

桌面云技术与产业白皮书

(2023 年)

二〇二三年 九月二十二日发布

版权声明

本白皮书版权属于深信服科技股份有限公司。未经许可，任何单位及个人不得以任何方式或理由对本报告内容进行使用、复制、修改或与其它产品捆绑使用。

转载、摘编或引用本报告内容和观点应注明“来源：深信服《桌面云技术与产业白皮书（2023 年）》”

本白皮书所涉及的部分内容来源于业内厂商、系统集成商、渠道以及客户和市场公开数据。由于收集方法本身的局限性，白皮书内容与市场真实可能存在误差。

本白皮书版权属于深信服科技股份有限公司，并受法律保护，凡侵犯版权等知识产权的，将依法追究其法律责任。

参编单位和人员

编写单位：深信服科技股份有限公司

参编单位：（排名按首字母先后顺序）

北京华夏威科软件技术有限公司

飞腾信息技术有限公司

广州云岫信息科技有限公司

海光信息技术股份有限公司

麒麟软件有限公司

深圳市连用科技有限公司

上海泛云信息科技有限公司

统信软件技术有限公司

AMD

Intel

NVIDIA

主要参编人员：

王 超 于志邦 李小龙 陈 旭 王保华

郑臣明 郭宇鹰 王 迪 高锦焱 尚 超

目录

目录	III
一、 桌面云概述	6
1.1. 桌面云定义及部署模式	6
1.1.1. 桌面云定义	6
1.1.2. 桌面云部署模式	6
1.2. 桌面云相关技术架构分类	7
1.2.1. VDI 虚拟桌面基础架构	7
1.2.2. IDV 智能桌面虚拟化	9
1.2.3. VOI 虚拟操作系统架构	10
1.2.4. TCI 透明终端架构	10
1.2.5. RDS 远程桌面服务	12
1.3. 桌面云的业务价值	13
1.4. 桌面云市场发展现状及趋势	13
1.4.1. 国外市场发展现状及趋势	13
1.4.2. 国内市场发展现状及趋势	14
二、 桌面云关键组件及核心技术分析	17
2.1. 桌面云关键组件	17
2.1.1. 接入终端	17
2.1.2. 接入管理平台	18
2.1.3. 云桌面资源池	18
2.1.4. 传输协议	18
2.2. 桌面云核心技术分析	18
2.2.1. 桌面云传输协议	18
2.2.2. 桌面云可靠性技术	22
2.2.3. 桌面云安全技术	24
2.2.4. 深信服自主研发掌握核心技术	28
三、 桌面云产业发展趋势分析	33
3.1. 混合办公成为新常态，桌面即服务成为未来发展趋势	33
3.2. 基于零信任架构的数字化工作空间应用广泛，平衡安全与生产力	36
3.3. 利用 AI 赋能桌面云，更加智能化	38
3.4. GPU 深度应用将成为桌面云计算密集场景专用方案	41
3.5. 超融合架构将开辟桌面云发展的新天地	41
3.6. 桌面云将覆盖更广泛的物联网终端	42
3.7. 内生安全	43
3.8. 满足信创要求	44
四、 生态整合解决方案	46
4.1. 华夏威科 AuditSys 用户实体行为分析系统解决方案	46

4.1.1. 应用背景	46
4.1.2. 解决方案	48
4.1.3. 方案价值	50
4.2. 飞腾从端到云全栈云桌面解决方案.....	51
4.2.1. 应用背景	51
4.2.2. 解决方案	52
4.2.3. 方案价值	53
4.3. 云岫科技多云融合完全解决方案.....	53
4.3.1. 应用背景	53
4.3.2. 解决方案	55
4.3.3. 方案价值	62
4.4. 海光桌面虚拟化解决方案.....	64
4.4.1. 应用背景	64
4.4.2. 解决方案	64
4.4.3. 方案价值	67
4.5. 麒麟软件银河麒麟操作系统桌面云解决方案.....	67
4.5.1. 应用背景	67
4.5.2. 解决方案	68
4.5.3. 方案价值	70
4.6. 连用科技内容安全协同解决方案.....	71
4.6.1. 应用背景	71
4.6.2. 解决方案	71
4.6.3. 方案价值	74
4.7. 泛云科技 SIMCLOUD 研发云解决方案.....	75
4.7.1. 应用背景	75
4.7.2. 解决方案	76
4.7.3. 方案价值	78
4.8. 统信软件统信 UOS 解决方案.....	79
4.8.1. 应用背景	79
4.8.2. 解决方案产品概述	80
4.8.3. 产品特性	81
4.9. AMD 桌面云 vGPU 解决方案	82
4.9.1. 应用背景	82
4.9.2. 解决方案	83
4.9.3. 方案价值	83
4.10. INTEL 超能云终端解决方案	84
4.10.1. 应用背景	84
4.10.2. 解决方案	84
4.10.3. 方案价值	85
4.11. NVIDIA 桌面云 vGPU 解决方案.....	86
4.11.1. 应用背景	86
4.11.2. 解决方案	87
4.11.3. 方案价值	88
五. 桌面云典型应用场景	89

5.1. 政府领域应用场景分析.....	89
5.1.1. 政府领域背景	89
5.1.2. 面临的问题	89
5.1.3. 解决方案	90
5.2. 金融领域应用场景分析.....	90
5.2.1. 金融领域背景	90
5.2.2. 面临的问题	91
5.2.3. 解决方案	91
5.3. 企业芯片领域应用场景分析.....	92
5.3.1. 芯片领域背景	92
5.3.2. 面临的问题	92
5.3.3. 解决方案	92
5.4. 教育领域应用场景分析.....	94
5.4.1. 教育领域背景	94
5.4.2. 面临的问题	94
5.4.3. 解决方案	95
5.5. 医疗领域应用场景分析.....	95
5.5.1. 医疗领域背景	95
5.5.2. 面临的问题	95
5.5.3. 解决方案	96
六. 参考文献.....	98

一.桌面云概述

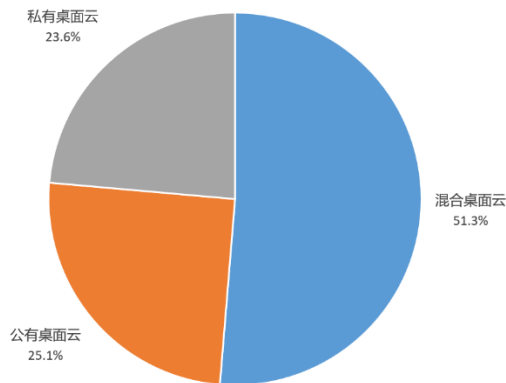
1.1. 桌面云定义及部署模式

1.1.1. 桌面云定义

桌面云是一种通过网络将可伸缩、弹性的共享物理或虚拟资源池按需供应和交付桌面的云服务模式，通过将用户的桌面环境和应用程序从本地设备转移到云端服务器，实现了桌面的远程访问和管理。用户可以通过任何设备（如瘦客户机、个人电脑、笔记本电脑、平板电脑和智能手机）连接到云端桌面，享受高度灵活性和便捷性。

1.1.2. 桌面云部署模式

按照部署方式划分，桌面云可分为私有桌面云、公有桌面云以及混合桌面云，混合桌面云凭借其更强大的兼容适配能力，可以服务于更多的行业领域以及应用场景，更被市场接受，2021年中国桌面云市场中，混合桌面云、公有桌面云与私有桌面云市场占比约为2:1:1，未来几年，随着中国混合云市场的不断扩大，随着企业云基础设施部署的不断深化，多云环境管理手段和方式不断优化，桌面云市场中混合桌面云部署比例会不断加大，未来将成为桌面云解决方案的主流部署形式。



数据来:CCW Research,2022/02

图 1-1 2021 年中国桌面云市场各部署模式占比

常见VDI用例有：

远程/混合办公：由于VDI使虚拟桌面易于从集中位置进行部署和更新，因此越来越多的公司正在实施 VDI 来支持远程工作人员和混合工作场所。

自带设备（BYOD）：VDI 是允许或要求员工和外包商使用自己的设备的环境的理想解决方案。由于计算处理是在集中式服务器上完成的，因此 VDI 允许使用更广泛的设备，

例如瘦客户端、平板电脑甚至智能手机。它还提供了更好的风险缓解，因为数据位于服务器上，不会保留在最终客户端设备上。

任务或轮班工作： 非持久性 VDI 是一种无状态虚拟机映像，或者通过使用虚拟应用方式，特别适合呼叫中心等组织，这些组织有许多员工使用相同的软件来执行有限的任务，并且不需要访问过多的应用程序。

1.2. 桌面云相关技术架构分类

云桌面技术作为云计算虚拟化技术的一种方式，因与传统PC相比的巨大优势，越来越受到广泛关注。得益于其具有的灵活性、安全性等特点大大的简化了运维人员对于终端设备的运维工作，同时也让用户可以不在局限于设备、地点、时间，随时随地都可以通过网络访问自己的桌面系统了。因此越来越多的企业、政府、学校等机构开始应用桌面虚拟化，以提升办公效率，降低运营成本。

在云计算持续发展背景下，桌面虚拟化相关技术提供商不断涌现，桌面虚拟化主要有两类架构，一类是主流的在服务器端进行集中计算的桌面云技术架构VDI（Virtual Desktop Infrastructure），即虚拟桌面基础架构；另一类是在用户端进行分布式计算的技术架构，有IDV（Intelligent Desktop Virtualization，智能桌面虚拟化）、TCI（Transparent Client Infrastructure，透明终端架构）、VOI（Virtual OS Infrastructure，虚拟操作系统架构）等架构。还有一种被用来远程访问桌面的架构服务RDS（远程桌面服务），其中VDI、IDV、TCI、VOI为主流交付架构。

1.2.1. VDI 虚拟桌面基础架构

VDI 是将终端的操作系统集中部署在数据中心的服务器上运行，将用户的桌面进行虚拟化。用户通过来自客户端设备（PC或瘦终端）的远程连接协议与虚拟桌面进行连接，用户访问它们的桌面就像使用传统本地安装的桌面操作系统一样。VDI的特点是由后端服务器硬件承载用户桌面的操作系统运行（VDI还有一种方式是可以直接托管物理PC上的操作系统），用户终端设备通过经过优化过的网络连接协议，访问运行在数据中心后台的用户桌面，进行图形图像的显示输出与用户信息的指令输入，从而实现集中运行、集中管控。

VDI虚拟桌面架构是一种“集中运算、集中存储”的桌面云架构。运行模式非常类似家里的电视机顶盒，所有的影视内容都在电视台，机顶盒只是用于显示电视台的传过来的图像。VDI的后台架构就像一个大衣柜（服务器）通过挡板（虚拟化管理程序Hypervisor）分出了很多小格子一样(虚拟化成多个虚拟机)，每个用户的桌面都是一个小格子，用户可根据自己的需求在小格子中存放不同的物品（安装不同需求的操作系统和软件）。

软硬件解耦合的架构，所有系统与应用程序运行、数据存储都始终在后台，终端只用于

显示服务器端发送过来的画面，使得对终端设备的依赖性大大降低，可以支持任意的终端设备访问，如瘦终端、传统PC、笔记本、智能手机、平板电脑等。

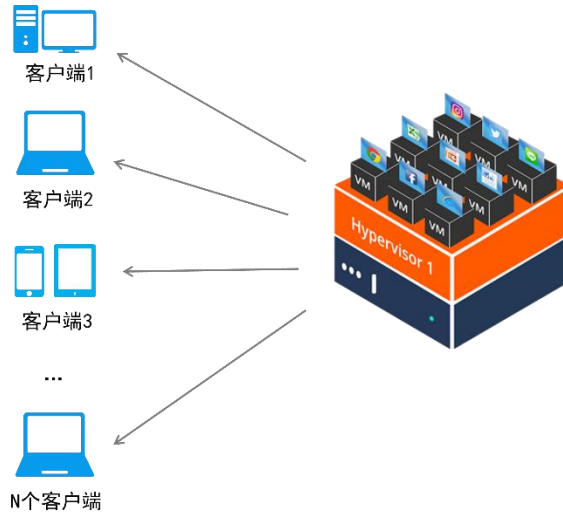


图 1-2 VDI 客户端通过远程协议于桌面云进行连接

VDI模式下，每个用户是一个独立的操作系统虚拟机，在逻辑上完全隔离。桌面的运行与数据存储都在后台，用户不直接接触数据，具备天生的安全性。用户所有的操作都是通过网络将键盘鼠标指令传递到后台，后台服务器再通过网络反馈图像的变化。

整个网络的传输就像一个大水管一样，为了方便用户在使用VDI的时候也能够像本地PC一样方便的使用USB外设、打印机，音频等，在大水管中（桌面云传输协议）还划分了很多小的管道，每个小管道可以单独传输不同的内容，如专门用于连接本地USB设备的管道，音频管道，图像管道，键鼠管道等。有管道就有开关，管理员可以灵活的设置管道的开和关来实现用户的访问安全控制，如部分用户在内网可以使用USB设备但在外网不能使用，部分用户无论在什么位置都不能使用USB等。



图 1-3 VDI 网络传输协议各个传输通道

VDI在资源按需分配、移动设备访问、集中管理控制、服务器架构设计、数据安全性、管理维护等方面都具有很大优势。它的劣势表现为：依赖网络环境，断网后就无法连接云桌面；同时集中存储运算的特点决定了需要配置高性能的服务器，前期投资成本较高。

VDI 桌面云的架构优势：

安全性高：VDI架构由于本身就具有数据不落地的特性，再加上有多套安全管控机制，

例如多副本技术，容灾技术，策略管控等，都可以有效的保障用户和系统数据安全。

资源利用率高：由于底层是采用虚拟化的技术，通过多台服务器集群组成虚拟化资源池，充分的利用了后端的服务器资源。

运维能力强：由于资源和桌面集中管理，整体的运维难度大大降低，运维效率远高于传统PC。

移动性强：VDI桌面只传输图像，不受地域和空间的限制，只需网络连通便可支持电脑、平板、手机等智能移动终端接入。

1.2.2. IDV 智能桌面虚拟化

IDV是“集中存储、分布式运算”的技术架构，用户的虚拟镜像在服务器统一存储和管理，但是虚拟桌面的运行位置是在用户的终端设备上。后端服务器会将镜像通过网络下发到用户的终端上，由用户的终端直接运行该虚拟桌面镜像，虚拟桌面镜像在运行过程中不对网络形成过度依赖，因此支持离线运行。

举例来说，如果把VDI比作在线视频(优酷、爱奇艺)的话，那么IDV就是本地视频(MP4、RMVB、MKV)，好比管理员在某资源网站上分门别类上传了很多的视频文件(在服务器上创建出多个不同的虚拟机操作系统模板)，小伙伴直接从网站上根据需求下载视频文件到本地，然后在本地安装播放器软件进行播放(在客户端安装虚拟化Hypervisor，然后根据需要把服务器上的虚拟机加载到客户端本地使用)。使用IDV虚拟桌面过程中，产生的个人数据可使用镜像同步或网盘方式同步到服务器端，实现数据的集中存储。IDV本质上属于终端管理的一种形式。

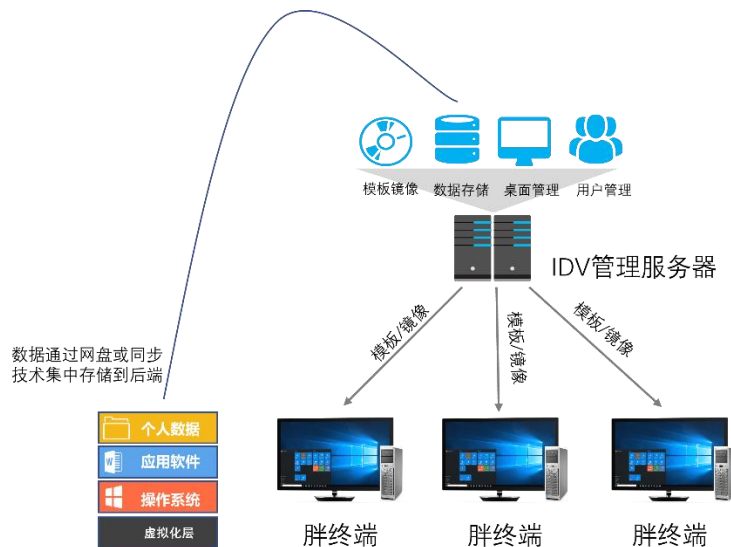


图1-4 IDV智能桌面虚拟化架构

IDV桌面架构优势：

接近本地物理PC体验：IDV的桌面使用体验接近于本地物理PC的使用体验，性能取决于本地终端的配置，外设兼容性表现优秀，不受网络波动影响。

不依赖网络：IDV采用的是本地虚拟化技术，数据存放在本地终端设备上，不依赖网络，支持本地离线访问。

成本较低：IDV的成本主要来自于终端设备的采购，相对于其他架构的桌面云，IDV的成本较低。

1.2.3. VOI 虚拟操作系统架构

VOI是“集中存储、分布式运算”的技术架构，在服务端集中存储用户的桌面云镜像，在用户终端运行虚拟机操作系统和桌面应用，与IDV不同之处在于抛弃了硬件虚拟化层，而采用类似无盘工作站的方式启动客户端系统，让桌面完全运行在本地物理机只上，支持离线运行，支持桌面系统集中安全管理，桌面性能完全保持传统PC的体验，对服务器计算资源占用少。VOI与IDV一样，不支持移动办公和多桌面灵活切换办公，同时不支持计算资源弹性扩容，数据在本地终端落地会导致数据安全隐患；与IDV不同的是，终端没有虚拟化层，兼容性更好，终端的性能也没有损耗。VOI本质上也是属于终端管理的一种形式。

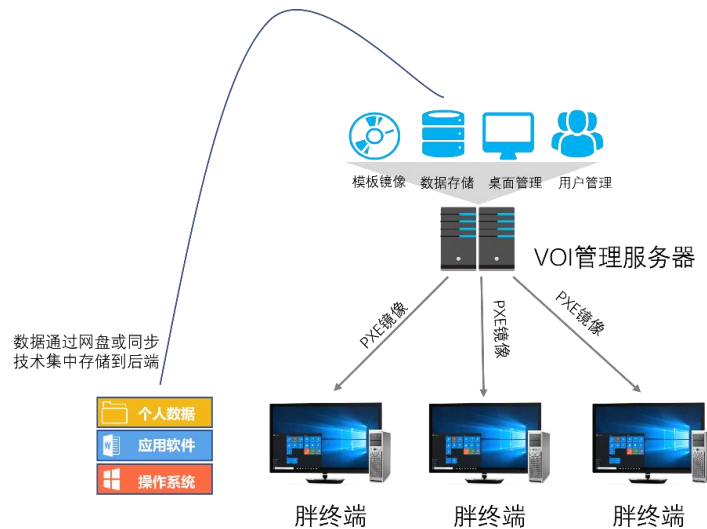


图1-5 VOI虚拟操作系统架构

1.2.4. TCI 透明终端架构

与IDV一样，TCI也是“集中存储、分布式运算”的技术架构，是由Intel提出的一种云终端架构，称之为“透明终端架构”，与IDV需要在本地运行虚拟化软件不同，TCI是一种非虚拟化的软件解决方案。它基于固件，旨在解决云终端规模化部署与使用中可能出现的性能损耗、集中管理、系统个性化、安全性和可靠性等问题。

相对于IDV的虚拟化技术而言，TCI没有虚拟化层，是一种基于固件层（所谓固件就是直接嵌入在硬件上的软件，我们常用的BIOS也是一种固件）的技术，所以TCI中透明的意思就是用户感受不到软件底层的架构变化，可实现账户随人而动的计算环境迁移，而无需依赖于固定的终端硬件。同时它还具有出色的外设兼容性，可以兼容普通PC上的所有外设。

TCI以虚拟磁盘镜像的方式管理客户端的软件系统，使得每个用户的软件环境仅与自己的个人账户关联，而不依赖于特定的硬件，改变了传统PC面向硬件的软件管理模式。终端用户的系统软件均通过后端统一管理，用户只需透明使用自己的业务软件，而无需关心系统软件（如操作系统）的日常维护。TCI设计中一个点是要尽量降低计算中的网络依赖性，由本地镜像缓存和差分文件共同构成可离线工作的计算环境。这一点在实际场景部署中是得到很多行业客户认同的功能点。

通俗一点讲，我们可以把TCI服务器当作一个共享猫舍，每个用户可以从猫舍中领养一只猫（桌面系统），猫的领养方式有两种，猫领养后，这只猫就专属于该用户（桌面分配），用户可以把猫领到家中养两天（系统加载到本地运行），用户无需为了养猫专门在家中建猫舍（虚拟化），直接在自己小屋里养就行（裸机运行）。当自己要出差时，可以把猫再寄存回猫舍（桌面变化数据回传到服务器），出差回来后，还可以继续从猫舍将猫再接回来（系统再次加载）。

TCI解决方案结合了IDV的优势同时屏蔽了IDV的缺点，去掉了虚拟化层，通过终端内置的硬件固件进行集中管理，客户端开机后直接基于裸机固件连接服务器获取操作系统镜像引导启动，操作系统直接运行在终端设备上，无虚拟化层的架构，对终端性能零损耗。

TCI解决方案，通过端到端的部署，在本地计算，集中管理、外设兼容性和账户个性化配置方面具有强大优势。TCI架构拥有账户导向型用户体验，可以做到高速批量操作系统部署、应用分发和用户数据保存，拥有离线连续计算、强大本地计算性能、I/O设备/软件全兼容、集中镜像与数据管理等多种卓越特性。

在数据保存方面，TCI服务器端可以保存所有用户的完整桌面数据，当用户使用时，桌面数据自动加载到本地终端使用，使用完毕后，自动上传到服务器端。同时，还支持用户的漫游使用，当用户更换位置使用其他终端时，只要登录个人账户，即可自动加载个人桌面数据到本地。

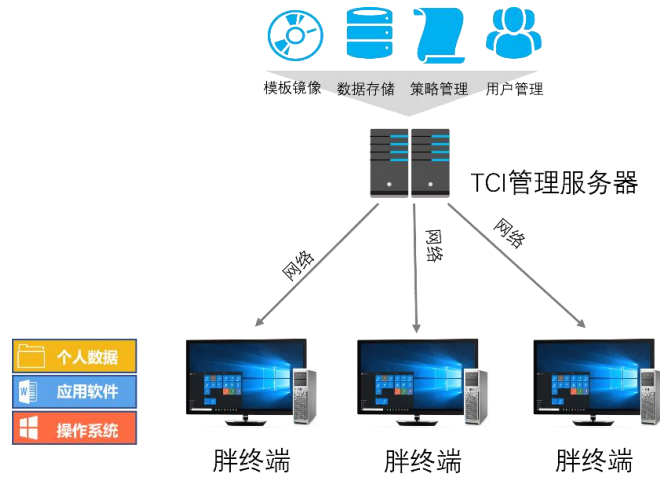


图1-6 TCI透明终端架构

1.2.5. RDS 远程桌面服务

RDS (Remote Desktop Services) 是基于Windows操作系统RDP的升级版，通过在一个Windows操作系统上创建多个用户帐号来使用，属于云桌面技术。其原理是基于多用户操作系统，在已安装了操作系统的服务器上安装共享云桌面的管理软件，再批量创建用户，然后通过传输协议发送到各个客户端上。

RDS远程桌面架构与VDI虚拟桌面架构同属于云桌面架构，均支持数据安全不落地、使用任意设备随时随地访问。

如果把普通VDI虚拟桌面比作一个专属私家车的话，RDS就是一辆公交车，所有用户的座位彼此隔离（会话间隔离），但共享同一辆公交车的基础空间（操作系统），个性化程度较低（不能自己安装应用程序）。

RDS远程桌面架构不一定非要虚拟化，可以是物理机直接部署Windows Server供用户访问。RDS通常被各厂家隶属到VDI产品中，作为VDI的一种桌面类型，称之为“共享桌面”。

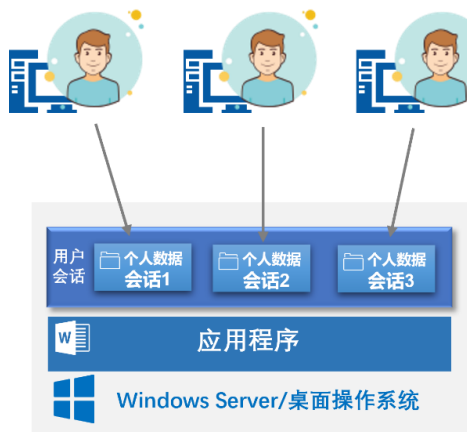


图1-7 RDS远程桌面服务架构

架构总结说明

通过以上的分析，我们不难发现，不同的技术架构有自己不同的特点和局限，适用的应用场景也各有不同，但是单一的云桌面技术架构只能解决企业一部分算力资源闲置、数据安全、移动办公应用等问题，但多数客户业务场景复杂多变。要实现桌面全云化，单一云桌面技术架构无法满足业务应用的需求。值得注意的是，为了解决用户复杂环节下的虚拟化应用，融合VDI、IDV、VOI、TCI多种架构的融合架构已经出现。

1.3. 桌面云的业务价值

灵活性和便利性：桌面云业务使用户可以随时随地通过网络访问自己的桌面环境，无论使用何种设备（如个人电脑、笔记本电脑、平板电脑或智能手机），都可以获得一致的工作环境和应用程序。用户可以在不同设备之间无缝切换，提高工作效率和灵活性。

安全性和数据保护：桌面云业务将用户的桌面环境和数据存储在云端服务器上，可以通过访问控制等安全措施来保护用户的数据安全。相比传统的本地存储方式，桌面云业务可以提供更高的安全性和数据保护，减少数据丢失和泄露的风险。桌面云可以为用户提供全方位的桌面安全防护，包括外设安全接入、网络带宽控制、应用黑白名单、屏幕水印和录屏、操作日志留存、数据不落地等安全措施。

成本效益：由于计算处理是在服务器上集中完成的，因此对终端设备的硬件要求不那么严格。用户可以从旧设备、瘦客户端甚至平板电脑访问其虚拟桌面，从而减少了 IT 购买新的昂贵硬件的需要。桌面云业务还可以降低维护成本，用户也无需担心桌面环境的维护和升级，节省了用户的时间和精力。

资源共享和协作：桌面云业务可以实现资源的共享和协作。多个用户可以同时访问和使用同一台云端服务器上的桌面环境，实现文件共享、协同办公和远程协作。这种方式可以提高团队的工作效率和协作能力，促进信息的共享和交流。

可扩展性和灵活性：桌面云业务可以根据用户的需求进行灵活扩展和调整。用户可以根据实际需要增加或减少服务器的资源，如计算能力、存储空间和带宽等，以满足不同规模和需求的用户。

1.4. 桌面云市场发展现状及趋势

1.4.1. 国外市场发展现状及趋势

全球虚拟客户端计算市场年环比增长12.4%，在2022H1年达到34.927亿美元。俄乌冲突和通货膨胀对全球经济产生了一定的影响，桌面云软件市场在2021开始出现下降迹象，

由于全球经济衰退和通货膨胀压力，这些迹象在2022年上半年迅速加速。尽管疫情将增加虚拟客户端计算的机会，但与之相关的严重经济影响将导致中小型企业和小型企业预算相应减少。在各个方面积极影响下，大型企业可能会持续信息化建设投资，但投资的速度会有所下降。IDC预计未来将出现积极增长，市场预测2021至2026年的复合年增长率将达到12.5%，2026年将达到116亿美元。

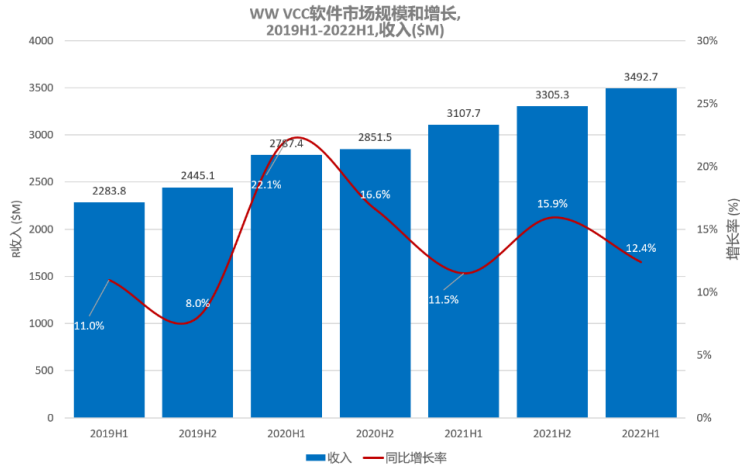
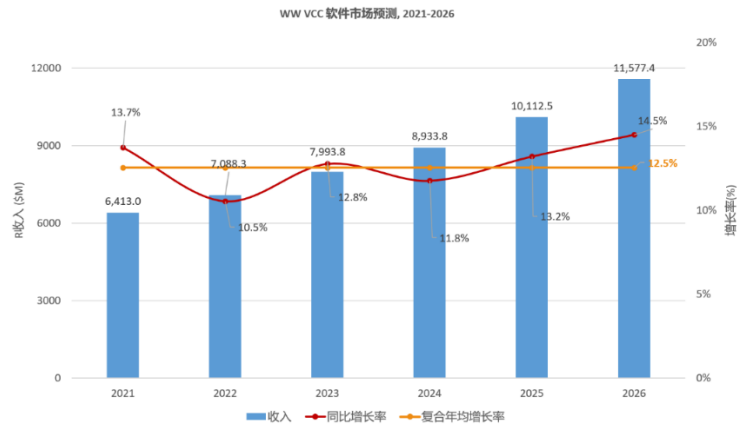


图 1-8 桌面云软件市场规模和增长，2019H1-2022H1，收入（百万美元）



数据来自 IDC, November 2022

图 1-9 桌面云软件预测，2021-2026，收入（百万美元）

在全球桌面云市场，Citrix、微软、VMware和亚马逊持续主导者虚拟客户端计算市场。市场表现出成熟市场的特征，75.1%的市场份额集中在前三名。Citrix被TIBCO收购，主要聚焦于只能数字化工作空间和SaaS产品主导的公司；由于用户对云服务的接受程度越来越高，微软和AWS的市场份额也在增加。

1.4.2. 国内市场发展现状及趋势

在国家上云政策的积极引导下，以及企业对数据安全和远程办公需求的强烈驱动下，桌面云解决方案的需求与日俱增，市面涌现出了越来越多的远程办公桌面云产品、服务和解决

方案。随着国内云计算的快速发展，桌面云产品在各场景渗透率不断提升，桌面云整体解决方案销售量增长。国内桌面云市场保持着蓬勃的增长态势。计世资讯发布的《2021-2022年中国桌面云市场发展研究报告》表明，2021年中国桌面云整体解决方案销售量达到299.4万个，较2020年增长21.7%。继续保持快速增长态势。

2022年，国内疫情的反复对整体经济产生了负面影响，导致虚拟客户端计算软件市场增速有所下滑。随着市场逐步放开，经济慢慢复苏，在2023年和2024年逐步恢复增长。

2022年，商业市场有显著增长，特别是制造业及金融垂直领域。但政府和教育受疫情影响较大，增速放缓。

Daas占比大幅提升：桌面云厂商和电信运营商在Daas上开展更深的合作，获得更多的企业客户和个人客户。国内部分公有云厂商逐步布局DaaS业务，在计算密集场景中与增强和客户更多粘性。

国外厂商和国内厂商比较：国内厂商更多聚焦信创桌面云需求满足，促使国外的厂商开发更多的商业市场及相关行业，比如医药制造、IT服务和互联网行业，涉及的有设计及研发场景相关；越来越多的国内厂商逐步开拓金融、制造、能源、电力、交通等大型企业市场。

据IDC报告，2022年中国虚拟客户端计算软件市场的市场规模达到了3.5亿美元，同比增长10.1%；未来五年（2022-2027年）该市场仍然会保持17.2%的年复合增长率，预计2027年将达到7.9亿美元的市场规模。



图1-10 中国虚拟客户端计算软件市场预测，2022-2027

桌面云行业继续保持增长态势，同时根据计世资讯调研。未来，企业上云用数赋智能能力进一步增强，企业研发、生产、销售等全流程环节开始进入数智化阶段，推动中国桌面云市场快速发展，并为企业数字化升级快速赋能。预计未来几年，中国桌面云市场销售量将以不低于20%的速度增长，到2025年，中国桌面云市场销售量将达到673.0万个。



数据来源: CCW Research, 2022/12

图 1-11 2021-2025 年中国桌面云市场销售量及增长率

二.桌面云关键组件及核心技术分析

2.1. 桌面云关键组件

桌面云整体架构由接入终端、接入管理平台、桌面云资源、桌面传输协议四部分组成，其中最为关键的技术为桌面云传输协议。见下图。

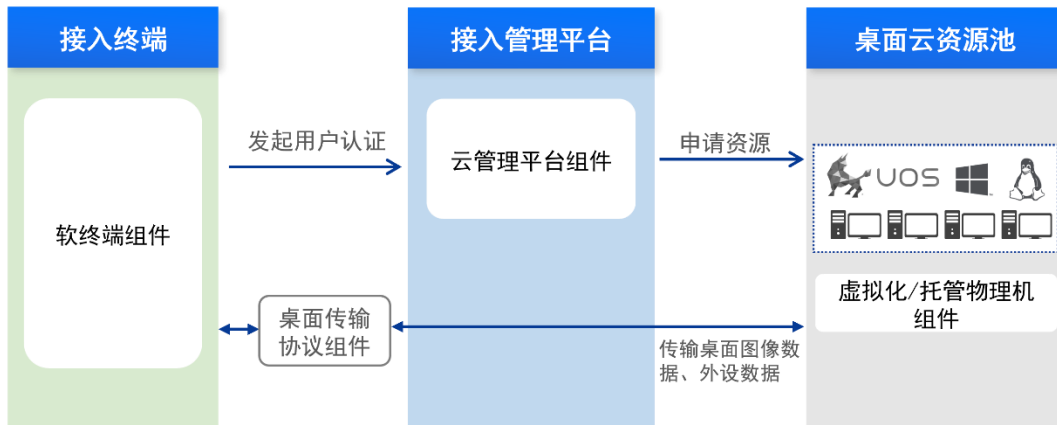


图 2-1 桌面云关键组件架构图

国内外主流桌面云厂商，在关键组件的组成上相差不大，都拥有自研的桌面云传输协议，且各厂商都基于用户使用体验与数据传输安全等方面，在桌面云传输协议上做出了独特的优化改进，建立了各自的优势。但在传输协议的优化和云端的能力上参差不齐：云端能力国外厂商普遍高于国内厂商，云端的能力跟虚拟化的技术积累有关，需要国内厂商继续投入补齐；传输协议的优化上面，国内厂商近几年基于画面传输、外设映射、弱网使用等方面，不断地追赶国外领先水平，已有所建树；接入管理上，国内的厂商在调研用户使用习惯和细化需求上，更符合国内的现状，功能性和安全性上已经有了较大优势。

终端用户使用桌面云的基本流程如下：终端用户通过接入终端发起用户认证，通过接入管理平台进行用户认证成功后，向桌面云资源池申请虚拟桌面资源，虚拟桌面资源通过桌面传输协议将虚拟桌面图像数据、外设数据传输给接入终端，同时接入终端可以将连接终端的终端数据、外设数据传递给虚拟桌面，实现数据交互，满足用户日常办公、日常研发等诉求。

2.1.1. 接入终端

接入终端属于软终端组件。桌面云的软终端组件安装在接入硬件终端或直接在终端行通过html5接入，用于用户登录认证，发起接入虚拟桌面等操作请求，进行桌面图像解码与显示。并通过底层桌面协议实现终端本地、输入输出设备与虚拟桌面之间的数据交互。用户接入设备包括瘦终端、笔记本电脑、平板电脑和智能手机等。

2.1.2. 接入管理平台

云平台管理组件用于管理用户账号，处理用户认证，并向虚拟化平台申请云桌面资源。同时可以设置安全策略、为用户创建、分配虚拟机、管理用户虚拟机，提升使用体验、保护数据。

2.1.3. 云桌面资源池

云桌面资源池整合了计算、存储、网络、GPU资源，以虚拟化技术为基础，通过远程桌面协议面向用户，交付易使用、易访问、易维护的云桌面、云应用。也可以托管物理工作站，通过远程桌面协议交付托管物理工作站方式，将整个物理工作站资源交付给用户使用。

2.1.4. 传输协议

桌面云传输协议用于接入终端与远程虚拟桌面/应用进行外设数据、图像数据交互。远程虚拟桌面/应用传送图形显示数据给终端，同时将终端输入的命令传输到远程虚拟桌面/应用。传输协议的效果是让用户感觉远程虚拟桌面上运行的桌面或应用似乎是在本地运行，保证用户体验。常见的桌面云协议如深信服HEDC、Citrix ICA/HDX、RDP、SPICE、VMware PCoIP/Blast。

2.2. 桌面云核心技术分析

2.2.1. 桌面云传输协议

桌面云传输协议是一种用于在云环境中传输桌面图像和用户输入的协议，是决定用户体验的关键技术之一。它允许用户通过云服务访问远程计算机的桌面界面，就像直接坐在本地计算机前一样。桌面云传输协议从架构上看主要分为桌面外部及桌面内部协议。

2.2.1.1. 桌面云外部协议

桌面外部协议通常指协议客户端直接连接的对象为物理主机层，而虚拟机层通过特殊的显卡驱动方式将虚拟机内的变化信息传输给物理主机层，典型的桌面外部协议如Spice、VNC等，在局域网内由于网络质量较好，通常能够获得较高质量的桌面体验。

桌面外部协议的优势是能够覆盖虚拟桌面的全生命周期的输入输出过程，能够从虚拟桌面外部对虚拟桌面进行方便的管理和维护，即使是断网，蓝屏等极端状态，亦可从容应对。

劣势是通常与主机平台“紧耦合”。

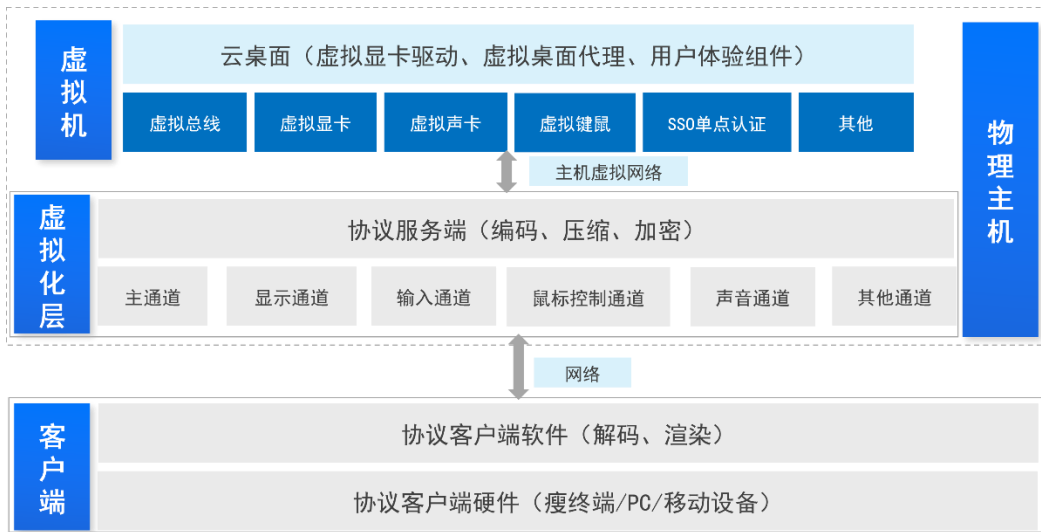


图 2-2 桌面云外部协议架构图

2.2.1.2. 桌面云内部协议

典型的桌面内部协议架构如：Citrix ICA/HDX、VMware的PCOIP、微软的RDP，优点是能够方便的跨平台，局域网表现与带内协议相当，广域网在带宽不太充裕时依然可以实现流畅操作。缺点是对虚拟机网络以及虚拟机内的操作系统依赖程度高，虚拟机网络故障或操作系统服务未就绪，桌面将无法连接，蓝屏或网络故障，将只有管理员在管理平台才能维护。此外，终端接入虚拟机之前，必须保证终端与虚拟机之间网络互通，由此可见终端与虚拟机是没有完全网络隔离的，需要通过桌面流量代理等组件规避此问题。数据安全需求较高的客户（如政府、军工、金融），终端与虚拟机隔离往往会纳入安全检查。终端与虚拟化层不隔离，会有安全性风险，如外设插入引入病毒、外网接入存在攻击风险等。

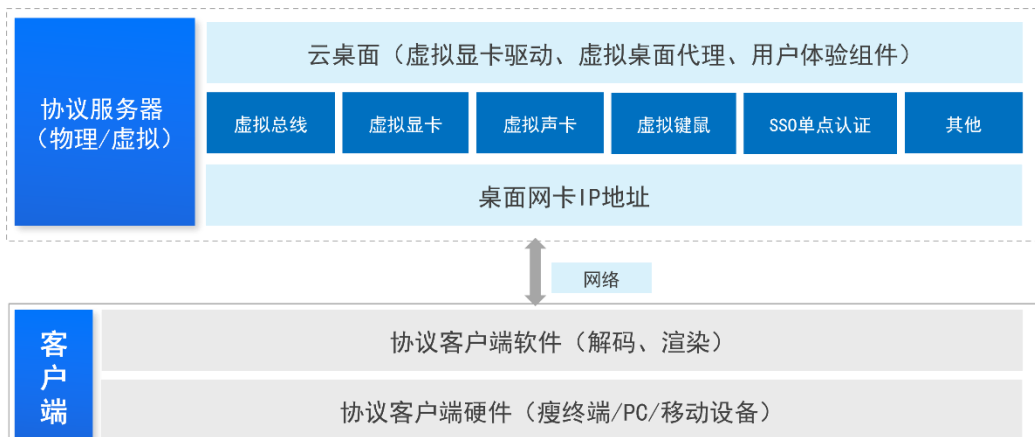


图 2-3 桌面云内部协议架构图

结合虚拟桌面内部协议和外部协议的优缺点，国内部分厂商采用了融合协议的方式，在客户端和管理平台中默认集成两种协议，在配置时，同一套用户名密码等配置信息，自动匹

配到两种协议的配置文件中,在连接时,自动探测连接网络质量,自动选择最优的连接协议,从而获得最佳的用户使用体验。

2.2.1.3. 桌面云传输协议关键优化技术

桌面传输协议成为决定桌面云用户体验的关键决定性因素之一,主要的原因在于桌面云架构路径冗长,任何一个环节的延迟、阻塞都会造成用户体验的感知。目前国内外传输协议的技术关键点有以下几方面:

(1) 传输算法优化

由于虚拟桌面传输协议的关键技术是将人机交互的界面和核心的计算分离开来,后台负责所有的计算,前端负责人机交互。如果需要把后台产生的桌面变化完整及时地反馈到前端,需要处理两个问题:一是要处理显示系统的数据传输,二是压缩解压缩处理及传输产生造成的延时问题。

首先,对于数据量大的数据传输问题,桌面云一般采用两种方法,一种方法基于增量更新画面的方法,也就是说界面刷新时只传输界面更新的部分,一般是通过客户端画面缓存机制,在桌面图像传输时,识别客户端是否有相同的缓存图像区域,如果有缓存,则认为是重复的图像,不需要传输,如果是非重复图像,则需要传输到终端,从而实现虚拟机画面增量更新的目的。另一种方法是在每一种指令集内部采用压缩的方法,在后台在对每一条指令内部选择合适的压缩方法进行压缩,经过传输,在前端先进行解码,然后再解析相应的指令,转化成相应的数据格式刷新到界面上。

其次,对于影响用户体验感知的延时问题,目前诸多厂商选择在画面质量,网络流量,压缩解压缩CPU 资源占用之间进行一个权衡折中是最主要的优化方向,画面质量可以通过降低分辨率、调整画面质量、降低画面帧率等方式,调整到可接受的最差的画面质量来实现,为了不影响正常的用户体验,还可以区分文本图像和非文本图像,针对文本图像不进行压缩,仅压缩非文本图像;网络流量尽量调整在大众可接受的最大网络流量范围上,压缩解压缩CPU负载也同样需要选择合适的压缩算法,在资源占用与压缩比之间取得最佳平衡。

(2) 协议安全优化

桌面云传输协议中安全技术是保证虚拟桌面数据传输的关键,大多数厂商都采用自研的加密算法进行协议加密,保证数据删除安全性;如果画面流量经过网关设备,还会通过网关设备进行二次加密,双重加密让桌面云数据传输的安全性进一步提高。

(3) 协议体验优化

视频优化

桌面云使用场景中,视频播放是桌面云中最基本的能力之一,桌面云视频播放有两种方式:

服务端渲染，即用虚拟机的CPU进行编解码、渲染后，发送到客户端进行显示，传的是图像，这时主要消耗的是虚拟机的CPU，如果多用户基于服务器端渲染，会造成单台主机视频播放的并发密度低；

客户端渲染，虚拟机内客户端或浏览器播放的视频文件是经过分片、压缩、打包、通过传输协议传输到客户端，利用客户端上的播放器程序进行播放，利用客户端本地的软件或硬件解码能力，完成视频的解码和播放。此时服务器端虚拟机的CPU消耗基本忽略不计，可以提高单台主机上虚拟机的视频并发密度。

音频优化

桌面云使用场景中，音频质量也极大的影响用户体验。常见的音频优化方式，服务端模拟一个音频设备给虚拟机，虚拟机直接使用标准的音频驱动即可，音频APP调用系统音频处理接口（录音、放音API），虚拟声卡设备进行交互，实现高质量、低延时的音频交互。

外设兼容性优化

在桌面云使用过程中，不同行业应用场景有不同的的外设需求，例如：金融、证券、保险、运营商、政务的营业厅通常需要对接大量的各式针式票据打印机、身份信息采集设备、密码键盘、SIM卡读写器、高拍仪、签字手写屏、评价器等外置设备，经常会碰到设备无法识别，能够识别设备但应用程序无法识别或工作或者功能不完整或效率低下等问题。通常各桌面云厂商会采用诸如：

针对驱动程序兼容性不好问题，通过优化传输协议，虚拟化底层去做外设映射，即不需改变和依赖虚拟机操作系统，保留了和PC一样的总线通道，这样可以完全消除总线和设备驱动的对接问题，不需要在虚拟机中安装专用USB设备驱动，虚拟机使用外设驱动与物理PC使用外设驱动保持一致，兼容性极大提升，让用户可以像在PC一样使用各种外设。

针对在同一台服务器中并发会话访问，且多用户使用同一型号外设时需要针对会话外设隔离问题进行定制开发会话隔离技术确保用户与设备的隔离并发访问，用户可以在终端设置外设映射到使用的某一个虚拟桌面，灵活切换外设，满足多桌面正常办公需求。

针对图像传输优化，使用云终端自身的处理能力进行图像处理，并将处理后的结果压缩后传输到服务器，如高拍仪外设，终端获取的外设数据通过终端压缩后，可在虚拟化层对摄像头数据进行解压，降低数据传输流量，提高外设使用体验。

3D应用优化

桌面云在Office办公场景能够满足绝大多数用户的需求，但是对于对图形性能要求较为苛刻的AutoCAD、3D Max类图形密集型用户，桌面云中难满足他们对图形和计算性能的需求。目前，各厂商主要的解决方案有如下技术路线：

共享GPU，基于GPU虚拟化厂商提供的共享GPU能力，将物理GPU虚拟成多份具有完整GPU功能和指令集的GPU，可满足绝大多数2D和3D图形密集型用户的需求。

GPU直通，将显卡上的单个物理核心透传给虚拟机使用，并通过远程协议使得用户可以从远程进行接入。**GPU直通方式**，将承载虚拟机的云平台的物理节点上的 GPU 显卡绑定分配给用户虚拟机，终端用户通过终端远程接入用户虚拟机，这样虚拟机就可以使用 GPU 获得 3D加速能力。

vGPU，将硬件资源切分，按需分配给虚拟机使用，能有限增强现有桌面云的图形处理能力，如支持较低版本的OpenGL和DirectX，同时保留云的特性，可实现跨主机迁移。

3D软件在桌面云中使用，其光标是服务端光标，即光标是显示在虚拟机端，通过显示通道将虚拟机画面传输到客户端渲染，显示通道中的数据量比较大，显示的效果受到服务端编码压缩、客户端解码渲染、网络延迟等因素影响，效果会有明显的延迟感，体验效果较差。因此各厂商为了优化用户体验，会进一步研究光标优化方法，大多数采用的光标优化方式是将3D软件的光标信息从服务端抓取到，信息通过光标通道传递到客户端缓存并渲染，不会受到编码解码的影响同时网络的影响也变小，此时的光标移动就会和本地光标移动同样流畅，大大增加了体验效果。

2.2.2. 桌面云可靠性技术

桌面云采用集中部署的方式，桌面云架构的可靠性是保证业务连续性的关键，桌面云可靠性技术主要分为以下几个方面：

2.2.2.1. 分布式架构设计

桌面云架构通常采用无中心化的设计，每个节点都是独立对等的工作节点，不存在单节点故障风险；集群内部平台通过算法自动选举主控节点，如果主控节点发生故障，平台会自动重新选举新的主控节点，确保集群管理能力的可用性，主控节点切换过程中，虚拟机业务、存储服务、网络服务正常运行不受影响。

2.2.2.2. 服务器数据可靠性

为了确保服务器数据的可靠性，服务器节点所有管理数据，包括网卡配置信息、相关配置信息、数据库信息、虚拟存储配置信息，通常会每天自动备份到其他节点，当某一个服务器节点故障且数据丢失的时候，可以通过重建桌面云系统，快速恢复重建系统盘数据。同时服务器主机一般采用双系统盘，系统盘数据自动同步，单出现一块数据盘故障，另一块数据盘会自动接管，采用双系统盘冗余的方式提高可靠性。

当主机硬件出现故障时，可以用新的服务器安装桌面云系统，然后采用更换主机的方式对主机进行故障迁移，虚拟存储的数据会同步到新加入的主机里面，数据自动恢复。

2.2.2.3. 虚拟机数据可靠性

为了确保虚拟机数据可靠性,各厂商一般会采用对虚拟机进行快照或备份的方式保护虚拟机数据,虚拟机出现故障后,可通过恢复快照或备份的方式恢复数据。

快照。虚拟机快照机制采用写时拷贝技术,实现对虚拟机磁盘文件的秒级操作,保证整个虚拟机快照操作可以在分钟级内完成。写时拷贝技术即在进行快照的时候,只需要对磁盘文件进行记录即可,创建一个快照记录,然后就可以继续读写磁盘,在涉及写磁盘操作时,再进行数据拷贝操作和更新操作。从而保证虚拟机快照可以在很短时间内完成,并且不影响虚拟机的数据读写操作。快照恢复则直接将磁盘数据恢复到之前的快照记录即可,这个快照恢复也可以在很短时间完成。

备份。为保证虚拟机数据备份性能与备份速度,各厂商一般会采用快速备份机制来应对,技术上采用首次全量备份+非首次增量备份+bitmap技术(bitmap的方式标记了QCOW2文件的变化的位置,也称脏数据位置,大多数厂商会采用该备份方式)实现快速备份。备份可以在本地分布式存储中进行,也可以将虚拟机数据备份到外置存储。当虚拟机出现故障后,用户可以通过虚拟机备份重建虚拟机数据,还原一个完整的虚拟机。

多副本。多副本机制是将数据保存多份的一种冗余技术,当单份数据损坏时业务不会因为无法访问数据而中断;多副本机制通过虚拟存储的副本复制模块来保证副本的一致性和副本之间的数据同步,避免多份副本数据存在差异,副本数据差异时将导致上层应用访问到不同数据影响业务结果。副本对上层业务服务是透明的,业务不感知副本的存在。虚拟机数据副本存放位置必须满足主机互斥原则,即同一数据的多个数据副本不允许存储在同一台主机上,当主机发生故障时,其他主机上仍然有数据副本可用。

2.2.2.4. 虚拟机高可用

对于外部环境故障(比如主机网线断了,所在存储不能访问等)和虚拟机操作系统故障两种情况导致的业务中断问题,一般会提供成熟可靠的虚拟机高可用机制保障业务不中断或短暂中断。

虚拟机高可用(High Availability高可用性集群),通常需要两个或者两个以上的主机节点组成集群,当启用了高可用功能的虚拟机所在节点发生意外(比如主机掉电、断网等)时,集群心跳机制侦测到后,将选择一台资源充足的节点自动重启故障虚拟机,从而实现业务的不中断或短暂中断。

2.2.2.5. 虚拟机热迁移

虚拟机热迁移(也称在线迁移)技术是指虚拟机业务几乎不中断地把虚拟机从一台物理

服务器迁移到另一台物理服务器上；设备维护时，可通过热迁移将应用迁移至另一台服务器，维护结束后再迁回来，中间应用不停机，减少计划内宕机时间；也可以通过热迁移方式实现虚拟机业务不中断地切换为高性能主机。

2.2.3. 桌面云安全技术

桌面云的出现，变革了传统办公桌面的IT安全架构。首先桌面云将桌面数据集中存储，用户终端与数据分离，用户终端无任何存储数据，实现数据不落地。其次通过云计算技术，在数据中心运行用户桌面云虚拟机，通过专用传输协议传输屏幕、鼠标、键盘、外设等信息，最终实现基于数据不落地的终端桌面环境，从根本上解决传统PC桌面数据泄露的问题。

常见的桌面云数据安全技术主要有以下几种：

2.2.3.1. 终端安全

各厂商对云终端内置的存储进行了硬件级别的加密，加密算法与硬件特征状态（硬盘序列号、网卡MAC、磁盘信息等）的唯一信息绑定，使得终端的内置存储放在其他任何一台机器上（包括其他的 PC、瘦终端），都无法引导，也无法访问该存储内置的信息。这种设计能够有效的防止客户端的数据被篡改，保证客户端本地系统的安全。

在终端入网前，可通过802.1X协议等安全认证方式，认证通过后，终端才能接入网络，防止非法的终端接入，同时可以设置接入终端的IP范围，保证终端入网的合法性与安全性。

其次还可以设置终端自定义安全检查规则，其规则有操作系统、文件、进程、注册表、登录IP、登录时间、终端识别、终端类型等相关规则，终端必须满足规则要求才能正常登录，进一步保证终端接入安全。

2.2.3.2. 认证安全

为确保用户登录桌面云认证安全，各厂商都进行了多种认证方式组合来保证认证安全，常见的认证方式有下列几种：

用户名密码认证。即管理员创建一个本地用户，然后给用户设置密码，然后在登陆页面输入用户名和密码即可完成登陆，获取桌面云资源。

证书认证。大多数厂商认证组件都内置了CA证书中心，同时企业或者事业单位可自建CA证书中心，用户可不必购买单独的CA证书认证体系，为企业减少了投入成本，采用证书认证体系保证认证安全。

USB-Key认证。采用硬件USB-Key进行认证时，当USB-Key插入终端后，终端解析USB-Key里面的证书，与证书服务器进行校验，通过证书认证体验保证认证安全。

外部认证。外部认证需要配置外部服务器，即管理平台本地不做认证校验，管理平台将用户名和密码发送到外部服务器进行认证，外部服务器校验用户名和密码，然后将认证结果返回给管理平台，常见的外部认证有AD域认证、CAS认证等方式。

硬件特征码认证。硬件特征码是根据终端的磁盘ID、MAC、SN码等硬件特性按一定的算法生成的一个序号，由于硬件特性的唯一性，使得该硬件特征码也是唯一的、不可伪造的，所以对于不同的计算机，此序号必然不同。通过将用户与硬件特征码绑定，可限制用户只能在特定设备上登录，保证认证安全。

短信认证。短信认证即管理平台短信网关会使用发送短信的方式向该用户的手机号码发送一个动态生成的随机密码，即短信验证码，登录用户必须输入该验证码，才能成功登录桌面云，访问内网资源。

动态令牌。动态令牌认证是Radius服务器的一种扩展使用，通过与Radius服务器结合并为用户配发动态令牌，通过动态令牌上的动态密码进行登录，由此增加登录的安全性。在使用动态令牌认证之前，需要添加动态令牌服务器，用来进行动态令牌的认证。

用户认证分为主认证和辅助认证，常见的主认证有用户名密码、证书、USB-key、第三方认证、，常见的辅助认证有硬件特征码、短信、动态令牌认证，主认证与辅助认证自由组合，保证用户认证安全。

2.2.3.3. 网络传输安全

为了防止桌面云数据在传输过程中被嗅探、复制、窃取、伪造、截断，桌面云传输安全从以下几个方面保障数据安全的完整性、机密性和有效性。

- 用户接入、管理员接入均采用HTTPS，传输通道采用SSL加密；
- 接入终端与虚拟机之间采用SSL加密代理模式进行数据传输；
- 桌面云组件之间通信采用专用通道进行传输，包含鉴权、加密特性。

同时为避免共用网口带来的网络性能问题与网络冗余性问题。各厂商桌面云提供业务网/管理网隔离服务，业务数据与管理数据通过不同网口传输。不仅避免了不同业务使用同一个网口可能造成的网络拥塞，也摒除了一个网口故障导致业务通信与管理通信皆中断的可能性。

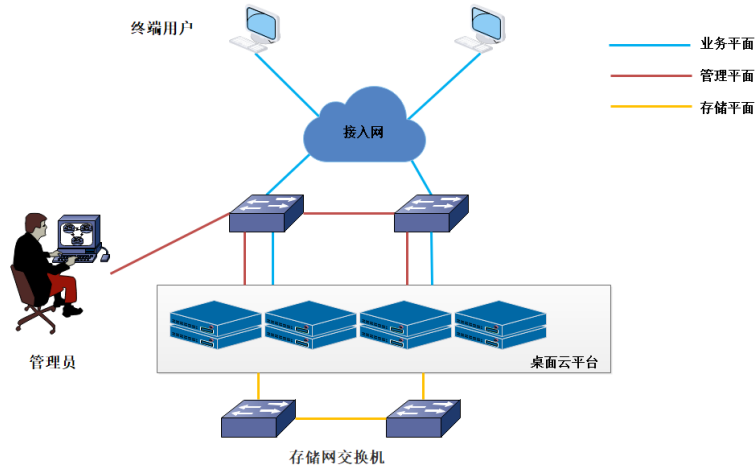


图 2-4 桌面云网络隔离示意图

•业务平面

以桌面云服务器业务通信端口作为物理传输端口，对接虚拟机虚拟机网卡的虚拟机业务数据通信平台，供虚拟机访问外部业务。

•存储平面

通过服务器分布式存储组件或对接共享存储，为虚拟机提供存储资源，存储网络原则上不直接与虚拟机通信，而通过虚拟化管理平台进行管理和连接。存储数据通过独立服务器网口进行通信。

•管理平面

承担桌面云平台管理、业务部署、平台更新等流量。该平台通过独立服务器网络进行通信，且通常与其他平面隔离。

2.2.3.4. 隔离安全

在数据中心桌面云平台内部能够提供有效的安全防护措施，主要从两方面考虑：一方面是虚拟化平台和外部之前的安全隔离；另一方面是虚拟机之间的安全防护。采用分布式防火墙提供VM到VM级细颗粒度的访问规则配置能力，对平台所有虚拟机提供东西向流量的安全防护，有效防止病毒等安全威胁横向扩散；分布式防火墙还可提供南北向流量的安全防护；可以与终端杀毒软件结合提供针对虚拟机的更好的安全防护，及时做好查杀工作；

2.2.3.5. 数据安全

为了防止桌面云数据外泄，虚拟桌面数据集中在云端服务器集群中进行管理，可以对用户设置数据外发权限，避免数据外发，导致数据泄密，同时还能够对桌面数据进行水印、防截屏、防录屏等安全保护，进一步保护桌面数据安全，常见的数据安全管控方式有如下几种。

USB权限控制。USB存储设备在桌面云端服务端通过加密策略实现根本的数据隔离，并且增加对USB存储设备底层访问的读写、只读命令控制，让攻击者无从下手，管理员可以根据不同用户的权限，设置USB存储器数据的读写权限。同时可以对其它USB设备控制是否允许映射使用。

剪切板权限控制。剪切板实现原理为剪切板映射，当开启“虚拟桌面单向拷贝至本地桌面”，则虚拟桌里面的剪切板可以映射到本地桌面，实现数据从虚拟桌面单向拷贝至本地桌面；当开启“本地桌面单向拷贝至虚拟桌面”，则本地桌里面的剪切板可以映射到虚拟桌面，实现数据从本地桌面单向拷贝至虚拟桌面；当开启“双向拷贝”，则虚拟桌面、本地桌面的剪切板会相互映射，实现数据双向拷贝。同时还能够实现剪切板内容过滤，实现逆向仅允许拷贝字符，不允许拷贝文件。管理员可以根据用户等级设置剪切板权限，保证本地PC与虚拟桌面之间的数据交互安全。

文件导出审计。由于部分用户有文件外发需求，但是用户外发的文件可能含有敏感信息，因此为了进一步规范用户文件外发行为，可以对用户外发的文件数据进行审计。通过在虚拟机内部实现驱动模块进行USB存储设备、剪切板等的访问控制，开启文件导出审计功能后，除导出审计进程以外其他所有的进程都不能向USB存储设备写数据，也不能通过剪切板向其他桌面拷贝数据，导出审计进程在导出数据到USB存储设备、本地映射磁盘的同时将导出的内容上报到审计中心进行审计，满足规范用户文件数据外发行为，同时满足事后追溯的需求。

屏幕水印。通常桌面水印分两种实现方式，客户端水印和虚拟机内部水印。客户端水印通过客户端绘图实现水印效果，而虚拟机内部水印将水印做到虚拟机里面，通过水印进程实现，但是虚拟机内部水印进程容易被用户重命名或杀掉，导致水印无法正常显示，存在安全风险，且水印进程运行在虚拟机里面，会导致虚拟机需要消耗额外的CPU资源。水印可以显示桌面云帐号、虚拟机IP、虚拟机MAC地址、虚拟机时间等信息，当用户拍照、截屏等操作，会携带用户的水印信息，对用户截图、拍照等外发桌面数据具有威慑作用，同事也可以通过水印满足事后追溯的要求。

防截屏。开启防截屏后，以及拦截可能切换顶层到窗口的命令，保证虚拟桌面窗口永远是置顶全屏显示。保证鼠标无法在本地进行操作，所以无法在本地系统通过鼠标操作截屏软件对独享桌面进行截图。同时，开启防截屏后，虚拟桌面窗口接管键盘输入，所有的键盘数据都不能传递到下层的窗口处理函数或者底层系统，这样就保证键盘消息无法传递到本地的其他应用程序，所以无法在本地系统通过键盘操作截屏软件对独享桌面进行截图，从而保证用户桌面数据安全。

防录屏。开启防录屏功能，虚拟机窗口会从底层进行保护，此功能使应用程序能够保护自己的屏幕窗口内容，不被通过一组特定的公共操作系统功能和API捕获或复制屏幕窗口，达到防录屏的效果，从而保护虚拟桌面数据。

文件流转审批。

2.2.3.6. 运维安全

为了保证桌面云运维安全，各厂商通常采用管理员分级分域的权限设置，给不同的管理员赋予不同的管理权限，从源头防止管理员越权导致数据外泄。不同的管理员可以属于不同的管理员角色，不同管理员角色拥有对不同功能的“编辑”或者“查看”权限。同时用管理区域来区分管理员可管理的虚拟机、用户、策略等资源范围，管理员在有权限的情况下，只能管理属于自己区域内的资源，有效控制管理员的管理权限。

同时管理员的操作记录、问题处理记录都记录在日志中心，可以通过日志审计和追溯管理员行为。

2.2.3.7. 行为安全

为了保证重要岗位和业务操作行为合规规范，桌面云不仅需要记录操作系统关键日志和业务日志，同时要将桌面云内所有操作行为进行全程监控，实现桌面云行为安全加固。既可以帮助企业了解涉敏岗位操作行为，用于事后审计监督，也可以防止别有用心心的员工（或外包商）等的不正当操作给企业带来安全事件和风险。行为安全主体由两个关键技术组成：行为审计和行为风险分析。

行为审计技术：用户登录桌面云后所有的操作动作自动生成日志，并形成完整的用户操作录屏画面证据链，同时录屏数据可以检索。当发生安全事件后，通过关键动作能够快速定位到责任人且完整还原当时操作画面，极大提高审计工作效率，弥补了传统依赖于有限的操作系统日志，且可视化程度不直观的特点。

行为风险分析技术：基于海量的操作行为日志自动发现高危行为，提前发现潜在的内部威胁。对于已知的潜在风险，利用安全规则在海量操作行为中发现高危风险行为；对于未知的潜在风险，利用机器学习算法，在大量的高危行为中自动发现异常行为，实现精准定位内部威胁和风险。对于业务操作风险，可以通过频次或时间异常监控，比如敏感信息查询次数分析和查询时间的监控，自动发现异常操作人员。

2.2.4. 深信服自主研发掌握核心技术

深信服桌面云（aDesk）是基于超融合架构的新型桌面模式，通过深度整合服务器虚拟化、桌面虚拟化及存储虚拟化，只需桌面云一体机和云终端两种硬件设备，即可实现云平台的快速交付，为用户提供操作体验及软硬件兼容性媲美物理PC，更安全、更高效的云桌面。

目前深信服桌面云产品已在政府、企业、金融、教育、医疗等行业规模化部署应用，帮

助用户实现统一运维、数据安全、移动桌面、降低运行成本等IT建设目标。

2.2.4.1. 深信服桌面云核心技术突破

自研传输协议技术

通过对三代传输协议更新迭代，成为国内首家技术突破实现广域网VDI自适应算法和流量削减的厂家。

深信服自研HEDC协议是Sangfor自主研发的远程协议，其有带宽占用低、CPU资源消耗小等优势，并支持了vGPU、视频重定向支持、H264压缩等，使得云桌面的体验性远远优于SPICE和RDP协议，且带宽消耗低于它们。深信服自研的 SRAP 高效交付协议，采用高效流压缩、智能数据缓存、动态图像优化等多项优化技术，相对 RDP 协议提升 6 倍传输效率，最大程度保障用户桌面体验。

首家零信任安全架构体系

随着办公终端多样化和协同技术发展，通过传统的终端加固来防止数据泄密会越来越难，而桌面云数据不落地架构正好适应组织的业务需求，随着近些年，安全威胁往往通过组织内部活动完成渗透，例如钓鱼邮件和网站，传统的被动式防御安全架构有一次面临挑战，所以深信服不断投入研发人力，推出国内首家零信任架构桌面云，通过aDesk内置的动态访问控制权限等策略，实现精细化的颗粒度授权，保护桌面使用安全不同用户，不同终端位置，匹配不同的安全访问策略。

支持全双活容灾桌面云架构

很多组织都有计划通过桌面云来取代传统PC，IT决策者不仅面对体验和场景适配的挑战，还要面对成千上万个桌面运维与管理的难题，随着容器化及AIOps逐步成熟，越来越多的桌面云常常开始将这两项技术应用于桌面云领域：

容器化技术主要将桌面系统上的应用软件和用户数据分离并可独立存储，真正实现了桌面，软件和数据松耦合；根据业务需要，IT管理员可以动态无缝地将应用软件和数据漫游到不同桌面，极大降低了桌面管理和运维的复杂度；



图 2-5 深信服桌面云容器化分层技术示意图

容器化主要应用于两个领域：

- UPM（用户配置文件管理）由微软和Citrix率先提出，主要用于大规模桌面部署场景下用户配置文件与数据的集中管理，例如还原桌面和SBC应用的数据保留；随着用户数据量的爆发式增长，上一代基于文件NAS存储的模式已经无法满足用户体验需求，而新一代基于容器化的UPM不仅兼容性更好，而且用户体验更接近于PC本地配置文件；
- 软件分发早期产品主要有微软Remote App和VMware Thin App，主要解决大规模桌面部署场景下应用部署安装与管理，第一代软件分发基于文件级别处理，类似于绿色软件模式，兼容性和性能较差，不利于大规模推广和部署；而新一代基于容器化的软件分发技术，不仅在兼容性处置和性能上都有质的飞跃，已经成为当前桌面云大规模部署中的关键核心技术；

应用容器化技术的典型厂商：

- CSG（Citrix）的UPM（用户配置文件管理）和App Layering（软件分发）
- 深信服的UPM2.0和软件分发2.0
- VMware App Volume软件分发

AI Ops技术主要将AI技术应用于智能排障、性能数据分析、桌面效能分析和安全威胁识别等等，AI技术在运维领域的广泛应用将提升运维效率和保障业务连续性，从而达到降低组织TCO的整体目标；

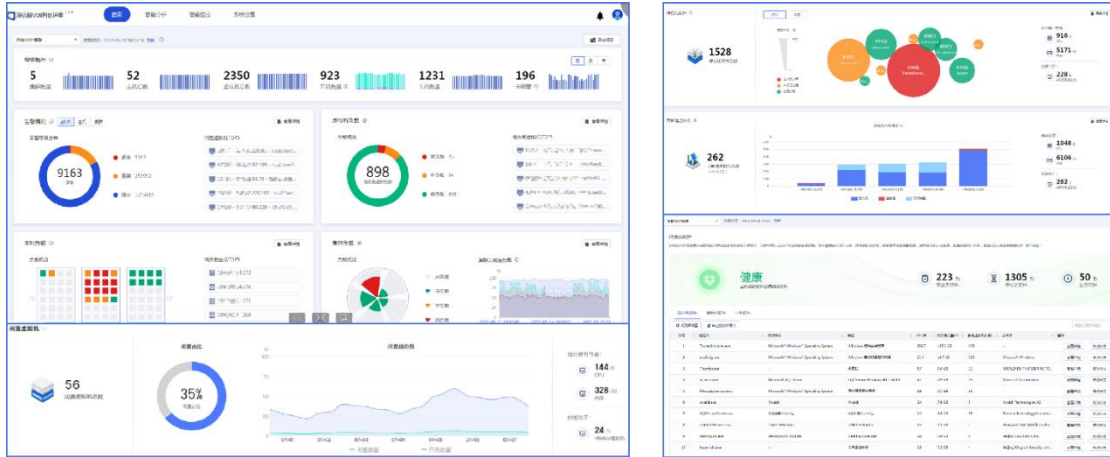


图 2-6 深信服桌面云智能运营平台

利用AIOps技术的典型厂商

- CSG（Citrix）的Citrix Director和Citrix analytics
- 深信服的IOM智能运营监控平台
- VMware vRealize Operations (vROps)

2.2.4.2. 技术架构重大创新

深信服提供端到端、从软件到硬件融合的极致体验。以更安全，更高效的桌面云解决方案为目标提供给用户。整套产品方案只需要云终端、桌面云一体机（预装桌面虚拟化、服务器虚拟化、存储虚拟化等软件平台）两种硬件，即可完成整套桌面云的快速上线，是国内首家打造深度融合的VDI解决方案厂商。

深信服桌面云和超融合架构一体化已经被业界认可，具有高可靠（分布式存储加多重实时副本，确保大规模部署时业务高可用）、高性能（分布式存储并发性能支撑，满足所有核心业务系统需求）、易扩展（性能和容量同时水平扩展）、易管理（基于软件实现网络、计算、存储功能，更加高效，更易管理）等技术优势。

- 国内首家拥有基于KVM vGPU方案的厂商
- 发布基于AIOps的智能运营平台IOM
- SBC多场景适配和创新
- 全场景的桌面云交付架构

2.2.4.3. 信创技术融合

围绕安全构建核心优势，打造数据安全全链条的信创安全办公，深信服信创桌面云关键技术主要体现在以下几个方面

- 关键技术指标全面对标非信创,例如传输协议、桌面云安全能力及超融合架构技术;
- 通过技术创新加快适配多种软硬件架构体系,推动“多模”统一架构,满足客户复杂的业务需求;
- 构建广泛信创生态体系,让信创架构真正好用,促进客户实现“真替真用”;
- 通过技术创新例如提升虚拟机密度,适配低成本终端等,不断降低信创桌面云总体拥有成本;

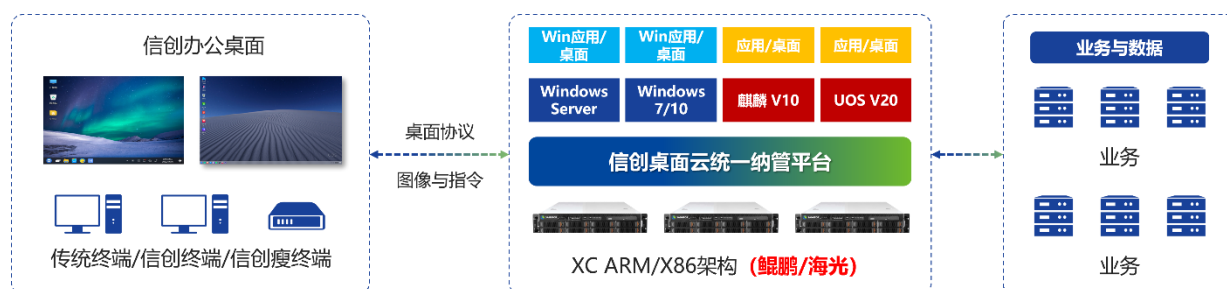


图 2-7 深信服信创桌面云统一纳管架构图

三.桌面云产业发展趋势分析

随着云计算技术的不断发展和普及，桌面云技术也在不断发展和完善。未来，桌面云产业将会呈现以下几个发展趋势：

1. 桌面云技术将更加普及。随着云计算技术的不断发展和普及，越来越多的企业和个人用户将会采用桌面云技术，以提高工作效率和使用体验。
2. 混合办公成为新的常态。混合云技术是指将公有云和私有云相结合，形成一种新的云计算模式。在桌面云领域，混合云技术可以实现桌面环境和应用程序等资源的灵活部署和管理，提高了桌面云的可靠性和安全性
3. 桌面云技术将更加智能化。桌面云技术结合AIOps、人工智能技术、元宇宙等技术，实现更加智能化的桌面环境，为用户提供更加个性化、智能化的服务。
4. 桌面云技术将更加安全可靠。桌面云技术结合零信任、区块链技术、加密技术等安全技术，保证用户数据的安全性和隐私性。
5. 桌面云技术将更加开放和标准化。桌面云技术将会更加开放和标准化，以促进产业的发展和创新。

3.1. 混合办公成为新常态，桌面即服务成为未来发展趋势

什么是混合办公？IDC定义混合办公：“是一种工作者在多个地点（例如本地、现场、居家和差旅等远程）和多种时间节奏（例如固定的，变化的，或临时的）中开展业务的动态工作模式。”

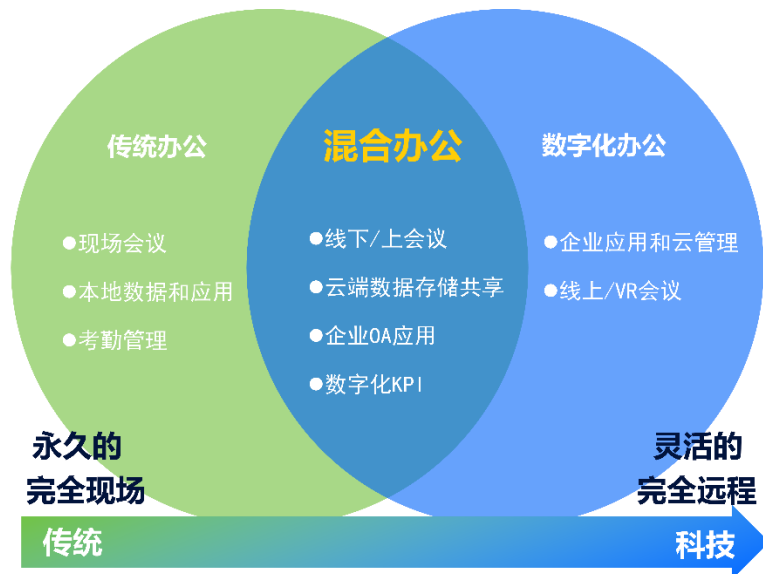


图 3-1 混合办公工作模式

过去三年的疫情推动了远程办公的发展，混合办公模式已经被越来越多的企业和员工所

接受。这也将成为未来的市场趋势之一，并且已经成为许多员工追求的福利。因此，吸引和留住人才已成为企业采用混合工作模式的最大动力之一。IDC的调研数据显示，随着社会发
展以及工作方式的改变，远程和混合工作模式以及智能数字工作空间在未来最有可能在企业
中持续下去。企业将在能够提供更加灵活办公方式的工具和服务上投入更多。随着混合工作
成为新常态，提高用户的访问、效率 and 安全性，无论他们身处何地，访问企业内部和云端的
资源，都将是现代企业的优先任务。

据IDC报告显示，2022年桌面即服务（Desktop as a Service，简称DaaS）的市场规模
达到了3.5亿美元，同比增长156.8%；未来五年（2022-2027年）该市场仍然会保持83.3%
的年复合增长率，预计2027年将达到73亿美元的市场规模。

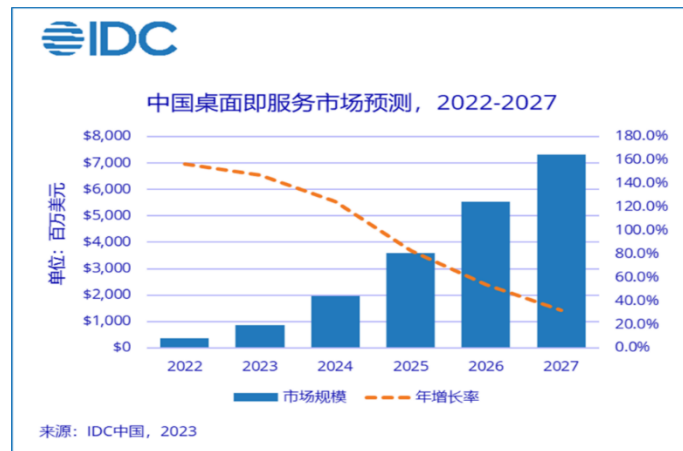


图 3-2 中国桌面即服务市场预测，2022-2027

疫情的影响，对企业的业务连续性和员工的正常办公带来了巨大挑战，使人们对混合办
公和远程办公的需求更加迫切。同时，疫情催生了企业实现工作方式转型的迫切性和动力。
通过数字化工作空间和混合办公模式，企业能够适应不断变化的环境和需求，更好地应对未
来的挑战。预计全国范围内的远程办公用户使用习惯将进一步提高。随着市场经济的恢复、
企业对灵活的远程办公模式的接受、对数据安全的需求以及对国产品牌的偏好、各大厂商
（桌面云厂商、电信运营商、云厂商等）的持续发力，同时将推动未来几年虚拟桌面软件及
DaaS市场的增长。

DaaS能够帮助客户减少前期资本支出、采购和供应负担，并具有按需购买、按时付费、
易于维护、随时随地使用等优点，因此在中小型和创新型企业中得到广泛接受。而对于大企
业来说，其带来的灵活性和高算力，也非常具有吸引力。



图 3-3 混合业务部署模式逐步成为主流

DaaS 的优势：

灵活性：DaaS支持便捷的环境迁移，仅用几小时（而不是几天）就可以完成各种应用程序与桌面的部署。

即用即付：DaaS采用的是一种简便、透明的“即用即付”服务订购模式，用户仅需要按用量支付费用。

节约成本：采用DaaS之后，用户不必再为数据中心维护投入任何硬件成本。更可预测的成本，如果用户想避免任何意外成本，因为在DaaS上成本定义相对明确，可以通过迁移到运营支出模型来控制。

按需调整规模：DaaS不仅支持即用即付的订购模式，还支持便捷的按需规模调整。

提升IT工作效率：由云服务合作伙伴代为执行日常管理、提供基础架构支持，让IT部门节省大量时间与资源，进而提升工作效率与效果。

安全与合规：数据安全地存放在云平台，不用再担心因设备遗失导致重要数据泄漏。

成套服务：DaaS服务提供商能够帮用户完成大部分的桌面日常管理工作。

简化管理：DaaS属于成套服务，易于管理，能够消减很多IT管理工作。

DaaS 的挑战：

安全：对于某些组织而言，DaaS 代表了利用服务提供商的安全专业知识和资源的机会。但是，在政府、医疗保健和金融服务等高度监管和安全意识的行业中，组织将有更多的工作要做，以找到满足其要求的供应商。或者，他们可能不认为共享资源的风险是可以接受的。

不受控制的成本飙升：尽管DaaS承诺降低成本，但随着时间的推移，用户可能会有更多的僵尸/未使用的资源来消耗用户的预算。当用户没有合适的云成本管理工具时，这可能会增加成本。建立正确的 KPI 有助于降低基础架构成本。

灵活性较低：购买供应商定义的解决方案时，无法自定义超出特定点的环境。如果用户

需要杠杆来更改配置或使用本地环境中免费的硬件，则最好开发客户端定义的DaaS或纯VDI环境。

DaaS 的常见用例：

长期项目支持：随着组织在新地区的扩张，快速配置新资源既耗时又费力。使用DaaS可以解决这一挑战，同时还支持扩展。

短期需求：例如由于折扣、劳动力扩张、紧急情况等原因导致客户数量激增。用户无需购买新的基础架构和资源，可以通过DaaS模式解决。

减少管理责任：在没有充足的IT预算及专门的管理人才时，用户可以将桌面虚拟化环境的管理工作留给DaaS后台专家。此外，如果用户需要支持全球客户群，确保用户的环境全天候运行。DaaS以可预测的价格为用户提供合适的工具，用户不需要深入了解所有系统。

VDI和DaaS的3个主要区别：

管理：VDI通常需要更多管理，包括硬件，桌面系统，应用等自行管理。除非用户使用同类VDI最佳的解决方案（例如Sangfor提供的一体化交付解决方案），否则需要更熟练的管理团队。相比之下DaaS环境由供应商管理。应用程序仍然需要IT部门进行一些实际管理。但是，所需的学习曲线和技能并不像VDI那样广泛。

成本：VDI利用本地基础架构，因此可能更昂贵。IT还需要考虑可扩展性所需的额外容量。加上电力、冷却和空间成本。在DaaS的情况下，用户可以按使用量付费，可能更便宜。但是，这些成本会随着环境的发展而增长，因此IT需要保持警惕。

最终用户体验的灵活性：VDI可以在虚拟机资源和桌面配置选项方面提供更大的灵活性，因此，可以根据不同的用例和工作负载更精细地调整用户体验。此外，通过使用应用分层，软件分发，应用商店等解决方案，IT可以进一步简化应用程序生命周期管理。使用DaaS，大多数用例都需要定制和更多时间投资。或者在某些情况下，某些用例甚至可能难以复制。通常情况下用户的业务系统先上云，桌面再上云，可以更好的增强用户访问体验。

3.2. 基于零信任架构的数字化工作空间应用广泛，平衡安全与生产力

受疫情的催化作用，混合办公、随处办公以及分布式的办公模式已经成为职场中的常态，尤其受年轻人的青睐。在混合办公的趋势下，接入公司网络的设备五花八门，接入网络、接入地点、接入方式的多样化使整体办公环境的复杂程度翻倍。同时，随着云化、移动化或数字化的兴起，企业业务变得更加开放，企业的数据资产越来越分散，网络边界、物理安全边界日益模糊，给企业带来了巨大挑战。

混合办公趋势下的四大挑战

企业从传统的集中办公转向“随处可用的工作空间”模式，面临四大挑战。

首先是可见。企业IT管理人员需要清楚“看见”公司网络中有多少设备，有多少员工在公司，有多少员工不在公司办公，员工的设备在哪里，有哪些种类等等。如果“看不到”员工和设备，IT管理将无从谈起，因此“可见性”非常重要。

第二是响应。大量员工分散在全国各地的不同场景下办公，一旦出现问题，服务响应时间要足够及时，任何场景下出现问题，IT要能在第一时间知道并且能够快速处理。

第三是体验。无论员工在哪里办公、无论用什么设备接入，必须保障员工在任何地点都能继续使用公司的业务系统、获取公司数据，包括核心系统和数据，并且能够获得一致的访问体验。

第四是安全。要保障员工在任何地点上班都不能有任何安全漏洞，尤其是个人设备参与办公后，员工的生活和工作完全融合，很难区分开。一旦黑客攻击了员工的个人设备，那么可以随时破坏企业应用、攻击企业内部系统。随着设备的增多，企业面临的安全风险陡增。

面对以上挑战，传统的VPN方案虽然能解决部分远程问题，但是存在业务暴露面大、过度授权、数据泄露等弊端。为了更加安全，部分企业采用“VPN+桌面云+堡垒机+共享桌面”等方案组合，但因为不同终端需要采用多种接入方式、多次登录、多个密码，限制较大，访问体验很差。总之，采用现有方案，安全和效率很难平衡、兼顾。

基于零信任+桌面云结合的架构，构建了统一的零信任桌面云工作空间新方案在金融、医疗、能源、企业制造、企业设计院、政府等行业应用越来越广泛。新方案采用零信任安全架构、虚拟桌面及虚拟应用、沙箱、UEBA等技术相互融合，构建一个安全的数字化工作平台，既能提供高效办公体验，又能确保访问业务的端到端安全。

在这个统一的零信任桌面云工作空间，内部员工、外包人员、甚至是供应商、合作伙伴，都可以在不同地点，采用不同类型的终端或不同操作系统接入，经过零信任组件进行身份验证后，即可访问权限范围内的桌面、应用、文件与数据。

例如：OA、邮件等低密级业务可以通过零信任构建加密隧道直接访问；BI等涉及业务敏感数据的中密级业务，可以通过沙箱构建一个隔离的环境进行访问；研发代码、财务数据等高密级或高风险业务，可以通过云桌面或云应用进行访问，确保数据不落地。以一个科技型公司为例，用户声音：“我需要同时访问市场、研发、财务、采购等不同密级的业务，只需要在统一的门户里点击一下图标就可以访问，整个过程很方便。如果要访问经营管理系统、财务系统、成本系统等相对敏感的系统，会调用云应用访问，云应用可以防截屏。如果需要访问研发业务和数据，或者财务经营报告，需要登录到云桌面访问。”

桌面云技术的架构与零信任安全理念紧密结合，从而构建了更加安全和灵活的工作环境。以下是融合架构特点：

①一致性办公体验，无边界工作空间环境：云桌面技术消除了传统办公环境中的地理和

设备限制。用户可以通过任何设备(包括个人电脑、移动执法终端、平板电脑、智能手机等)、任何时间、任何地点访问其云桌面,内外网一致性的办公体验,实现真正的移动办公。这种架构与零信任的理念相契合,因为访问不再取决于特定的网络位置。

②多维度身份认证与访问控制:在云桌面架构中,身份认证不仅仅限于用户本身,还涵盖了设备、应用程序等多个维度。用户需要进行身份验证后,才能访问其云桌面。这种多维度的认证与零信任的核心原则一致,确保访问的安全性。

③数据隔离与安全性:云桌面技术通过在云端维护用户的工作环境,实现了数据的隔离和集中管理。敏感数据不再存储在本地设备上,减少了数据泄露的风险。此外,零信任的思想也在这一层面体现,只有经过授权的用户才能访问特定的数据和应用。

④桌面内动态访问授权,保护核心业务:传统的桌面云方案实现了数据不落地级的防泄密效果,但是用户一旦接入桌面云后,访问内部业务将会完全依靠桌面云开放的网络访问权限,无法实现动态业务访问权限控制,传统的零信任架构将在桌面云内访问内部业务时变得毫无意义,如在用户不同环境接入桌面云后严格限制业务网络访问权限,面对不同类型人员访问需求,网络管理员将会设置复杂网络ACL访问策略,效率低,体验差。采用新型桌面云+零信任融合架构,允许资源动态分配,根据用户需求提供所需的计算和存储资源。这种灵活性有助于提高效率,并降低成本。同时,融合后也强调了访问控制的动态性,用户的权限和访问范围可以根据实时需求进行调整。通过零信任“持续验证、永不信任”结合桌面云内防火墙或零信任组件,实时检测用户终端健康状态,自动调整可访问的业务系统范围,让外网和内网变得同样安全。

云桌面技术与零信任安全理念的融合,为组织提供了更加安全、高效的办公环境。通过将工作环境从本地解放出来,实现了真正的混合办公,同时也在安全性方面迈出了重要一步。这种架构不仅满足了组织的云化、集约化需求,还为未来的工作方式奠定了坚实的基础。

3.3. 利用 AI 赋能桌面云, 更加智能化

AIOps赋能桌面云, 更加智能化的运维管理

相比于传统pc,桌面云赢得用户青睐的一大特性就是其省心便捷的运维能力。但真正投入使用时,却发现运维没那么简单。虚拟机故障停摆后,监控平台的告警才姗姗来迟;用户反馈桌面云卡慢后,无法快速找到根本问题;哪些桌面云闲置,哪些桌面利用率比较高,哪些桌面需要扩容,哪些应用影响用户体验,桌面使用情况,应用使用情况,从集群到物理主机到虚拟机到应用,是否有必然的关联影响,面对这些问题,管理员常常被动应对和管理,无法运筹帷幄,了如指掌。桌面云的运维,似乎也没有那么简单。

在桌面云领域,管理员正在逐步通过AIOps赋能桌面云,利用AIOps可以实现更加智能化的运维管理,具体来说利用AIOps可以实现以下几个方面的优化:

自动化运维：AI Ops可以通过自动化的方式来完成一些重复性的、繁琐的运维任务，如监控、告警、日志分析等，从而减轻运维人员的工作负担，提高运维效率。

智能化故障诊断：AI Ops可以通过分析桌面云的运行数据，识别出潜在的故障点，并给出相应的解决方案，从而提高故障诊断的准确性和速度。

预测性维护：AI Ops可以通过分析桌面云的历史数据，预测出未来可能出现的故障，并提前采取相应的措施，从而避免故障的发生，提高桌面云的可靠性。

自适应优化：AI Ops可以根据桌面云的实际运行情况，自动调整配置参数，优化桌面云的性能和资源利用率，从而提高桌面云的效率和稳定性。

ChatOps赋能桌面云，提高工作效率

桌面云管理员通过深入利用AI Ops可以实现桌面云的智能化运维管理，为桌面云管理员提供更加优质的服务。我们也发现一些组织正在通过更的AI能力赋能帮助桌面云使用者提供更优质的服务。在过去，当用户终端访问桌面云或桌面云内使用一旦出现问题，包括不可预见故障或 workflow 协作等问题，用户大多通过求助IT或者自行百度处理，求助IT需要排队等候；自行解决往往处理难度高，也会带来更多的出现问题。这样不仅对用户的体验不佳，也会成为管理员运维负担。

ChatOps是一种基于聊天工具的工作方式。通过**ChatOps**赋能桌面云，有以下几个方面优点：

提高问题处理效率：用户可以一键求助此工具，对话式AI持续给出处置建议，通过将机器人植入聊天会话，形成人、机器、数据的自动化、透明化的联动，使运维团队能够高效执行任务和沟通协作，提升用户问题解决体验及减少管理员运维工作量，“用聊天的方式来做运维工作”成为可能，持续对话式处理问题，直至最后解决问题，无需挨个寻找解决方案，高效率处理复杂故障。

简化工作流程：通过桌面云和**ChatOps**的结合，用户可以在一个集成的环境中完成各种任务，无需切换不同的工具和界面。他们可以通过聊天界面直接与桌面云进行交互，执行各种操作，如启动应用程序、访问文件、管理虚拟机等，从而简化了工作流程。

提高工作效率：桌面云结合**ChatOps**可以提供快速、实时的反馈和响应。用户可以通过聊天界面发送指令，桌面云会立即执行相应的操作，并将结果返回给用户。这种实时的交互方式可以大大提高工作效率，减少等待时间。

增强协作能力：**ChatOps**使得团队成员可以在一个共享的聊天环境中进行实时协作。通过桌面云结合**ChatOps**，用户可以与团队成员共享桌面、文件和应用程序，进行实时的讨论和协作。这种协作方式可以促进团队之间的沟通和合作，提高工作效率和质量。

提供更好的可追溯性和可管理性：通过**ChatOps**，用户可以在聊天记录中查看和追溯所有的操作和交互。这种可追溯性可以帮助用户更好地管理和跟踪工作进展，及时发现和解决

问题。同时，ChatOps还可以提供权限管理和审计功能，确保操作的安全性和合规性。

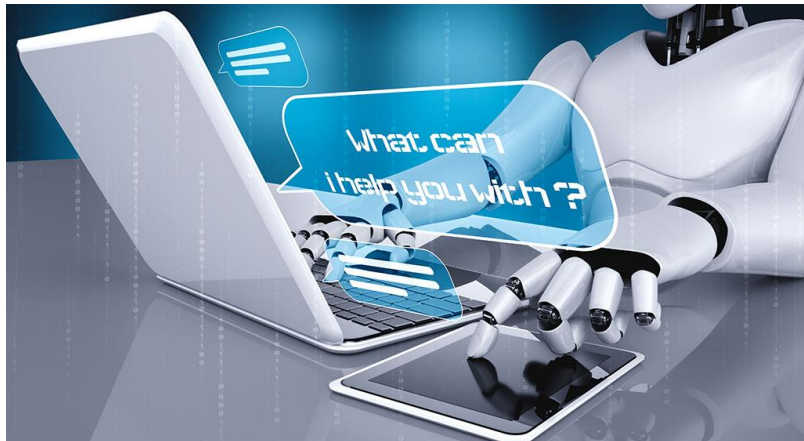


图 3-4 通过聊天的方式完成各种任务

总之，桌面云结合ChatOps可以为用户提供更简化、高效、协作和可管理的工作环境，帮助他们更好地完成任务并提高工作效率。当前桌面云结合ChatOps还处在初级结合阶段，完成简单的问题处理能力，未来将会发挥更大的价值！

桌面云可能是元宇宙切入办公场景的入口

元宇宙是一种虚拟的数字世界，可以模拟现实世界中的各种场景和体验，包括社交、娱乐、教育、商业、办公等。在后疫情时代，人们在现实世界中自由出行受到限制，这在一定程度上也激发了远程交互技术和产品的发展，以帮助人们跨越物理的限制。元宇宙概念的流行，不仅满足了人们对于未来娱乐生活的想象，也映射出当下现实的需求。桌面云作为一种基于云计算技术的服务，未来可以为元宇宙提供云上办公基础设施和支持，为用户提供更加便捷、高效的办公体验。例如，用户可以通过桌面云在元宇宙中访问自己的桌面环境和应用程序，进行办公和协作，同时也可以与其他用户进行社交和交流。在理想状态下，元宇宙可以应用于任何事物。元宇宙办公平台，可以让员工在任何地方进行虚拟工作。



图 3-5 虚拟的工作空间

桌面云可以通过应用AI技术提供更智能化的办公方式，例如自动化的文件管理、智能化

的日程安排、语音识别的办公助手等。这些功能可以大大提高员工的工作效率和协作能力，同时也可以增强员工的使用体验。

此外，一些科技型公司正在打造“员工体验平台”，如微软Viva等。这些平台旨在通过联系、成长和学习机会、更好的见解以及对业务目标的一致性来改进员工体验和员工生产力。这些平台通常包括智能化的办公工具、个性化的工作环境、以及丰富的员工福利和社交活动等。“员工体验平台”一个面向企业的AI信息中心，未来桌面云与“员工体验平台”更好的融合，公司可以提高员工的满意度和忠诚度，从而提高企业的生产力和竞争力。

总之，利用AI技术赋能桌面云，可以为企业带来更加高效、协作、智能、人性化的工作方式，从而提高员工的工作效率和企业的竞争力。

3.4. GPU 深度应用将成为桌面云计算密集场景专用方案

基于GPU构建的桌面云产品具备更高性能、高密度的良好用户体验，无论是采用GPU直通模式还是GPU虚拟化模式，都会保障用户在复杂的图像数字场景中享受流畅的云桌面体验，伴随桌面云客户业务持续创新，企业对大数据分析、复杂图形处理、多媒体编辑、VR与AR等应用场景的GPU需求持续增长，带有GPU的桌面云解决方案市场有望持续扩容。

3.5. 超融合架构将开辟桌面云发展的新天地

有观点认为，超融合架构是实现“软件定义数据中心”(SDDC)的终极技术途径，其类似Google、Facebook后台的大规模基础架构模式，可以为数据中心带来非常优秀的效率、灵活性、规模、成本和数据保护。由于超融合技术可以给IT部门带来的简化管理、扩容方便，以及具备极致性能的特点，在桌面云市场也得到了广泛的应用。

桌面云通过超融合基础架构技术虚拟化产生的移动工作空间，融合了企业级的服务器和虚拟化所需的功能和优势，采用集中管控的云主机替代传统的PC，最大化企业IT资源的效率和利用率，为企业带来高效、可控的办公环境和一致的用户体验。用户可以通过瘦客户端、PC、PAD、手机或者其他任何与网络相连的设备，访问跨平台的应用程序以及整个客户桌面，帮助用户突破时间、地点、终端的限制，随时随地接入自己办公桌面实现移动办公。



图 3-6 超融合架构无缝运营

超融合架构和桌面云结合的优势如下：

简化管理：超融合架构将计算、存储和网络资源整合在一起，而桌面云提供了集中式的虚拟桌面管理。结合两者可以实现统一的管理平台，简化了整个系统的管理和维护工作。

提高灵活性：超融合架构的弹性扩展和虚拟化技术使得资源的分配更加灵活，而桌面云可以将虚拟桌面随时分配给用户。结合两者可以实现按需分配和动态调整资源，提高了系统的灵活性和适应性。

提升性能：超融合架构的高性能存储和计算能力，结合桌面云的虚拟化技术，可以提供更高的性能和响应速度。用户可以在任何时间、任何地点通过桌面云访问资源，享受到高性能的体验。

提高安全性：超融合架构和桌面云都注重安全性。超融合架构通过数据冗余和备份保护数据安全，而桌面云通过集中管理和访问控制保护用户数据。结合两者可以提供更全面的安全保护，减少数据泄露和风险。

降低成本：超融合架构和桌面云的结合可以减少硬件设备和维护成本。超融合架构整合了计算、存储和网络设备，减少了设备的购买和维护成本；桌面云提供了虚拟桌面，减少了终端设备的需求。整合两者可以降低总体的IT成本。

综上所述，超融合架构和桌面云的结合可以简化管理、提高灵活性、提升性能、提高安全性和降低成本，为企业提供更高效、可靠和安全的IT解决方案。

3.6. 桌面云将覆盖更广泛的物联网终端

随着物联网技术的快速发展，借助下一代桌面云的前后端混合计算特性，物联网终端的计算能力将被充分发挥，同时随着物联网底层硬件操作系统和驱动问题的逐步解决，下一代桌面云将可以适配不同类型的物联网终端设备，真正为万物互联提供稳定的管理支撑。

在基于5G甚至未来6G技术的助力下，桌面云应用的交付速度将大大加快，甚至能够媲美基于本地终端的桌面应用交付速度，让广域网环境下的桌面云也能拥有与局域网相同的应

用体验，这将让下一代桌面云的应用范围大大扩展，并覆盖到更多的物联网终端。多样化智能办公设备，不仅仅提升工作效率，更将赋能混合办公模式在不同物理空间之间无缝连接。



图 3-7 多样化设备无缝连接

3.7. 内生安全

桌面云内生安全是指在桌面云环境中，通过内生安全技术来保障桌面云环境的安全性。这种技术可以在桌面云环境中实现自动开启防护，安全隔离、数据加密、访问控制等安全措施，从而保障桌面云环境的安全性。

通过桌面云内生安全，桌面上线即安全，用户的希望是桌面云在创建和上线的时候就实现安全，并通过自动化、向导化的方式来实现安全的效果，而减少用户操作上的难度，为组织提供更加安全、可靠的桌面云服务。

我们认为，桌面云内生安全主要包含桌面安全、网络安全、数据安全3个方面。

在桌面安全方面，可以实现虚拟机创建的时候，就自动安装相关的桌面安全组件、自动开启实时防护、自动打快照等，整个过程无需繁琐的、手动安装和处置。

在网络安全方面，过去，桌面上线后，需要到防火墙上人工配置ACL策略。现在，通过平台在底层内置了分布式防火墙，实现东西向、南北向安全防护，支持基于单个用户和用户群组一键生效安全策略，颗粒度可以到虚拟这个层面，而且这个安全策略会随着云桌面迁移、扩展而跟随。

在数据安全方面，最常用的USB外设管控、违规外联管控、文件导出管控、防截屏防录屏等都是直接以无插件的方式支持，安全策略都是基于用户层级来设置的，无论桌面资源怎么调整、采用什么终端设备、在什么地点登录，策略都是生效的，实现了更广泛、更灵活的管控。

桌面云内生安的价值和意义主要体现在以下几个方面：

提高安全性：桌面云内生安全可以通过多种技术手段，如虚拟化、隔离、加密等，来保护用户数据和系统安全，从而提高整个桌面云环境的安全性。

降低风险：桌面云内生安全可以有效降低因为用户操作不当、恶意软件攻击等原因导致的安全风险，从而保障用户数据和系统的安全。

提高效率：桌面云内生安全可以自动化管理和监控安全事件，减少人工干预，提高安全管理效率。

降低成本：桌面云内生安全可以通过共享安全资源、自动化管理等方式，降低安全管理成本，提高整个桌面云环境的经济效益。

总之，桌面云内生安全是未来发展的趋势之一，随着技术的不断发展，桌面云内生安全的安全性能将会不断提升，安全管理将会更加智能化，安全防护措施将会更加多层次，安全合规性将会更加注重。这些趋势将会为桌面云的安全提供更加全面和有效的保护。

3.8. 满足信创要求

桌面云诞生之初，Citrix和VMware两家国外桌面云厂商占据了我国大部分桌面云市场。当国内互联网厂商效仿亚马逊开始开拓云计算市场时，一些传统IT厂商(包括一些创新企业)开始基于服务器虚拟化技术推出了国内桌面云产品。

经过十余年的发展，国内桌面云产品凭借着其优异的性能、实惠的价格和更符合国人习惯的产品设计成功占据了国内桌面云市场的半壁江山。如今，各行业所看到的桌面云应用场景80%以上来自国内桌面云厂商，越来越多的行业用户选择国内厂商产品取代国外厂商实现数字化转型。

近几年，随着信创基础软硬件的飞速发展，国内厂商也推出了全栈信创桌面云解决方案，并在一些行业得到了应用，预计不久桌面云解决方案在性能、性价比和用户体验上会得到快速提升，可以和非信创类桌面云解决方案媲美。信创桌面云依托信创芯片服务器，承载主流信创操作系统，通过基于信创操作系统的云桌面、云应用资源服务模型，逐渐满足各行业场景多元化、个性化的桌面需要，持续不断地提高用户桌面的使用体验。

信创桌面云满足信创要求成为趋势，但是也存在以下挑战：

(一) 关键能力差距导致推广受到阻碍

从桌面云的关键部件、核心技术到供应链安全情况分析，国内桌面云整体上与国外厂商接近，且在部分场景下也建立了一定的领先优势，但若要保持持续稳定发展和进一步突破，需要持续补充短板差距。首先，在桌面云关键部件方面，桌面云资源池即云端虚拟化能力与国外厂商存在差距，国内桌面云对于虚拟化层(Hypervisor)的技术积累较少，很多是基于国外开源的Hypervisor组件进行修改，缺乏自主的虚拟化技术突破，需要持续追赶和补齐；其次，

在供应链安全方面，国内CPU在性能上仍和国外主流CPU（诸如Intel、AMD）存在一定的差距，如主频低、功耗大、并发核数不足等，集中表现在一些复杂业务在桌面云上运行时效果不佳，这导致桌面云解决方案在制造设计、企业开发等高性能场景下的推广受到阻碍。

（二）复杂生态加重桌面云软硬件适配工作

当前，我国的信创基础软硬件生态比较复杂，主要表现为存在多个互不兼容的信创CPU指令集，围绕这些CPU指令集建立起来的信创生态相互孤立。比如，我国现有信创CPU包括X86指令集、ARM指令集、LoongArch指令集等，他们相互不兼容，导致运行在其上的信创操作系统和应用软件相互不兼容。由于现有应用软件编程技术限制，研发的应用软件目前很难做到跨异构硬件架构，导致桌面云软件必须适配多种类型的信创CPU和信创操作系统，极大增加了桌面云厂商的信创适配工作量。当前我国桌面云产品已基本适配了X86和ARM架构，但针对LoongArch架构的适配还未完全完成，除此之外ARM架构方案上还存在桌面云功能与X86架构不对齐、上层应用软件缺乏等问题；如在架构对比上，ARM架构的桌面云产品的功能相比X86桌面云要少很多，基于ARM架构开发的应用软件也较少，尤其是和行业相关的业务类软件十分缺乏，难以支撑设计、制造等行业的业务运行。

（三）缺少行业标准阻碍生态建设

桌面云建设一方面面临着从评估、适配到项目实施、运维等完整项目周期系统化标准的缺失，另一方面又面临着国家、行业到各地区等多层标准的正确解读与遵循。从CPU到整机服务器厂商，到PC终端厂商，从操作系统到数据库、中间件及上百种国内化业务软件，桌面云的生态面临着上千种无序的组合。并且项目完成后并不意味着就已经完成了桌面云的建设，桌面云中的业务系统仍需要较长时间周期的检验，简单的桌面运维不能解决此阶段出现的问题，仍需要各厂商深度的联合排障甚至定制开发。

当前桌面云很多关键技术（例如多核心高性能CPU芯片、桌面操作系统，软件生态，应用管理等）还依赖于WinTel平台，Windows+Intel联盟根深蒂固，明确的指引和生态扶持政策有助于生态建设，如根据市场自然规律来选择，很难打破WinTel垄断；

（四）人才匮乏导致项目建设复杂

桌面云项目的实施缺少信创服务器、操作系统、软件等专业资质的项目实施人员，缺少专业的培训机构开展针对性的课程，能够帮助企业深刻理解信创的政策、生态、管理要点、技术细节、故障排错经验等。

四.生态整合解决方案

4.1. 华夏威科 AuditSys 用户实体行为分析系统解决方案

4.1.1. 应用背景

北京华夏威科软件技术有限公司（以下简称“华夏威科”）成立于2011年，总部位于北京，2021年被评定为北京市“专精特新”企业。拥有多年云计算、大数据、行为安全分析等领域市场经验，是中国内控管理市场领导者。公司总部设在北京，在上海、深圳、长沙设有办事处。配备专业的技术服务人员，研发与技术服务团队占比达70%，良好的服务体系能快速响应客户需求。自主研发项目申请专利7项、软件著作权59项。针对各行业、企业级客户，梳理出超过100+典型案例，有效的覆盖了各体量、各类型的客户信息化需求。

自主研发的产品SinoUEBA（AuditSys），利用大数据、UEBA实现用户内部人员行为可视化及行为风险数字化管理，是中国内控管理市场领导者。帮助企业发现来自内部的威胁和风险，实现行为审计与追溯、内部威胁管理、应用访问控制、工作效率分析、动态水印应用、敏感数据保护；产品主要应用于金融、能源、电信、政府以及制造业等各行业客户，尤其在金融领域得到了广泛的应用，Top10银行客户占有率70%、Top10保险客户占有率60%、Top10证券客户占有率60%、Top10基金客户占有率70%。

桌面云提供了一个完整的桌面应用平台，构建了一套数据不落地的安全模型，从很大程度上确保了数据安全，但无法量化用户在桌面云上的操作行为及操作风险，应用场景涵盖研发中心、呼叫中心、营业厅或分支机构、运维中心、远程居家办公等，具体需求挑战表现如下：

研发中心场景需求：

- 1、人员需求逐年增加，大部分是外包人员，难以管理，无法评估工作饱和度；
- 2、人员成本高，按照人均30万计算，200人外包，年投入约6000万；
- 3、目前行为监控采用人工检查方式，监控效率低，无法全程监控；
- 4、虽然已经有DLP产品，不能实现对研发岗离职前审计和离职后追责、不能对文件的流转做全程的监控，且不能分析监控敏感数据浏览行为；
- 5、2021年12月银保监会发布《银行保险机构信息科技外包风险监管办法》，在研发场景下，如何满足外包研发的监管要求？

呼叫中心场景需求：

- 1、呼叫中心岗位工作质检要求：传统双录（录音、录像）不能满足业务发展要求，需要增加录屏质检，即录音、录像、录屏的三录。

2、传统安全手段无法满足信息防泄露需求：

- 不能做用户实体行为分析，无法识别压缩、加密等动作，导致无法识别外发的加密文件内容；
- 传统的DLP类产品改变用户使用习惯，影响用户办公效率，而且资源消耗大，影响终端性能；
- 无法判断呼叫中心的B/S业务系统是否明文显示个人信息；
- 如何保护屏幕上的信息安全？

3、窃取个人信息犯罪行为呈组织化、专业化、高科技化发展趋势：内外勾结、安排人员到企业应聘、利用专业破解软件等获取客户完整身份证号码和手机号，已成为窃取用户隐私的常态。

营业厅或分支机构场景需求：

1、营业厅、网点数量多，而且地域分布广，营业厅、网点工作人员的个人信息保护、业务飞单监控、合规检查等，成为监管难点。目前通常采用去现场进行人工检查（走查）方式，但该方式存在以下问题：

- 成本高：一级分行、二级分行、支行或营业网点较多，去现场进行人工审计（走查）投入成本较大；
- 效率低：现场安全审计监控效率低，无法全程监控；
- 无法实现实时安全审计及时发现不合规行为；
- 营业厅业务形式的独特性。

2、营业厅地域分散、且无IT维护人员，对于营业厅上、下午交易时间，网络资源要优先保证交易系统，即交易时间尽可能不传输非交易数据。并且营业厅没有机房，需要有独特的架构设计才能实现网点的监管。

运维中心场景需求：

- 1、审计存在盲点：堡垒机系统不支持的应用软件无法审计，例如：**Google**浏览器；
- 2、数据采集能力薄弱：仅仅能获得复制文件、运维命令及回显内容，不能获得窗口标题、文件操作、**B/S**操作、**C/S**操作、邮件操作等行为数据；
- 3、事件追溯时间长：无法直接定位和检索行为，安全事件调查等工作时间长；
- 4、异常行为无法发现：无法判断和识别其中的异常和风险行为，无法对风险行为进行监控和告警；
- 5、无法实现大量行为数据处理：基于传统的关系型数据库作为存储，无法对大量行为数据进行分析 and 处理。

远程居家办公场景需求：

1、传统的日志审计产品完全依赖云桌面日志，而实际上云桌面日志信息非常少，通常只记录登录、退出、登陆失败等信息，无法掌握云桌面用户的具体操作情况，如何满足等保2.0的安全审计要求？

2、如何在海量行为中发现以及监控风险行为？

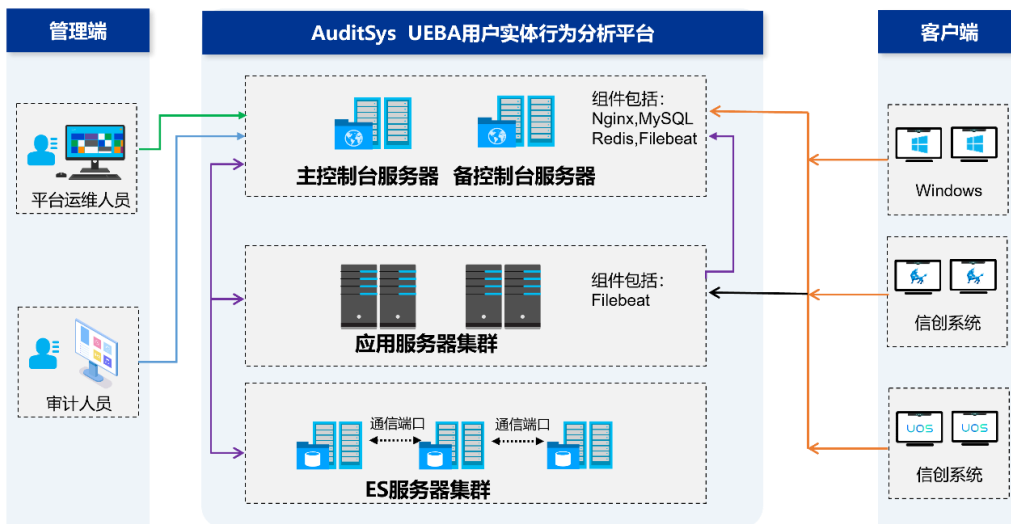
3、脱离职场办公，居家办公(远程办公)终端屏幕信息成为潜在的风险点，如何保证屏幕信息安全？

4、如何科学量化居家办公的工作状态?通过虚拟桌面日志计算工时的方法，无法准确反映居家办公的工作状态。

4.1.2. 解决方案

企事业单位信息化建设过程中，部署了终端安全产品或数据防泄漏产品，但敏感信息泄露事件等安全问题呈上升趋势。桌面云结合华夏威科AuditSys用户实体行为分析系统可以很好的解决这个问题，方案以“人”的操作行为为管理核心，将桌面云内的操作行为数字化，实现内部人员的风险行为和异常行为监控、应用访问控制、行为审计与追溯、工作效率分析以及用户行为画像分析。为企业提供更加安全可靠的一体化办公平台，提升企业核心竞争力，为企业信息化数字化转型保驾护航。

AuditSys利用大数据、UEBA技术理念实现用户内部人员的行为分析，通过在桌面云内部署行为数据采集器（Agent），实现内部授权用户所有行为全程监控、自动生成操作行为日志、全程分析发现内部异常行为以及信息泄露风险画像等。



(一) 行为全面记录、审计与追溯

- 实现云桌面用户所有操作行为全面采集、记录，风险全程可视可追溯；同时视频记录可以和操作内容文本记录进行匹配，精确定位操作画面及操作内容信息。
- 弥补桌面云操作行为审计监控的缺失，对运维、研发、业务等办公人员进行多维化、

全流程监控，加强内控管理；

- 敏感信息泄露事件发生时，提供不可抵赖录屏证据，佐证操作行为真实性；

华夏威科行为审计与追溯产品，自动生成所有操作行为日志，并可选择录屏取证，为审计合规管理提供可视化、不可抵赖的证据；所有录屏视频可以检索，可以通过检索迅速定位到操作视频，极大提高审计工作效率；可以支持分支机构或多中心部署模式，在总部随时可对任何人、任何时间、任何业务操作进行审计，极大提高审计的广度和深度。

(二) 行为安全管理，监控高危风险操作，发现内部威胁行为

- 通过预置或自定义风险行为规则，自动发现和统计风险行为，减少信息安全风险，比如监控飞秋程序的使用，飞秋程序极易造成数据泄露。并减少审计工作量，更有效的提升审计效率和质量；
- 对操作行为进行数据泄露风险分析，提供员工的个人信息泄露风险画像，提前发现可疑人员，帮助企业做好敏感信息保护；
- 实现高危操作行为人员画像，分析异常操作行为。运用大数据及机器学习算法模型，通过多维度计算异常操作风险，对潜在可能造成数据泄露人员进行风险评分；
- 安全防护软件失效，或者恶意绕过行为提供实时预警能力，及时发现潜在安全风险事件，避免因信息泄露给企业产生负面社会影响；

华夏威科内部威胁管理产品，实现对操作行为风险的全程监控。对于已知的潜在风险，利用安全规则在海量操作行为中发现高危风险行为；对于未知的潜在风险，利用机器学习算法，在大量的高危行为中自动发现异常行为，实现精准定位内部威胁和风险。对于业务操作风险，可以通过频次或时间异常监控，比如敏感信息查询次数分析和查询时间的监控，自动发现异常操作人员。

(三) 敏感数据保护

华夏威科敏感数据保护系统基于UEBA理念的数据泄露管理，全程记录并监控内部人员的所有操作行为，对操作行为进行数据泄露风险分析，提供员工的个人信息泄露风险画像，提前发现可疑人员，帮助企业做好敏感信息保护。

(四) 工作效率分析，提高工作效率

工作效率分析系统基于用户行为分析和大数据技术，按企业的组织架构和业务，对不同岗位的人员进行业务操作、非业务操作的工作分析，实现人员的工作状态监督、工作效率分析、工作饱和度的可量化管理。

(五) 屏幕动态水印，保护屏幕信息安全

华夏威科的屏幕动态水印技术，震慑手机拍照或截屏操作行为。水印内容可为当前账号和时间戳。当发生数据信息外泄时，结合水印信息和SinoUEBA (AuditSys) 行为风险监控和审计系统，迅速定位和找到责任人。

4.1.3. 方案价值

在桌面云内部署华夏威科AuditSys用户实体行为分析平台,可以解决用户的多种行为安全问题,满足桌面云中关于安全审计要求:

开发人员离职前审计、离职后追责:可以审计、发现研发人员离职前,是否有危害公司利益的行为;对于已经离职人员一旦有侵犯公司知识产权行为,可以审计追溯其在职时行为,为起诉、追责提供证据。

及时发现违规行为:对于安装绿色软件、卸载安全防护软件、抹除浏览器操作轨迹、改变防火墙状态、修改注册表、打印敏感文件等高危行为进行监控。

监控文件流转过程:监控文件、代码流转过程,包括文件外传到GitHub上的行为。

保护客户信息:发现业务软件明文显示个人敏感信息的情况,如身份证号码、手机号;发现业务系统个人信息已做脱敏,但被“内鬼”利用业务软件漏洞窃取个人信息的行为;发现包含个人敏感数据的文件传入U盘、QQ、微信等,造成客户信息泄露事件;发现文件的隐匿外发行为,包括文件压缩、加密后的外发行为。

运维高危指令监控:Linux系统运维、DBA数据库运维等高危命令监控、B/S应用关键操作标签监控。

弥补传统堡垒机在审计方面的盲点以及堡垒机采集信息不足的问题:堡垒机在工作中经常出现被绕过不能审计的情况,并且在信息采集方面,只能获得运维命令、回显结果等,不能获得窗口标题、B/S运维系统操作标签、POST表单信息等等各个方面的信息,对于Windows应用支持不足。

工作饱和度分析:统计分析电脑上的工作时长,监督开发工作,提升工作效率。

屏幕动态水印:震慑手机或其它设备拍照行为,减少屏幕信息泄露事件,增强屏幕信息安全。

提升审计效率:基于专有技术将录屏和操作行为日志关联播放,实现员工操作行为快速回溯,简化事故调查和根因分析,极大地缩短安全事件调查时间,提升审计效率。

降低审计成本:非现场审计方式,大大减少现场审计工作时间,满足经常性审计监督的需要,且可以扩大审计覆盖面,并降低审计成本;

法规遵从:满足等保2.0中关于桌面云用户行为审计的要求,保障系统安全审计基虚拟

化环境安全；

树立行业榜样，提升公司核心竞争力：率先开展UEBA探索与实践，帮助做好信息安全管理、内控管理和工作效率管理，为信息安全和实现数字化转型服务，助力信息安全、审计、合规以及提高人员工作效率；树立行业榜样，提升公司核心竞争力。

4.2. 飞腾从端到云全栈云桌面解决方案

4.2.1. 应用背景

云桌面是计算、存储、交换资源的虚拟化，在服务器上运行虚拟化操作系统并通过云桌面协议推送到云终端办公使用的技术。在虚拟化技术的支持下，网络软件和硬件设备之间的联系会更加灵活，可拓展性也会大大提升，使得它在教育、医疗、政务等领域迅速成为传统商用PC的替代。

云桌面优势如下：第一：信息安全，所有数据都在云平台，员工本地没有任何数据；第二：维护方便，所有的应用程序和数据都在云平台，可以由维护人员统一安装、统一杀毒、统一升级、统一备份数据，再也不用一台电脑一台电脑的去进行维护了；第三：节能，云终端一般是很多个（几千、几万甚至几十万）用户产生几千瓦或者几万瓦功耗送，平均下来功耗在10万以下。第四：快速部署，新员工报道，领一台云终端，配上外设就能办公；第五：设备更换频率低，普通电脑，一般3~4年后就会因为性能不高需要淘汰更新；而对于云桌面方案，云平台后续发现性能不够时，增加新的服务器和磁阵扩容就可以，使用寿命可达8~10年。

传统PC办公在安全、运维效率等方面存在诸多问题。比如在政企办公存在计算机噪音大、能耗高、故障多、维护难、使用体验差问题；教育行业由于不同课程需要而频繁重新安装大量操作系统、校园网内系统的安全管理困难、教学管理效率低下；医疗行业也存在业务繁多，护士站、挂号室、影像室等不同场景需要 HIS、LIS、PACS、RIS、CIS、OA 等不同系统，维护困难问题。而云桌面解决方案具备部署快、易管理、维护效率高、安全可靠、能耗低等优点，可以有效解决各行业面临的各方面问题。

飞腾作为国内领先的自主核心芯片提供商，致力于“飞腾”系列国产高性能、低功耗通用计算微处理器的设计研发和产业化推广。飞腾CPU基于全自主设计研发的处理器内核，内置硬件级安全机制、飞腾自定义的处理器安全架构标准和多种低功耗技术，具备高性能、低功耗、高可靠和安全可信等特点。飞腾芯片目前拥有高性能服务器CPU、高效能桌面CPU、高端嵌入式CPU和飞腾套片四大系列，形成了完整的自主CPU产品谱系，为从端到云的各型设备提供核心算力支撑。云桌面服务器方面有飞腾腾云S2500、飞腾FT-2000+/64；终端方面有VDI终端芯片飞腾腾珑E2000Q及VDI、VOI飞腾腾锐D2000、飞腾FT-2000/4；其中飞

腾腾锐D2000、飞腾FT-2000/4也可用于VDI终端。

4.2.2. 解决方案

飞腾从端到云的芯片解决方案如下，分VDI、IDV、VOI三个方面：

架构	VDI	IDV	VOI
服务器	飞腾 FT-2000+/64 飞腾腾云S2500	飞腾 FT-2000+/64 飞腾腾云S2500	飞腾 FT-2000+/64 飞腾腾云S2500
终端	飞腾腾锐 D2000 FT-2000/4 飞腾腾珑E2000Q	飞腾腾锐 D2000 飞腾FT-2000/4	飞腾腾锐 D2000 飞腾FT-2000/4
软件	RDP、Clink、Spice优化协议、 国内云桌面厂商协议	不涉及	不涉及
方案体验	基于现有方案： 在日常基本办公或2D场景下 运行良好	基于现有方案： 在日常基本办公流 畅、支持3D图形需求 场景	基于现有方案： 在日常基本办公运行 流畅、支持3D图形需求 场景

（一）云桌面服务器：

1、芯片产品

飞腾提供两款服务器芯片，分别是飞腾腾云S2500及飞腾FT2000+/64。其中飞腾腾云S2500主要规格如下：64×FTC663（2.1GHz）、支持2~8路，128核~512核、8×DDR4、17路PCIe3.0；飞腾FT-2000+/64主要规格如下：64×FTC662（2.0~2.3GHz）、8×DDR4、33路PCIe3.0。

2、生态方面：

基于飞腾芯片的通用型计算、存储服务器都可以用于云桌面服务器。代表服务器生态有长城、浪潮、同方、联想等。

（二）云终端方面：

1、芯片产品

VDI终端有飞腾腾珑E2000Q规格如下：2×FTC664（2GHz）、2×FTC310（1.5GHz）H.264/265解码，2K@30fps、6路PCIe3.0、支持PSPA 1.0安全规范；VDI、IDV云终端芯片有飞腾腾锐D2000、飞腾FT-2000/4，其中飞腾腾锐D2000规格如下：8×FTC663内核（2.0~2.3GHz）、34lane PCIe3.0接口、支持PSPA 1.0安全规范；飞腾FT-2000/4规格如下：4×FTC663内核（2.2~2.6GHz）、34lane PCIe3.0接口、支持PSPA 1.0安全规范。

2、VDI终端生态

基于飞腾腾珑E2000Q，深信服、长城、汉为、云涌、卓怡恒通、亿道、中科网威推出了VDI云终端产品。

3、IDV、VOI终端生态

基于飞腾腾锐D2000、FT-2000/4的普通台式机终端、瘦客户机均可支持。

(三) 视频编码卡

在云桌面视频方面，镭铭微电子Codensity T408 (T408-AIC) 及涌现科技的Seirios-P1VPU编码卡完成飞腾的适配。二者单模块可达4K@60fps或 8x 1080p@30fps编/解码，有效降低服务器芯片计算资源，可支持更多虚拟桌面运行。

(四) GPU透传及3D加速

飞腾的某生态伙伴的信创安全云桌面系统基于自主云桌面显示控制协议，可提供对基于飞腾腾云S2500芯片的宿主服务器上的云桌面提供 GPU 直通虚拟化管理，使云桌面具有与同等配置的物理图形PC工作站相近的3D图形图像显示计算处理性能。

4.2.3. 方案价值

(1) 飞腾云桌面服务器及终端芯片产品，符合信创要求、安全合规且供应链稳定。其基于Arm V8指令集授权100%自主设计，杜绝后门；支持我国的高密SM2/3/4算法、支持PSPA1.0。飞腾也是国产CPU国家队和排头兵，可支撑国家信息安全和重要工业安全。

(2) 飞腾云桌面服务器及终端芯片产品可支持高性能云桌面使用需求。飞腾腾云S2500及FT2000+/64兼容 ARM v8 虚拟化体系结构、支持业界主流的 KVM 虚拟机。假定单虚拟桌面配置为2C/8G内存，飞腾腾云S2500、FT2000+/64单路服务器可以同时支持30-40路虚拟桌面运行。终端方面E2000Q支持2K@30fps硬件解码。可释放CPU算力约70%，提升了视频解码性能。可用于云桌面客户端软件、开源chrome浏览器（如教育课件播放）视频解码优化。同一路1080P视频解码CPU资源占用统计(一路1080P视频解码)，CPU软件解码占用一个CPU core77.2%；VPU硬件解码占用一个CPU core 22.8%，CPU大幅卸载。

(3) 基于飞腾产品的云桌面软件硬件生态繁荣。从云桌面生态方面到服务器、编码卡、GPU卡产品方面，均有大量生态伙伴基于飞腾适配。可以为客户提供更多方案选择。

4.3. 云岫科技多云融合完全解决方案

4.3.1. 应用背景

云岫信息科技有限公司（简称“云岫科技”），是国家高新技术企业，专心研究应用及桌面虚拟化、人工智能、大数据三大核心技术，专注于企业移动化转型和云计算产品的研发，

在该领域具有深厚的经验；依托渠道合作，云岫科技自研产品行销海内外，部分产品已部署于英国、德国、罗马尼亚、俄罗斯、土耳其、埃及、印度、日本、巴西、墨西哥等国家和地区的数据中心，服务全球客户。拥有一支高素质的研发团队和专业化的服务团队，100%以上员工拥有本科以上学历。

桌面云已成为一种强大且灵活的IT解决方案，在中国推行有15年之久，不同品牌的产品百花齐放，不少客户先后启用多家产品解决方案。桌面云推广过程中，也遇到不少现实问题：客户有多套云桌面而无法统一访问多套异构桌面云架构，云桌面不适用移动开发和嵌入式开发场景，License授权共享和节约使用需求，用户行为审计能力不足；大规模桌面云、异构桌面云的监控和运维问题。具体表现在：

存在多套异构桌面云架构，无法统一视图展示和管理

企业存在多套异构桌面云架构，每套桌面云都拥有自己独立的资源池，无法进行整合和共享，缺乏一个统一的桌面云门户。

1) 没有跨平台的桌面云客户端

由于存在Web安全漏洞，企业可能需要跨平台的桌面客户端来提供更安全可靠的服务，以保护用户数据和防止潜在的网络攻击。

2) 五花八门的认证方式

桌面云普遍跟AD紧密相关，个别基于数据库认证，而用户IT已经多年形成了统一的身份认证系统、单点登录系统，为上桌面云而新建一套认证系统并不符合用户需求，长期困扰上云的客户决策。

3) 无法对账号异常进行告警及阻断

此外，即使用户意识到账号异常活动，但缺乏相应的告警机制和阻断措施，也无法及时采取应对行动，进一步加剧了账号安全性的不足。

4) 没有用户自助服务的功能

在日常使用桌面云系统中，用户可能会遇到一些简单的故障或问题，例如注销用户会话，重启虚机等。然而，一般的流程是用户需要通过联系管理人员来解决这些问题，这往往需要等待、排队、沟通等步骤，不仅耗用户的时间和精力，同时也给维护部门带来了压力和负担。

5) 异构桌面云、不同版本的桌面的集中管理

同个品牌的云桌面，建立多个Farm，或者先后开建多套不同品牌的云桌面系统，此类案例比比皆是。如何统一管理这些异构的虚拟机和云桌面资源，真正实现“云”的按需使用、用之不完的能力，是客户关心的一个关键话题。

云桌面不适用移动APP开发和嵌入式开发场景

目前在各个企业客户，只要是手机真机调试、嵌入式开发，便很难上云桌面。

移动化开发、嵌入式开发，通常需要对接手机真机、嵌入式开发板，需要频繁的向设备烧录。云桌面虽然可以将设备映射进去，但是烧录成功率很低，真机调试不方便。

因此，客户对于手机APP开发和嵌入式开发，通常都还是本地PC开发，但是容易造成数据泄漏，一般只能通过签订保密协议、设置门禁、摄像头等方式来监督和威慑。

没有智能运维监控系统

桌面云系统是一个跨越多层次技术的复杂系统，其中包括：服务器虚拟化技术、操作系统技术（Windows、Linux、Mac OS ...）、网络技术、虚拟化远程传输协议、桌面即应用虚拟化技术、数据库技术、如此多方面多层次技术的综合运用，对运维人员的培训和养成提出很高的要求，特别是企业内部拥有多套异构桌面云系统的情况，因此存在系统运维水平的瓶颈难以克服。由此需要有一整套主动智能的、兼容多套异构桌面云、拥有人工智能技术的解决方案，帮助管理员进行系统监控、故障分析、数据自动汇总、系统调整规划等。

审计软件不支持录音、行为分析不够智能

在桌面云运维管理中，安全事件发生后，我们常常只能依赖有限的系统日志来尝试找出问题的根本原因，而无法真正还原桌面操作的画面和桌面音视频。这使得我们在解决问题时面临困难，同时也无法对责任进行明确追究。特别是在桌面云被广泛用于远程办公的情况下，无法有效监控远程接入用户的操作行为更是一大隐忧。

当前市场上虽然已经有少数厂商提供录屏审计产品，但仍存在不足：不支持录音取证，不支持国产新创桌面操作系统，视频文件大且不方便检索，没有任何人工智能的能力；用户行为监控，缺乏智能，跟应用绑定太深。

效率分析停留在桌管软件时代、未结合桌面云特色

桌面云是一个多人协同工作平台，现有的桌面云系统往往无法对用户的工作效率进行实时监控和分析，这会使管理人员难以及时了解用户的工作情况、工作效率。

4.3.2. 解决方案

为了满足统一访问多套异构桌面云架构、多因素认证方式、账号异常告警及阻断、移动开发辅助、智能监控运维、录屏及工作效率分析等需求，深信服与云岫科技合作，推出了云岫科技多云融合完全解决方案。

本方案中，云岫科技多云融合产品与桌面云相结合，能够实现高效的桌面云使用和管理、提升办公效率和数据安全性、提示移动开发效率、提升开发环境安全性，并且能够进一步针对用户的工作效率进行一定分析。

云岫科技多云融合完全解决方案，主要包括云岫多云桌面融合、云桌面移动化和嵌入式开发、桌面云智能监控运维、音视频审计及用户行为智能分析等多套产品组成。

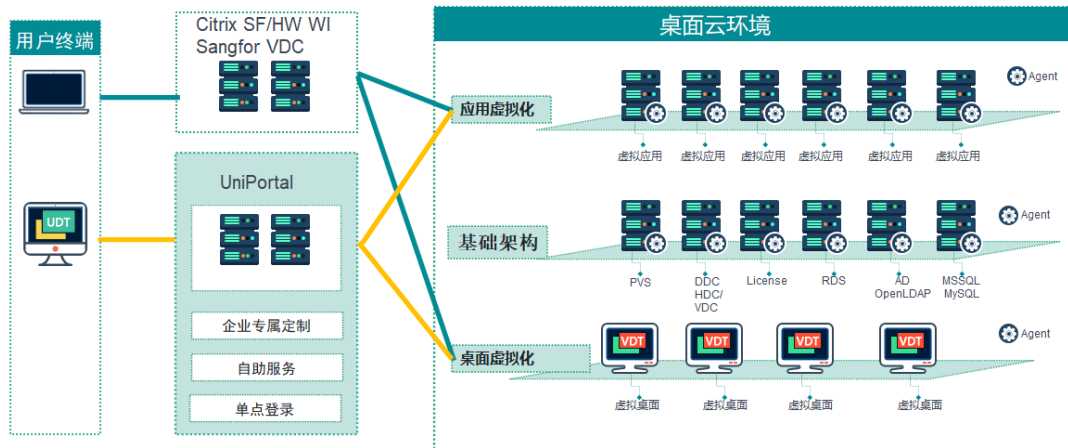
4.3.2.1. 异构云桌面融合解决方案

在过去的15年时间里，云桌面市场一直存在多个品牌的厂商，不少客户先后上线了不同的桌面虚拟化平台，结果造成了多套门户入口，后台管理复杂、运维复杂。为此，客户期望有统一的针对异构云桌面的解决方案，能够兼容Citrix, Huawei, Sangfor, VMWare等品牌。

为了满足客户的需求，深信服与云岫科技合作，推出了多云桌面融合解决方案。涵盖了桌面云资源的统一门户、用户自助处理、多因素认证、安全审计及用户行为分析等多方向关键功能。通过该解决方案，企业可以实现高效的多云桌面使用和管理，提升办公效率和数据安全性。

多云统一桌面云门户 (UniPortal)

- 支持多套异构桌面云统一入口访问，兼容Citrix 5.0及以后所有版本虚拟桌面和应用、兼容Huawei FC/FA 6.5及以后版本、兼容Sangfor aDesk 最新版本，集中访问各个桌面云资源，提高用户访问资源的效率。
- 提供了可定制的企业形象门户，企业可以根据自身需求和品牌形象设计门户页面，并在门户上发布公告和消息通知，方便与员工及时沟通和交流。
- 不依赖AD的认证方式：微信/企业微信扫码，企业单点登录，更有人脸识别认证，提高账号的安全性。同时还提供异常账号告警和阻断功能，及时发现和处理账号异常情况。
- 提供用户自助会话管理和电源管理功能，用户可以根据自身需求进行桌面云相关操作，如重置密码、注销会话、重启虚机等，减轻管理员的工作负担，提高用户满意度。
- 丰富的安全管理能力：内外网、黑白名单、授权、终端检测、系统消息等。
- 提供安全日志：个人轨迹记录个人用户在Portal平台的操作记录，方便用户对自己操作进行跟踪记录，出现异常可以及时核查。系统日志记录所有用户Portal平台的操作记录，方便管理员进行审查与统计。



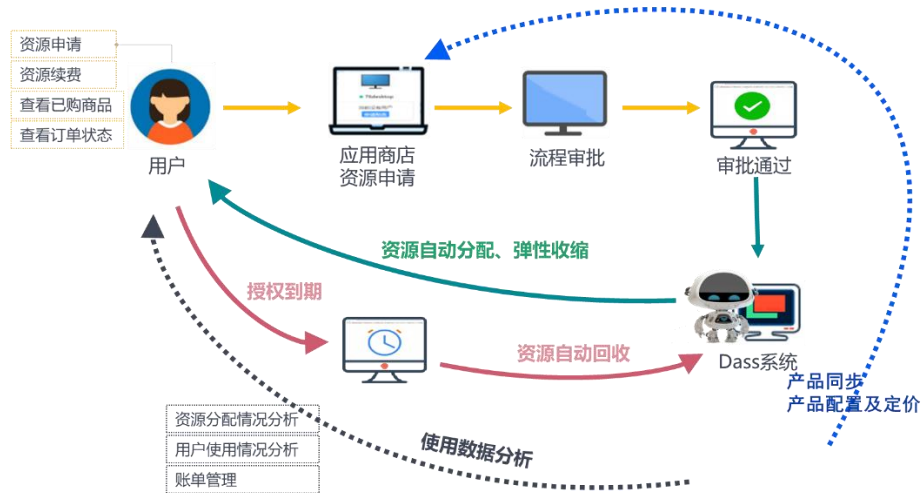
跨平台多云统一桌面客户端（UDT）

- 支持多套异构桌面云统一入口访问，兼容Citrix 5.0及以后所有版本虚拟桌面和应用、兼容Huawei FC/FA 6.5及以后版本、兼容Sangfor aDesk 最新版本，集中访问各个桌面云资源，提高用户访问资源的效率。
- 支持跨平台的桌面客户端（兼容X86和ARM处理器(树莓派)、兼容Windows、Mac和Linux操作系统），用户可以在不同的设备和操作系统上访问桌面云，并享受一致的使用体验，提高灵活性和便利性。
- 支持工作空间(桌面,应用,自助服务)、文档上传下载及记录、本地环境监测、环境监测数据上传、使用帮助FAQ，知识库，升级、本地终端信息、
- 支持不依赖AD的认证方式：微信/企业微信扫码，企业单点登录，更有人脸识别认证，提高账号的安全性。
- 支持短信和OTP等双因子、三因子安全认证；
- 客户端方式屏蔽一切安防漏洞；

后台资源统一管理（Daas）

- 同时对接多种异构桌面和应用虚拟化：
 - 1.兼容Citrix 5.0及以后所有版本虚拟桌面和应用；
 - 2.兼容Huawei FC/FA 6.5及以后版本；
 - 3.兼容Sangfor aDesk 最新版本
 - 4.即将兼容VMWare View桌面
- 同时对接多种异构服务器虚拟化：
 - 1.兼容Citrix XenServer，VMWare ESXi，Huawei FC
 - 2.兼容Sangfor VMP/HCI
- 支持多租户管理，每个租户只能看到所属的资源池，并根据权限级别做管理；
- 资源管理：资源池创建，支持流模式，链接克隆池模式，

- 资源分配：自动分配、手动分配（管多Farm）、HR联动分配、项目组分配、工单联动分配
- 工单申请（申请、变更等）、审批分配
- 会话管理：断开、注销、关机、强制关机、重启、强制重启
- 产品管理：产品上架、下架，产品分配，资源同步、产品定价、产品使用分析、库存管理
- 智能规划、自动启动和弹性扩展
- 生命周期管理：过期提醒、过期时间到，定期重启、空会话重启、未注册重启；帐号回收、资源回收、数据回收；



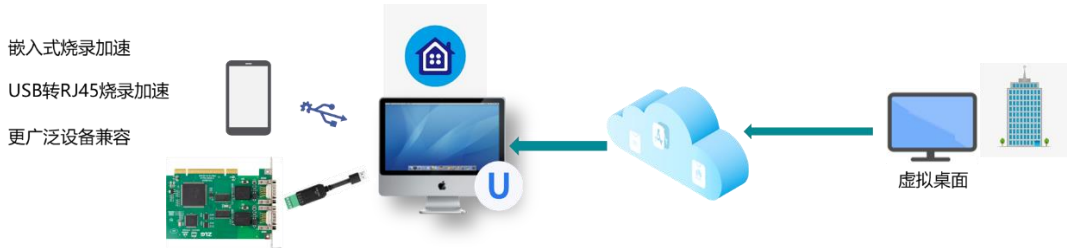
4.3.2.2. 云桌面移动化和嵌入式开发解决方案

目前对于移动APP开发和嵌入式开发，有四个选项：

#	方案描述	问题	
选项 1	本地 PC 开发、烧录	安全漏洞较多 不支持远程开发、不能灵活开发	
选项 2	每个区域就近部署虚拟桌面	不是每个区域都有硬件资源 扩展性差	
选项 3	云桌面开发； 安全软件检测 + 文件摆渡（从研发桌面传到本地 PC）； PC 本地烧录；	步骤繁琐、动作不连贯	云岫 AV 云岫 DSC

选项 4	创新的 MDW 技术： -云桌面开发、调试； -云桌面触发终端进行烧录	无	云岫 MDW
------	---	---	--------

“选项4”是云岫科技率先提出和实现的“移动开发辅助软件”（Mobile Device Writer，简写MDW）方案，将移动APP开发、嵌入式开发锁定在云桌面，数据高速传输，数据不落地、可审计；支持云端调试；成功率100%；



该方案中，用户PC端下载和烧录的文件，后台管理员可事后审计+数据保险箱
-可查看日志，显示用户在“什么时间、安装了什么安装包，成功还是失败”。
-文档被锁在安全保险箱，支持以应用虚拟化方式在线打开文档，数据不落地。

用户ID: IP: 开始时间: 结束时间:

用户	IP地址	文件名	时间
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:26:50
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:32:09
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:34:09
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:36:33
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:37:40
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:37:51
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:38:15
Administrator	192.168.2.41	app-debug.apk	2022-07-15 15:45:40
mac	192.168.2.41	app-debug.apk	2022-07-29 13:48:41
mac	192.168.2.41	app-debug.apk	2022-07-29 14:55:49

上一页 1 下一页

4.3.2.3. 桌面云智能监控运维方案

桌面云运维管理员的日常工作一般有：日常运维、故障处理、数据分析、系统调整规划等等，目前技术难度大、技术手段缺乏，主要靠手工处理，存在被动处理故障、故障处理效率低、用户体验无法感知、业务数据收集与分析困难等等问题，导致系统运转效率难以提高，用户满意度低，大规模使用推广难以执行。

在数字化转型的时代，获取和存储专业、全面、细致的桌面云运行数据，是高效管理和使用桌面云系统的重要基础。通过CenterView系统，可以实现：

异构桌面云兼容性：通过部署CenterView系统，支持监控及运维企业内部多套异构的桌面云系统，如Citrix、Huawei FC/FA、Sangfor aDesk等。

拥有人工智能专利技术的智能故障定位：通过预设逻辑分析语句确定存在的故障集合，所述故障集合中包含有全部存在的故障；获取故障知识图谱，所述故障知识图谱包含各个故障与对应的故障根因的关联关系；根据所述故障知识图谱对应的根因拓扑图，确定所述故障

集合中每个故障对应的故障根因；根据所述故障根因及预设算法，确定出所述故障对应关键节点，以使得及时根据所述关键节点进行故障处理

系统监控：通过实时监测和分析桌面云系统的各项指标，包括资源利用率、性能表现和安全状态等，及时发现问题，保障桌面云环境稳定和高效运行。

主动巡检：拥有自动化检测功能，实时监测服务器、数据库和应用程序的运行状况。

实时告警：通过监测系统状态、性能指标以及安全事件等，一旦发现异常情况或潜在风险，系统会立即触发告警并发送通知给管理员，以便管理员能够迅速采取行动来解决问题。

多种辅助功能：通过部署CenterView系统，拥有多种辅助功能，深入分析用户或架构的问题，从而更好地解决和优化系统。

案例知识库：案例知识库不仅包括问题的描述和解决方法，还涵盖了解决问题所使用的工具、技术和步骤等详细信息。管理员和其他用户可以通过案例知识库来查找并获取相关的解决方案，从而快速解决类似问题，提高工作效率和减少重复劳动。

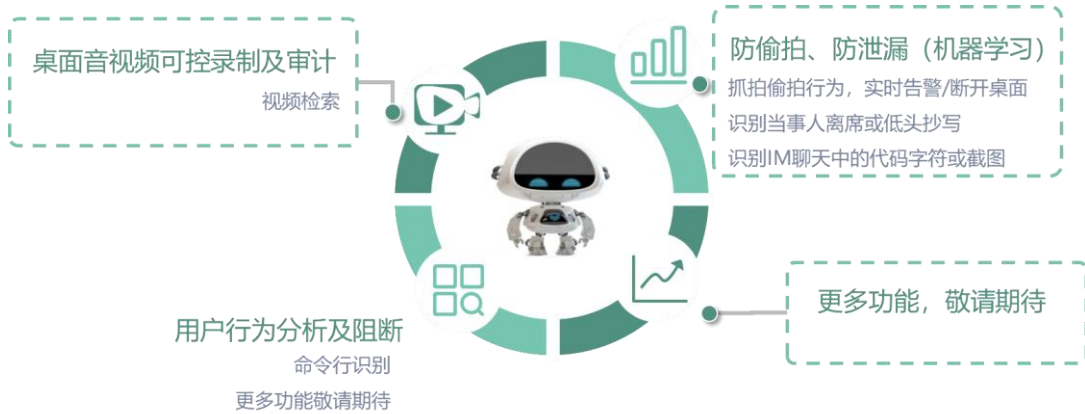
丰富的报表功能：拥有丰富的报表功能，包括用户登录记录，Agent运行状态等多种报表，满足管理员日常工作需求。



4.3.2.4. 音视频审计及用户行为智能分析解决方案（AuditView）

针对当前市场上的录屏审计和行为分析产品的诸多不足，深信服与云岫科技合作，推出了带智能的桌面云操作行为审计方案。本方案中，录音、录屏审计与桌面云相结合，能够有效提高开发环境安全性，并且能够进一步针对用户的工作效率进行准确分析。支持统信UOS及麒麟等信创系统。系统支持AD和非AD两种桌面。

系统根据策略自动监控记录桌面云内重点关注的用户的操作行为，并通过独有的人工智能技术，实现云桌面内用户的风险行为和异常行为监控、行为审计与追溯。



录音与录屏、人工智能视频检索：

通过部署在虚拟桌面上的客户端程序，实现桌面录屏、录音，捕获键盘、鼠标以及应用窗体事件的功能，占用资源少，产生的文件小，视频播放平滑。通过视频识别人工智能专利技术，支持基于文本或图片检索定位视频。进一步对视频进行标签化管理，以便进行文字检索和在线播放；同时为用户行为和工作效率分析提供可靠的数据依据。

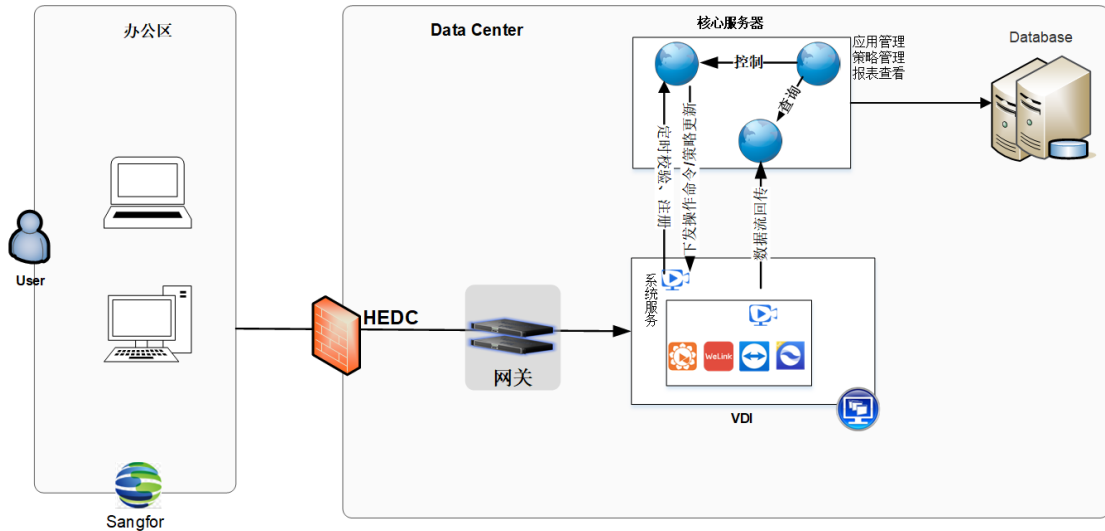
AI赋能的行为审计及阻断：

AuditView能够实时追踪和记录用户在系统中的操作行为，收集详细的日志信息；通过独有的视频格式及视频识别人工智能技术，可以近乎实时识别特定的危险行为（如通过IM软件往外发送代码）和输入的命令行。行为告警和报表分析工具帮助我们及时发现异常行为并生成详尽的报表，而桌面行为定位回放及监控工具可以实时监测和记录用户的桌面行为。这些工具的应用使我们能够深入了解用户行为、保障系统安全，并优化用户体验和界面。

应用授权分析与阻断：

AuditView产品开创性提出“授权分析与阻断”功能，节约昂贵软件的License：

- 系统自动监控专门应用的空闲时长；
- 空闲时长超出设定时间的，保存文件并关断应用，从而释放License
- 与虚拟桌面的空闲会话策略无关，释放特定软件许可，并不需要注销整个会话



业务相关的效率分析：

AuditView基于虚拟桌面会话状态，通过岗位关联应用，通过应用的实际被操作时间得出每个个体用户的工作时长；这与当前包括桌管软件在内的一些“效率分析”算法有本质不同。真正体现出了用户的有效工作时长，为进一步判断用户效率提供了数字依据，这为管理者优化企业管理制度和考核员工工作量提供客观的决策依据和参考。

AuditView支持可视化图表展现用户工作时长、了解员工的工作饱和情况，通过工作效率率图表，可以查看指定时间内各部门整体的工作效率，并进行个体用户的深入分析。支持关注特定用户使用时长并通过消息形式主动通知管理者。

数据分析结果支持以邮件等多种方式主动告警通知管理者。同时，也支持提供对外API接口，供专业人事系统调用和回放

4.3.3. 方案价值

在桌面云内部署云岫科技多云融合完全解决方案，可以满足多桌面融合管理、解决了长期以来原生APP开发上云困难、多云桌面全方面运维监控、行为审计及员工工作效率分析的需求，让员工创造更大的价值。

支持信创系统：产品支持信创虚拟化系统，包括统信UOS、麒麟等。

提升用户体验：兼容多种桌面云架构，如Citrix、Huawei FC/FA、Sangfor aDesk等，通过统一门户访问，用户可以方便地访问不同桌面云，并享受统一的用户体验。无论是使用何种桌面云架构，用户都能够获得一致的操作界面和便捷的访问方式，提高用户体验和操作的便捷性。

加强安全性和风险控制：采用多种安全措施，如人脸识别认证方式、异常账号告警和阻断功能等，有效提高账号的安全性。通过引入人脸识别认证，确保账号的身份验证更加可靠；通过异常账号告警和阻断功能，及时发现并处理异常账号行为。此外，系统还拥有系统安全

审计功能，能够实时监控和记录用户的操作行为，以满足合规性要求，保护系统和数据的安全。这些安全性和风险控制措施有助于增强整个系统的安全性，为用户提供更加可信赖的服务。

跨平台的桌面客户端：UDT客户端支持web门户所有功能，兼容X86和ARM处理器，以及Windows、Mac和Linux操作系统，实现跨平台的桌面云服务。

提高资源利用率：该方案通过自动分配/回收“应用和桌面”资源给用户，优化资源利用率，降低成本。同时具备自主服务和流程自动化功能，大大减轻了管理员的工作负担，提高了工作效率。

实现原生APP开发和调试的便利性与安全保障：解决了长期以来原生APP开发上云的困难，提供了远程开发和调试的便利性。同时也可以进行嵌入式开发，将调试包下发到开发板进行仿真调试。此外，使用PC作为通道，在数据不落地的情况下支持远程开发，并且提供事后审计的功能。兼容Sangfor aDesk虚拟化桌面。因此，该产品解决了开发效率、真机调试、核心代码安全防护等问题，让远程的原生APP开发和调试成为现实，并带来巨大的价值。

移动开发模块与虚拟桌面相结合，能够保证移动开发各项工作的顺利开展，保障开发安全和开发效率，保障疫情情况下的远程移动化开发。

提升IT维护效率：拥有多套异构桌面云系统的集中管理和自动隔离功能，管理员无需登录多个管理平台，可以一站式处理多个桌面云系统。异常应用/桌面自动隔离能够自动将超出设定阈值的机器置于维护模式，保证系统稳定性。智能规划工具从用户使用虚拟桌面的过程中占用的CPU、内存、磁盘性能、网络性能进行数据统计，给出资源规划建议。这样可以节省管理员的时间和精力，提高故障处理效率。

提升故障处理效率：一种基于人工智能专利的故障根因推断定位方法，通过预设逻辑分析语句确定存在的故障集合，所述故障集合中包含有全部存在的故障；获取故障知识图谱，所述故障知识图谱包含各个故障与对应的故障根因的关联关系；根据所述故障知识图谱对应的根因拓扑图，确定所述故障集合中每个故障对应的故障根因；根据所述故障根因及预设算法，确定出所述故障对应关键节点，以使得及时根据所述关键节点进行故障处理。

实时监控与故障发现：系统支持定时拨测、模拟用户访问和应用打开过程，帮助管理员及时了解系统的可用性状态。同时，系统能够通过多路径告知管理员系统异常信息，管理员可以第一时间收到故障信息并及时处理。这种实时监控和故障发现的能力可以减少故障对业务的影响，并提高故障处理的效率。此外，系统还提供经验共享的功能，通过案例知识库和管理员的经验共享，提升维护知识，进一步提高问题处理效率。

录屏审计能力：通过录屏和事件捕获，企业可以全面了解员工在虚拟桌面上的音频、应用操作、键盘鼠标操作等。通过人工智能专利技术进行关联匹配和标签化管理，企业可以轻松检索和回放特定时间段内的行为记录。

全面了解员工的工作行为：通过行为审计与追溯技术，企业能够实时监控员工在虚拟桌面上的操作情况，包括应用使用、键盘鼠标操作等。这种全面了解员工的工作行为有助于发现潜在的工作瓶颈和低效操作。通过及时发现和解决问题，可以提高员工的工作效率和质量，进一步提升整个团队的绩效。

AI赋能的行为审计及阻断：实时追踪和记录用户在系统中的操作行为，并收集详细的日志信息。应用空闲监视能力能够监控系统的空闲状态，进而自动关闭不必要的应用程序，以提高系统效率和节省能源。同时通过操作安全分析能力，我们可以对用户的操作进行安全性评估。行为告警和报表分析工具帮助我们及时发现异常行为并生成详尽的报表，而桌面行为定位回放及监控工具可以实时监测和记录用户的桌面行为。

4.4. 海光桌面虚拟化解决方案

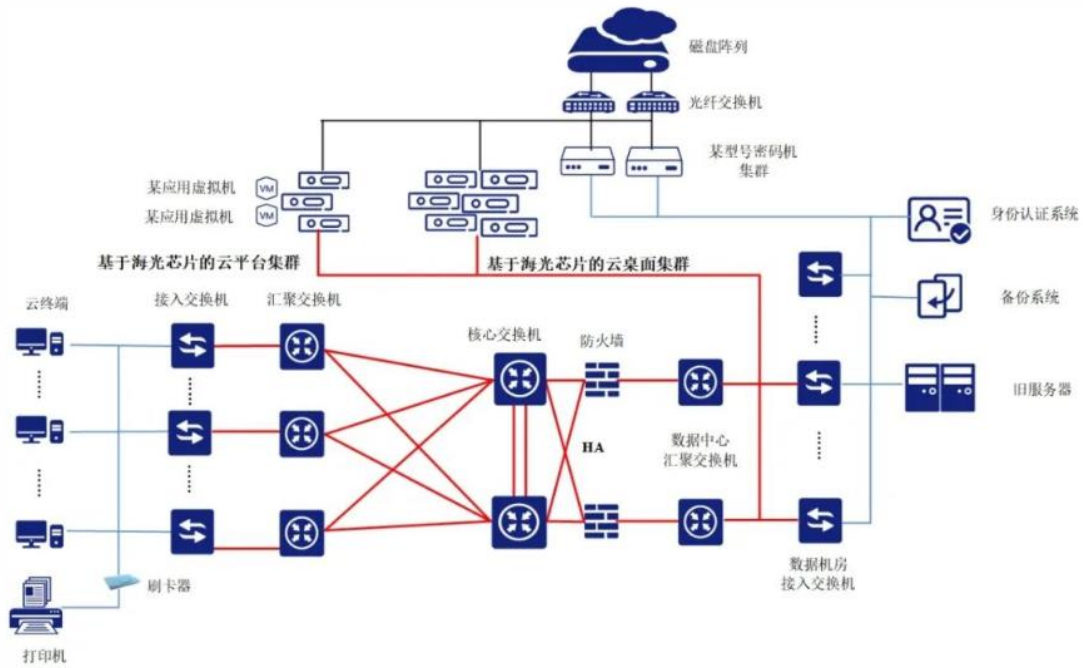
4.4.1. 应用背景

海光信息技术股份有限公司主要从事高端处理器、加速器等计算芯片产品和系统的研究、开发，目标成为世界一流的芯片企业，为数字中国提供核心计算引擎。作为国产先进微处理器产业的推动者，海光信息以务实的态度、创新的理念、先进的技术和可靠的产品，致力于促进我国信息产业核心竞争力的提升。

海光处理器兼容市场主流的x86指令集，具有成熟而丰富的应用生态环境海光处理器内置专用安全硬件，支持多种先进的漏洞防御技术，内置高性能的国密协处理器和密码指令集，支持可信计算的国内、国际标准，支持领先的机密计算技术，能够进行主动安全防御，通过了相关权威机构的安全测试，满足信息安全、数据要素安全流通的发展需求。面向桌面云、企业计算、云计算数据中心、大数据分析、人工智能、边缘计算等众多领域，海光信息提供了多种形态的海光处理器芯片，满足互联网、电信、金融、交通、能源、中小企业等行业的广泛应用需求。

4.4.2. 解决方案

海光公司致力于成为中国最重要的计算机芯片设计企业，为中国信息产业的强盛提供核心计算引擎。通过几年的努力，海光先后设计并量产了完全兼容x86生态的处理器产品，达到了国际主流CPU同等技术水平。海光处理器提供从4到32物理核心，8到64线程，最多128PCIe扩展，8通道内存支持，以及针对虚拟机性能优化的大容量缓存设计，能够为桌面云、云计算、大数据推分析、分布式云存储、Web应用，人工智能、数据库等众多场景，提供强劲计算能力。基于海光芯片能够为桌面云系统提供云平台集群、云桌面集群等，助理桌面云解决方案的高效、安全实施和部署。



基于海光CPU的桌面云系统

海光处理器能够为桌面云提供内生安全属性，助力桌面云实现安全特性。海光处理器具有高性能和高安全性的特点，能够给各种行业应用提供足够的算力，同时保证运算过程和运算结果安全可信。海光处理器在设计上采用权限划分、加密、隔离等技术来保证安全性。处理器内各个模块的安全属性不同，有些模块用来完成通用计算，安全级别低，有些模块需要访问密钥等敏感数据，安全级别高。在处理器设计时，根据不同的安全属性在处理器内部划分不同的安全域，使各个安全域的模块能够协同工作但是不能跨域访问，保证敏感数据的安全性。海光处理器内置安全处理器（Platform Secure Processor, PSP），支持安全启动、国密加速、内存加密、机密计算、可信计算等安全技术。综合选用这些技术，可以实现从底层固件到上层应用软件的整体安全。

安全处理器：

桌面云技术可使用海光CPU的安全处理器提升安全性。海光处理器中的C86核心用来进行通用计算，安全处理器用来进行安全管理。安全处理器比C86核心具有更高的安全权限，可以访问芯片密钥等安全资源，C86核心不能访问这些安全资源。安全处理器有自己的ROM、RAM，能够访问系统中的内存和设备，芯片上电之后首先执行安全处理器的ROM代码，ROM代码执行完成后，加载执行存储器中的安全处理器固件，固件执行完成后，安全处理器激活C86核心开始运行，此后安全处理器运行固件，C86核心运行用户操作系统，两者同时运行。安全处理器具有更高的安全权限，用来实现芯片的安全管理。C86程序通过安全处理器固件提供的接口调用安全处理器实现的安全服务。

安全启动：

桌面云技术可使用海光CPU的安全启动技术提升安全性。安全启动功能保证芯片上电

启动后运行的软件是合法的，非法的软件导致启动流程失败，芯片不能正常工作，以此来保证用户的程序运行在安全的软件环境中。海光处理器内置了固件验签公钥，固化的ROM代码使用此公钥验证被加载固件的签名，通过验证的固件使用BIOS厂商的公钥验证BIOS代码的签名，通过验证的BIOS代码使用操作系统厂商的公钥验证操作系统的签名，只有签名合法的软件才能被加载并执行，否则启动过程中止，保证了整个启动流程是安全的。

国密加速：

桌面云技术可使用海光CPU的国密加速功能提升安全性。海光通过密码协处理器（CCP）和指令集（ISA）两种方式实现了国密算法。密码协处理器置于CPU内部，包含商用密码算法SM2、SM3、SM4和真随机数发生器(TRNG)。通过综合利用密码协处理器和密码指令集，可以有效提升国密加解密、签名验签、以及TLS、IPSec等密码协议的性能。支持OpenSSL、BabaSSL、DPDK、VPP等开源软件库。

内存加密：

桌面云技术可使用海光内存加密功能保护用户的运行时数据。海光CPU支持实时加解密主机内存数据。海光CPU使用国密SM4算法加密主机系统内存。处理器写入数据至内存时，明文数据被加密后储存于内存中；处理器从内存读取数据时，密文数据实时解密后返回给处理器。实时加解密过程对操作系统和应用程序透明，引入的性能开销在1%以下。系统重启后随机再生成加密密钥，密钥安全性高。

机密计算：

机密计算指利用处理器的可信执行环境保护计算机系统最终用户的数据安全，最终用户处于可信执行环境中的数据具有机密性和完整性。最终用户仅相信基于处理器自身创建的可信执行环境，除处理器本身外，主机操作系统，虚拟机管理器，系统管理员等被认为是不安全的实体，不需要被最终用户信任。

在桌面云系统中，海光CPU可构建以安全加密虚拟机为基础的可信执行环境。安全加密虚拟机的cache和TLB等资源独立，与其他安全加密虚拟机和主机隔离。安全加密虚拟机支持启动镜像度量和运行时远程身份认证，度量和认证结果由处理器签名，主机操作系统和虚拟机管理无法伪造。安全加密虚拟机支持内存实时加解密，主机操作系统和虚拟机管理器无法获取，密钥由处理器随机生成并管理，永不外泄。在安全加密虚拟机保证了虚拟机数据机密性的基础上，更进一步保证了虚拟机数据的完整性，主机操作系统和虚拟机管理无法通过改写虚拟机嵌套页表对虚拟机实施重映射攻击。

可信计算：

海光CPU支持原生可信，相比外置可信硬件模块，CPU内置的可信模块具有安全性高、使用成本低且更易用的优点。海光CPU同时内置国际和国内主流可信计算标准支持，支持TPM2.0，支持TCM2.0以及TPCM可信计算3.0体系架构。相比传统外置可信模块，海光CPU原生可信支持具有安全性、易用性及性能上的显著优势。在桌面云系统中，海光CPU可为桌

面云用户提供物理机、虚拟机级别的可信计算，提升系统安全性。

4.4.3. 方案价值

海光CPU的桌面云解决方案，为用户带来强劲算力的同时，具有如下方案价值：

兼容性：

- 支持国产和国际主流Linux操作系统
- 支持多个版本的主流x86操作系统
- 全面兼容国内外关键云应用
- 支持国产和国际通用商用数据库
- 支持与国内外主要AI加速卡进行适配
- 支持主流AI厂商算法

安全性：

- 内置专用安全硬件，支持通用可信计算标准
- 构建具有主动防御能力的新一代可信计算平台
- 提供芯片级信任根，可解决各类潜在安全漏派
- 免疫“熔断漏洞”，修复了“幽灵漏断”

4.5. 麒麟软件银河麒麟操作系统桌面云解决方案

4.5.1. 应用背景

麒麟软件有限公司（简称“麒麟软件”）是中国电子旗下科技企业，由天津麒麟信息技术有限公司和中标软件有限公司整合而成。

麒麟软件主要面向通用和专用领域打造安全创新操作系统产品和相应解决方案，以安全可靠操作系统技术为核心，现已形成桌面操作系统、服务器操作系统、智能终端操作系统、嵌入式操作系统、麒麟云、操作系统增值产品为代表的产品线。麒麟软件旗下品牌包括银河麒麟、中标麒麟、星光麒麟。麒麟操作系统能全面支持飞腾、鲲鹏、龙芯等主流国产CPU，在安全性、稳定性、易用性和系统整体性能等方面远超国内同类产品，实现国产操作系统的跨越式发展。目前，公司旗下产品已全面应用于党政、金融、交通、通信、能源、教育等重点行业，服务用户覆盖所有的中央部委、政府机关、地市党委。根据赛迪顾问统计，麒麟软件旗下操作系统产品连续12年位列中国Linux市场占有率第一名。

应用场景一：为云桌面资源池和管理平台提供可靠稳定的安全底座

麒麟软件旗下产品——银河麒麟高级服务器操作系统V10为云桌面资源池和管理平台提供可靠性、安全性、高性能、高扩展性的服务器操作系统。该产品为依据CMMI5级标准研制的提供内生安全、虚拟化支持、国产平台深入优化、高性能、易管理的新一代自主服务器操作系统；同源支持飞腾、鲲鹏、龙芯、兆芯、海光、Intel/AMD架构的处理器，并对上百款的读写、存储、网络设备提供了驱动支持；可支撑构建大型数据中心服务器高可用集群、负载均衡集群、分布式集群文件系统、虚拟化应用和容器云平台等。

应用场景二：为虚拟化层提供简单易用的安全虚拟桌面

麒麟软件旗下产品——银河麒麟桌面操作系统V10为虚拟化层提供适配国产软硬件平台并深入优化和创新的简单易用、稳定高效、安全创新的新一代图形化桌面操作系统。实现了同源支持飞腾、龙芯、申威、兆芯、海光、鲲鹏、海思麒麟等国产处理器平台和Intel/AMD等国际主流处理器平台；界面风格和交互设计全新升级，提供更好的硬件兼容性。系统融入更多企业级使用场景，增加多种触控手势和统一认证方式，自研应用和工具软件全面提升，让您的办公更加高效；注重移动设备协同，优化驱动管理，引入可信安全计算体系，封装系统级SDK，操作简便，上手快速。

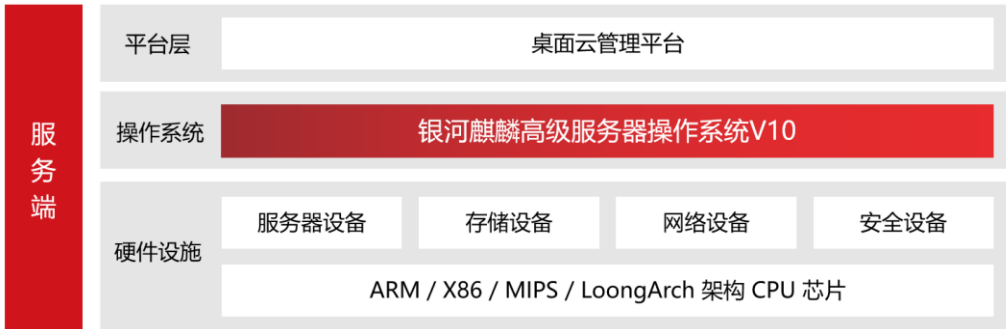
应用场景三：为终端提供按需定制的安全终端操作系统

麒麟软件旗下产品——银河麒麟桌面操作系统V10和银河麒麟嵌入式操作系统V10提供面向桌面云场景终端设备的操作系统。其中银河麒麟嵌入式操作系统V10是基于银河麒麟桌面操作系统V10作为基线，继承了银河麒麟通用操作系统在安全创新、生态丰富方面的先进优势，具有嵌入式芯片兼容性广泛、生态丰富、轻量化系统设计、灵活定制开发等优点，可满足嵌入式场景对操作系统小型化、可靠性、安全性、实时性、互联性的需求。支持主流瘦客户机嵌入式CPU，搭载轻量化UKUI桌面，实现系统小型化，资源占用少，可灵活运行在2G内存+8G存储环境下，并具有多显示支持、视频硬解码、安全套件、定制文件系统、快速工厂批量安装、快速开机优化等功能。

4.5.2. 解决方案

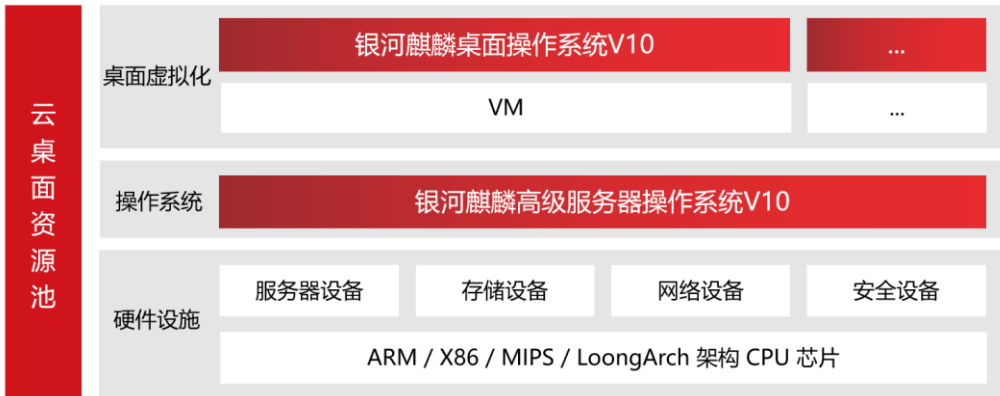
管理平台解决方案：

以飞腾、鲲鹏、龙芯、兆芯、海光、Intel/AMD等主流处理器的服务器为硬件底层设备，承载银河麒麟高级服务器操作系统V10作为软件底层操作系统，搭载桌面云管理平台，为硬件层与平台层提供稳定、安全、可扩展、高性能的桥梁。



云桌面资源池解决方案：

以飞腾、鲲鹏、龙芯、兆芯、海光、Intel/AMD等主流处理器的服务器为硬件底层设备，承载银河麒麟高级服务器操作系统V10作为软件底层操作系统，对虚拟化技术具有良好的支持；并通过虚拟化技术运行银河麒麟桌面操作系统V10作为虚拟化的操作系统，提供简单易用、生态丰富的图形化桌面，适用于企业级各种办公场景。



云终端解决方案：

根据终端硬件配置提供银河麒麟桌面操作系统V10或嵌入式操作系统V10作为软件底层操作系统，支持PC、瘦终端、胖终端、平板等设备，提供按需定制、简单易用、生态丰富的操作系统。



4.5.3. 方案价值

服务器层面：为桌面云资源池和管理平台提供内生安全、虚拟化支持、国产平台深入优化、高性能、易管理的新一代自主服务器操作系统。

- **同源优化支持自主CPU，提供丰富的软硬件生态：**同源构建支持六大平台，内核、核心库和桌面环境等所有组件基于同一套源代码构建，并面向各自主CPU及服务器整机进行了针对性优化适配，为不同平台的软硬件生态提供兼容一致的开发和运行接口，为管理员提供一致的运维管理体验。
- **一体化内生本质安全，提供专业的安全防护：**基于自主软硬件、密码技术的内核与应用一体化的内生本质安全体系：自研内核安全执行控制机制KYSEC、生物识别管理框架和安全管理工具，支持多策略融合的强制访问控制机制；支持国密算法SMx和可信计算TCM/TPCM、TPM2.0 等；达到GB/T20272第四级。
- **虚拟化及云原生支持：**优化支持 KVM、Docker、LXC 虚拟化，以及 Ceph、GlusterFS、OpenStack、k8s 等原生技术生态，实现对容器、虚拟化、云平台、大数据等云原生应用的良好支持。
- **高可用性支持：**通过XFS文件系统、备份恢复、网卡绑定、硬件冗余等技术和配套磁盘心跳级高可用集群软件，实现主机系统和业务应用的高可用保护。
- **国产平台功能和性能深入优化：**针对不同自主CPU平台在内核安全、RAS 特性、IO性能、虚拟化和国产硬件（桥片、网卡、显卡、AI 卡、加速卡等）及驱动支持等方面优化增强。

桌面层面：为终端和虚拟化桌面提供适配国产软硬件平台并深入优化和创新的简单易用、稳定高效、安全创新的新一代图形化桌面操作系统。

- **主流硬件全面支持：**与国内外主流CPU做了深入优化，充分发挥处理器性能。支持大多数基于国产处理器平台的整机，适配了市场上主流的打印机、扫描仪、高拍仪、摄像头、投影仪、指纹仪、读卡器、手写板等外设设备，满足绝大多数用户的外设使用需求，同时针对特殊场景，增加触摸屏和触控板的支持，通过不同手势进行操作。
- **交互体验全面提升：**大道至简，衍化至繁。遵循通用操作交互习惯，融入移动操作交互长处；采用卡片式设计模拟自然界中物体的层叠组合，还原事物原本的模样；轻质感、微渐变、圆角、毛玻璃效果的图标，赋予界面温度和亲和力。
- **软件商店内容丰富：**为用户提供内容丰富的图形化软件管理工具，通过搜索、下载、安装、更新、卸载进行软件应用的一站式管理。不仅可以快速搜索需要的软件，还可根据具体需求，通过商店的分类查找相关的软件。每款上架的软件都有详细的软件信息以供参考，可根据实际需要进行下载安装。

- **系统安全能力提升：**通过安全中心对系统进行安全体检、账户保护、网络保护、病毒防护、应用保护与设备安全等；支持可信启动，通过指令流安全预检测技术测试检测系统安全，可发现未知漏洞发起的攻击。通过文件保护箱对特殊目录进行数据隔离与加密保护；通过日志查看器实现系统日志内容的分类显示和结构化解析。
- **灵活定制的终端：**为瘦终端设备提供具有银河麒麟桌面操作系统V10特性的、系统轻量化、嵌入式芯片兼容性广泛、灵活定制的嵌入式操作系统，并具有多域隔离、功耗管理、掉电保护、实时性增强等特性。

4.6. 连用科技内容安全协同解决方案

4.6.1. 应用背景

深圳连用科技有限公司成立于2008年，是国内非结构化数据管理的先行者，一直致力于为客户提供海量非结构化数据存储管理和安全协同应用的全融合、一体化、本地化、智能化的解决方案。产品应用行业遍及政企、金融、军工、能源电力、大型制造业、公检法、医疗、教育等。

桌面云已经提供了良好的数据隔离、数据防拷贝、数据防泄漏功能，但数据是需要流动中才能更好的创造价值，包括但不限于以下应用场景：

- 生产数据借用，生产/业务系统导出的报表数据安全传输到办公网或者分发到营业网点；
- 研发新编译版本测试，从研发网桌面云外发到测试环境的物理机；
- 财务报告外部审计，从财经桌面云中外发到互联网域的PC；
- 敏感数据跨隔离网络的流转，涉敏文件通过网闸进行安全流转；

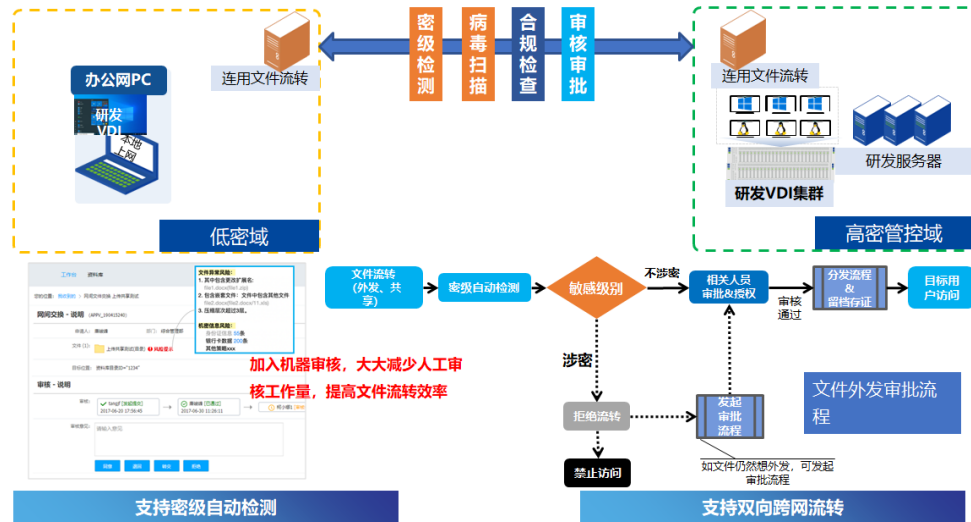
怎么样确保这些场景下的数据安全流转协同，既能符合法律法规和行业监管的要求，又能满足企业自身管理规范，让数据创造更大价值，是连用科技内容安全协同解决方案的建设目标。

4.6.2. 解决方案

为连用内容安全协同解决方案与深信服桌面云相结合，旨在为企业建立安全可信的内外部协作渠道，打造集个人生产力、团队协作和跨网数据流转的一体化协同平台。基于连用文件云海量数据安全存储、统一管理底座，拥有网间文件安全交换、文件邮件安全交换、办公云盘、团队协同空间、AI能力摆渡、微应用等多个能力，全面提升企业内容协作维度，满足企业数字化转型过程中内容管理的共享协同需求。

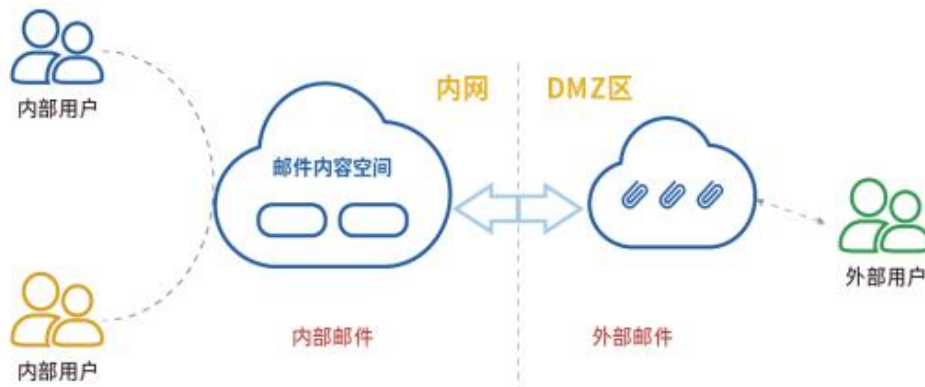
1、网间文件安全交换

连用通过网间文件安全交换能力，为深信服桌面云构建了安全可信的文件流转管控渠道。基于对文件交换场景分析，以内、外网系统独立、网闸、细粒度的文件权限管控、敏感词检测和文件定级、动态水印、线上浏览编辑和防病毒等能力，确保文件交换的安全高效和可管、可控、可审计。使企业可以高效便捷地在内外网之间传输文件，无需担心数据泄露或被篡改的风险，构建安全可信的企业内部、外部内容共享协作渠道，让数据在流动中创造价值。



2、网间邮件安全交换

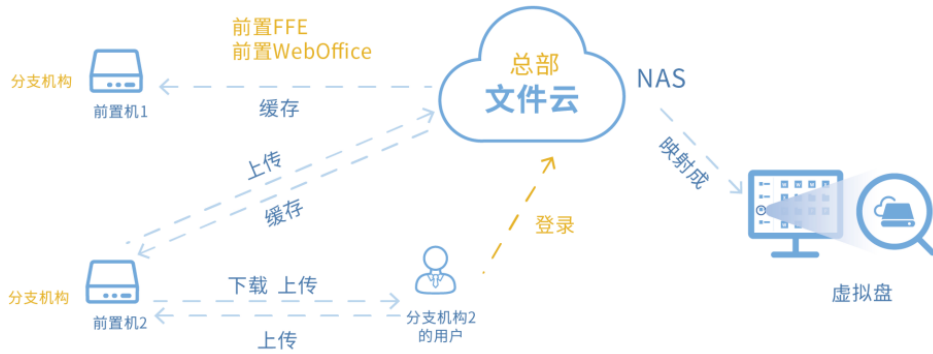
连用的网间交换还能提供邮件安全交换能力，实现在隔离的虚拟桌面中也能安全的与外界进行邮件收发。支持对外发邮件进行内容检查，确保外发内容的安全合规；支持分级审批，根据内容敏感程度自动关联对应的审批流程；支持附件链方式，实现外发数据不落地。



3、办公云盘

同时为深信服桌面云提供了安全高效的办公云盘，通过归集企业内部分散的海量办公数据，集中存储，统一管控，并提供安全、可靠的内容数据全生命周期管理，有效防范数据丢失、勒索病毒攻击。拥有安全共享协同，在线预览编辑，智能化内容识别，多终端接

入等能力，让企业用户轻松实现移动办公，提升业务处理效率。还支持NAS挂载映射为本地虚拟盘，大大降低开发成本。



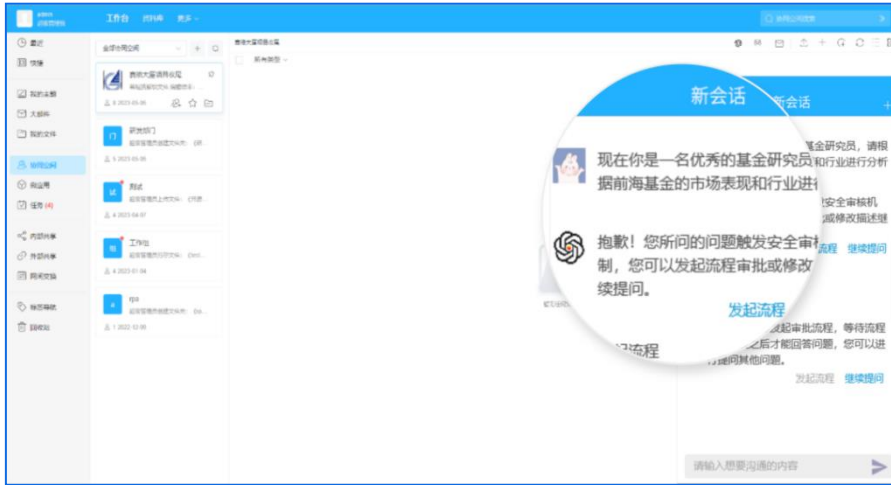
4、团队协同平台

在提升桌面云用户项目内容协作和项目信息扁平化管理方面，支持以项目组队的形式进行内容协作，可汇聚项目相关的文件、邮件、第三方IM消息，并支持项目计划管理。集成企业微信后，协同空间管理员可将协同组和企业微信群进行关联，获取到相关群的聊天记录信息并进行内容归档管理。支持本地内容通过一键共享、一键交换、双向自动同步等能力，使项目协作更顺畅、内容更齐全，全面提升日常工作内容协同效率。



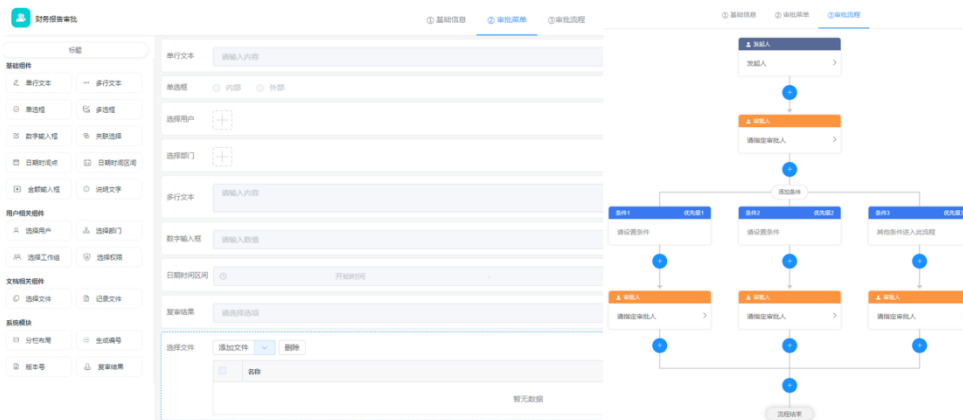
5、AI能力摆渡

通过连用的网间安全交换能力，还能实现在虚拟桌面内网中，也能安全使用公网的AIGC能力（ChatGPT、百度文心一言等）。支持对提问内容进行安全监控、消息内容审计，在安全合规的前提下，协助客户快速获取信息和答案、提供数据智能分析和洞察能力，帮助客户进行智能决策、节省客户时间和精力、提升工作效率和降低成本。



6、微应用

为虚拟桌面用户提供低代码轻量级业务流程应用，可以自定义表单，自定义审批流程和任务，实现虚拟桌面针对文件的自定义审批协同功能，满足业务在各种复杂场景下，对文档数据进行流程管控的需求。



4.6.3. 方案价值

连用科技在企业内容管理软件领域深耕十余年，始终致力于数字化内容安全管理和协同平台的研发，并坚持以客户需求为先，通过对产品不断的打磨，其安全性、稳定性、可靠性和易用性完全满足客户多样化的数据管理需求。并通过与深信服桌面云方案的强强联合，帮助企业内外部数据安全合规高效的共享协同，让数据在流动中创造更大的价值。

- 真正的安全隔离，支持网闸/光闸，实现隔离网络的数据安全流转。
- 以项目组队的形式进行内容协作，业务处理效率将提升3倍以上。
- 智能高效的传输能力，支持高速、增量、加密传输和断点续传，提升整体业务效率。
- 数据自动分类分级及合规脱敏管理，让企业数据可管、可控、可审计，防止敏感信息泄露，确保数据安全。

- 便于企业全面掌控数据资产，支持决策和业务运营，提升企业核心竞争力。
- 支持近百种格式文件在线浏览编辑，本地无需部署软件，审批/查看过程文件不落地，更安全，并降低软件购置成本。
- 企业级病毒查杀能力，文件上传时自动扫描，避免受到勒索病毒侵害。

4.7. 泛云科技 SimCloud 研发云解决方案

4.7.1. 应用背景

上海泛云信息科技有限公司简称“泛云科技”，长期致力于工业研发云计算平台的研发与实践。泛云科技依托企业计算资源计划（Enterprise Computing Resource Planning，简称 ECRP）系列方法论，面向先进制造业的设计、仿真等数字化研发计算业务管理需求，专注淬炼 SimCloud 研发云计算平台管理软件及整体解决方案，可适配私有云、公共云、IaaS/SaaS 混合云等多种基础架构场景，迄今已为百余家大中型企业、研究院所以及超级计算中心提供产品与服务，为中国先进制造业数字化转型打造高效、弹性、安全的算力引擎。

数字化研发创新，是先进制造业、工程建设、勘测设计以及相关科研单位的竞争力源泉，更是“中国制造”向“中国智造”转型升级的核心驱动力之一。在智能制造时代，以 CAD、CAE、EDA、CAM、BIM 为代表的 CAX 类软件及相关计算设备正在被投入大量使用，必然形成种类繁多、规模可观的企业级计算资源，成为泛工业领域数字化创新工作中的重要生产工具。如何科学规范地进行软件资产购置规划与集约化管理？如何高效调度高端数字化生产工具，持续优化研发人员的工业计算体验，科学构建智慧创新协同管理体系？这些疑问已经成为中国制造业无法回避的重要课题。

近年以来，不少企业正在尝试采用桌面云基础架构产品解决以上问题，但是在实践过程中往往遇到若干新难题：

- 1) 针对部分许可证资源紧张的软件工具，迫切需要合法合规的分时调度技术，并通过智能分析用户行为数据，指导企业科学增购软件许可证；
- 2) 针对某些重度三维设计软件，迫切需要简便快捷的资源模板化配置方法，并可在企业内部快速推广特定软件的最佳应用模式；
- 3) 针对某些静默计算型软件（如数值仿真、动画渲染等），迫切需要从桌面云基础架构中剥离，重定向至高性能计算基础架构，并构建生产数据联动机制；
- 4) 针对软件工具生产出来非结构化数据，迫切需要构建规范、统一的生产数据管理机制，并与第三方数据流程管理平台（如 PDM、SPDM 等）形成双向耦合的数据流通路；

.....

针对以上新难题，泛云科技聚合桌面云基础架构、高性能计算调度系统以及工业软件许可证管控技术，统一构建弹性化、可扩展、自学习的企业计算资源管理组件，并可基于此组件发展差异化、跨领域、多焦点的流程协同管理应用，成功推出SimCloud研发云计算平台管理软件。

SimCloud研发云可统一管理数字化研发相关的硬件、软件、数据以及知识，提供办公、设计、仿真等在线服务，充分融合本地化计算资源以及外部互联计算资源，围绕企业研发主体构建一个矩阵式智慧创新空间。

4.7.2. 解决方案

SimCloud研发云科学构建并实现计算资源统一调度策略及管理方法，可以覆盖研发过程中的交互类、计算类软件工具的全过程云端服务，亦可智能监控、统计并分析以软件许可证为代表的企业核心计算资源利用情况。



如上图所示，SimCloud研发云平台可整合、调度、管理多种计算资源池：

- 集群计算资源池

负责集成以CAE求解器为代表的计算类应用软件，并向用户提供并行/并发计算调度与管理服务；

- 虚拟应用资源池

负责集成以CAD设计软件为代表的交互类应用软件，并向用户提供云端交互应用的调度与管理服务；

- 智汇星云资源池

负责提供流程协同类应用服务的统一入口，向用户提供数据、知识等高阶计算资源的调度与管理服务；

●应用许可资源池

负责聚合CAX软件相关的网络浮动型许可证，为计算、应用子平台提供软件授权支撑服务以及软件利用行为数据。

●高速存储资源池

负责储存CAX软件相关的非结构化数据及文件，为计算、应用子平台提供数据支撑服务，亦向用户提供个人数据私密级隔离及管控能力；

●企业云盘资源池

负责提供面向企业、部门或项目组的非结构化数据存储服务，可以在指定组织单元内实现非结构化数据的流通与共享。

在与深信服桌面云产品的协作研发过程中，泛云科技专注于提升工业研发云平台管理能力，同时也注重兼容并蓄、竞合相长，持续丰富SimCloud产品的架构内容与功能特色，进一步强化了产品优势与创新能力：

●基础架构兼容性：

以深信服桌面云为代表的国产IT基础架构技术发展迅猛，结合中国企业数字化转型工作的持续深入，IT基础架构多样性特征必然愈发显著，因此SimCloud研发云平台顺应这一发展趋势，采用“业务中间件 + 基础架构插件”的技术路线，广泛整合相关基础架构技术，从数字化研发业务的视角解构并重塑核心计算服务、监管及运维能力；

●资源服务完整性：

企业级计算资源可以按操作模式划分为计算型和交互型，前者注重计算性能与稳定性，而后者则注重图形表现力与操作流畅度，SimCloud研发云平台是业内首个全面覆盖计算型与交互型计算资源服务能力的云计算架构管理平台。相较于传统的HPC调度平台、桌面云接入门户，SimCloud平台继承并发展了具有更加全面的服务能力、更加便捷的应用体验、更加科学的管控机制；

●服务秩序科学性：

企业计算资源服务的秩序需求存在多样化、动态性、不均衡等明显特征，传统调度软件在企业级应用场景中呈现出异常脆弱的适应性，难以满足企业管理需求。SimCloud研发云平台利用业务中间件解构并转译企业计算资源服务秩序，利用基础架构插件控制计算资源物理调度逻辑，通过二者功能耦合，成功构建面向用户、项目组、部门、软件等业务对象的高效率、科学化服务体系；

●平台接口开放性：

现代化企业级IT系统都是为企业研发、生产工作提供信息化服务的，若计算资源服务平台长期游离于业务流程管理系统之外，必然引发项目—资源匹配差、业务需求—资源供应差异大、计算平台生产数据流失等严重问题。SimCloud研发云平台定位于企业研发流程管理体系之中的资源组件，为业务流程管理系统提供二次开发接口，帮助企业针对现有业务流程管理系统进行升级与扩展，全面兼容云基础架构与核心计算资源服务能力，从而实现从“计算资源服务”到“数据业务引擎”的顺利转型。

4.7.3. 方案价值

SimCloud研发云平台管理系统及相关解决方案完全依托于“企业计算资源计划”系统思想与方法论，在十余年的项目实践过程中已经为众多企业客户构建了科学规范的企业计算资源管理体系，充分验证了其在中国企业数字化转型进程中的独特价值，尤其突出表现在以下六个方面：

- 整合性

SimCloud研发云平台对IT基础架构具备较为全面的整合能力，通过“软件定义基础架构”屏蔽底层IT技术细节特征并进行异构整合与统一，从资源应用的角度入手重新塑造计算资源功能视图，为企业计算业务提供整合性功能支持；

- 高弹性

SimCloud研发云平台采用模块化设计方式，分类别、分层次、泛云化实现计算资源管理能力，覆盖企业计算资源的规划、建设、监控、维护、更新乃至废止等流程环节，为企业计算资源的管理工作提供高弹性业务支持；

- 实时性

SimCloud研发云平台是整个企业的计算资源统一管理平台，全面反映企业计算资源的实时运行状态，及时预警计算资源的能力缺口、异常情况等重要实时信息，为企业计算资源的监管运维工作提供数字化驾驶舱监管能力；

- 绩效性

SimCloud研发云平台在企业计算资源管理业务中引入最佳资源调度规范，形成一系列计算资源服务绩效指标，科学指导企业计算资源服务流程的持续优化，提升计算资源服务能力，为企业计算资源管理工作提供绩效量化评估工具；

- 战略性

SimCloud研发云平台利用精益化管理理念精准解构企业计算资源管理对象及相关管理流程，是在数字化时代针对企业数字化生产要素的崭新审视与深度融合，是创新型企业数字化运营工作中的不可或缺的战略举措；

●可持续发展

SimCloud研发云平台智能感知企业数字化研发业务的变化动态，推动高端计算资源的快速升级与迭代，同时为企业开展工业研发类APP的孵化、研究与推广提供了平台级支撑，可持续完善企业级知识软件工具族，进一步塑造企业自主技术品牌。

4.8. 统信软件统信 UOS 解决方案

4.8.1. 应用背景

统信软件技术有限公司（简称：统信软件），成立于2019年，是中国操作系统的领创企业。统信软件以“打造操作系统创新生态，给世界更好的选择”为愿景，致力于研发安全稳定、智能易用的中国操作系统产品，在操作系统研发、行业定制、国际化、迁移适配、交互设计等多方面拥有深厚的技术积淀，现已形成桌面、服务器、智能终端等操作系统产品线，以及集中域管平台、企业级应用商店、“有”系列平台迁移软件等应用产品，能够满足不同用户和应用场景对操作系统产品与解决方案的广泛需求，其市场占有率及生态成熟度均位于行业前列。据第三方机构统计数据，统信UOS操作系统在桌面端持续保持市占率第一，在服务器端增速行业第一。截止到2023年9月，生态适配总数突破300万，统信UOS操作系统在政府，金融，运营商等关键行业部署数量超过500万套，服务于多个国家部委、地方政府以及中国移动、工商银行等行业头部企业，为千行百业数智化转型和数字经济建设，提供了坚实可信的底座支撑。

国家相继出台一系列政策，布局核心技术创新，推动国产化操作系统及其创新生态建设。随即国内各大科研院所及企业对国产操作系统的研发开展技术攻关，并取得重大突破，使国产操作系统实现从“可用”向“好用易用”迈进。随着大数据、云计算、人工智能等新一代信息技术的发展，统信软件积极融入国产化操作系统的建设中，努力研发新一代操作系统，使其更人性化、智能化。

2014年和2020年，微软分别正式停止了对WindowsXP和Windows7的服务，不再提供任何技术支持、软件更新、安全更新及漏洞修复，国内各领域网络空间均面临着潜在安全风险。

在国产化替代建设任务中，统信软件持续加大研发投入力度，提升技术创新能力，不断提升桌面操作系统的性能与稳定性，使其与新一代信息技术进一步融合。统信软件积极拥抱开源，自主维护了deepin开源社区，并持续推进生态共建，通过自建适配中心并积极共建“联合生态共建理事会”、“同心生态联盟”等生态组织，共同推进生态全面发展。统信软件在服务范围上除面向党政军及关键行业大体量用户外，还面向中小型企业，提供专业的安全保障措施以及完善的技术支持服务。

4.8.2. 解决方案产品概述

统信桌面操作系统V20基于Linux内核研发，同源异构支持全系列CPU架构，提供高效简洁的人机交互、美观易用的桌面应用与安全稳定的系统服务。

在软件方面，系统提供近50款自研应用、第三方厂商应用以及众多开源社区原生应用，并兼容主流流版签和电子公文应用。在硬件方面，兼容众多整机厂商的主流终端设备，在外设方面，兼容主流的打印机、扫描仪、高拍仪、读卡器等。

统信桌面操作系统V20基于丰富的软硬件生态和应用场景解决方案，为党政军以及金融、电力、能源、教育等关键行业提供信息化建设的基础平台以及项目支撑、平台应用、软件开发和系统定制等能力，完全满足各行业用户与个人消费者的办公、娱乐、生活以及个性化需求，体现了当今国产操作系统发展的前沿水平。



全栈生态

在硬件层，统信桌面操作系统V20全面支持主流CPU架构和国产CPU平台，广泛兼容国产整机配件和外设。在软件层，统信桌面操作系统V20预装了近50款功能强大的自研软件，支持日常办公、系统管理、网络服务等多种场景开箱即用，并通过软件商店提供6.6万余款软件免费下载，满足用户丰富的个性化需求。此外，统信桌面操作系统V20提供与之搭配的多种解决方案产品，如集中域管平台、企业级应用商店、私有化更新管理平台、统信有应、统信有往、统信有来、统信有墨、云打印、云扫描、统信有乔、统信应用全栈等，支持定制开发、专有环境部署，全面支撑党政军以及金融、电力、能源、教育等关键行业用户的业务需求。

4.8.3. 产品特性

智能易用

统信软件对国内用户的心智模型持续进行了大量的研究和探索，遵循科学和设计美学相结合的设计理念研发了统信桌面操作系统V20，统信软件对系统的各个模块及细节都进行了深度思考和交互优化，以保证用户在使用统信桌面操作系统V20时能够得到行云流水的操作体验。

统信桌面操作系统V20的安装提供全中文图形操作引导界面，支持手动安装和全盘安装，用户只需根据安装提示进行简单操作即可快速完成系统安装。在Windows环境下，用户不必卸载原系统，即可通过体验工具快速试用统信桌面操作系统V20。

统信桌面环境交互便捷为原则，提供了极简的交互逻辑和功能层级设计，打通多应用底层，深度融合，提供了帮助用户提高工作效率的强大功能，如：工作区功能支持用户为多任务创建不同桌面，实现快速切换；全文检索功能支持用户通过文本关键词快速查找文件位置；桌面智能助手支持用户通过语音指令快速调起其他应用完成网页搜索、查询天气、会议日程创建与提醒等操作，智能互通、便捷高效。

统信桌面环境使用充满活力的动效设计和色彩风格给用户带来极致审美体验，极简的交互降低操作的复杂度，避免长期使用带来的审美疲劳。此外，统信桌面环境还支持用户高度自定义，可设置窗口特效模式、深浅色系系统主题等，用户也可根据喜好随心选择各种风格的应用图标。

安全稳定

统信软件是国内信创领域首家通过等保2.0四级最新标准、商用密码产品认证的操作系统厂商，还是国内首家通过UEFI安全启动认证的厂商，用户无需关闭安全启动，也可以安装统信桌面操作系统V20。

统信软件还打造了专业的系统安全漏洞管理机制，成立了统信安全应急响应中心（简称“USRC”），并部署了对外网站协助完成漏洞管理。USRC提供了漏洞在线提交、漏洞公布、漏洞查询、漏洞情报等功能。此外，统信软件拥有成熟的漏洞跟踪机制，除了紧跟上游社区漏洞修复方式外，统信软件专业安全团队会主动修复漏洞，并将修复后的升级包第一时间同步给用户，最大限度的减少用户因为漏洞而产生的损失。

统信桌面操作系统V20基于长期维护的稳定版内核研发，定期合入上游的缺陷修复、安全漏洞修复、性能优化等补丁，同时与国产硬件、软件、外设生态进行了广泛适配，兼容17万余款上下游生态产品，确保系统能够满足不同类型业务的需要。

统信桌面操作系统每个大版本具备11年产品生命周期，周期内提供功能更新、性能优化、

漏洞修复等服务支持，确保产品长时间稳定运行。统信桌面操作系统每个版本发布均经过 LTP、Benchmark、SpecCPU、Nessus等工具严格测试和一系列高负载场景使用测试，确保在真实业务场景和复杂使用环境中依旧流畅、安全、稳定。

自主创新

统信软件基于Linux内核采用同源异构技术打造创新的统信桌面操作系统V20，支持主流CPU架构（AMD64、ARM64、LoongArch、SW64、MIPS64等）和国产CPU平台（鲲鹏、飞腾、龙芯、海光、兆芯、申威、海思麒麟等）。

统信桌面操作系统V20从内核、桌面环境到系统基础应用均使用开源技术自主研发，开放源代码超过600万行，不依赖任何国外商用软件，实现了核心技术和知识产权的自主创新。

除此之外，统信软件还自主研发了近50款自研桌面应用，如应用商店、控制中心、系统监视器、终端等系统应用，浏览器、文档查看器、文本编辑器、下载器、邮箱等办公软件，音乐、影院、相机等娱乐应用，全部支持开箱即用。

4.9. AMD 桌面云 vGPU 解决方案

4.9.1. 应用背景

AMD 是高性能与自适应计算领域的领先企业，致力于提供优质的产品和服务，助力客户解决各种重大的挑战。我们的技术推动着数据中心、嵌入式系统、游戏和 PC 市场迈向未来。AMD 于 1969 年在硅谷创立，最初只有几十名员工，从那时起 AMD 便踏上创新之路，致力于引领半导体产品领域的最前沿。如今，AMD 已经成长为一家现代化的全球性企业，凭借先进技术和诸多突破性行业创新，树立现代计算新标杆。

桌面云已经成为用户终端建设的主流方案和趋势，应用于3D设计场景能够实现设计图纸等数据防泄密、远程工作和集中运维。大部分传统2D云桌面的虚拟化方案完全基于CPU构建，鉴于CPU在并行计算方面的劣势，视频处理、图像渲染、3D建模等专用场景下CPU的占用率将一路飙升甚至达到满载水平，导致响应慢、延迟高、卡顿明显等用户诟病已久的问题，一系列短板局限了云桌面在各行业、场景的适用范围。传统解决方案中CPU职能过重的缺陷亟待解决，云桌面底座升级迫在眉睫。

GPU发挥并行计算优势前景广阔。GPU（图形处理器）是一种专用的图形处理器，与CPU相比，GPU的优势主要体现在大规模并行计算领域，适用于处理类型相同且重复性较大的规模化任务。GPU作为CPU在图像领域的有利补充，能够高效协助CPU完成多重并行任务。GPU在诞生之初主要用于优化图形处理效率，随着数字化进程的深化，GPU的潜力正在被逐步挖掘，目前已应用于人工智能、自动驾驶、金融分析等领域。

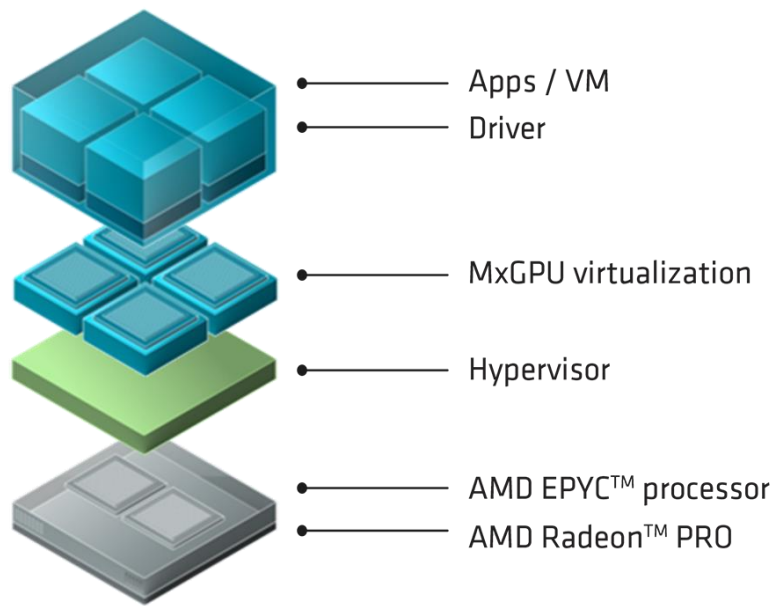
云桌面融合GPU将成为新业态。GPU在国内的大规模应用条件逐步成熟，在用户需求与技术革新的双轮驱动下，在现有云桌面方案中采纳GPU能够充分发挥其优势，显著提升图像、视频、渲染、浏览器等方面的处理效率，满足数字化场景下用户日益攀升的性能需求。可以预见，GPU技术的创新应用将全面提升云桌面竞争力，缩小云桌面与物理PC之间的体

验差异，驱动云桌面进入发展新阶段。

4.9.2. 解决方案

为满足专业设计的需求，深信服桌面云支持与AMD GPU结合构建桌面云显卡虚拟化方案。GPU虚拟化（vGPU）可帮助用户实现对物理GPU的资源切割，可以实现和物理GPU完全一致的功能，可支持OpenGL和DirectX标准及主流的3D设计类软件（如CAD、UG NX、Solidworks、ProE等），可满足用户对GPU在图形、计算机人工智能方面的需求，并且提供易管理、高性价比、安全有保障的设计云桌面。

通过把vGPU软件部署到深信服桌面云超融合平台，从而实现超融合对GPU的虚拟化功能。深信服桌面云vGPU技术原理实现如下：



目前，深信服vGPU桌面云3D设计解决方案可支持AMD V620显卡，搭配专用服务器，可以兼容常见的2D/3D图形设计软件，构建性价比高的显卡虚拟化解决方案。

4.9.3. 方案价值

最大化硬件效用：带有图形界面的应用程序通常需要相关图形处理运算，如果没有GPU来协助CPU执行这些任务，CPU会消耗大量的计算资源导致系统变慢，响应时间变长，影响用户体验。在GPU的协助之下，CPU的负载将有效减轻，系统性能也将大幅提升。被解放出来的CPU算力，可用来支持更多的虚拟云桌面运行，从而减少硬件购买和维护成本。

提升用户操作体验：利用GPU加速技术，GPU云桌面可以支持更复杂的图形应用程序和3D模型等,适用范围更广。同时GPU云桌面具备更快的渲染速度、更好的图像质量和更流畅的运行效果,大大提升云桌面性能,能够全方位多维度提升用户体验,显著提高工作效率。

扩大应用适配范围：随着技术的进步，GPU已成为物理机的标准配置，众多软件厂商在开发时都假设硬件具有足够的图形支持能力，因此编写的软件可以通过GPU并行计算能力进一步提升用户体验，这使得传统CPU云桌面无法较好支持现代软件的运行。GPU云桌面的出现补齐了传统云桌面相对于PC没有GPU加速的短板，为云桌面加入了专业级别的图形处理能力，显著提高云桌面的图形性能。很多以前只能在物理PC上运行的软件也可以在GPU云桌面上流畅的运行，从而更好地满足了用户需求。

4.10. Intel 超能云终端解决方案

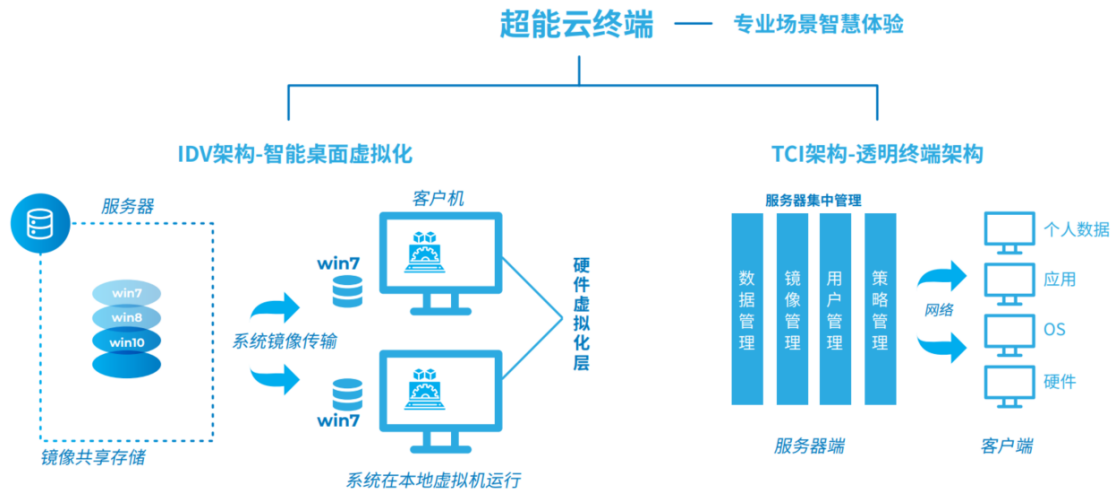
4.10.1. 应用背景

英特尔（NASDAQ: INTC）作为行业引领者，创造改变世界的技术，推动全球进步并让生活丰富多彩。在摩尔定律的启迪下，我们不断致力于推进半导体设计与制造，帮助我们的客户应对最重大的挑战。通过将智能融入云、网络、边缘和各种计算设备，我们释放数据潜能，助力商业和社会变得更美好。

随着各个行业的业务复杂程度不断提高，不同行业对云终端也提出了更高的要求，以往单一的云终端解决方案无法完全满足各类行业的特殊应用场景，因此云终端提供商需要整合各类技术方案的优势，推出技术架构更加先进的云终端解决方案，来满足各行各业对安全性、稳定性、集中管理性、可扩展性、兼容性和个性化配置的需求。

4.10.2. 解决方案

随着应用场景和计算模式的多样化，云端与终端的计算能力需要平衡分配。英特尔超能云终端解决方案能够满足云端管理和本地计算的要求，能够避免对网络和云端服务器的过度依赖，启动风暴或网络中断，都不会对终端运作产生影响。英特尔超能云终端解决方案包含了IDV架构与TCI（Transparent Client Infrastructure）架构，兼顾了用户对终端性能、融合性、灵活性和稳定性的要求，并具备对复杂业务进行管控的能力，为客户的不同应用场景提供相匹配的本地计算力，实现个性化的用户体验。



IDV可以利用本地算力降低对云端的依赖，同时在扩展性、稳定性、灵活性、和集中管理性等方面具备较大优势。IDV可以实现智能桌面的虚拟化，部署灵活且容易管理。通过将客户端进行虚拟化软件部署，轻松实现全面集中管控，包括带外管理和个性化数据管理。同时还完美平衡了云端与本地计算力，支持操作系统和扩展应用的灵活部署，便于对接标准的网络存储与分布式存储。

TCI透明终端架构是Intel的软件解决方案，通过端到端的部署，在本地计算，集中管理、外设兼容性和账户个性化配置等方面具备更大优势。

TCI可以满足用户对透明终端的个性化需求，并提供丰富的外设体验。通过端到端的软件部署，可以实现灵活的集中管理，同时赋予终端原生的本地计算能力、离线操作和强大的外设兼容性，进而提供了与PC无差别的个性化云计算体验。用户摆脱了硬件和网络的束缚，可以在不同终端之间实现计算环境的灵活迁移。

4.10.3. 方案价值

超能云终端是基于云端管理、本地计算理念的新型云终端解决方案，具备强大的本地计算性能，同时在外设与软件兼容性、复杂的集中管理、个性化配置以及英特尔处理器支持等方面具备很大优势，为客户的不同应用场景提供相匹配的云端与本地计算力，实现个性化的用户体验。企业在领导力、运营模式、工作资源、信息技术以及全方位体验等领域的数字化转型进程不断推进，将对新型云终端解决方案提出更高的要求。

国家“上云用数赋智”政策，以及企业业务云化带来的IT架构升级，都推动了新型云终端市场的发展。此外，超能云终端迁移难度较低，在实现对企业终端设备利旧的同时，可以让用户获得等同于PC的应用体验。具备终端算力的超能云终端解决方案可以覆盖更多的应用场景，未来随着教育信息化与医疗信息化的全面升级，超能云终端解决方案在各个行业将

迎来更加广阔的前景。

4.11. NVIDIA 桌面云 vGPU 解决方案

4.11.1. 应用背景

英伟达（NVIDIA）是一家人工智能计算公司，成立于1993年。公司主要从事图形处理器（GPU）和人工智能（AI）计算技术的研发、设计和销售。英伟达的GPU产品广泛应用于游戏、专业可视化、数据中心和自动驾驶等领域，其AI计算平台则被广泛应用于机器学习、深度学习、自然语言处理等领域。

桌面云已经成为用户终端建设的主流方案和趋势，应用于3D设计场景能够实现设计图纸等数据防泄密、远程工作和集中运维。传统2D云桌面无显卡支持，要运行DX和OpenGL的3D应用只能通过CPU模拟，从而经常面对性能低、兼容性差、色彩失真、CPU负载高等问题，无法满足图形加速等设计业务的要求。

业务痛点：

显卡资源无法灵活调度

传统图形工作站显卡是单独存在于每台工作站上面，并且性能受限于单块显卡的最大性能。企业在进行设计时，不同的设计人员对资源的要求不一样，需要为他们购买不同显卡配置的图形工作站，这些工作站也都是专人专用，无法实现显卡的灵活调度与复用，导致显卡的资源利用率低。另外随着业务的发展，应用和图纸的变化，工作站资源不足（计算，内存，硬盘，显存）时，升级也不方便。

设计图纸的安全无法保障

设计图纸是公司的核心机密信息，传统图形工作站在业务处理过程中会将敏感信息留存在本地硬盘，U盘拷贝、网络外发等行为会造成较大的信息泄密风险，难以满足对数据安全管控的要求。

数据可靠性方案缺失，数据丢失风险高

随着PC逐步老化，难免会发生硬盘损坏、主机故障、勒索病毒等意外事件，如果图纸数据没有提前备份，那么硬盘文件将直接丢失或被加密，恢复难度高。同时，又因为这些信息散落在每台终端上，只能依靠员工主动备份，个人行为难以约束，极易造成办公资产的丢失。

管理运维工作量大

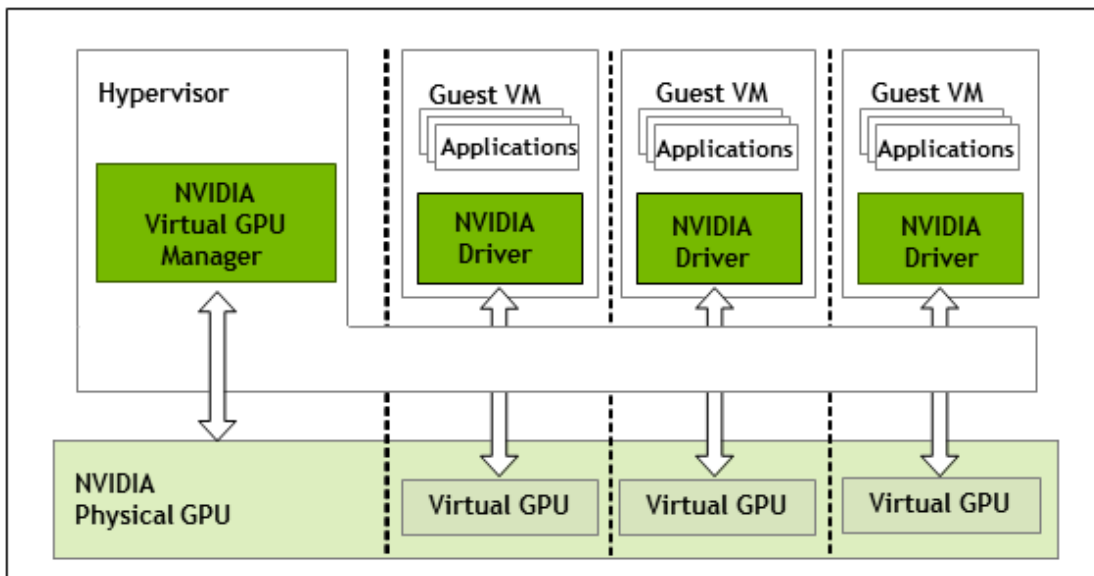
图形工作站分散在各个设计团队中，难以进行统一管理维护，传统pc使用过程中，经常出现软硬件问题，如系统崩溃、病毒感染、硬盘故障等，需要IT运维人员到现场进行排查

和维护，严重影响了工作效率。

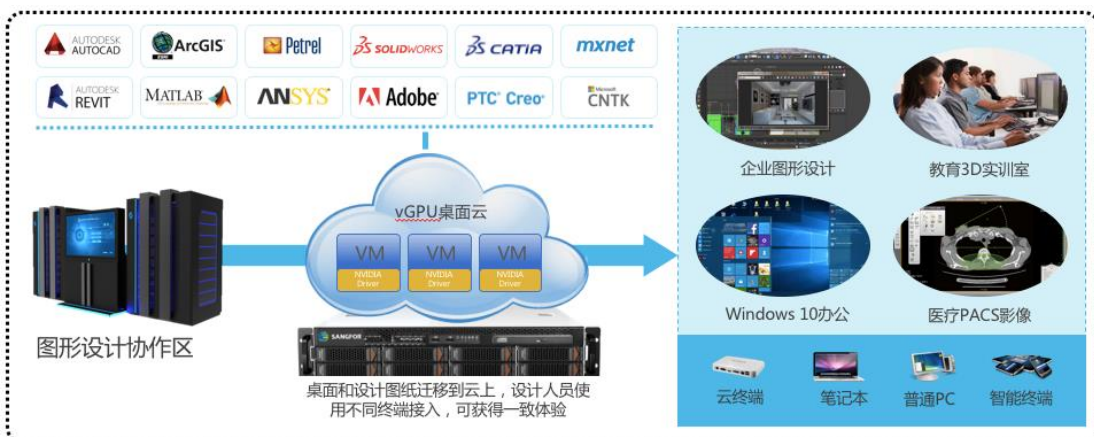
4.11.2. 解决方案

为满足专业设计的需求，深信服与英伟达合作推出业内首款基于KVM的vGPU（Virtual GPU）显卡虚拟化方案。GPU虚拟化（vGPU）可帮助用户实现对物理GPU的资源切割，可以实现和物理GPU完全一致的功能，可支持OpenGL和DirectX标准及主流的3D设计类软件（如CAD、UG NX、Solidworks、ProE等），可满足用户对GPU在图形、计算机人工智能方面的需求，并且提供易管理、高性价比、安全有保障的设计云桌面。

通过把vGPU软件部署到深信服桌面云超融合平台，从而实现超融合对GPU的虚拟化功能。深信服桌面云vGPU技术原理实现如下：



目前，深信服vGPU桌面云3D设计解决方案可支持NVIDIA M10、M60、P40、T4、RTX6000、RTX8000、A16和A40等显卡，可以兼容Catia、UG NX、Solidworks、PTC Creo、AutoCAD、Maya、3DMAX等常见的2D/3D图形设计软件。



深信服vGPU桌面云解决方案广泛适用于汽车零部件、精密器件、电气设备等企业设计场景，以及设计院和研究院，同时也满足高校设计类专业、3D学生机房的桌面云建设需求。

4.11.3. 方案价值

深信服桌面云3D设计解决方案通过虚拟化层对服务器显卡资源进行分割，创建显卡资源池，根据需求分配显卡资源，进行资源动态调整，通过GPU资源可视化帮助企业信息部门作出更好的决策，实现更高的业务效率。

GPU资源池化和可视化：通过vGPU实现显卡资源池化，并且实现显卡虚拟化资源及授权在云桌面关机后自动释放，可以实现多用户共享GPU资源，降低用户投资成本。并且在使用过程中可以实时显示当前的显卡负载情况，通过业务负载可视化做到按需灵活分配，实现资源利用的最大化。同样，决策者也可以通过显卡资源的可视管理，来做出合理购买决策。

提升用户体验：深信服自研HEDC协议采用H264/H265编解码技术，通过调用NVENC来加速HEDC传输协议，这个机制不仅大幅提升用户体验和降低传输带宽，还可以有效降低CPU资源消耗，将有限的CPU资源用于业务软件，并可显著提升服务器承载密度。

提升资源利用率：显卡虚拟化通过灵活的切割方式，让用户能够以更理想的方式和更高的灵活性提升资源利用率，对于企业设计场景，不同员工可以交替使用桌面，白天用于设计，晚上用于渲染，减少软件授权和硬件采购的成本，提高业务软件 and 设备的利用率。

数据高安全：设计相关核心数据全部集中存储在后端服务器上，前端接入设备不存储任何业务数据。同时支持对USB接口进行统一的管控，可有效地保障数据的安全性，防止数据外泄。如果需要外发文件可通过系统自带的导出审计功能，既能满足外发功能需求，又能做到外发数据的事后可追溯。

简化管理运维：信息部门能够对数据中心内的所有设计用户的资源进行集中管理，提高设计桌面系统的部署与运维效率。IT运维人员无需前往各个部门，通过统一控制台就可实现远程桌面批量操作，如系统补丁升级、故障排查、桌面还原等。

五.桌面云典型应用场景

5.1. 政府领域应用场景分析

5.1.1. 政府领域背景

为提升政府各部门的协作能力和办事效率，国家通过政务信息化工程大力推进机关单位的电子政务建设，从而为公众提供高效的政府服务。近年各级政府的电子政务系统建设日趋完善，从最初的办公自动化逐步实现政务线上化和协同化，通过信息化的方式不断提升政府部门的办公效率。同时，国家对网络信息安全保护的重视程度不断加强，也相继出台了一系列的文件来规范电子政务的建设。

随之而来的是业务应用环境越来越复杂（比如多级架构、多业务、多套网络、多种系统等）。所以，政务终端在使用过程中难免会遇到安全管理难度大、文件失密风险大、办公桌面繁杂等诸多困境，不符合政府对公文流转和业务系统的安全保密要求，需要优化现有模式，建立安全、便捷、灵活的政务桌面平台。

桌面云在帮助政府完善电子政务系统建设的同时，桌面云解决方案可为用户提供基于物理隔离的内外网桌面云基础架构平台，可以有效保障系统的安全与稳定，保障敏感数据不外泄，提升设备安全可靠，有效降低系统风险，缓解政府电子政务系统的运维压力。

5.1.2. 面临的问题

路线选择问题。CPU主流路径有六条，操作系统主流路径选择有两种，选择哪种技术路线？是单技术路线还是双技术路线？交叉选择是否会有兼容性问题？是否会导致重复投资和成本的浪费？这些都是需要考虑的问题。

数据安全问题。计算机的终端选择众多，本身也是分散在各地，如果未进行统一管控，那么任何一个点都存着数据丢失、数据泄露的安全隐患。政府需要经常与外部进行数据交互，数据的安全传输依然非常重要，一旦被非法人员获取，将造成重大的经济或名誉损失。

成本效率问题。目前政府部分的业务系统还未完成业务改造，很多还是基于Win+Intel的架构，导致当前阶段用户必须使用两台PC，一台使用PC在统信或麒麟环境下办公，另一台使用Windows电脑来承载传统业务系统。这种方式不仅效率低下，而且成本较高。

终端运维复杂。自主创新终端缺乏有效的外部生态，各类管理软件缺失，导致自主创新终端管理工作复杂、效率低下。并且，由于短时间内Windows业务改造无法完成，双桌面的现状使得运维人员不得不同时运维两台PC，导致运维工作量倍增。

5.1.3. 解决方案

桌面云方案可同时支持X86和ARM架构的服务器，并支持按需发布windows、统信、麒麟等操作系统的桌面，从而可同时满足在Windows操作系统上办公和在统信、麒麟操作系统上办公。

同时，桌面云将办公应用及数据集中部署在后端数据中心，利用虚拟化技术提升桌面运维效率，并只将桌面图像交付给用户，网络中传输的仅仅是屏幕增量变化和指令信息，终端不会留存任何办公数据，从根本上保障了用户数据资产的安全性。

该方案价值如下：

技术创新：整个方案从服务器、终端、操作系统以及应用软件多个方面实现了自主创新，同时能兼容主流的各种国内外CPU和各类操作系统，大大降低了投入成本和适配难度。

极简运维：桌面云可以从桌面首次上线、软件更新与维护、软硬件资源的统一管理、故障检测与排障、资源的扩容和回收等多个维度提供完整的虚拟机全生命周期管理，并且基于可视化管理平台以及丰富的自动化运维工具，极大地提升运维管理效率。

数据安全：将数据全部保存在后端服务器，前端不留数据，只传递桌面图像，并通过USB外设黑白名单及管控策略、政务虚拟桌面数据卷全盘加密等技术实现政务数据的立体式防护，有效防范信息泄密。

全面防护：桌面云由于本身的架构优势和支持的其他安全特性，提供更安全的保障方案。从接入安全、网络安全、数据安全、终端安全、隔离安全、平台安全这六个维度保障终端办公安全。

5.2. 金融领域应用场景分析

5.2.1. 金融领域背景

在互联网的大潮下，金融机构对信息化系统的需求越来越多样化，传统直接购买系统的模式，已经难以满足业务需求，国内金融机构相继成立软件开发中心，以科技创新驱动业务、服务和管理创新。在这个过程中，均衡业务需要和投入产出，借外力来发展自己，开展金融服务外包成为很多金融机构的选择，特别是IT开发和系统维护。

与此同时，金融外包的潜在风险也不容忽视，根据国际上最早关注外包风险和监管的巴塞尔委员会的定义，金融服务外包的主要风险主要包括：战略风险，声誉风险，操作风险，退包风险，信用风险，国家风险，履约风险，监管障碍风险，集中和系统性风险，以上十种。在银监《商业银行信息科技风险管理指引》的指导下，金融机构都搭建了信息科技“三道防线”防控体系，而在当前愈发开放、外化的趋势下，IT风险管理很难做到面面俱到，这就需

要集中力量加强关键部位和薄弱环节的风险管控，以应对复杂的内外部挑战。

5.2.2. 面临的问题

开发代码及文档丢失风险。作为开发测试终端，本地PC磁盘上会留存很多开发源代码、项目文档等重要数据和敏感信息，随着设备老化，硬盘或主机无法避免地会发生不可预知的故障，如果没有定期备份数据，那么部分重要开发代码和文档将直接丢失，难以恢复。

存在开发代码外泄隐患。金融机构中开发测试所用的PC有USB、网络等各类接口，部分金融机构可能通过封锁USB接口或部署安全组件，包括杀毒软件、加密软件、个人防火墙、USB管控、上网审计、防非法外联等方法，但仍然难以有效控制敏感代码和文档在内部的流转范围和访问控制。而且，封锁USB接口或部署安全组件，不仅导致电脑不堪重负，维护成本高，更让开发测试人员使用不便捷，影响办公效率。同时，也无法从根源上解决问题，比如开发测试人员把电脑硬盘拿下来，作为从盘挂接到另外一台电脑上，此时开发测试相关材料可以不留痕迹地拷贝和外发，造成知识产权泄密。

上网信息安全风险。开发人员普遍需要访问互联网查询信息，对于部分没有做桌面隔离的金融机构，研发人员使用的开发桌面和上网桌面是同一个，而自主创新终端在这个过程中会面临中毒、数据泄密等安全风险。

5.2.3. 解决方案

在金融领域，桌面云通过构建一体机为主体的桌面云解决方案，各分支机构以及外设自助终端通过专有网络连接到总部，由总部的IT运维部门统一调配和管理，通过虚拟桌面策略，禁止虚拟桌面任何应用访问金融行业用户的任何本地存储设备，从而保证用户的数据安全。

该方案价值如下：

提升资源利用效率。桌面云可以在很大程度上降低系统建设成本，根据不同用户的需求弹性地设置云主机的资源配备，实现资源按需分配，最大限度地提升资源利用效率，将系统建设成本降到最低。

提升运维管理效率。桌面云在金融行业的应用涉及权限分配、用户管理、主机管理、应用监控等多个层面，桌面云管理系统是进行系统运维管理的唯一接入口，可有效地实现对系统的控制和监控，提升运维管理的效率和安全性。

保证系统信息的安全性。首先，桌面云系统的应用是存在安全限制的，用户在密码验证通过后才能进入系统，并访问和更改相关数据。其次，系统可以将用户数据和存储数据放置在服务器终端，使任何与实际业务相关的数据都可以不被传输到桌面，极大地提升数据的安全性。最后，云主机和终端设备需要在授权的情况下才能访问，这样，USB、多屏幕和声卡等设备都可以处于安全状态之内。所有云主机在经过桌面云系统的防火墙后才能进行访

问，从源头上保障了数据的安全性。

5.3. 企业芯片领域应用场景分析

企业有众多的行业领域，如制造业、电力、交通、建筑等，本企业典型案例以企业芯片领域为例。

5.3.1. 芯片领域背景

芯片集成电路（IC）是信息社会的基石，也是信息技术的重要基础。芯片产业的高质量发展，关系到现代信息产业和产业链发展。国务院早在2015年就提出《中国制造2025》，提出在2025年，中国芯片自给率要达到70%，而2019年，我国芯片自给率为30%左右。近两年，我国的许多科技企业都面临着“缺芯”之痛。国家层面也明确大力支持国产芯片行业的发展，是《十四五》国家研发计划确定的重要发展方向。

芯片作为“高精尖”工业产品，拥有极高的技术壁垒。企业的研发生产数据，是企业的生命力和基石。芯片行业中使用桌面云，既可以保障终端数据安全，又可以提升整体办公体验和效率。

5.3.2. 面临的问题

终端PC性能差，体验不佳。芯片设计岗位，对终端计算和显卡性能有一定要求，普通PC无法满足要求，往往需要使用高性能工作站。

重要数据重要，安全管理难。传统PC叠加安全软件的方式，仍然漏洞百出，并且会消耗PC性能，间接影响到体验。

多网隔离，办公使用复杂。基于安全的安全因素的考虑，芯片行业会建设多张内部网络，员工访问多张网使用多个PC，办公体验差，影响工作效率。

行业吞并，协作困难。芯片行业处于高速发展，企业的吞并时常发生，如何处理新入企业的办公和数据流转，需要更弹性的办公终端方式。

移动办公和远程办公困难。芯片行业需要多部门协作，需要移动化办公，传统PC难以满足。尤其是疫情期间为保证企业进度不受影响，需要支持移动化和远程办公。

5.3.3. 解决方案

场景	需求	方案	价值
----	----	----	----

<p>安全研发中心</p>	<p>IC 研发中最重要是数据的安全保护和协调开发，在实施 PLM 系统后能够将一个独立的项目分割多个小型的子项目，但是数据安全风险还是没有得到有效的解决。另外，针对大型计算和特殊的应用，需要购置大量的工作站和昂贵的软件，大部分时间这些资源利用率非常低。</p>	<p>研发开发：采用桌面云架构，企业可以将可现有的研发工作站集中在数据中心。 内网上网：研发人员可以通过现有设备连接到虚拟桌面，并且在虚拟桌面中使用虚拟应用发布的浏览器等上网工具。 高性能设计：桌面云 vGPU 技术和显卡虚拟化的天作之合，实现了工作站的集中化、高密度化的虚拟化转变。</p>	<p>降低成本、提高利用率 确保“数据不落地” 远程成果展示 协同开发 优化开发流程</p>
<p>网络安全隔离</p>	<p>基于安全的安全因素的考虑，在大型芯片制造企业中会根据涉密、数据访问的要求将网络分割成生产网、办公网以及互联网区。从实施角度来看这个架构将增加 PC 机的数量、降低员工的工作效率、增加运维成本，同时安全性方面还是存在诸多的漏洞。</p>	<p>逻辑隔离：后端部署一套桌面云集群，进行逻辑划分，实际分成生产、办公、上网等多个集群，用户使用瘦客户机连接到生产网的虚拟桌面云集群，通过这一步骤可以将用户网络和生产网络隔离。 物理隔离：后端部署两套或三套桌面云集群，进行物理划分，实际分成生产、办公、上网等多个集群，用户使用双网瘦客户端或者分开单独的客户端，连接到对应网络的虚拟桌面云集群。</p>	<p>精简了终端设备 提高投资回报率 符合了安全隔离要求 安全控制</p>
<p>企业扩张、公司兼并、新厂</p>	<p>IC 企业通过不断扩张、兼并、不断在全国布局建设新厂等一系列方式促使企业快速发展壮大，使企业在发展过程中迅速上升的、进步。这对企业的 IT 建设提出了新的挑战和机遇。首先是如何确保核心业务系统统一性避免重复建设和分散架设的问题，其次是如何有效的整合资源实现弹性交付的方式，再次是 IT 团队建设和如何实施支持体系的问题。</p>	<p>使用虚拟应用技术实现了 ERP、OA、CRM、供应链等系统的应用虚拟化，结合外网安全零信任安全网关功能，实现了端到端的安全访问。大概 200bkps 的左右的网络带宽需求，从任何设备的访问，数据不落地的特性，完成了核心业务系统去专线化、移动化、高安全性、易于使用的华丽转身。通过建设桌面云的技术，为这个企业和新厂、兼并的企业快速通过桌面云的支持，为企业通过了一套弹性、灵活、标准的桌面环境。</p>	<p>快速部署 实现数据的实时性 核心系统访问移动化 有助于优化企业流程 减少带宽租借费用：</p>
<p>远程和移动办公</p>	<p>受疫情影响，芯片企业都尝试了居家办公，大量客户接触了居家办公的模式后，已有客户思考将远程办公常态化建设。既保障了企业关键岗位工作正常开展，又能内外网办公方式统一，很好的践行了数字化转型提升企业生产力的初衷。</p>	<p>需在企业数据中心部署桌面云一体机构建统一的桌面云资源池，并给员工分配好各自的 VDI 账号和桌面资源，办公人员只需通过在家的 PC 或笔记本登录自己的云桌面即可实现正常办公。</p>	<p>端到端构建更全面的安全办公空间 高效传输协议有效降低对广域网带宽的依赖</p>
<p>无纸化车间</p>	<p>现代化 IC 生产线上传递生产信息要求越来越方便高效，现 LED 屏的生产线看板管理系统越来越满足不了当下快速高效的生产信息传递的高要求，现在越来越多的工厂关注并使用云终端机+显示屏的生产线看板，这样操作方便工人通过人机交互方式更快地阅读到生产看板上的信息，避免了工人遗漏、忘记某些重要生产细节信息没有看到时，可自行触摸点击查阅。</p>	<p>通过使用虚拟桌面技术，所有的虚拟桌面统一部署在数据中心，按照工种的不同分配相应的虚拟桌面。灵活的部署模式可以降低服务器、存储投入成本，重启系统即自动恢复模式可以减少故障处理时间，三维软件远程发布可以减少工作站、三维软件许可证的投入。结合瘦客户机的应用，真正做到了“重”后台，“轻”前端。瘦客户机“零”维护、长寿命、低功耗、高度集成的特点，有效的克服了“高温、大灰尘、频震动”的工作场景，集中配置和闪存卡模式简化了车间的终端运维。</p>	<p>延长设备使用寿命 终端“零”维护 无纸化车间 实现了 MES 数据实时性</p>

5.4. 教育领域应用场景分析

5.4.1. 教育领域背景

教育信息化经过多年的飞速发展，高校数字化校园建设日趋完善，为了实现智慧校园应用体系建设，中小学每年都会增配不少电脑装备，一方面可推进基础教育的均衡发展，另一方面可大幅提高中小学校生机比，从而使得信息技术更好服务于现代教育，培养学生信息化能力。

当下校园的信息化建设和建设仍然以各种型号的计算机为主，在“集约化建设”的原则上，推出智慧校园桌面云解决方案，为计算机教室、教师办公等多种业务场景提供全新的云IT建设方案，从而实现教学集中化、管理智能化、维护简单化、校园绿色化，将师生桌面计算机带入云时代，同时也进一步加速义务教育均衡发展和中小学生机比的建设进程。

桌面云恰好是一种能显著提高管理效率、降低 IT 基础架构复杂性的服务，通过将原有 PC 的操作系统和应用软件统一迁移到云端的虚拟机中，使所有用户的运算、处理请求都由云端服务器完成，从而实现桌面环境集中管理、终端零维护和硬件资源的弹性分配。

与传统 PC 相比，桌面云拥有很多优点。高校部署桌面云的场景包括计算机基础实验室、计算机专业实验室、多媒体教室、教师办公等。不同场景使用桌面云的需求不同，并且差异较大，部署时应按需配置。

5.4.2. 面临的问题

传统 PC 机房管理维护难，教学环境准备费时费力。PC 的硬盘、风扇、电源、还原卡的接插件多，外设管理困难，系统及软件维护需要逐台管理，一间教室即便利用同传技术也要花费至少 2 小时。在新课改中，学校不同年级信息课的教学所需的操作系统，应用软件不同，且多样化，PC 仅能提供单一环境。

新课改应用软件对终端性能要求高，传统方案建设难兼顾性价比。新课改信息技术课程新增加的可视化编程、3D、图形编程等教学软件，在运行过程中需要执行编译，建模，渲染等操作，对终端的 CPU，内存，和显卡性能要求教高。

学生管控难，上课终端广告弹窗，影响教学秩序。信息技术课与主课教学最大的区别是需要进行操作性演示和练习，这需要以良好课堂秩序为基础，同时终端大量的广告和弹窗软件，补丁更新困难，影响课堂教学秩序。

5.4.3. 解决方案

为更好满足学校在教学、办公、管理等场景下的不同应用需求，桌面云提供VDI&IDV的双架构融合解决方案。在满足学生学习、老师教学、领导决策等需求的同时，着力于改善使用者的上机体验，降低管理员的运维难度，另外提供了灵活的产品配置和便捷的升级扩展方案，降低信息化建设的总拥有成本。为实现学校或教育局级的云桌面统一大平台打下基础，迎接教育信息化2.0时代的到来。

全场景支撑、全业务服务。方案可根据不同的班级规模、学校规模，选择不同的配置，同时充分考虑了现有设备的利旧和新旧设备的统一管理维护。而在教学方面，能够良好的支撑信息技术课以及听说教学、人机交互考试等业务。

在办公方面，能够为老师提供灵活的数据随行、桌面随行服务，帮助老师随时随地的进行办公业务的开展。

在管理方面，则灵活地提供多种教学系统镜像并可进行实时切换，还可以有效的保障教学秩序，加强教学管理，提升教学质量。

5.5. 医疗领域应用场景分析

5.5.1. 医疗领域背景

医疗卫生信息化是国家信息化发展的重点，各省市接连出台相关政策明确医疗信息化推进方向，包括远程/移动医疗、健康物联网、医疗系统数据安全、区域医疗信息化等，这也是整个医疗卫生行业未来发展的趋势。

近年来，新技术在医疗行业的应用正在快速与对应的医疗场景进行融合。例如，《关于促进“互联网+医疗健康”发展的意见》等政策发布以来，互联网技术正在快速构建诊前、诊中、诊后的院内外一体化医疗服务模式。同时，随着医疗物联网应用的普及，越来越多的医院设备连接到医院网络和互联网中。加上将来，5G+AI的应用，必将加速终端之间的数据流动，终端面临的风险类型和暴露面也将持续扩大。

5.5.2. 面临的问题

在医疗改革和信息化发展趋势下，数据安全、敏捷高效、移动医疗等IT方向是医院信息化建设重点。然而，医院终端设备和支撑网络日趋庞大，形式更是复杂多样，所引发的信息泄密、管理低效、运维成本高、业务不灵活等问题让医院CIO们头痛不已，具体如下：

医护工作桌面数量多、环境复杂。在国家政策的支持下，医院的规模会不断扩大，可能

还会在各地建设分院,此时桌面终端的类型和数量会迅速增多,从而变得更加不可控。同时,医疗桌面应用需要涉及HIS、RIS、CIS、PACS、CMS、OA、LIS等几十个子系统,每个系统的应用需求和适配环境存在较大的差异,这就对医护工作站的兼容性和部署效率提出了更高的要求。

医生、护士多人共用一机,职责不明。门诊、住院等不同科室每天当班医生不同,护士也是早中晚轮班,而医院为了资源的充分利用,大多数医生或护士都是多人共用一台主机,所以这就对IT管理提出了更高的要求。对于不同医护人员,管理策略太松可能会引发安全问题,但如果太紧又可能会影响医生、护士的正常使用,所以,IT需要配备灵活、标准化的桌面策略,从而才能同时兼顾桌面使用的安全性和便捷性。

医院IT人员少,但管理工作量巨大。医院的PC数量庞大,在出现软硬件故障后,有限的IT人员在多个维护点反复奔波,严重影响工作效率,从而对医院的日常工作造成了很大困扰。同时,每家医院的医疗信息系统有几十个,分别由多个软件厂商开发,有不少还是C/S架构的,这也意味着部署和维护工作量会更大。而伴随着医疗系统的不断开发和升级,部署更新的工作变得越来越复杂。在这个过程中,IT人员大量的时间和精力就会消耗在这些事务性的工作上,根本没有精力去关注核心系统的建设。

医疗系统繁多、接口复杂,安全管控难。医院信息系统涉及大量医院经营和患者医疗等私密信息,信息的泄露和传播将会给医院、社会 and 患者带来安全风险。但是,PC使用时容易在本地遗留个人病历、药品统方等敏感信息,即使把医疗系统进行内外网隔离,但毕竟医院PC众多,对外设的需求较高,而这些通用的USB接口往往会成为医院网络中的一个安全缺口,不仅容易感染病毒与木马而导致系统不可用,而且还会引发数据丢失、数据泄密等问题。

5.5.3. 解决方案

针对医疗行业特点,桌面云通过虚拟化技术构建一体化桌面云资源池,提供统一管理平台。采用多种架构同时融合,为医院提供挂号、诊疗、办公、运维、培训、互联网等场景所需的桌面环境,为每个场景赋予用户极致的桌面体验。同时提供个性化配置、打印机管理、模板一键部署、智能运维平台等关键功能与智能工具,助力实现桌面终端的高效运维。

同时针对医疗行业高可靠性的要求,桌面云还能提供透明终端架构IDV的解决方案。其中服务器端集中管理,去掉了虚拟化层,通过终端PC内置的硬件进行集中管理,应用运行在终端上。IDV的解决方案在管理和性能上取得了完美的平衡,IDV客户端具备强本地算力,无需依赖于云终端,能够轻松应对高负载带来的挑战。IDV架构支持云端统一管理,实现了终端集中管理,简化运维流程。同时IDV架构支持终端兼容丰富的外设,满足医疗行业外设兼容性的要求。

极致体验。本方案将瘦终端、VDI全套组件、服务器、存储进行深度融合与优化,可以

兼容各类医疗应用，并且为医生、护士、职能等不同人员提供媲美PC的桌面体验，满足医院业务实时响应需求。

随时可用。本方案基于超融合架构，利用服务器集群、虚机迁移、分布式虚拟存储、端口汇聚等技术，为医院提供一套成熟稳定的桌面云平台，应对故障所带来的影响，提升医疗服务质量。

敏捷高效。本方案利用单点登录、联动关机等技术延续了PC使用习惯，医护人员（尤其是老医师）无需培训即可快速上手。同时，采用超融合部署架构和单一管理控制台，提高了医疗IT工作效率。

安全可控。本方案充分考虑了医院信息安全要求，采用了多重认证、终端准入、外设管控、传输加密、防中间人攻击、个人盘加密等安全技术，从端到端层面保障医疗系统的安全使用。

六.参考文献

《中国桌面云标准化白皮书（V1.0）》。

《桌面即服务市场快速增长，混合办公成为新常态》，来自微信公众号“IDC咨询”及IDC相关报告。

《新型GPU云桌面发展白皮书》。

百度百科关于“信创云桌面”介绍。

计世资讯《2021-2022年中国桌面云市场发展研究报告》及微信公众号。