 ，为用户从私有云迁移到公有云提供无缝对接。
- 云灾备：在云端提供灾备服务，当数据中心发生故障时，受保护的虚机可以在云端恢复服务。
- 桌面云：在云端提供虚拟桌面和远程应用托管服务。

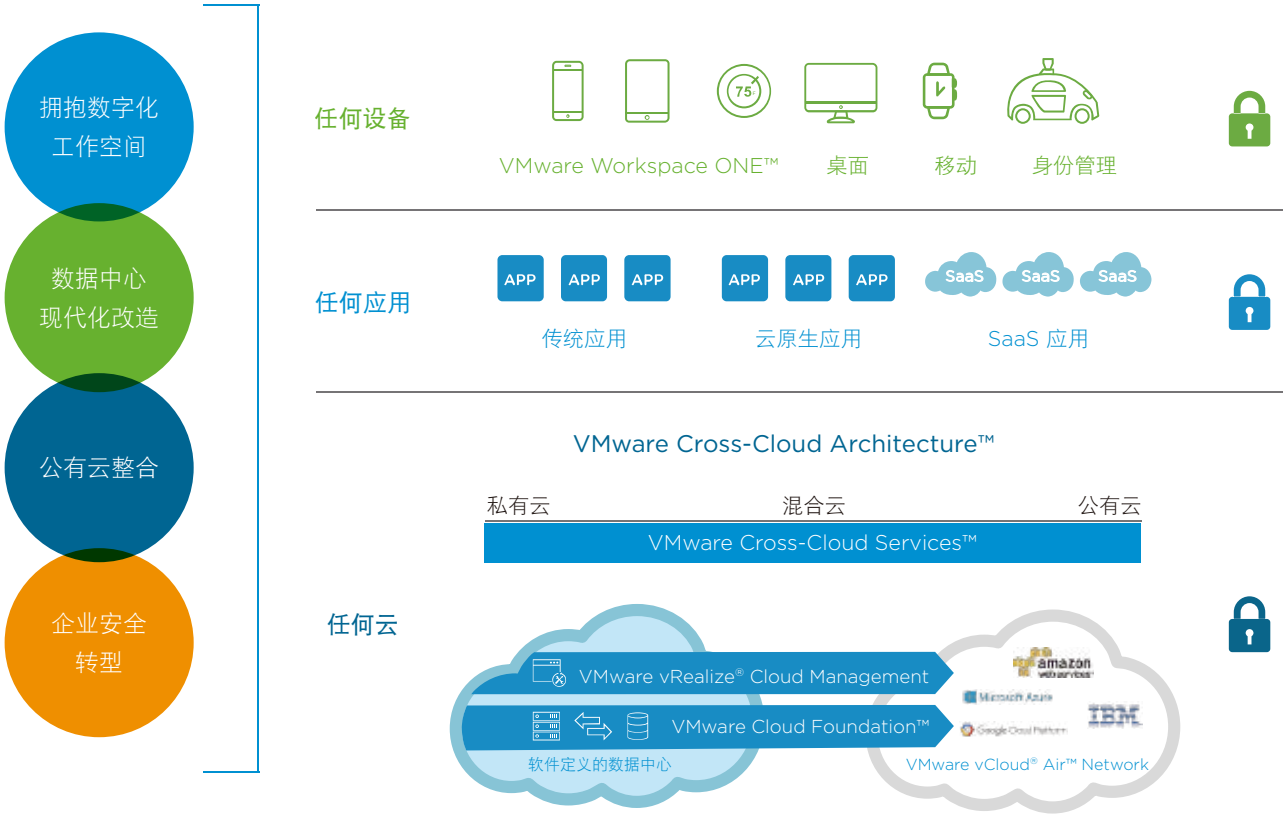
VCP 是 VMware 的云服务合作伙伴计划 (原名 vCAN – vCloud Air Network)，任何有兴趣提供基于 VMware 产品云服务的服务供应商都可以申请加入该计划，然后将云服务提供给它的客户，VMware 会对该合作伙伴提供云服务部署、运维方面的业务指导。

发展新的 VCP 合作伙伴

国内的金融企业可以使用现有的 VCP 合作伙伴提供的云服务，也可以根据业务需要，自己选择一家云服务供应商，以满足金融行业的一些特殊要求。VMware 可以跟用户推荐的第三方服务商签订 VCP 合作协议，帮助服务商建立相关的云服务，以满足最终用户的需求。

随着金融行业的发展，有越来越多的中小型金融机构加入了金融服务行业，基于风险控制和资源优化的目的，监管部门也鼓励大型金融企业为小型机构提供相关的IT服务。在这种业务背景下，金融企业自身也能成为 VMware 的 VCP 合作伙伴，例如大型金融集团下属的科技公司可以成为 VMware 的合作伙伴，为集团内的其他企业或者是外部的中小企业提供基于 VMware 技术的云服务。

VMware 的愿景



拥抱数字化工作空间

在云计算和移动互联大潮下，为了赶上时代的步伐，所有的企业都在通过数字化转型来创新自己的业务，使得自己在改革创新的浪潮中能够立于不败之地。数字化工作空间就是数字化转型中的重要一环，VMware 的愿景是让员工能够在通过任何设备 (Any Device) 访问所有的企业应用 (Any Application)，实现随时随地地办公，从而大大提高企业员工的生产效率，让员工能够以自己最便利的方式来完成工作，从而实现企业和员工的共赢。

移动办公

我们已经进入到了移动-云计算时代，为了提高工作效率，无论是企业还是员工都希望能够随时随地利用手头的任何设备来办公。我们迫切地需要手机或平板也具有笔记本电脑相同的工作支持能力，以更加便利地方式来处理工作相关的事务，以跟上这个竞争时代的飞快节奏。伴随着互联网+热潮的兴起，企业移动化正在进入各个 CIO 的工作日程，成为企业数字化建设的一个重要组成部分。

Workspace ONE 是VVMware 支持移动办公的数字化工作空间平台，它支持VWindows、Mac OS、iOS、Android 等多种设备，具有跨平台的一致用户体验。Workspace ONE 提供了以下五大功能来支持企业移动办公的需要：

- 统一身份认证：企业内的所有应用只需要一套身份系统来认别，支持应用实现单点登录，并且提供原生的多因子身份认证方案。
- 企业应用商店：员工要用的应用只需要到统一的企业应用商店中去下载，大大简化IT支持工作，提高用户满意度。
- 移动设备管理：支持员工自带设备 (BYOD) 办公，对办公设备进行安全管控，当设备失窃或丢失时及时擦除设备上的数据，保证企业数据安全。
- 生产力工具：内置安全邮箱、浏览器、企业网盘等生产力工具，注册以后立即可以满足基本办公需求。
- 远程桌面和应用：整合VMware虚拟桌面和应用交付平台Horizon，可以在任何设备上远程访问办公桌面，使用各种办公软件。

Workspace ONE

自助式的企业应用商店（支持单点登录）

各种应用类型

Windows　Virtual Apps　Web　Legacy　Mobile

Workspace ONE Apps Suite

EMAIL　CONTENT　BROWSER　CHAT

条件访问控制、数据防丢失

统一端点管理
- 空中设备配置
- 应用自动安装和配置
- 设备注册管理
- 自动修复

身份、安全和合规
- 身份联邦 / 身份认证
- 访问策略
- 报告、审计和分析
- 自动循规处理

传统的 Windows 应用
- 完整桌面或远程应用
- 现场或云端部署
- 完全隔离

灵活的应用生命周期管理平台（开发、部署、管理、支持）

安全和网络虚拟化

企业文档管理

金融企业在日常工作中经常会涉及到一些高度机密的文档，如：监管部门的金融政策、客户的融资计划、商业促销计划等等，需要严格限制这些文档的分发对象，并且在业务过程中要严格注意保密。

针对这种业务场景，VMware 专门提供了企业文档管理平台 Content Locker，它可以在企业内部安全地分享文档资料。普通用户可以通过移动设备或个人电脑上的 Content Locker 应用来上传、下载文档，并且。管理员可以向指定的用户组分发企业文档，并监控分发情况。企业员工可以在多种设备上通过 Content Locker 应用审阅文档，并对文档进行批注。

Content Locker 提供了完善的安全措施来从各种各个维度保证企业文档的安全。

文档加密：

Content Locker 无论在移动设备端存储文档，还是在网络传输过程中，都是对文档的内容进行加密的。

数据防丢失 DLP (Data Loss Prevention)：

Content Locker 中可以设制各种安全选项来防止信息外泄，如禁用复制/粘贴、禁止把文件作为邮件附件转发、禁止在不合规设备的设备上打开文档等。当设备丢失或失窃时，可以马上实施远程擦除，擦除设备上所保留的文档。

动态水印：

Content Locker 可以在显示文件内容动态附加一个水印，这个水印显示的是当前用户的身份标识，从而在数据被窃时及时查找到泄密的源头，防止通过截屏、拍照等手段泄密。

移动金融

对于金融企业来讲，移动化转型带来了创新的业务模式，如移动银行：客户不再需要到营业网点排队办理业务，只要通过电话、网络或微信平台预约好了服务，业务员就会上门办理，他们利用基于平板电脑的终端来办理几乎所有的银行业务，如银行帐户开门、贷款申请、个人理财等等，从而最大程度地节省客户的时间，这些体贴的服务对于高净值客户是最具吸引力的，移动业务成为了银行新的业务增长引擎。

将金融业务从传统的柜面转向移动设备的过程中，IT 团队最关心的是安全问题。在目前网络犯罪日益猖獗的大环境下，办理业务的终端却脱离了传统的 IT 安全监管，不再在柜面摄像头的监控之下，敏感数据的访问也不再通过企业的内部网络。Workspace ONE 为客户提供了移动端的全面安全解决方案，可以实现业务数据在存储、使用、传输中的安全保障；业务应用也是在 Workspace ONE 的安全沙箱中运行，可以有效抵抗恶意软件的攻击。

开发桌面管理

金融企业的大部分业务系统都是自主开发的，由于企业自身的开发资源有限，往往引进软件开发外包团队进行协作开发。这些业务系统的代码是金融企业的核心资产，同时这些代码也涉及到金融交易的安全性，所以必须严格保证代码的安全性。针对这种业务场景，VMware提供了基于虚拟化桌面平台 Horizon 和网络虚拟化软件NSX的开发桌面云方案。

- 数据不落地：所有的开发工作都在虚拟桌面上完成，代码完全保存在服务器端的虚拟开发桌面上，在开发人员的笔记本上完全不保存代码。
- 网络隔离不同的开发团队：利用NSX的微分段技术来完全隔离不同的项目团队，每一位开发人员仅能访问他所在项目的文档和代码，这样就最小化了代码泄露的风险。

呼叫中心

大部分金融企业都设立有呼叫中心，通过电话来为客户提供各种金融服务。呼叫中心客服人员座席的需求是高可靠性和低成本，要求维护简单，可靠性高，成本尽可能的低。VMware 基于虚拟化桌面平台 Horizon 的座席管理方案可以很好地满足这方面的需求。

- 共享桌面池：每个客服的工作桌面都是一样的，所以他们可以共享同一组桌面，只要以自己的用户身份登录就可以开始工作了。利用 Horizon 的即时克隆技术，所有的桌面都可以共享同一个虚机的镜像，大大降低了存储空间的占用。对于桌面的升级维护操作也非常简单，只要升级父虚机的操作系统 和应用软件就可以，简化了管理人员的工作量。
- 托管应用：呼叫中心的应用比较简单的话，甚至都可以不用虚拟桌面，而只需要采用托管应用的方式在服务器上运行座席软件，每个客服务人员通过瘦客户机使用服务器上的托管应用就可以了。

集中管理的虚拟化桌面或者托管应用可以大大提高每个座席的可靠性，避免由于客服人员随意安装软件而造成的各种问题，即使发生问题也可以很快地排错。

物联网解决方案

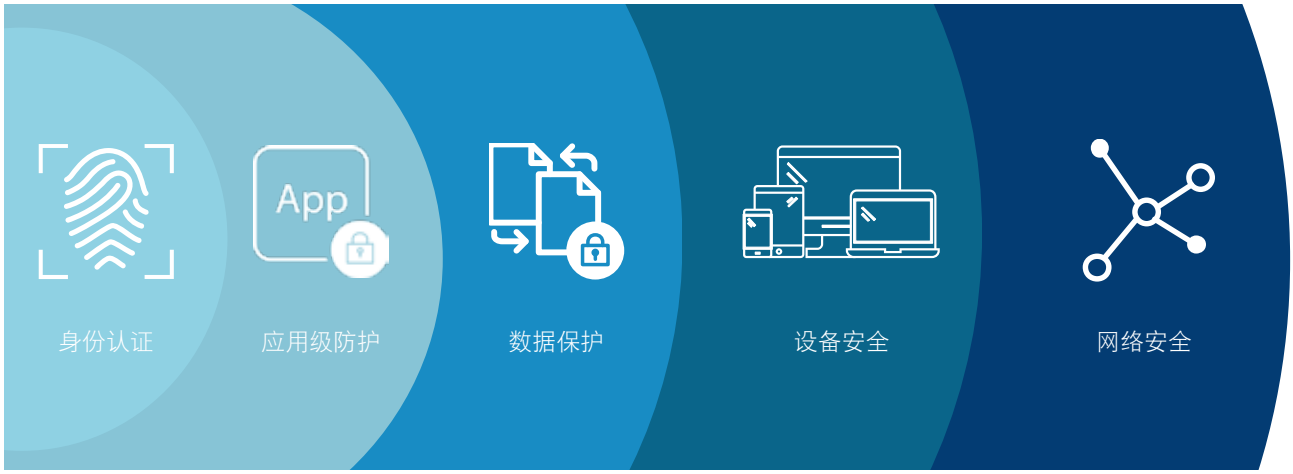
随着物联网技术在全球范围的广泛应用，“物联网+金融”这一新业态也应运而生。将传感器、数据采集等物联网技术应用到金融领域，增强信息的真实性，从而建立更为客观的信用体系。金融企业基于物联网技术开发出了物联网动产融资、物联网仓单、物联网新金融等新业务，实现了银行信用体系的变革，帮助金融企业更好地防范经营风险、提升管理效能和改善客户体验。

VMware 针对物联网也有完整的解决方案，如企业级物联网基础架构管理管理解决方案平台 Pulse IoT Center，可支持IT与运营技术团队全面管控物联网基础架构与设备。Pulse IoT Center将为客户带来以下强大功能：

- 管理更全面：简化互联“物件”的管理复杂度。
- 运行更智能：准确而实时地掌握“物件”的健康状况，并能够防患于未然。
- 保护更完善：确保整个物联网基础架构的设备、边缘、网络与应用的安全。
- 创新更快速：优化与加速物联网的部署与扩展。

企业安全转型

2017 年中的比特币敲诈病毒让很多办公电脑和 ATM 机陷于瘫痪，这次病毒攻击事件又一次敲响了信息安全的警钟，让我们认识到网络信息安全不能有任何松懈。金融企业因为其经营业务的特殊性尤其需要重视信息安全，VMware 从客户端到数据中心提供了全套的安全解决方案，帮助金融企业进行安全转型。



移动设备安全

移动设备用于办公，其管理难度比传统的个人电脑更大，因为设备的移动特性，存在易丢失、易损坏的情况；另一方面，允许员工自带设备，也给企业安全带来了新的挑战，比起统一的企业配发设备，更难控制自带设备上安装的软件，有些设备还被破解了，更容易受到恶意软件的入侵。

Workspace ONE 提供了全面的安全手段来保护移动设备上应用和数据的安全。

应用安全容器

Workspace ONE 为企业应用提供了安全沙箱，把企业空间和员工私人空间隔离开来。企业应用 App 都是在一个安全容器中运行，不会受到恶意软件的攻击和影响。哪怕移动设备中了病毒，企业应用还是可以安全运行，不会受到病毒的感染。

基于合规性检查的条件访问

Workspace ONE 在允许员工访问设备或启动应用之前，都会进行合规性检查，确保安全之后才会允许员工使用某项功能。管理员可以制定各种安全策略，来详细设定设备必须满足的一组规定，主要包括以下两大类：

- 设备合规性：规定设备上的软硬件配置必须满足的一组条件，例如操作系统必须在一定的版本之上，低版本的往往有安全漏洞或者不能支持某些应用；移动设备不允许破解，破解的设备失去了操作系统级的保护，容易受到恶意代码的利用和攻击。
- 身份合规性：规定访问设备的用户必须满足的一组条件，如身份验证的强度，是否强制要求多因素身份验证，用户能否访问某个特定的应用等等。

Workspace ONE 会针对管理员设定的安全规则来进行检查，当检查的结果显示不合规时，就会发邮件通知管理员，并且提示用户修改设备配置（如升级操作系统版本）来满足合规要求，在某些特定的条件下（如设备已被破解并且检测到恶意软件）甚至可以执行删除操作，把所有的企业应用和数据从设备上擦除掉。

数据防丢失 DLP (Data Loss Prevention)

移动设备体积较小，又是在移动中办公，容易发生设备丢失、被窃等现象。一旦这种情况发生，只要是设备在 Workspace ONE 中注册过的，每个用户都可以登录进自服务门户，远程定位设备，尽量找回设备；或者是对设备进行远程数据擦除，最大限度地保护企业数据安全。

网络传输安全

另外一个重要环节就是网络传输，Workspace ONE 提供了应用级（Per-App）VPN 来灵活保护数据安全。

应用级 VPN

Workspace ONE 可以让移动应用跟后台数据中心建立起应用级（Per-App）VPN，即建立的 VPN 通道仅供当前的企业应用使用，所有其他的应用都无法访问该加密通道。这种方式可以大大提高数据通讯的安全性，杜绝了其他无关应用（甚至是恶意软件）通过 VPN 通道访问企业数据中心的可能。

集成 NSX 提供端到端的保护

建议在数据中心内部署 VMware 的网络虚拟化产品 NSX，还可以进一步提高网络传输安全性。通过 Workspace ONE 与 NSX 的集成，建立从单个应用到对应服务器的 VPN 微分段连接，应用只能访问它对应的后台服务器，而不能访问数据中心内任何其他的资源。这是利用 NSX 独有的微分段技术而建立的真正端到端的安全通道，具有最高的安全性。

数据中心安全

安全合规

为了加强 vSphere 操作系统的安全性，VMware 专门制定了《vSphere 硬化指南》，规定了 vSphere 安装之后需要的一些配置工作，例如关闭某些不用的端口、修改默认的登录密码、禁止从控制台登录等，以使 vSphere 具有最大的安全性 (足够硬化以抵御恶意攻击)。VMware 运维工具 vRealize Operations 会检查服务器上安装的 vSphere 是否符合这些硬化规定，把系统违规的风险显示在管理员仪表板上，提示管理员及时改正这些问题，以提高系统的安全程度。

针对支付卡行业标准 PCI DSS (The Payment Card Industry Data Security Standard)，VMware 专门定义了相应的验证设计架构 (Validated Design) 来为用户搭建合规的软件定义数据中心提供指南。该验证设计定义了数据中心物理硬件层、虚拟化层和云平台管理层的详细架构和管理指南，符合该验证设计的数据中心，可以满足 PCI DSS 标准对于数据中心的以下需求：

- 目标：构建和维护安全的网络系统；

  需求1：安装和维护防火墙配置以保护持卡人数据。

- 目标：定期监控和测试网络；

  需求10：跟踪和监控对于网络资源和持卡人数据的访问。

数据安全

对于存储在硬盘上的数据，VMware 提供了高可靠的加密功能，vSphere 和vSAN 都采用对称加密算法 AES 来对存储数据进行加密。VMware 的加密是针对底层的所有数据的，即使硬盘被窃，也无法从硬盘上破解出原始数据来。加密密钥来自于用户自购的第三方密钥管理系统，支持任何符合 KMIP (Key Management Interoperability Protocol) 标准的 KMS 系统。

VMware 提供的加密是通过软件方式实现的，利用了 CPU 的 AES-NI (Advanced Encryption Standard - New Instruction) 指令集来进行硬件加速，所以不用担心对于性能的影响。基于软件的加密技术也降低了用户的安全防护成本，用户不再需要购买支持加密的 Raid 控制器、或是自加密 SED 硬盘 (Self Envrypting Drive) 来实现加密功能，这些带加密功能的硬件都比较昂贵。

网络安全

防火墙是数据中心网络常用的安全措施，传统的防火墙一般都部署在数据中心的网络出口，以隔离数据中心的内部和外部网络，防止来自外部的网络攻击。利用 NSX 实现网络虚拟化之后，可以部署分布式的防火墙。传统的边界防火墙只能监控南北流量，而基于软件的分布式防火墙每个虚机都有一个，从而可以实现东西流量的监控。通过分布式防火墙可以实现服务器的隔离，这称之为微分段，不同部门的虚机可以被划分在独立的微分段中。NSX 分布式防火墙可以实现非常灵活的安全策略配置，大大简化了数据中心网络的安全管理。

金融企业一般都有两张网络，一张是包含核心业务系统的生产网络，另一张是办公网络，为了保证生产系统的安全运行，很多企业都有双网隔离的业务需求，VMware 专门提供了双网隔离的解决方案。传统的双网隔离方案一般采用基于硬件的解决方案，例 如采用两台办公电脑，一台连接生产网络，用于生产系统的管理监控；另一台连接办公网络，以完成日常工作的各种需要。利用 Horizon 的虚拟桌面方案可以减少物理 PC 的数量，用户只需要从同一台瘦客户机上分别访问内外网中的虚拟桌面，就可以很好的满足双网隔离的需求；同时也节省了两台 PC 的费用，用户的办公桌面也变得整洁多了。

应用安全

对于运行在虚拟服务器中的应用，VMware 也提供了一套保护措施。AppDefense 是内嵌在 vSphere 操作系统中的一个安全模块，它能够检测虚机运行的状态，并且跟以前记录的虚机运行正常状态进行比对。当虚机被恶意攻击时，AppDefense 就会及时发这一现异常现象，从而及时采取告警、强制修复等各种响应措施。

AppDefense 是运行于 vSphere Hypervisor 中的，所以它不需要安装任何代理软件到虚拟机， 自身也不会受到恶意软件的攻击，这是 AppDefense 跟基他 EDR (Endpoint Detection and Response) 软件最大的不同点。

更新日期：2017年8月2日

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：+86-10-59934200
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：+86-21-80249200
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