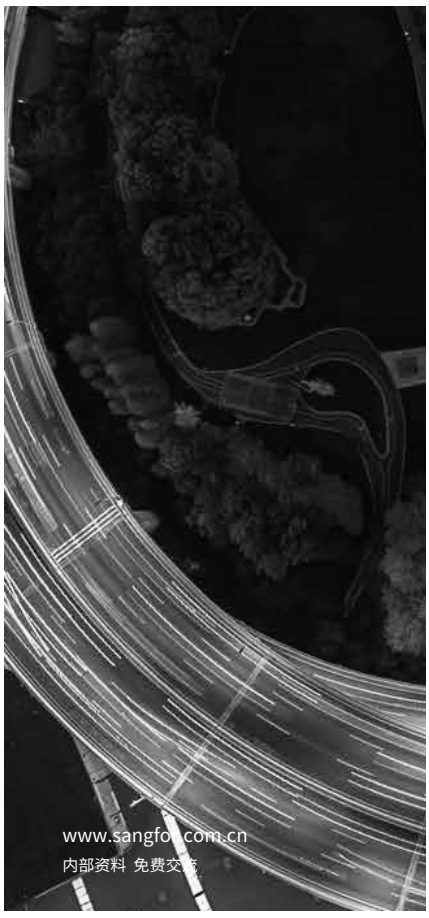
SANGFOR
深信服科技



IT深视野 2020

10 月 | 总第四十七期

让每个用户的数字化
更简单、更安全

深洞察

安全趋势洞察
AI 是未知威胁检测的有效手段

深案例

这一杯酒：
是瓶中方寸千年香 也是智慧化的未来

从无接触经济，到数字化智慧医疗，
2020 年的疫情显然对经济发展和企业运行产生了深刻影响，
加速数字化已经从转型趋势，
变为了事关生死的竞争压力，
留给企业考虑或犹豫的时间已经很少，
提高科技创新能力迫在眉睫。

值得关注的是，
各项极具颠覆潜力的新技术正在逐步实现应用，
它们正在让客户体验上升一个台阶。
一切努力，都让数字化转型离我们更近一步。

本期杂志，
将带来网络安全、用户上云、新型 IT 基础建设等相关内容，
期望让您有所收获。

目录

CONTENTS

01

深洞察

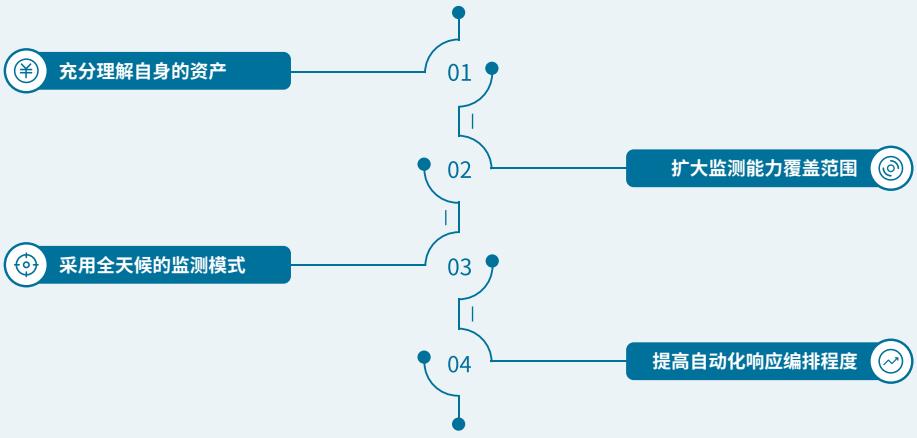
如何快速扩展威胁持续对抗能力？看“四步走计划”有效实践

在安全攻防新常态下，攻击者越来越产业化、智能化、隐匿化，威胁复杂度日益加剧，单纯的防御措施无法阻止蓄意的攻击者，安全建设思路逐渐从被动防御转向持续检测和主动响应。

2019 年 Gartner 发布影响首席信息安全官的七大网络安全和风险管理趋势，强调了威胁监测与响应能力的重要性。无独有偶，IBM、德勤等全球顶尖的咨询机构最新提出的安全模型与框架，也无一例外地传达了对威胁监测与响应能力的重点关注。

本文基于多年的安全研究、趋势洞察以及大量用户的安全服务经验，总结提炼“四步走计划”，有效整合与优化已有的技术和管理流程，快速扩展威胁监测与响应能力，帮助用户构建威胁持续监测与响应的有效实践。

四步计划，快速扩展威胁持续监测与响应能力



什么是威胁监测与响应能力

简单来说，威胁监测即组织通过攻击者留下的蛛丝马迹尽可能早地识别出所遭受的各种威胁的能力，而响应则是指包括威胁分析研判、通告、处置及加固等一系列动作。

当前，组织单位面对的是目标坚定、资源丰富、手段灵活的产业化攻击对手，他们训练有素，利用人工智能手段来武装攻击工具，使得攻击更加频繁，交易方式更加隐蔽。如果不匹配同样先进智能的技术产品、训练有素的人员、高效清晰的流程，难以形成有效对抗。因此，组织需要一套行之有效的威胁监测与响应闭环流程、一群经验丰富的专家以及配套的安全设备，需要快速扩展威胁持续监测与主动响应能力，实现威胁持续对抗。

四步计划，快速扩展威胁持续检测与响应能力

1 充分理解自身的资产

随着业务系统边界逐渐模糊，资产不可视导致的问题日益凸显：悄然上线的资产无从知晓，直至系统感染病毒后才被通知；服务器不知在哪，处置问题时定位设备耗时耗力；Web 系统版本记不住，加固操作无从下手 ..... 安全建设必须在安全可视的基础上，如果没有完整的、详细的资产清单，安全运维人员就无法确保组织的安全。因此资产管理作为安全运营的基础，是监测与响应的根本，是务必重点完成的一项工作。

那么如何有效落地资产管理呢?

首先，以行政部门或采购部门的固定资产表为起点，梳理出资产基本信息，如所属部门、物理位置、用途、责任人、联系电话等。

然后，在资产发现工具的支撑或专业服务人员的指导下，以主动和被动结合的方式识别出资产的更多信息，包括 IP、MAC、端口、系统版本。

其次，采取增量式更新的方式全面地理清应用系统资产信息，如 Web 服务器版本、中间件版本、开放端口等，通过把时间窗口拉长的方式降低工作难度。

最后，进行长效的资产日常运营，包括不断对资产信息清单进行更新和对资产进行更细致规范的分类分级管理 ，从评估不同资产的重要性及其所对应的安全等级，到设计出不同安全等级资产对应所需的安全保护措施，并通过网络分区分域优化、安全设备差异化部署、安全策略强化配置等方式合理配置安全资源，优先保障高价值资产得到有效保护。

2 扩大监测能力覆盖范围

监测能力需要结合资产梳理的结果，覆盖高价值资产范围，如暴露在互联网的资产，日常运维中关注较少的资产。同时，根据业务和资产的特性扩大监测能力涵盖的数据范围。这就需要充分用好已有的安全产品，并视情况新增设备来实现多种类型数据的采集和过滤。一般来说，系统日志、网络流量和端点日志必不可少，这些数据中蕴含着攻击行为必然会留下的脚印和轨迹，有助于描绘出整体网络环境中的正常访问与异常攻击，同时它们也是主动开展威胁狩猎、攻击溯源的重要支撑。

用户行为也必须纳入监测监控的范围。访问和操作行为及其相关的数据有助于安全系统观察和统计用户的行为基准，生成画像，而通过持续监控和机器学习算法发现的偏离基准的某些行为即可被判定为异常访问，这往往是用户账户被劫持进行横向扩散或内鬼正在违规操作窃取数据的表现。举个例子，如果某终端与某系统之间的访问通信量一直相对稳定，且集中在某一特定时段，但突然在某个特定时间访问量激增，即使系统类型或所用协议的详细信息均未知，威胁监测也必须对该危险信号进行通告并立即展开调查。

3 采用全天侯的监测模式

安全设备具备实时监控网络中异常态势的能力，通过设备告警的方式提醒用户关注和处置，其对威胁监测与响应的价值不言而喻。同时，经验丰富能力充分的安全分析人员可与安全设备实现互补，主动进行高阶威胁分析，对成功入侵到内网的攻击行为进行持续搜寻，通过安全策略加固以防范类似的威胁，最终通过分析人员与安全设备的各取所长与协同配合，成功实现持续监测模式。

此外，通过对黑客的活动规律进行统计，黑客组织往往在防守者较为放松的时候发动攻击，如夜间凌晨、节假日，因此 7*24 小时云端远程进行持续监测与响应是大势所趋，既能有效监控安全态势、提前通知事件，又能节省成本、释放人员精力。

以深圳一高校为例，前不久的某个深夜，该高校 IT 运维人员张工突然接到电话，朦胧的睡眼被电话中传来的“勒索病毒”4 个字彻底惊醒，原来是深信服 MSS 服务云端专家通过云端运营平台进行持续监测的过程中发现了病毒的活动迹象。张工迅速连入学校内网，在云端专家的指导下进行事件初步分析判断，发现是某台终端感染了勒索病毒最新变种，电脑中文件正在被加密，张工果断通过 EDR 的微隔离功能将该终端“断网”以防止病毒扩散，并开展查杀、更大范围排查等操作。幸运的是该终端属于非关键设备，通过重装系统快速恢复了正常办公，事后张工感叹，这种持续监测模式价值非常明显，已多次提前识别到威胁，现在工作省心多了，晚上终于可以睡个踏实觉。

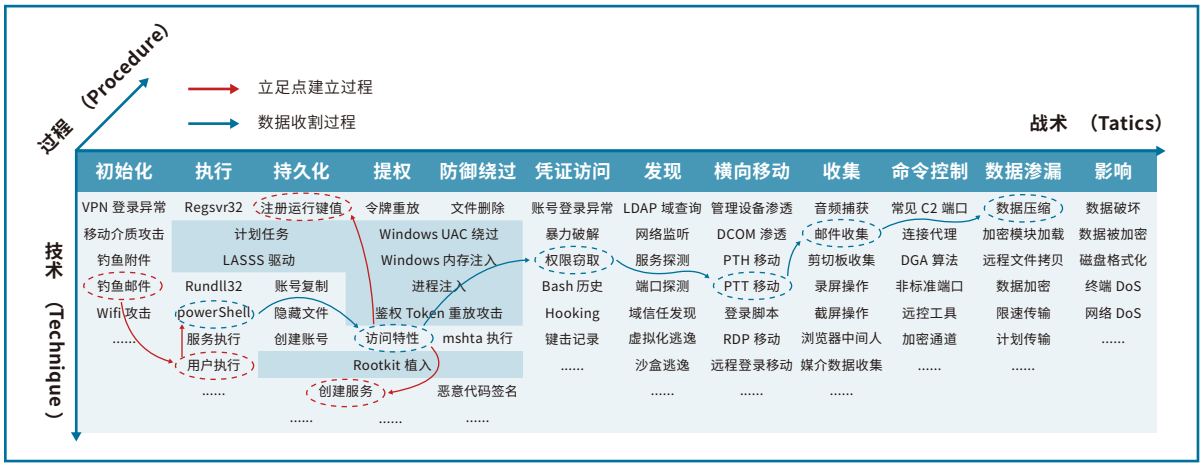
4 提高响应自动化编排程度

安全编排与自动化响应 SOAR 是当前安全领域热点技术之一。安全运营过中，手动和自动协同的定制化工作流的有效运用和高效运转可降低不同产品间切换需耗费的人力、时间，而完备的信息收集、多种互相配合的监测算法、规范工作流的编排可保证威胁监测与响应的效果。安全编排中的自动化程度，决定了威胁监测与响应的效率和准确性，这里务必关注 2 个重点技术能力的建设——Use Case 和 Playbook。

未知威胁或高级持续威胁之所以破坏性强，皆因攻击者是具有自适应能力的智慧型对手，正在采用鱼叉攻击、水坑攻击甚至是人工智能等丰富的攻击方式强化攻击能力，而目前分析师做日志分析、威胁狩猎时，需要多种平台工具之间频繁切换，容易被海量的告警信息所淹没，甚至忽视掉关键线索，因此我们需要灵活、智慧的防守者精准、主动、快速地识别威胁，Use Case 技术可有助于实现上述目标。

Use Case 基于对常见攻击场景、攻击目标、攻击技术、入侵手法、攻击路径的研究和掌握，站在攻击者的角度还原攻击各个阶段的常见做法，思考攻击者会如何绕过或躲避安全产品，预测攻击者为了达成目标会有哪些行为，最终可清晰地告诉设备平台和分析人员当前场景下攻击一般分为哪几步，需要到哪些设备哪些终端提取日志数据，怎么对这些数据进行聚合和关联，如何根据以上信息对威胁进行研判和告警，哪些威胁是需要优先重点关注的，从而有助于监测与响应能力自动化的提高。

2019 年 Gartner 发布的一篇研究报告指出，任何监测能力离不开安全监测用例 Use Case，只有它被恰当地设计和实施好，包括 EDR、防火墙、全流量监测设备在内的监测技术才能更好发挥作用。业内著名的 MITRE ATT&CK 框架详尽地描述了攻击者普遍使用的战术与技术，深信服基于此设计了大量 Use Case，融合到安全运营平台，增强对未知威胁识别的准确率和效率。

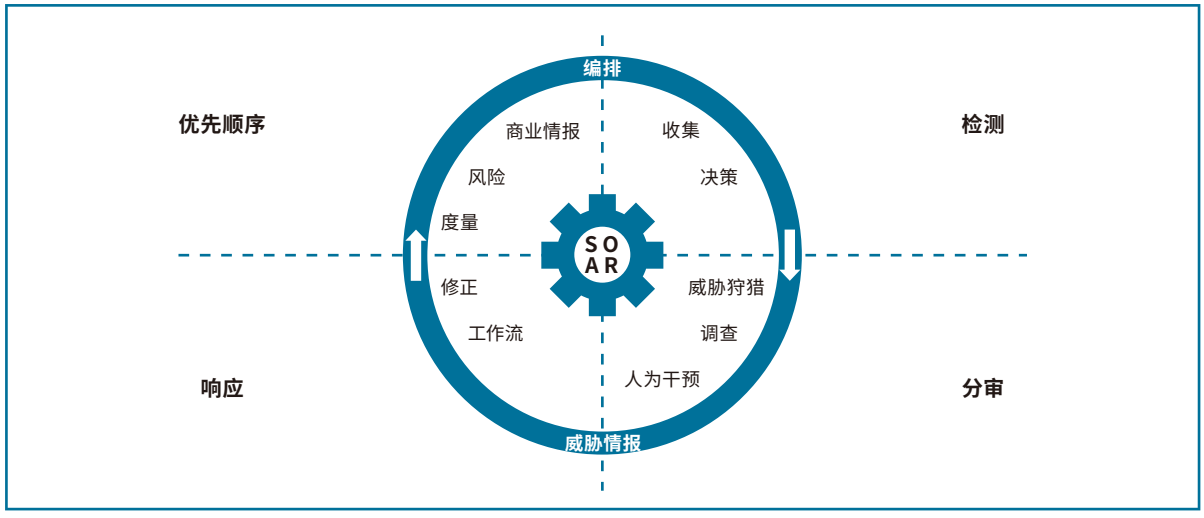


▲ 基于MITRE ATT@CK框架的Use Case设计示例

响应处置工作是安全运营中较为复杂的部分。传统的做法是，加固人员按照威胁处置建议逐个完成响应动作，但一方面担心操作经验的缺乏导致响应效果无法保证，另一方面担心加固存在遗漏导致同类威胁频繁发生甚至转变为事件酿成损失。

而响应处置脚本 Playbook 可有效实现响应工作的自动化编排，降低响应处置的平均时间，确保响应动作的完备和全面。Playbook 针对不同安全事件类型规定了最佳处置流程，划分工作优先级，使人员、流程、技术无缝融合在一起，共同完成从分析研判、误报确认、上下文信息收集、处置分工、效果核验、日志记录和总结归档等工作，大大缩短响应时间。

以深信服安全运营平台为例，在 SOAR 技术的赋能下，通过 Use Case 和 Playbook 等技术的应用，安全运营平台可帮助用户建立规范的监测与响应的流程，实现过程的自动化无感知，只需要在工单系统中对结果进行检查确认，实现闭环。值得一提的是，其中多产品联动处置的功能利用策略下发机制可协助用户实现以点带面的自动化安全加固。



▲ 安全自动化编排与响应SOAR技术框架

充分理解自身的资产以实现全方位的“自知之明”、明确监测能力覆盖的范围与场景以实现数据分析的“面面俱到”、采用全天候的监测模式以实现安全监测的“不眠不休”、提高响应自动化程度以实现安全运营的“事半功倍”。“四步走计划”的建设思路将协助各组织稳步提升自身的威胁监测与主动响应能力，从而能够在外部攻防不对等、内部安全监管趋严的大环境下，有条不紊地开展日常运营工作，胸有成竹地实现安全能力提升。

一

安全趋势洞察
AI是未知威胁检测的有效手段

据 MarketsandMarkets 人工智能网络安全预测报告，到 2026 年，AI 赋能的网络安全市场规模预计将从 2019 年的 88 亿美元增长到 382 亿美元，年复合增长率高达 23.3%。

市场增长的主要驱动力源于当前日益复杂的网络安全形势，网络犯罪和黑客攻击的规模和频率不断增加，且黑客不断试水新技术来进行攻击，未知威胁频发。安全团队对于未知威胁的抵御越来越捉襟见肘，行业开始寻求更先进的解决方案来抵御未知威胁。深信服认为，为达成上述效果，在未知威胁检测方面，AI 技术具有不可替代的优势。

为什么利用 AI 能够检测未知威胁?

泛化能力越强，检测未知威胁的能力就越强 , 检出率就越高。

随着新型病毒的大量出现以及网络攻击的愈加频繁，现在业界普遍使用的基于规则或特征码的检测方案的有效性正在变得越来越低。一方面，黑白名单和传统特征规则只能处理已知的恶意软件，而对于未知攻击，这类检测方案的效用通常很低。另一方面，攻击者的技术升级，新型恶意软件越来越多，安全专家通过人工分析恶意样本以提取新规则或特征码的难度大大增加。

而基于人工智能的恶意文件查杀引擎优于传统基于特征码的查杀引擎，原因在于机器学习、神经网络等 AI 技术具有泛化能力，通过使用已知样本进行训练就可以在未知样本集达到很好的效果，因此可以发现新型的恶意文件。

以黑样本为例，在攻击手段迭代更新的过程中，黑客并不总是另起炉灶来重新制作攻击向量。他们常常是通过对现有攻击手段进行优化、整合和更新，进而实施下一次攻击。因此，**未知威胁和已知威胁通常具有某种意义上的相似性。而 AI 检测算法就是期望通过对已知数据的学习，提取其中的固定模式，最终达到检测相似未知的目的。**相似的，白样本的演进流程中同样存在这样的比变量，比如开发代码复用等。综上所述，安全检测场景中的泛化能力其本质是检测算法是否能够提取潜在的固定模式，进而在相似样本集上输出一致的检测结果。

那么，如何评估检测算法的泛化能力呢?

基于前面对泛化能力的分析，深信服安全专家给出了检测算法泛化能力的一个评估方法：检测算法的泛化能力等同其对相似样本检测结果的一致性。

简单来说，可以通过以下两步来衡量一个检测算法的泛化能力：

- 定义样本相似性，用来描述你的泛化需求。比如指定相差 10 条指令的恶意文件为相似文件，那么你所关注的就是在已知样本和未知样本拥有 10 条指令差异下的泛化检测能力。
- 统计检测算法在这些相似样本上的结果一致性。一致性是表示检测算法输出的统一程度，具有强泛化能力的检测算法应当在相似样本上输出相同的检测结果。因此，一致性越高，则说明算法的泛化能力越强；反之，泛化能力越弱。

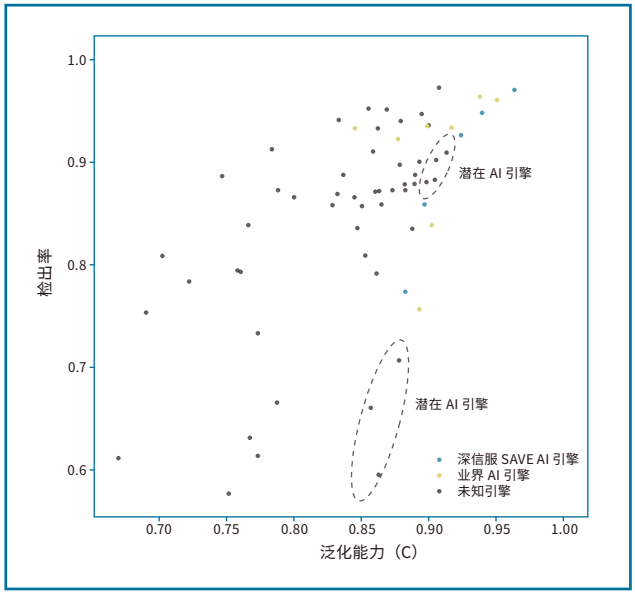
泛化能力的量化评估公式具体如下：

- 随机选取 N 个样本集，每个集合内的样本相互间具有相似性，标记为 $S_1,S_2,...,S_n$。
- 对每一个集合 S_i, 评估检测算法的结果一致性。假设 S_i 有 M 个样本，将算法的检测结果序列记为 $o_1,o_2,...,o_M$，计算 $o_1,o_2,...,o_M$ 表征的熵，记为 e_i。假设此检测任务的理论最大熵值为 E，则可以使用 $E-e_i$ 表征算法对 S_i 的结果一致性。
- $C= E- (e_1 + e_2 + ... + e_N)/_N$ 则表征了算法在整个样本集上的平均一致性 , 即泛化能力。

业界引擎的泛化能力分布

目前很多安全产品中都集成了恶意文件检测能力，在 Virustotal 平台上就有 70 多家的恶意文件检测引擎。从公开信息上看，不少检测引擎都标称采用了机器学习算法。那么现在业界检测引擎的泛化能力到底如何，AI 检测引擎之间是否有差异?

我们构建了包含 15 万黑样本的共 7256 个相似样本集。这些样本覆盖了 2019.1.1~2020.5.20 期间的线上热门样本。此外，通过 VT 平台获取 70+ 业界引擎对相似样本集的检测结果（手动触发重分析，确保为引擎最新结果），以公平比较他们的泛化能力。如下图所示。图中的每一个点对应 VT 上一种检测引擎，其中蓝色的点表示深信服 SAVE 引擎的 AI 模型在不同配置下的效果；黄色实心点表示可从公开信息确认的业界机器学习引擎；灰色的点表示技术路线未知的其他引擎。



▲ 业界引擎的泛化能力分布

从图中可以观测到，检测率的整体趋势是随着泛化能力增强而增强。将业界所有引擎综合起来看，随着泛化能力数值变大，检出率的变化范围越来越窄，并最终收敛到 100%。

大部分业界已知 AI 引擎均较其他未知引擎有更强的泛化能力，而未知引擎的泛化能力普遍较弱。但部分技术未知引擎也体现出了很强的泛化能力，可能也使用了 AI 技术来支撑检测。

相较于其他所有引擎，深信服安全智能检测引擎 SAVE AI 模型几乎总是能在相同检出率下，达到最强的泛化能力。需要注意的是，此 AI 模型训练于去年 10 月份，相似样本集中约有一半样本属于 AI 模型的未知样本。

如何构建泛化能力

以深信服 SAVE 安全智能检测引擎为例，SAVE 在设计过程中，从样本质量、特征设计、算法组合、以及模型训练方法等多个维度来思考 AI 的泛化能力构建方法。

提升泛化能力的前提是理解泛化的本质。因此深信服构建了多个内部系统来支撑算法团队对样本演变过程理解和使用，比如 NLP 标签系统和 Origin 相似代码搜索系统：

数据标签的质量决定了最终 AI 模型的能力上限。我们利用 NLP 技术将样本来自多个源头的文本标签信息进行整合（黑白标签，家族标签等），用以提升数据标签精度以及信息含量。通过 NLP 系统处理过的标签，可以更好的掌握样本间的家族关系。

为了从更深层次理解样本代码的关联关系，我们基于大数据平台构建了 Origin 系统。通过 Origin，可以从海量样本中进行快速的相似代码匹配，定位样本代码片段的来源、属性、以及演变过程。更可以对线上样本进行快速的聚类分析，加快对问题的闭环速度。

随着对泛化能力本质的理解深入，SAVE AI 算法也在持续演进。前述分析系统获得的准确标签和关联关系，支撑安全专家不断挖掘更优质的判别输入，选择更有效的高维特征提取方法，细化模型的检测的功能，以及提升模型的精度。与此同时，为了保证 AI 模型的泛化能力持续保持在较高水准，深信服对端到端的训练流程进行了分布式重构。通过分布式集群，可以在数千万量级的样本集上，以天为单位进行模型更新迭代，确保线上模型效果的稳定性。

恶意软件的检测流程往往是将 AI 检测算法和传统检测算法结合使用，大致有两种思路来进行整合：第一种是以传统检测技术为主，同时以 AI 为辅来提升未知检测能力；第二种是以 AI 能力为主，尽可能释放 AI 模型的泛化能力，同时利用其他手段来提升鉴白能力。

从前面的实验结果看，业界大部分基于 AI 的文件检测引擎的确较其他类型引擎有明显的泛化能力提升。为提升对未知威胁的检测能力，适应病毒瞬息万变的发展态势，厂商应尽可能释放 AI 模型的泛化能力。

新基建背景下，如何搭建数据与业务之间的“桥梁”

8 月 14 日，第八届中国电子信息博览会（CITE 2020）在深圳会展中心举行，本届博览会以“创新共享 开放合作”为主题，深信服 EDS 存储运营总监杨欢应邀出席，并发表题为《新基建、新数据、新存储——软件定义存储应用与实践》的主题演讲，他表示新技术、新业务催生出了新的数据存储需求，存储系统必须拥有强大的数据承载能力，以实现数据价值增值。

▲ 深信服 EDS 存储运营总监杨欢发表演讲

新基建下数据存储挑战激增

2020 年以来，国家明确将“新基建”作为未来经济增长的驱动力，其涵盖了以云计算、人工智能、5G、数据中心等为代表的众多数字化基础设施，其中最核心的资产便是数据，而存储则是数据与业务之间的“桥梁”。在云计算、大数据、人工智能等一系列新兴技术的驱动下，业务形态正在发生转变，存储需要面对全新的数据挑战。

1 数据体量持续爆炸式增长

据 IDC 数据统计报告，2020 年数据体量将达到 44ZB，2025 年数据体量将达到 164ZB。

2 数据类型将更加多样

不同的业务系统将产生不同的数据类型，对于块存储、文件存储、对象存储需求需要同时满足。

3 数据处理效率要更高

大规模图像业务、视频应用都在往智能分析、大数据分析方向发展，对于这些数据处理要有更快的读写速度。

4 数据安全防护要更全面

存储设备软硬件的故障、人为操作的误删、外部病毒的攻击都会对数据安全造成威胁，数据安全需要全方位防护。

5 数据价值将被进一步共享和挖掘

当下数据都在追求全局最大化共享，旧数据将被重新分析以产生新的价值。

在全新的数据业务场景下，存储需要具备高扩展性、高性能并满足多资源存储需求，保障数据的安全性，同时实现数据的实时共享。

四大核心场景下深信服 EDS 存储的价值呈现

在此次主题分享中，杨欢基于四大核心应用场景，结合不同场景下的挑战分析了深信服企业级分布式存储 EDS 的价值，包括智能型的视频监控场景、海量数据的长期保存场景、数据中心统一存储场景以及融合 + 数据增值场景。

智能视频监控场景

所谓智能视频就是加入 AI 技术处理的视频监控场景，具体包括智慧交通、平安城市、人脸识别等。这一场景的特点是数据增长迅速且体量庞大，并有海量的小文件处理需求。海量数据在存储和使用时会面临元数据索引效率低和扩容困难的问题。深信服 EDS 采用全对称分布式架构支持 EB 级别的存储容量，并实现按需弹性扩容；以创新分布式数据库 KV 实现百亿小文件高性能读写；通过 AI 技术实现涵盖故障预测、趋势分析、智能 Qos 的智能化集群管理，降低运维成本同时优化业务体验。

海量数据长期保存场景

根据国家法律法规要求，部分行业客户数据要实现 15 年甚至永久保存。在进行数据保存时用户普遍会面临投入成本过高、数据可靠性差的问题。深信服 EDS 通过自动数据重构、自动数据平衡分布、自动数据迁移、全生命周期迭代四大能力保障数据的超长期保存，这一极致高性价比存储方案，让 15 年数据存储相较传统方案实现 TCO 成本降低 75%。

数据中心统一存储场景

这一场景要求存储要具备高性能实时响应能力，同时满足多类型的存储需求。在兼容性层面，深信服 EDS 通过多协议接口实现一套存储满足业务对于块、文件、对象等多种存储服务的需求，并实现不同协议共享调度保障数据互联互通；在性能层面，据泰尔实验室测试结果显示，EDS 在结构化数据场景下可低配置实现 34 万 IOPS，非结构化数据场景实现 100 亿文件性能衰减低于 5%。在安全层面，EDS 利用人工智能技术，实时收集各节点的信息，在故障发生之前就能预判软硬件的风险点，并加入病毒防控查杀、数据安全兜底方案保障业务的正常运转。

融合 +，数据增值场景

EDS 利用容器技术，建立围绕存储的“应用商店”，将备份软件、网盘软件直接预装到 EDS 存储平台中，可以直接在 EDS 的容器上安装备份和网盘软件。同时实现数据的平台化，统一平台管理实现数据互联互通，支持 ISCSI/NFS/CIFS/FTP/HDFS/S3，并支持相同数据不同协议互操作，对于后续的数据管理、共享利用都更加便捷高效。深信服 EDS 深度融合，集成数据应用，不仅仅发挥数据价值，同时立足存储，关注数据的安全和可用。

早在 2013 年深信服便开始了对软件定义存储的布局，为各个产品线持续提供技术模块输出，七年的时间积累了大量的实践经验。如今深信服独立的分布式存储产品 EDS 已经为不同领域的上千家用户提供服务，多项指标已经处于业界前沿。未来，深信服 EDS 将持续强化产品力，为千行百业数字化转型提供更坚实的数据底座。

一

一个关于农商行数字化转型的“春天”

农信社一直以来都是农村金融市场最重要的金融机构，2000 年 8 月，在人行的批准下，江苏省率先开展了农信社改革的试点工作，2003 年国务院印发了《深化农村信用社改革试点方案的通知》（国发〔2003〕15 号），将改革试点扩大至全国 8 省市，明确提出要对农信社的管理体制进行改革，由此农商行的发展迎来了春天。

随着市场目标客户群体的变化，互联网金融的兴起，外部市场云计算、大数据、AI 等技术的广泛验证使用，“数字化转型”已经引起越来越多的农商行客户重视，这不仅是农商行业务模式的转变，更是农商行实现科技信息化的重要抓手，主要体现在如下几个方面：

业务量大幅增长推动 IT 基础架构转型

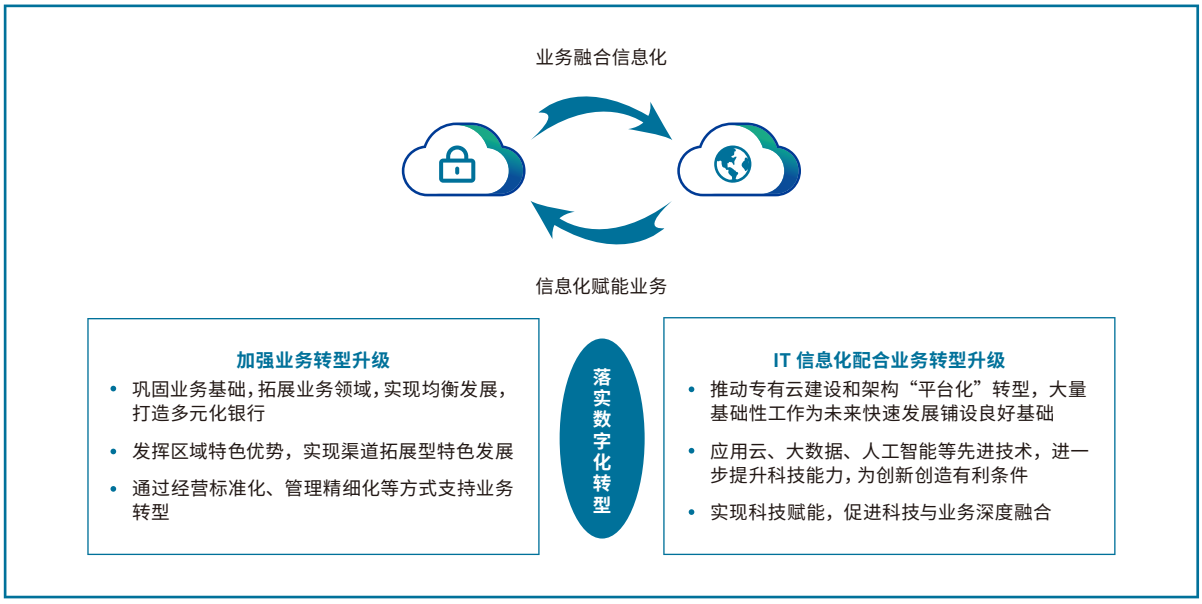
移动互联催生出了移动金融、互联网金融、手机银行、网上银行、电子商务支付平台等新型业务系统，金融产品与服务已经呈现出了“小微化、高频化”趋势，信息系统业务量也快速上升，新产品发布日益频繁，甚至每天就要做业务系统补丁或版本小范围升级。业务量高速增长、适应频繁变化、成本控制与严苛的业务高可用性要求对集中式架构提出了严峻挑战，这就需要更弹性、更经济的 IT 架构作为农商行客户的补充。

业务经营综合化要求应用系统多样化

金融服务场景愈发多样，农商行与证券、基金等各类金融机构之间合作愈加频繁，各个银行机构也纷纷试水电商零售等业务，例如，农商行推出的理财业务、基金业务等，都是打破农商行单一业务模式、增加农商行收益的新尝试。在快速实现业务系统上线运行和服务客户的同时，对于系统软件承载的稳定性、高性能、快速变更等都提出了更高的技术要求。

分布式架构技术日益广泛与成熟

传统集中式三层架构发展的放缓，处理能力已经难以满足业务高速增长要求。计算虚拟化、高速网络与分布式存储技术的广泛使用，为分布式架构的广泛应用奠定了基础。



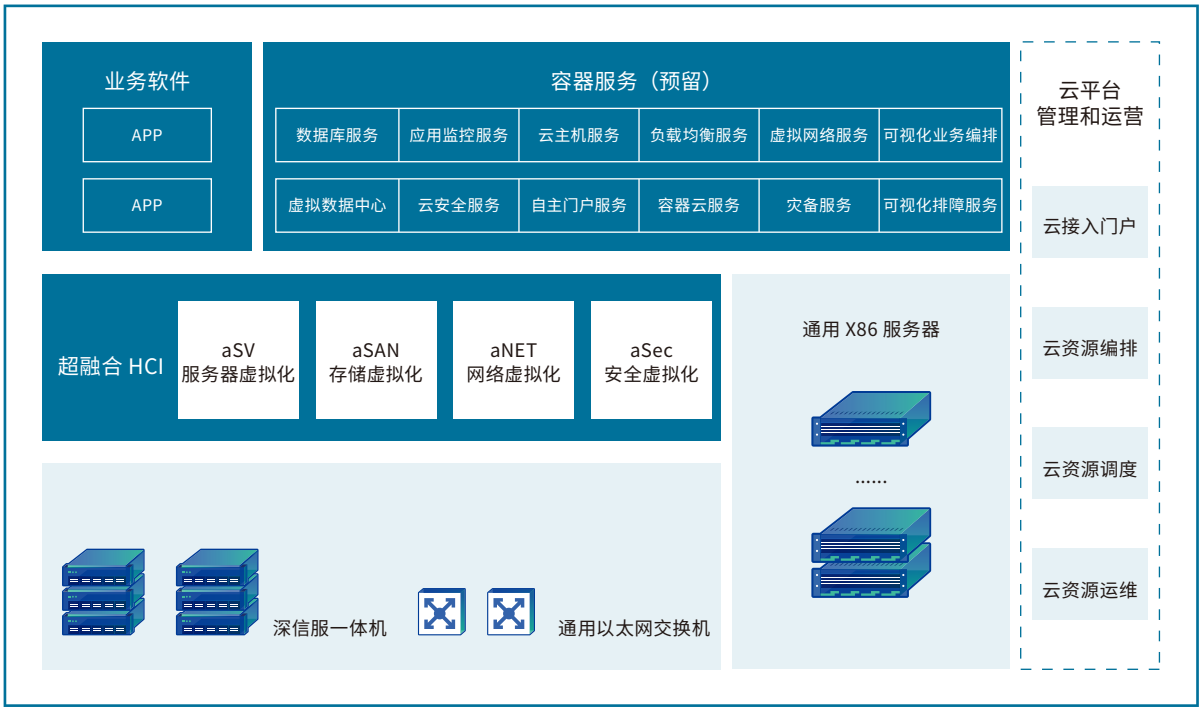
对于大部分的农商银行客户而言，伴随着数字化转型的落地与实践，打破业务单一来源模式，增加新业务系统的盈利模式，提高农商行抗风险的能力，这背后都是对信息化 IT 架构稳定运行、灵活多变的新尝试、新挑战、新要求，农商行用户希望能够采用更灵活、具备弹性、快速投入使用的 IT 基础架构多资源池，借助于大数据、AI 等技术更精准可靠的推送给目标市场群体客户，满足当下使用的同时，还能从容对应未来发展的变化。

深信服超融合为深圳农商行开发测试平台注入新活力

随着“信息化科技赋能业务”成为银行业的共识，深圳市农村商业银行也提出来“零售 + 科技”的发展战略，手机银行、互联网银行就成了业务发展的重要门户，业务软件系统需要更好的技术框架体系支撑并落地实现，同时也能够更好的服务于传统核心业务系统软件的运行和持续开发迭代，深圳农商行对于构建新一代本地数据中心的开发测试分区提出了如下需求：

1. **稳定承载新业务系统的开发测试一体化平台的落地、迭代**
2. **具备更加灵活的 IT 基础架构资源，实现灵活的分配资源、释放资源、调度资源**
3. **未来能够通过该架构平台可以支持并对接容器云平台，具备更好的适配性**
4. **更具价值回报的建设成本，减少对资源及空间的浪费，提高资源使用率**
5. **资源的统一管理及维护，解决后期 IT 运维压力**

根据深圳农商行对开发测试分区资源使用、部署的实际情况，本地数据中心既需要满足灵活上线、快速拓展等敏捷需求，又要确保业务安全与可靠，与此同时，还需达到服务器简单运维的诉求，决定采用深信服超融合架构作为本次开发测试平台的建设方向：



整体开发测试云平台基于深信服超融合 HCI 基础架构打造，将客户现有的开发测试系统、准上线系统、开发中间件、开发测试用例等内容全部迁移到了深信服超融合平台上。深信服创新打造的简单、稳定、高性能、安全的产品平台，更好的帮助用户实现开发测试云平台的建设，具体体现在：

数据安全可靠

通过超融合虚拟化，实现数据的实时备份，实现物理故障对业务的零影响，保障业务的良好有序运行。

多平台统一化管理

通过统一的 Web 界面进行计算、网络、存储全资源的管理，让管理运维更加便捷、简单，零学习成本，大幅释放运维人员的管理压力。

平台更灵活

加速项目开发部署和业务需求响应速度，缩短 IT 基础设施资源的交付周期，进而缩减项目整体实施周期，实现 IT 的价值转型。

更具价值的平台

控制 IT 投资成本，实现更加精细化的 IT 成本控制，同时提高资源利用率，节省机房空间，并且适应以后三年的业务上线需求。

在云计算业务上，深信服经过八年的积累沉淀，服务了全国超过 200 家金融客户，包括交通银行、民生银行、中国银行、华夏银行、建设银行、华润银行、深圳农商行等，覆盖银行、保险、证券、期货等行业。

2020 年，深信服重磅升级云计算战略，推出信服云品牌，以全新的战略、能力和解决方案亮相，从以超融合承载业务应用为中心，变成助力数据中心的云化演进。升级后的信服云，能为用户提供包括虚拟化平台在内的软件定义数据中心全套解决方案。

未来，具备全栈生态能力的信服云，将继续充分利用技术和平台优势，快速助力用户实现新形势下数据中心的云化演进。

一

“安全”“上云”二者可否兼得？

近日，由国家发改委、科技部、工信部、国家广电总局、国家互联网信息办公室、中国工程院、中国科学院、中国科协和天津市人民政府共同主办的第四届世界智能大会在天津举办。大会以“智能新时代 创新、赋能、生态”为主题，采用云上办会全新模式，打破线上线下的空间桎梏，搭建“云上世界智能大会”平台。

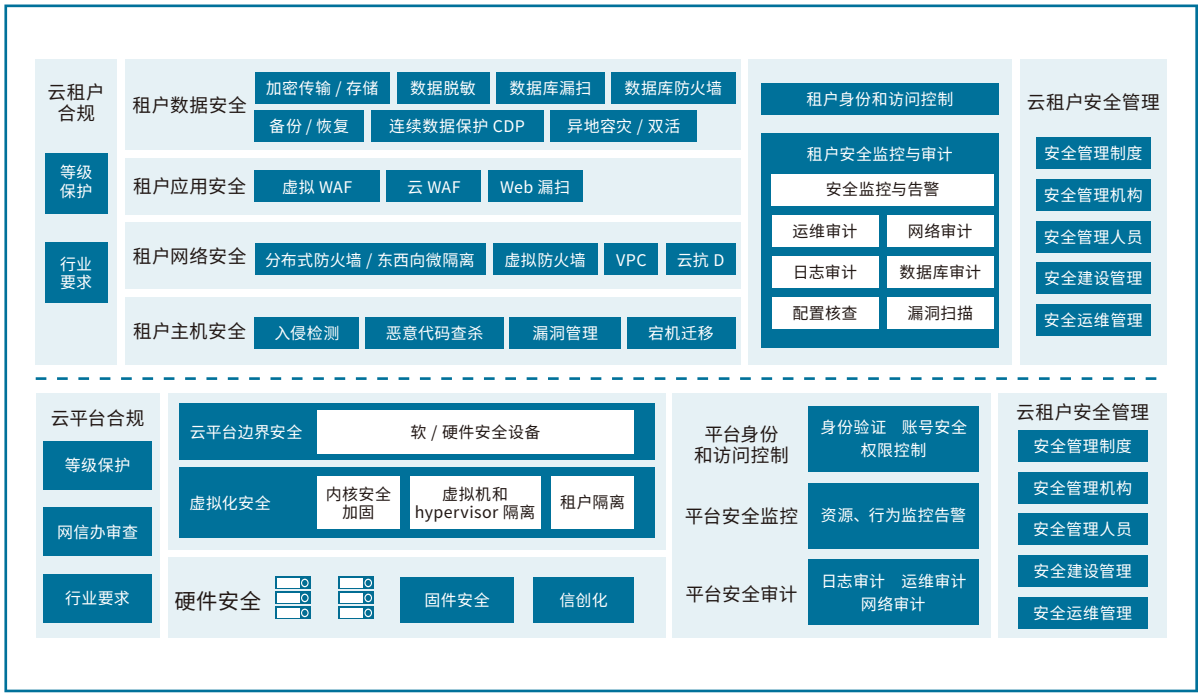
在云主题峰会中，深信服云计算专家欧阳瑞彬以《云数据中心如何“长出”内生安全能力》为主题，与大家深入交流在智能产业下的云数据中心安全建设思路。

安全能力如何融入云计算环境？

数据中心本身承载着企业的数据及业务，因此用户一般关注对数据和业务会造成比较大影响的威胁。与传统的数据中心不同，云数据中心算力集中，具有“高度集成”、“按需交付”、“快速部署”的特点，同时还产生了一些特有的云安全威胁：

- IT 架构不断变化，难以持续提供业务保护
- 缺乏丰富的安全服务目录，云服务商难以满足云服务用户的个性化安全需求
- 云上安全不可视，缺乏适宜的技术手段
- 合规要求日趋严格，平台与租户均需满足
- 业务集中运维带来运维管理工作的压力

针对数字化转型中的云安全威胁，如何全面应对是关键。深信服分享了云数据中心安全建设思路：围绕“云内安全能力、安全联动防护体系、自动化运营”三大特性打造全生命周期的云数据中心安全体系。

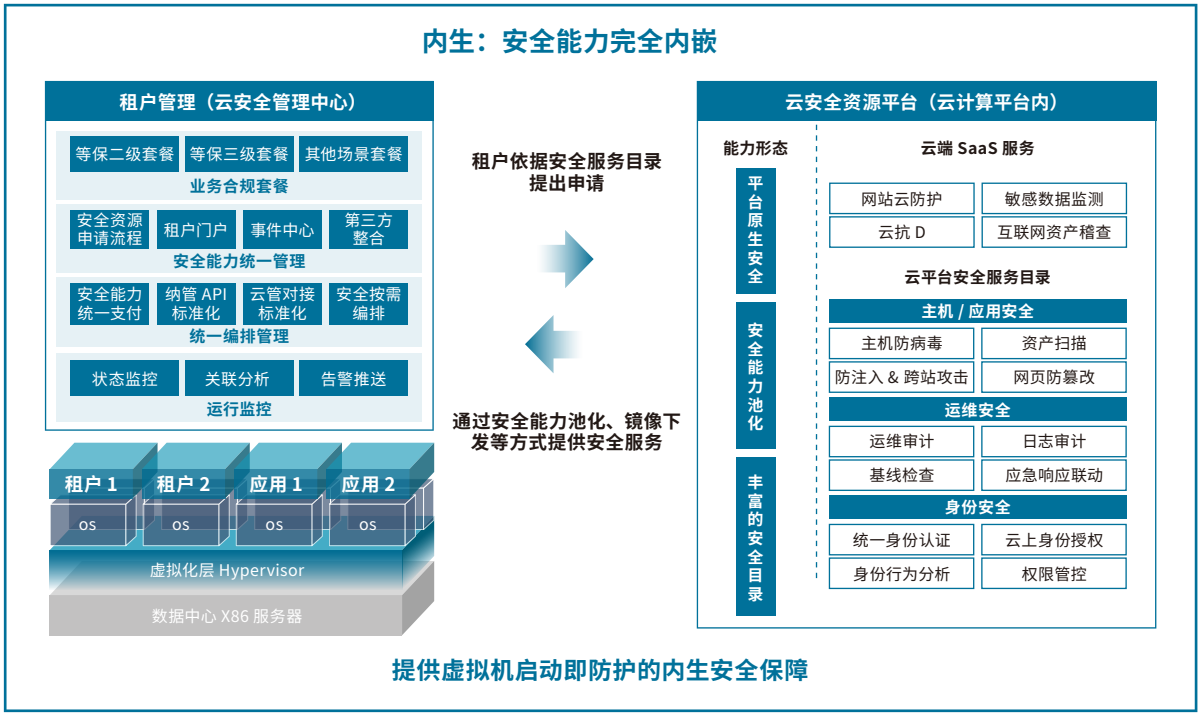


▲ 云安全整体架构

深信服云数据中心安全体系核心能力

1 云内长出安全能力，保障云平台和租户安全，满足合规要求

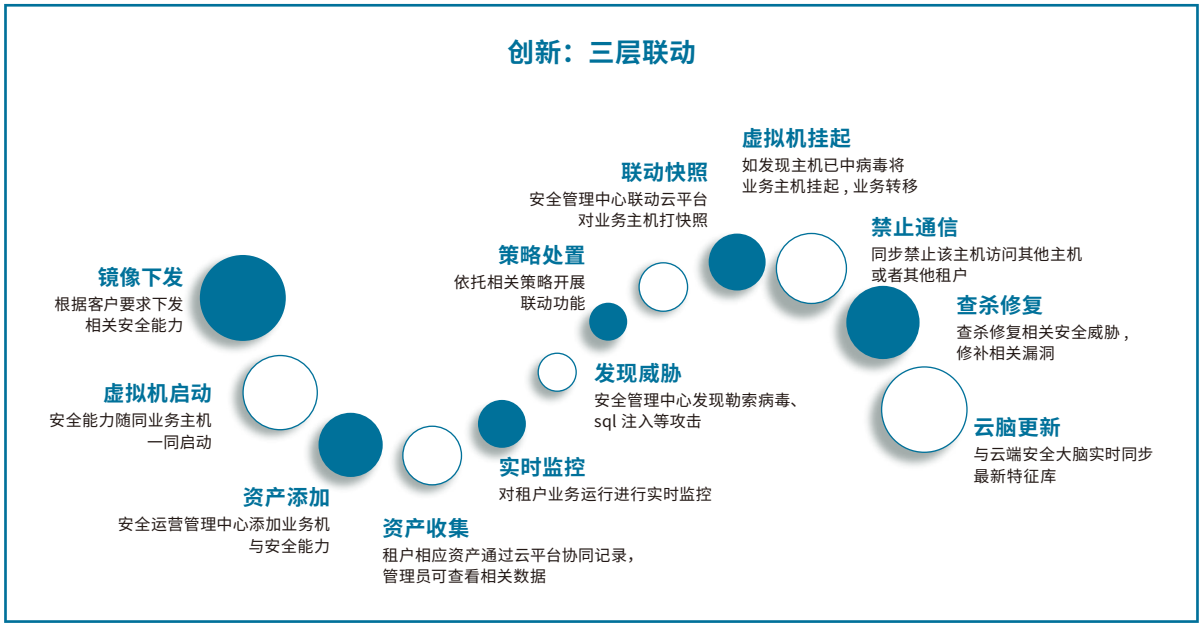
深信服云计算打造开放兼容的云安全平台，按需集成安全组件，内容涵盖硬件安全、虚拟化安全、边界安全等维度，为云上业务或租户敏捷交付安全能力，满足合规及业务的个性化需求。



另外，深信服云平台根据“一个中心，三重防护”的思想进行云计算平台以及云服务用户的业务应用系统的等级保护建设，具备满足等级保护三级要求的能力，且满足国家信息中心发布的《政务云安全要求》及网信办增强型网络安全审查要求。

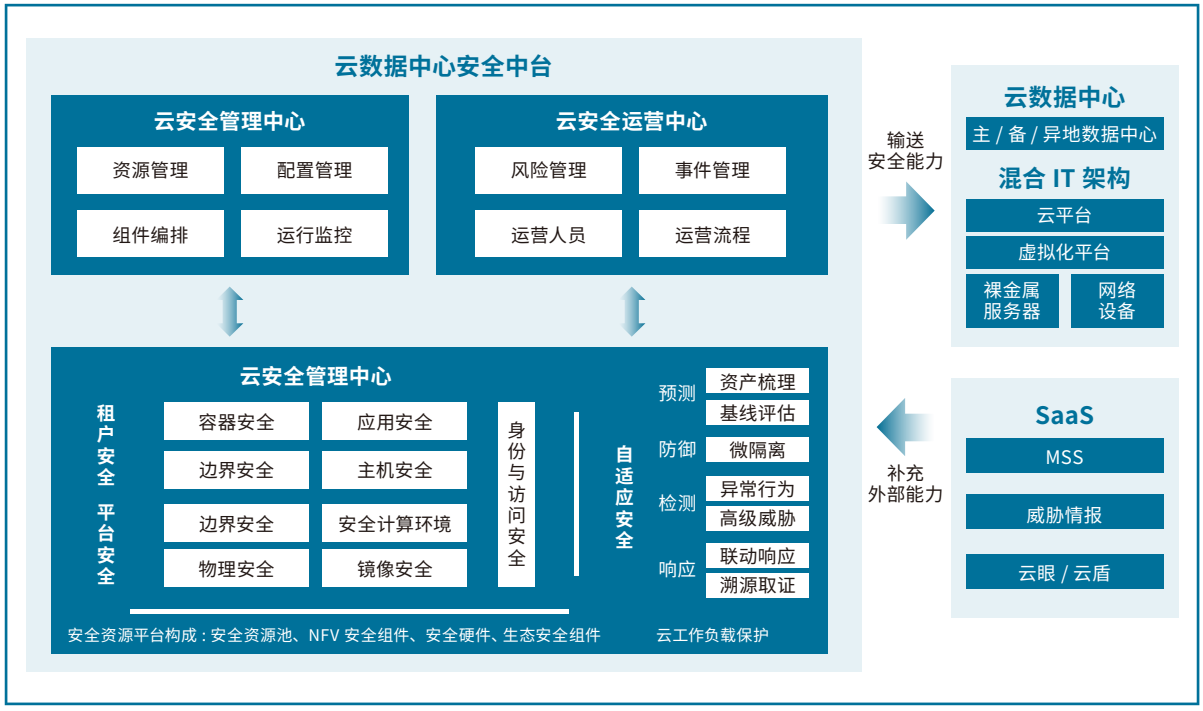
2 构建以“业务为核心的”三层安全联动防护体系

深信服基于在安全领域的深厚积累，保障云平台安全的基础上，建设云内自适应防护体系，解决云内风险不可视不可控的问题，为租户提供全面的安全保障手段；适应未来 IT 架构变化，持续业务保护。通过预测、防御、持续检测、快速响应、全天候安全运营，构建系统化智能协同联动防护体系，有效保障用户承载业务的安全。



3 持续业务保护，建设云安全运营中心，进行自动化运营

建立面向云数据的中心的安全运营平台，通过 SOAR 提升运营效率，人机共智保障运营效果，解决安全运维压力大的问题。



深信服云数据中心安全中台在满足前面三大特性的同时，基于软件定义安全技术，连接云安全资源平台、云安全管理中心、云安全运营中心三部分，持续为云数据中心的 IT 基础架构或业务应用输送安全能力。

企业进行数字化转型，向软件定义的基础架构转变过程中，深信服云数据中心安全中台能够帮助用户在快速迭代、规模庞大的云计算环境中，更好地应对安全风险，拥抱变化，并能够让云上安全管理更简单、更高效。

信服博士谈存储
浅谈分布式存储中的网络通信

在各行各业数字化转型深入的当下，数据呈爆炸式增长。面对海量数据的存储需求，分布式存储显然在架构上有着天然优势，但在这波数据洪流之中也面临着性能上的全新挑战。

由于分布式存储的工作原理是将各个存储节点使用网络互联的方式构建为集群，向外部提供更加可靠的高性能服务，因此可以说分布式存储本质上是一种网络存储，其性能在很大程度上受网络的影响。

在高性能的分布式存储中，使用传统的 TCP 网络进行各存储节点之间的网络互联很容易形成网络瓶颈，**而在分布式存储最容易让用户诟病的 IO 延时方面，网络部分的开销是不可忽视的一部分。**

随着网络带宽的高速增长，在软件上的消耗已成为网络性能的瓶颈，而通过绕过 CPU 实现高性能传输的 RDMA 网络成为分布式存储不错的选择。

RDMA（Remote Direct Memory Access），可以简单理解为网卡完全绕过 CPU 实现两个服务器之间的内存数据交换。其作为一种硬件实现的网络传输技术，可以大幅提升网络传输效率，帮助网络 IO 密集的业务（比如分布式存储、分布式数据库等）获得更低的时延以及更高的吞吐。

最初的 RDMA 是实现在 IB（Infiniband）上，由于其新的硬件技术栈成本比较高，主要用于 HPC（高性能计算）等少数场景。而新的技术发展下，能够实现在以太网上使用 RDMA。

当前 RDMA 在以太网上的传输协议是 RoCEv2，RoCEv2 是基于无连接协议的 UDP 协议，相比面向连接的 TCP 协议，UDP 协议更加快速、占用 CPU 资源更少，但其不像 TCP 协议那样有滑动窗口、确认应答等机制来实现可靠传输，一旦出现丢包，依靠上层应用检查到了再做重传，会大大降低 RDMA 的传输效率。

所以要想发挥出 RDMA 真正的性能，突破数据中心大规模分布式系统的网络性能瓶颈，势必要为 RDMA 搭建一套不丢包的无损网络环境，而实现不丢包的关键就是解决网络拥塞。**在解决拥塞问题的关键在支持 ECN 等特性的交换机，而这个技术在一般的交换机都普遍支持。**

既然 RDMA 是一个硬件技术方案，而且在分布式存储中又能快速地解决网络高延时等相关问题，是不是直接更换上这个新的硬件技术就能万事大吉？**实际可能并没有那么简单，那么我们就来简单聊聊 RDMA 技术实践过程中踩过的坑。**

RDMA 想说爱你却不容易

对于“增强”具体体现在哪里，Gartner 研究总监孙鑫先生有过这样的解释：“首先体现在业务，不是技术。在增强型分析技术的支持下，分析的门槛降低了，业务人员主动进行数据分析，并不依赖类似技术人员提供的‘报表’。”

1 RDMA 的使用需要应用程序的代码配合（RDMA 编程）

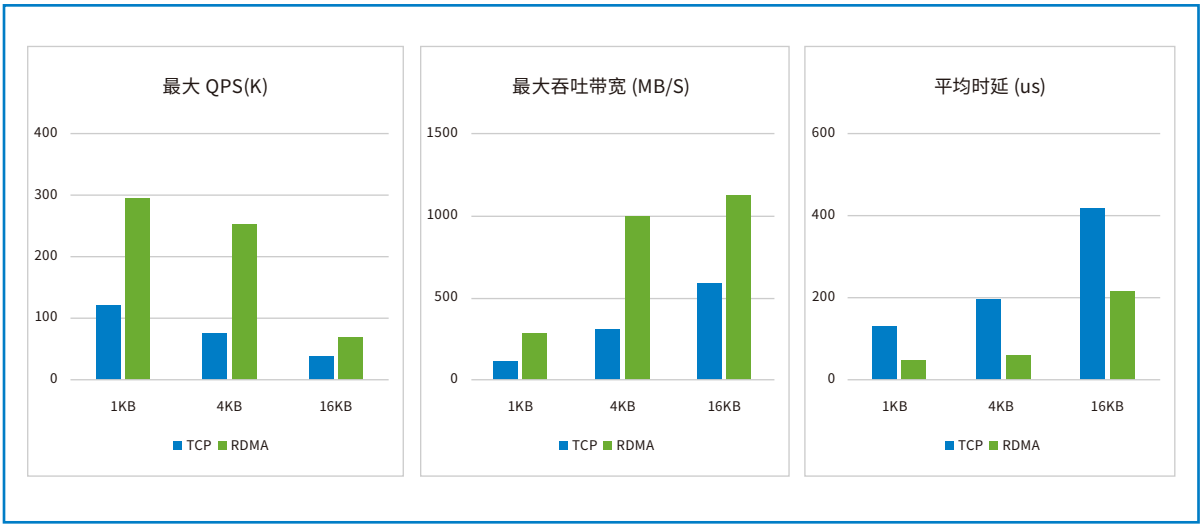
RDMA 操作的语义更加贴近硬件实现的语义形态，与传统 TCP/IP 的 Socket 编程有很大的差别，不能直接将现有程序简单地直接套用 RDMA 接口，而使用原生 RDMA 编程库比 Socket 编程要复杂很多。

并且在编程方式上 RDMA 编程是异步的，而原始的 Socket 编程是同步的。这样将导致对大多数开发者来说，无论是改造原有应用程序适配 RDMA，还是写一个全新的 RDMA 原生应用程序，都不容易。

那么如果完成了 RDMA 对接，是否就能使我们的程序获得高性能呢？我们再看看在通信模块中对接完 RDMA 的对比性能测试。

2 RDMA 在 RPC 模块中使用

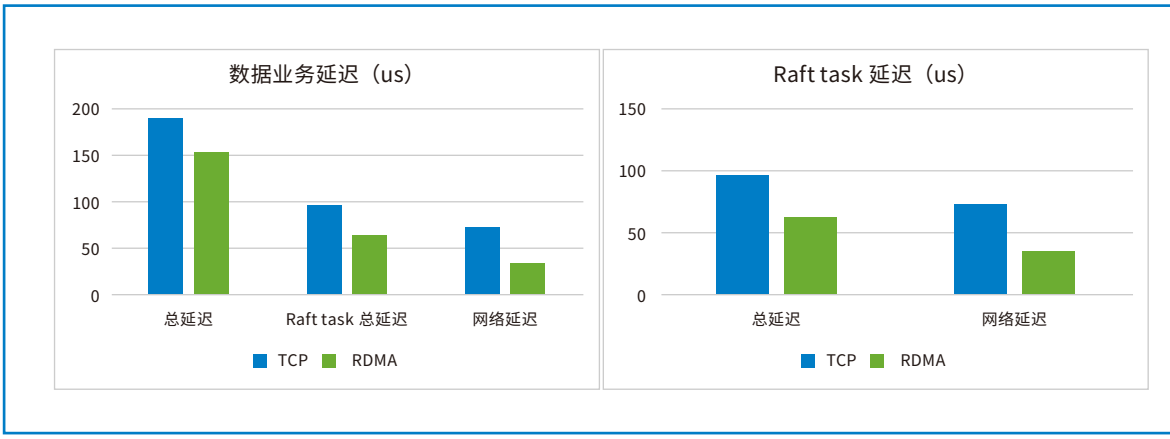
分布式存储中通常使用 RPC 框架进行节点之间的通信，RPC 性能对整体的存储性能有重要的影响。笔者团队实现了一个基于 C++ 的 RPC 框架，可以灵活支持多种数据传输协议并支持协程快速处理，适用于有高性能需求的场景。该 RPC 框架同时支持传统 TCP 和 RDMA 两种传输方式，RDMA 方式下注册了统一管理的 RDMA 内存，并采用双边操作进行数据传输，支持事件和轮询的请求检测机制。笔者团队对两种传输方式的性能进行了对比测试，测试结果参见下图：



▲ RPC TCP 与 RDMA 性能测试

（测试说明：使用同一张 10Gb 网卡，采用不同的模式进行对比测试）

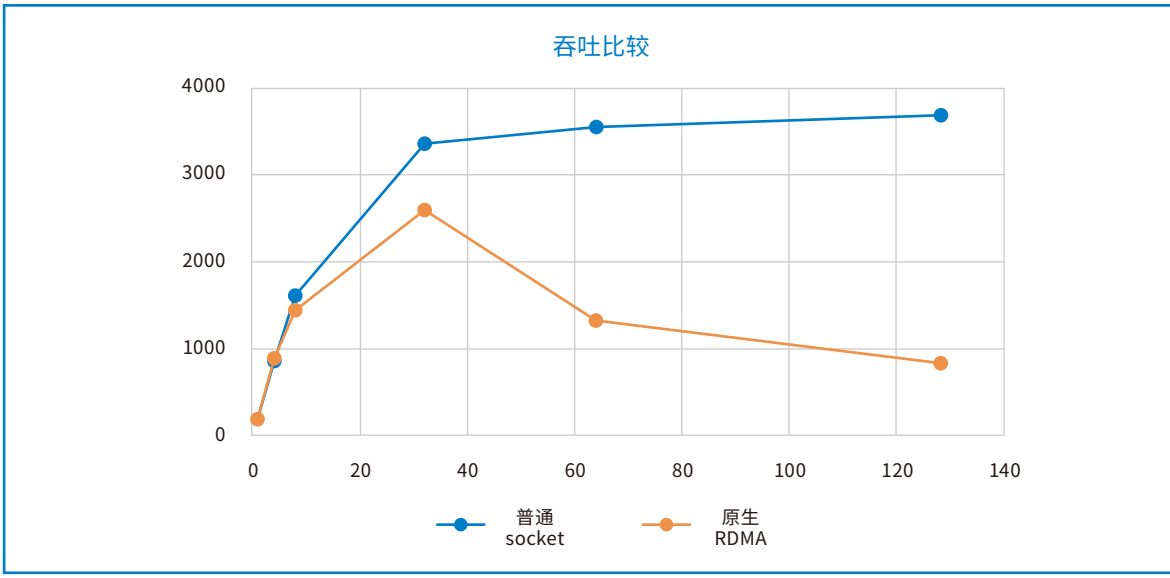
通过测试我们发现 RDMA 的方式具有明显的优势，尤其在低深度的场景下能获得更好的性能。我们继续将 RPC 对接实际业务进行了测试，在这里我们对接了一个基于 RAFT 一致性协议的多副本数据存储业务，测试结果参见下页图：



▲ 对接实际业务后的性能对比测试

从上面的测试结果看到，在包含有实际业务的测试中，RDMA 的表现并没有原始的 RDMA 测试表现那么优异，我们分析了其主要原因是线程切换、数据复制等操作以及 IO 路径上其它模块引入了额外的开销。

那么怎样才能发挥出 RDMA 的优异性能？在实践过程中我们也针对分布式存储系统 Ceph 分别使用 TCP 和 RDMA 进行了对比测试，测试结果也不是十分满意，我们发现在 Ceph 中对于小 IO 的场景使用不同的传输模式都没有明显的提升，甚至还有略微的下降，对于大 IO 的高吞吐情况，还会出现性能的明显下降，测试结果见下图：



▲ Ceph 原生 RDMA 1M 大块吞吐测试结果

在测试结果的基础上我们分析了 Ceph 中关于 RDMA 部分的实现，主要发现存在下面几个问题：

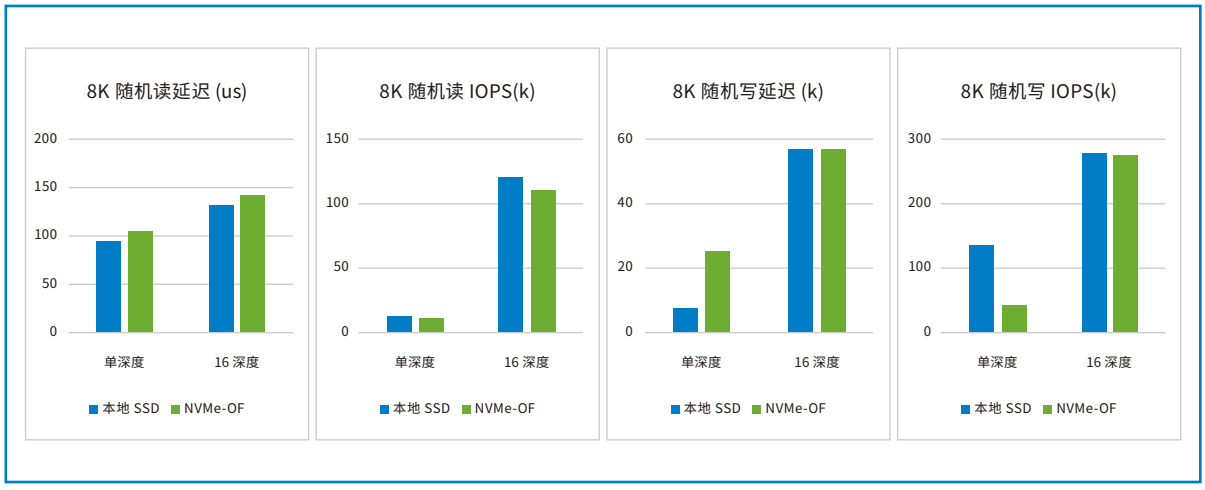
1、Ceph 中使用双边的编程方式，传输的过程并没有绕开 CPU，同时 Ceph 内部使用 bufferlist 的数据结构，需要多次进行内存拷贝，没有充分发挥 RDMA 中零拷贝的特性。

2、由于 RDMA 的异步编程模型，需要进行 Polling 来检测数据操作的完成，使用单独的线程轮询不但没有降低 CPU，反而有更多的 CPU 开销，而如果使用事件机制则会增加延迟降低性能。

RDMA 在上述的各个场景中，都没能充分发挥其优越性能，那么需要怎样的编程方式才能发挥其价值呢？笔者团队又探索了 SPDK（Storage performance development kit）的 NVMe-oF 中的 RMDA 使用方式。

3 RDMA 在 NVMe-oF 中的使用

NVMe Over Fabrics（NVMe-oF）是使用 RDMA 或光纤通道（FC）架构等 Fabric 技术取代 PCIe 传输，从而将把本地高速访问的优势暴露给远端应用的一种传输技术。在 SPDK 中实现了相关的逻辑，下图是分别通过 SPDK 的 NVMe-oF 的 target 访问与本地访问 SSD 的性能对比测试。



▲ NVMe-OF 与原始 SSD 的性能对比测试

通过上面的数据我们发现，通过 RDMA 的网络传输的性能和原始的性能非常接近，在单深度的情况下读延时只增加了 11us，写延时只增加了 18 us。通过多深度能够跑出与本地 SSD 相当的性能。上面的测试也进一步论证了正确地使用 RDMA 的相关编程技术是能够充分发挥出硬件优越性能的。

我们分析了 SPDK 中关于 RDMA 相关的实现，认为以下因素是 RDMA 编程实现的关键：

1、充分利用 RDMA 的内存注册机制，整个 IO 路径过程中使用内存池中的内存，实现全流程零拷贝。

2、对于控制消息（小 IO）使用 send/recv 的双边编程方式，对于数据消息（大 IO）使用 write/read 的单边编程方式。

3、RDMA 的 poll 与 NVMe 盘的读写处于同一个线程，整个过程没有线程切换，是全用户态的 IO 处理。

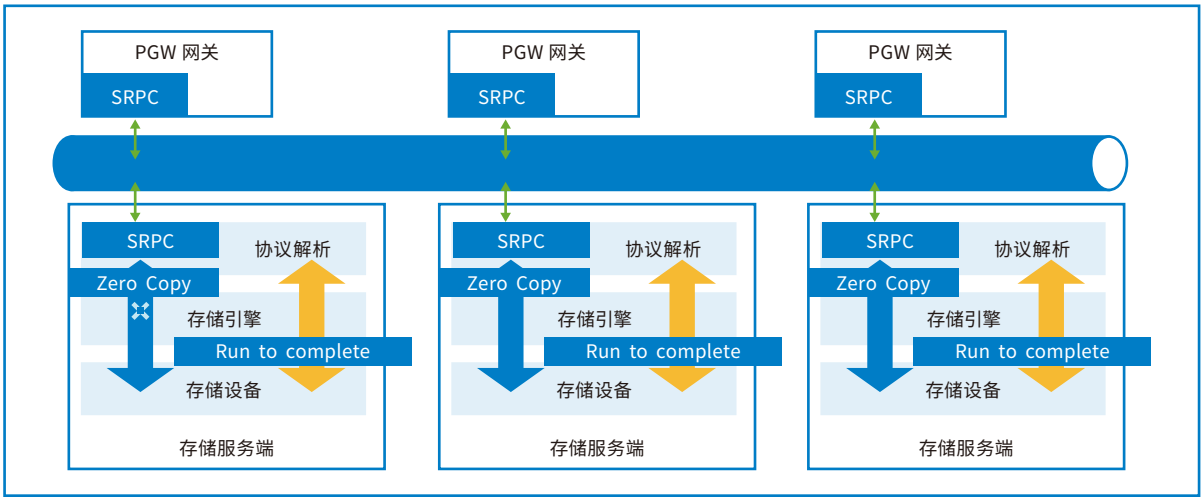
EDS 中的 RDMA 应用

基于以上对于分布式存储中 RDMA 使用的分析，笔者团队认为简单地生搬硬套发挥不了 RDMA 与新型存储设备的性能优势，从整体框架上进行 RDMA 适配，将 IO 路径上各模块联动优化才是分布式存储追求优秀性能之路。为此我们设计验证了面向 RDMA 的高性能分布式存储框架和实现方案，并在深信服企业级分布式存储 EDS 中落地应用。

EDS 针对 RDMA 网络和 NVMe SSD 设计了低延迟高并发的存储架构，将存储节点前后端网络使用 RDMA RoCE 接入，实现低延迟极速网络传输，并对 IO 栈上各模块进行了相应的优化设计。深信服 EDS 存储架构采用了 run to complete 和无锁化编程模型，并优化了各模块之间的数据处理，实现系统内全 IO 栈的内存零拷贝，使整体性能得到了极大的提升。

如下页图片所示，前端协议网关（Protocol Gateway，PGW）接收来自用户的多种协议类型请求（包括 NFS，SAMBA，S3，Swift，iSCSI，NVMe-OF 等），将这些请求封装后通过 SRPC 通信模块发送到存储服务端进行处理。存储服务端解析请求后由存储引擎进行相应的处理并访问存储设备完成数据的写入和读取。

前端 PGW 请求发送和回调、存储服务端请求处理采用 run to complete 的方式在同一线程完成，大幅提高单个请求的处理速度，并采用无锁化编程的方式启用多个线程分组处理请求，达到请求的高并发。此外设计了统一的数据缓存管理机制，整个请求处理过程从数据经 RDMA 接收后，经过各模块处理，再到通过 RDMA 发送出去，全程不需要对数据进行内存拷贝，进一步减少系统开销并大幅降低了延迟。



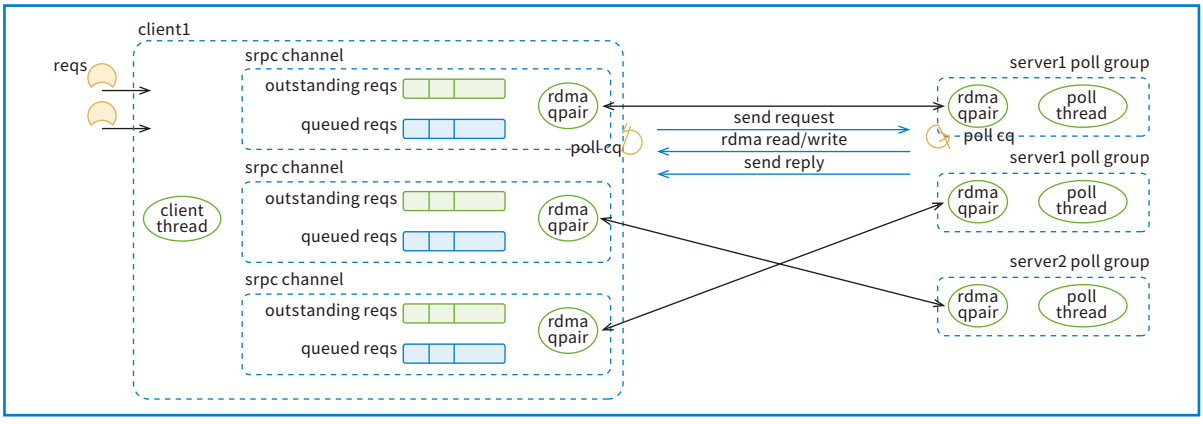
▲ EDS 存储软件架构示意图

SRPC 通信模块设计

1 通信架构

深信服 EDS 存储设计了面向存储系统消息传输的专用网络通信模块 SRPC，将上层多种类型请求消息封装，使用 RDMA 进行快速数据传输，可以灵活扩展支持上层 NVMe-OF、iSCSI 等多种类型协议，并对消息封装进行了抽象和简化，减少 RPC 数据包大小和处理时间。

SRPC 的架构如下图所示，一个服务端 server 进程绑定一个 port 监听连接，server 可以设置多个线程作为多个 poll group 并行处理请求，从请求接收到处理和回调 Reply 的整个过程都在同一线程内完成；客户端 client 创建 channel 连接 server，可以指定要连接的 server 线程，client 可以设置多线程，并在创建 channel 时分配其所在的线程。SRPC 同时也支持使用 TCP 协议兼容未配置专用 RDMA 网卡的场景。

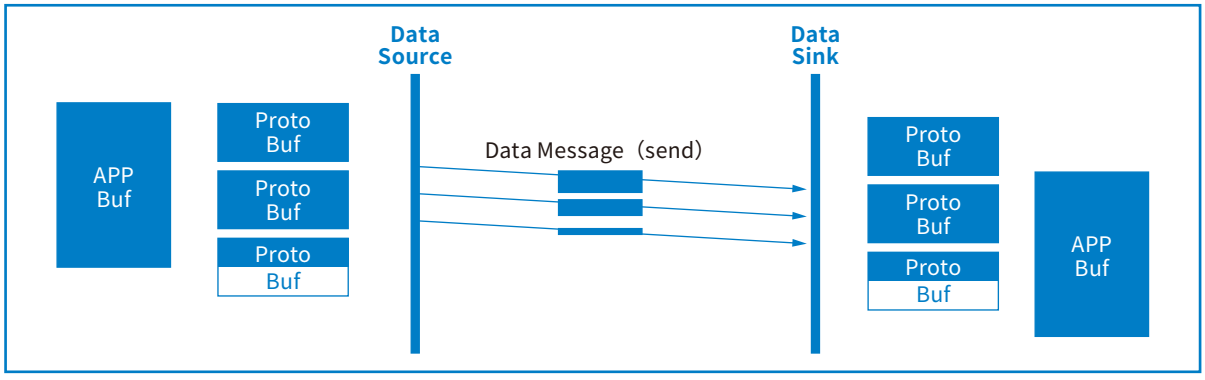


▲ SRPC 通信架构

2 数据传输方式

在使用 RDMA 操作数据传输时，通常有使用双边操作传输和使用单双边操作结合传输两种方式，SRPC 选择了更为灵活的单双边操作结合的方式。

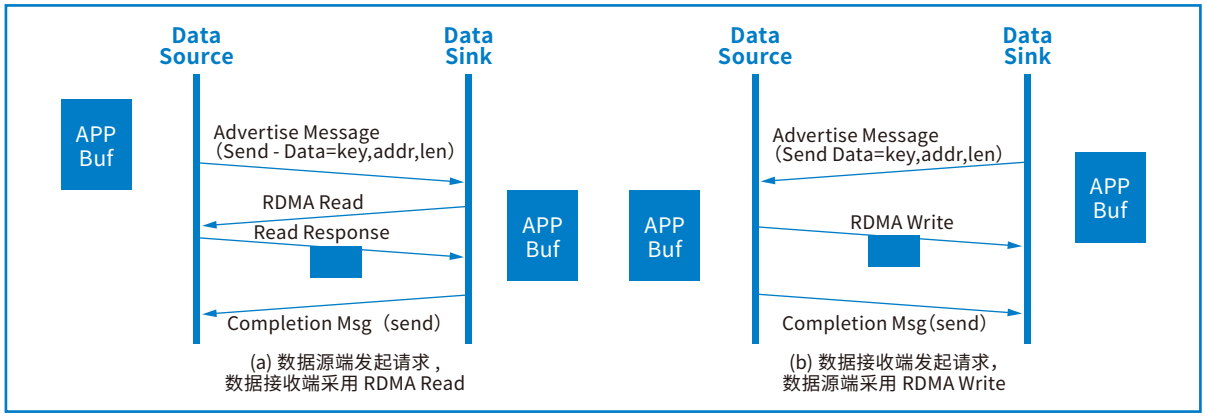
如下图所示，使用双边操作（SEND/RECV）传输数据与传统 Socket 网络传输类似，发送端使用 RDMA SEND 发送数据，接收端使用 RDMA RECV 接收数据。但是在发送端发起 RDMA SEND 操作之前，接收端需要准备好接收数据的内存区并发起 RDMA RECV 操作，否则就会发送失败。因此双方需要约定一次传输最大的数据大小，一般在在创建 RDMA 连接时协商，接收端以该大小准备接收内存区，发送端以该大小对大请求进行切分。使用双边 RDMA SEND/RECV 的限制在于当请求小于约定大小时存在接收端内存浪费的现象，而请求大于约定大小时需要发送端切分多次传输并在接收端重组，并且通常需要应用 Buffer 到 RDMA 协议 Buffer 之间的内存拷贝，增加了开销和延迟。



▲ RDMA 双边传输方式

如下图所示，在单双边结合的传输方式下，双边 SEND/RECV 多用于控制类消息传输，而实际数据则是通过单边 READ/WRITE 来完成。在实际场景中每次需要传输的数据大小不是固定的，所以发起单边操作前需要先协商好数据长度和相应的内存区信息。其方式为先使用双边 SEND/RECV 操作把待传输数据的内存地址、大小、rkey 等控制信息进行传输，然后根据传输类型选择单边 READ 或 WRITE 操作完成实际数据的传输，最后使用双边 SEND/RECV 操作发送 Reply 结果。

数据发送到对端在实际场景中每次需要传输的数据大小不是固定的，所以发起单边操作前需要先协商好数据长度和相应的内存区信息。单双边结合传输的方式具有灵活适应各种大小请求的特点，尤其在传输大请求时具有明显优势，只需要一次单边操作即可将数据全部传输，同时单双边结合的方式也实现了应用 Buffer 到 RDMA 协议 Buffer 之间的数据零拷贝，进一步降低了开销和延迟。



▲ RDMA 单双边结合传输方式

SRPC 设置了两种模式进行请求的检测和处理，分别是性能模式和经济模式。性能模式下 SRPC 不间断轮询 RDMA CQ 队列获取请求，可以更快地响应请求并进行处理。而经济模式下 SRPC 采用 RDMA 事件触发与低频率轮询相结合的方式来进行请求检测处理，可以降低对 CPU 等资源的消耗。

SRPC 根据负载采用智能算法自动在两种模式之间切换，当请求密集时采用性能模式快速处理请求，降低延迟，而当负载较低时则转入经济模式，降低 CPU 等资源使用，降低能耗。

总结

RDMA 的编程模式与传统 TCP/IP 相比有很大的不同，不管是内存使用机制，还是数据操作逻辑都发生了很大的变化。使用 RDMA 可以减少在内核协议栈处理和内存拷贝等开销，从而大幅降低数据在网络上传输的延迟，但实际数据访问需要经过软件栈多个模块的处理，这其中可能存在数据拷贝和同步等开销，当存储设备的访问延迟和网络传输延迟都达到 10us 级别时，这些软件栈上的开销对整体性能的影响变得愈发明显。

从 TCP/IP 网络通信切换到 RDMA 通信不仅仅是数据收发网络接口的简单替换，而是需要进行整体的软件架构的优化设计，使 IO 路径上各模块契合 RDMA 的特点整体联动，才能充分发挥 RDMA 的优势，并与 NVMe SSD 等高性能低延迟设备结合，取得存储性能的突破。

深信服企业分布式存储 EDS 面向 RDMA 和新型存储设备打造了全新的存储架构，并采用零拷贝和 Run-to-Completion 等机制降低延迟，追求极致存储性能，将给我们带来更多的惊喜。

作者介绍

火尉子，华中科技大学博士，研究分布式存储、大数据存储中的数据分布、性能和可靠性，在国际会议和期刊上发表多篇相关论文，目前主要从事分布式存储系统性能提升、网络通信优化的研发工作，专注于存储性能优化、RDMA 等领域，2018 年加入深信服科技。

医院如何打赢桌面终端运维“战役”？

《论语 · 卫灵公》中有云：“工欲善其事，必先利其器。”对于医院而言，“利器”便是支撑业务运转的信息化系统。随着医院信息化建设逐年深入，医院信息系统的规模日益庞大，随之而来的是系统变得愈发复杂。对于当下的许多医院来说，软件、终端、外设等运维难题已经成为业务高效运转的“掣肘”。

软件、外设、终端齐“发难”

包括系统软件、桌面 PC 机、打印机在内的多种软硬件，其复杂的管理为日常运维工作带来很大工作量，一旦发生故障将直接影响医护人员正常工作，运维部门员工只能像“救火队员”一样被动地处理各种紧急故障。即便运维人员使出“浑身解数”，依然无法撼动软件运维、外设运维、终端运维这“三座大山”。

软件运维难度大

目前医院核心业务系统以 C/S 架构较多，应用前端上线、部署、更新配置、维护等操作难度大，经常发生软件配置错误的情况，容易导致软件故障。

外设管理复杂

医疗外设种类多、复杂程度高，终端和外设数量比高达 3:1 甚至 2:1，目前医院的众多外设一直是管理的“盲区”，没有较好的手段和方案与办公终端形成一体化管理。

终端故障解决难以标准化

随着硬件的老化，传统 PC 容易出现故障，传统架构在故障定位、远程处理等方面很难形成场景标准化的解决方案，只能依靠经验进行故障恢复，故障恢复时间基本在半小时以上，直接影响医护人员办公效率。

外包、桌面管理“杯水车薪”

为了降低故障率，提高运维效率，医院也推出系列举措，但实际效果并不尽如人意。

1 “治标不治本”的第三方外包

终端第三方外包虽然可以释放医院管理人员精力，但这种方式并不能从根本上快速解决终端故障。硬件故障必须现场排查，故障恢复时间过长依然给医护人员正常工作造成了很大影响。更快速的故障响应和恢复效率，降低终端故障对于医护人员诊疗的影响已成为医院的重要需求。

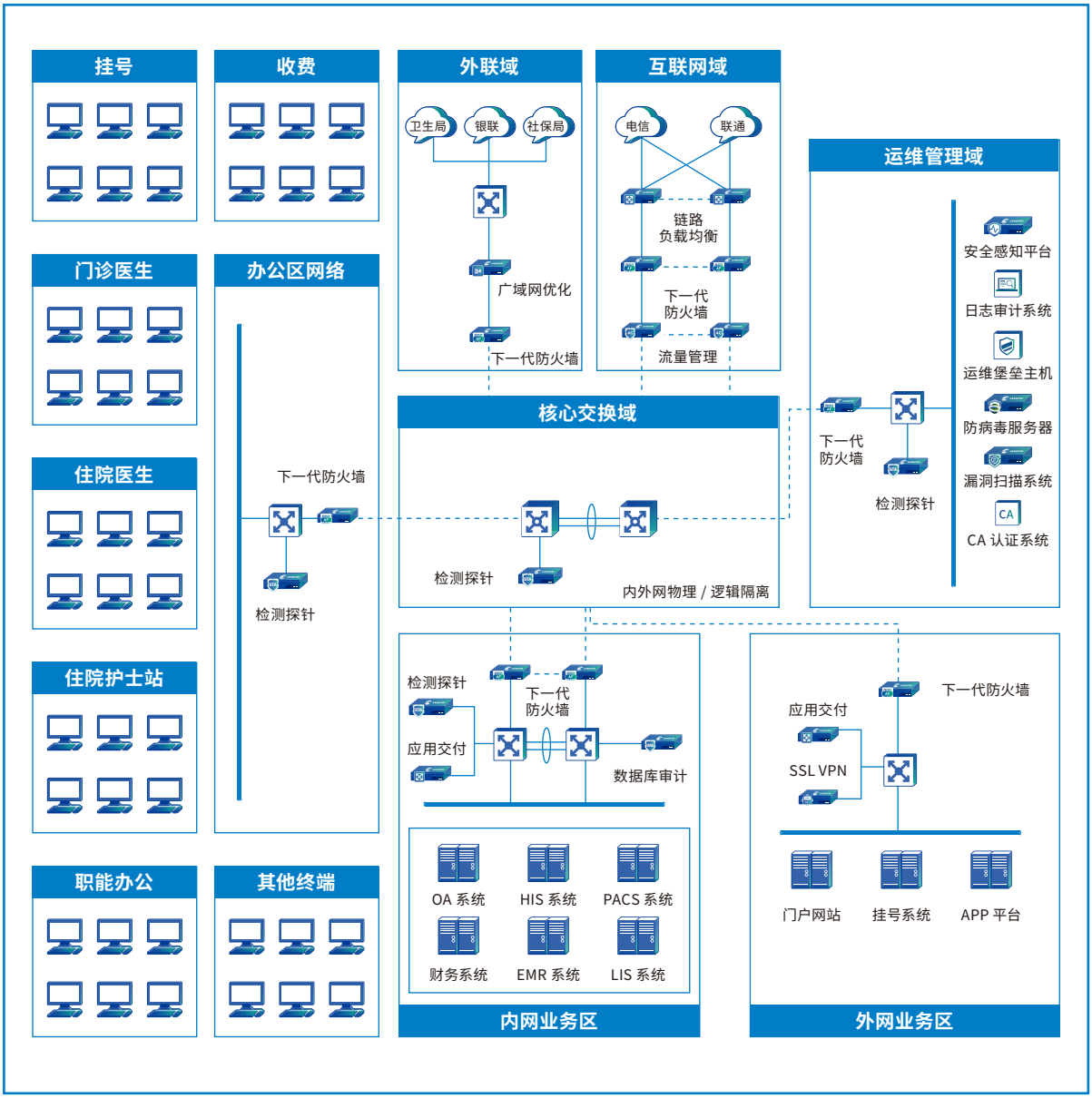
2 “软硬不能兼顾”的桌管软件

虽然桌管软件可以有效进行系统层面日常管理和故障解决，但只能解决操作系统层面的管理运维问题，针对医院多外设的场景，特别是打印机等方面故障缺乏有效的处理方法，一旦发生故障便需要工作人员现场或者远程进行复杂的操作处理，影响了整体管理效率，诊疗业务难以快速恢复。

软件、外设、终端，桌面云“以一敌三”

所谓“底层基础决定上层建筑”，作为医院底层建筑，医院的信息化运维既需要降低故障率，同时也要提高故障恢复效率，而在近几年已广泛应用于各行各业的桌面云将成为行之有效的解决方案。

桌面云技术，通过将桌面、数据、软件全部部署在数据中心进行集中管理，利用先进的智能运维工具，实现统一管理和远程处理故障，大幅缩短故障恢复效率。深信服桌面云目前已有多项创新助力解决医院信息系统运维的痛点，并持续提升医护满意度。



▲ 医院 IT 桌面云拓扑图

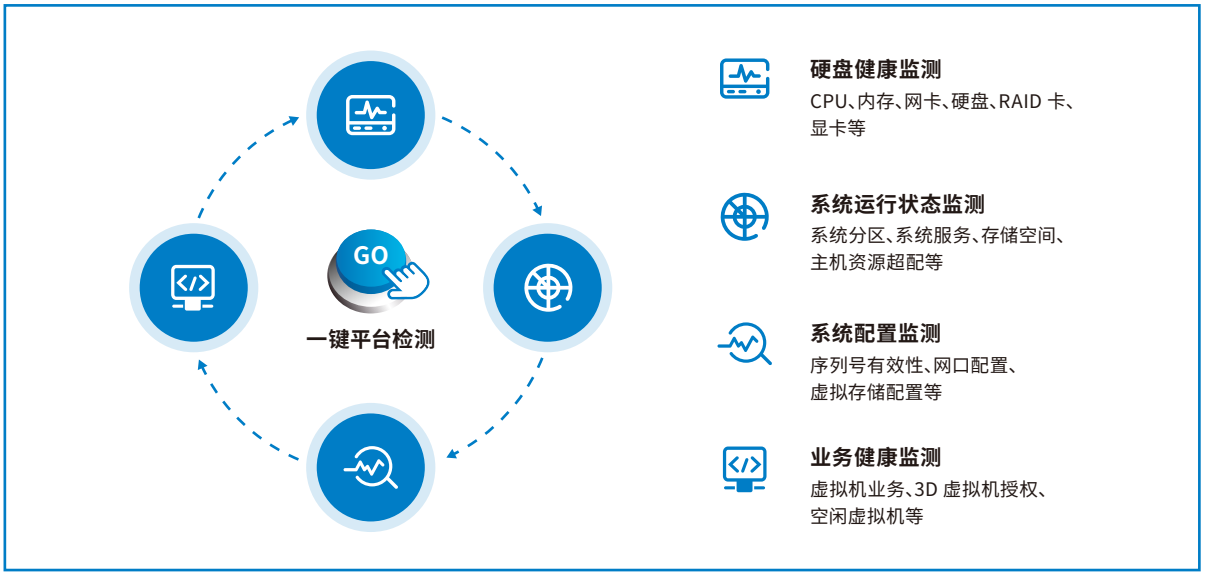
1 重定向、一件检测对软件实时防护

○ 配置文件重定向，确保数据不丢失：

在故障发生时，医护人员往往需要重启电脑。在深信服配置文件重定向的功能支持下，可将 HIS、ERM、PACS 等配置文件重定向到个人盘，即使因为模板更新或者系统还原导致系统盘内的数据丢失，也能在用户重启登录后，自动将这些配置文件恢复，有效避免了因配置文件丢失导致的软件故障。

○ 平台一键检测，运行环境全知晓：

软件故障往往存在一定的突发性。桌面云的一键平台检测功能，可快速识别软件环境中所存在的不稳定因素，在故障爆发前，提前识别出风险，有效规避软件故障造成的业务停摆。



▲ 平台检测仅需一键

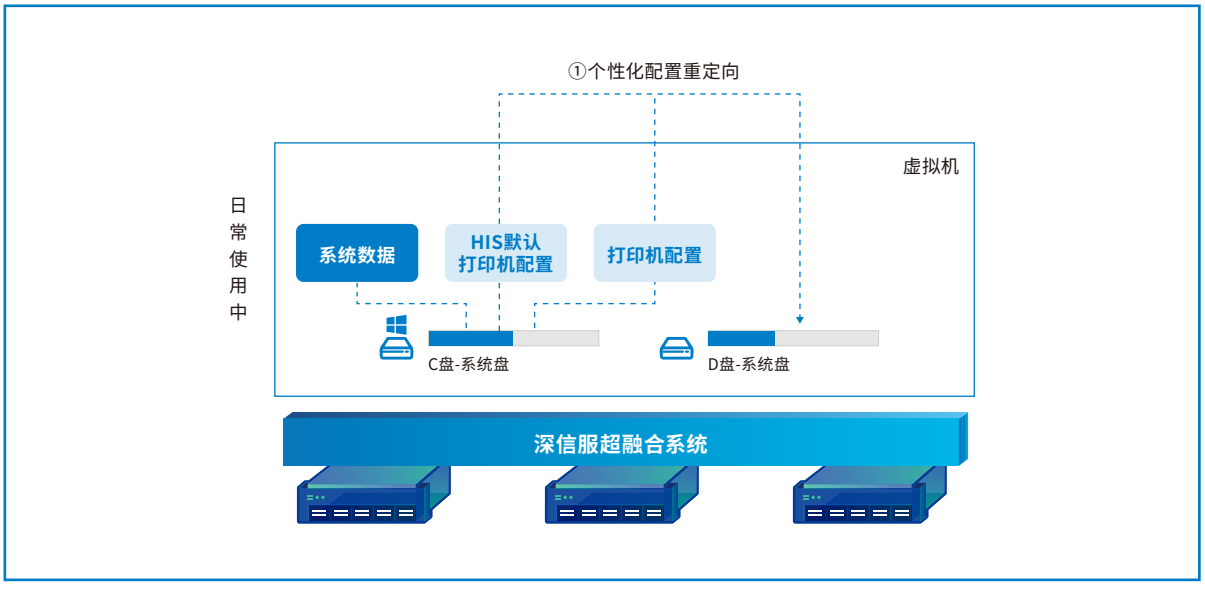
2 批量部署、智能运维保障外设运维效率

模板批量部署，解决驱动问题：

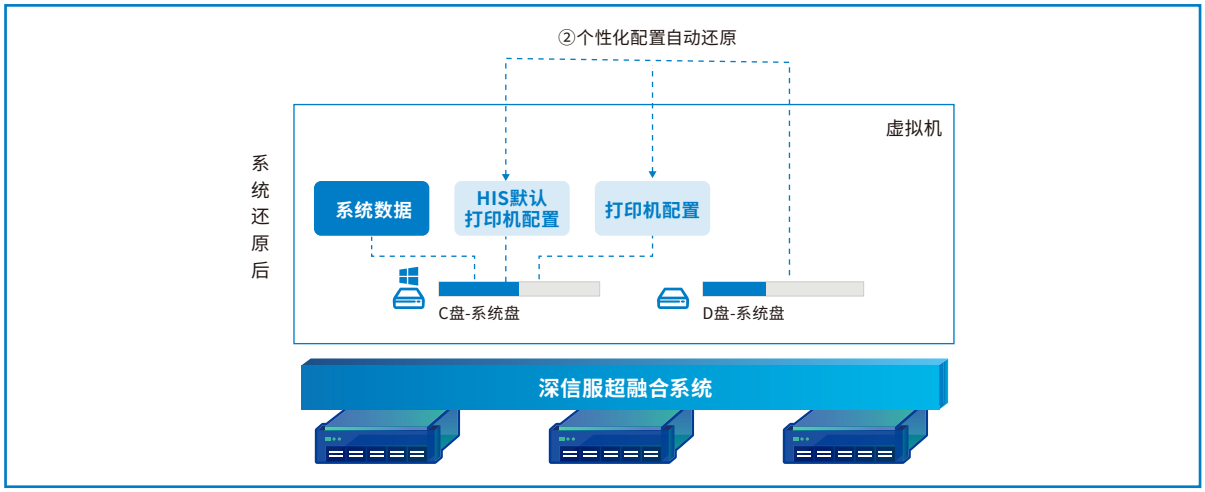
外设的逐台更新部署需要耗费大量时间，深信服桌面云支持模板部署，以打印机为例，可将医院打印机驱动安装到模板，并进行批量下发，提高打印机驱动部署效率。当后期打印机驱动需要新增或者更新时，可通过模板实现逐台更新，不影响医护人员正常工作。

智能运维工具，解决配置问题：

通过打印机智能运维工具，可实现对打印机配置进行下发、保留和更新，从而有效避免了因打印机配置人为修改、丢失等故障，导致打印机无法正常使用。



▲ 个性化配置自动还原（过程一）



▲ 个性化配置自动还原（过程二）

3 即换即用、自动恢复实现终端业务连续

- **终端即换即用，硬件故障零运维：**

由于终端只负责接收后端的图像并进行显示，因此可支持即换即用，终端故障只需直接更换，无须任何配置，重新登录即可实现快速恢复诊疗工作。

- **服务器故障，自动快速恢复：**

后端采用高可靠的超融合架构，单一配件故障不会影响业务正常运行，数据不会丢失，即使出现服务器故障这种极端情况，受影响的云桌面也能在 2-3 分钟内自动恢复。

目前，深信服桌面云已服务于上百家三甲医院，其中不乏广西医科大学第一附属医院、南昌大学第一附属医院、东南大学附属中大医院等全国 TOP100 医院，总计交付 8 万个云桌面，保障各大医院信息系统的正常运行，7*24 小时支撑着 10 多万医护人员夜以继日的辛勤工作，医护人员提供更高效便捷的 IT 服务。

态势感知——
新一代防御体系的技术核心

以下文章来源于金融电子化

近年来，网络安全受到了越来越多的关注和重视。随着云计算、大数据、物联网等新型基础设施建设加速推进，网络的规模逐渐扩大，网络的结构、应用变得更加复杂，网络安全问题更加值得关注。网络安全态势感知”作为网络安全主动防御的新技术，越来越受到业界的关注和认可。态势感知在许多国家被提升到了战略高度，政府、监管机构、企业等相继开始建设和积极应用态势感知系统。2016 年，我国提出了“全天候全方位感知网络安全态势”的基本要求。今年，人民银行发文要求地方性银行业机构和非银行支付机构接入“金融行业态势感知与信息共享平台”，通过统一监管及安全赋能，提升金融机构应对威胁风险的能力。

态势感知，新一代防御体系的核心

随着 IT 基础架构大量引入云计算、移动计算等新兴技术，内外网络物理边界日趋模糊。从金融行业来看，开放银行的发展模式会推动这种趋势加速发展，传统边界防御措施面临失效挑战。为解决这些问题，“零信任”架构应运而生，首创者 John Kindervag 指出，以往可信的内部网络现在充满威胁，提倡从网络中心走向身份中心，在零信任网络中，通过实现对人、设备、系统、应用的自适应访问控制构建安全系统。零信任要求通过“态势感知”和强大的漏洞事件管理能力，将安全性构建到 IT 架构中，因此态势感知成为新一代防御体系的技术核心。

态势感知是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了决策与行动，是安全能力的落地。安全态势感知系统是安全防护的大脑，可以更好地加强纵深防御，通过建设主动防御、持续监测、应急响应、溯源取证、风险预警等安全能力，最终实现安全运营等闭环管理。

态势感知的核心技术分为“态势”和“感知”两部分。态势是指，首先要了解所有的情况，这样才能帮助决策。网络安全态势感知过程可以分为以下四个过程。

数据采集

通过各种检测工具，对各种影响系统安全性的要素进行检测采集获取，这一步是态势感知的前提。

态势理解

对各种网络安全要素进行分类、归并、关联分析并进行处理融合，对融合的信息进行综合分析，得出网络的整体安全状况，这一步是态势感知基础。

态势评估

定性、定量分析当前网络的安全状态和薄弱环节，并给出相应的应对措施，这一步是态势感知的核心。

态势预测

通过态势评估输出的数据，预测网络安全状况的发展趋势，这一步是态势感知的目标。

最后，根据评估结果联动或人工进行威胁处置，形成安全闭环，此过程也称为态势感知 1.0。以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析和响应处置，有了可视化的安全态势感知，各种威胁及风险可以变得一目了然，通过提前预警，做到防患于未然。

态势感知 2.0，更好感知安全态势

目前在国内，传统安全厂商以日志、流量、沙箱为主构建态势感知，特点是组件较全面，缺点是没有优势组件；大数据平台厂商是以日志收集和分析为主，其他组件较弱或没有；小部分厂商以沙箱或者威胁情报为主，在态势感知领域中有明显短板。深信服的安全感知平台组件比较全面，以流量分析为主，再加上元数据、日志、沙箱、威胁情报等功能组件，采用机器学习模式，针对 APT 全攻击链中的每个步骤，渗透、驻点、提权、侦查、外发等各个阶段进行检测，建立文件异常、Mail 异常、C&C 异常检测、流量异常、日志关联、Web 异常检测、隐蔽通道等检测模型并关联检测出高级威胁。

近两年，深信服在态势感知上扎扎实实做了几件事：第一，采用传统规则和机器学习互相融合的方式，通过 DPI 和 DFI 相互结合的核心技术，把流量检测能力做到了业界先进水平。用 AI 来提高检测算法的精度和应变能力，构建了包含攻防专家、数据科学家和安全分析师在内的三位一体架构，攻防专家负责安全问题的定义，数据科学家负责把问题转换成 AI 模型，安全分析师负责训练 AI 模型进行优化，三者互相配合，使得 AI 能够不停地迭代进化，保持对最新威胁和黑客常见攻击手法的检测能力。比如在僵尸网络检测任务的对比训练里，深信服的 AI 已经把检测的准确度提升到 99.7%，内网穿透检测水平也相当精准。第二，结合入侵分析的钻石模型，通过保护对象来进行态势感知。钻石模型最简表述：对手借助基础设施针对受害者部署能力。除了攻击链覆盖手法以外，以资产和保护对象为中心，进行防守和态势感知，即围绕资产展开，将整个被保护系统中所需保护的资产和对象进行体系化的识别和科学建模，围绕资产行为进行异常检测。第三，深信服本身拥有全方位的安全产品体系，态势感知不只是产品更是解决方案，与其他产品相互结合，以点带面进行突破，发挥更大作用。

凭借多年金融行业实践经验，深信服发布的态势感知 2.0，从概念上更为清晰，吸收 PPDR5 安全模型，借鉴 Gartner 自适应安全防御理念，在获取、理解、评估和预测的基础上，增加了行动环节，使整个态势感知 2.0 更为完整，更好地支撑安全运营领域的应用。

态势感知 2.0 通过在网络、中间件、主机等设备上部署探针和日志收集程序，获取基础设施、安全设施、网络和应用系统等相关的日志信息。将获取到的信息使用大数据技术存储到大数据日志平台，同时将资产信息、安全扫描结果、威胁情报等信息一并存储到大数据平台，利用规则引擎和智能分析模型对数据进行统计、分析和挖掘，结合历史的基线数据与分析结果一起输出给到 Dashboard 图和风险态势视图，运营人员通过监控告警或预测信息，即可全面了解安全风险，识别到安全风险后即可生成工作流任务工单，按照企业事件管理流程，协调各责任方进行快速处置。在处置过程中，可通过软件定义安全平台与安全设备、系统或安全管理平台进行联动，自动下发拦截和阻断策略。

深信服安全感知平台上分析和预测的结果可以按要求生成合规报告，也可以通过第三方接口输出给行业共享与系统对接，让整个安全感知平台服务于更多的行业和应用场景。

金融行业“态势感知”建设路线

金融机构建设态势感知系统，首先要明确建设的目标和范围，梳理清晰需要监测与防护的最关键的业务资产，然后应用合适的技术获取完整的安全数据，再结合态势感知系统平台以及大数据威胁情报，分析数据、发现威胁和异常，合理运用安全服务来落地安全能力。态势感知系统，旨在实现“安全集成、智能分析、态势感知、协同处置、运营可视”五大目标。

大型金融机构在原有大数据平台除了对日志进行收集分析外还进行大量其他来源数据收集和对接，如流量、威胁情报等，投入开发和安全人员进行模型抽取和模型匹配，通过人工和 AI 技术进行威胁分析，以工单或其他方式通知安全运维团队进行处置，已经形成初代 SOC 规模，建立了较为完整的安全运营中心。因为他们的开发和安全人员较为齐全，通过大量资金和时间来进行威胁分析和闭环处置，联合其他团队分析整个内外部安全威胁，已具备初代 SOC 雏形，为金融机构探索出一条通往安全运营中心的可行路线。

中大型金融机构使用安全平台部分开源软件进行开发，先进行安全设备日志、流量收集，配合安全平台自身模型进行威胁分析，同时配合安全运维团队进行处置；部分用户使用流量分析先了解内部安全问题，再根据自身人员和业务发展情况选择合适时间建立 SIEM 平台，逐步通过日志和流量结合完善安全模型。中大型用户要根据自身业务情况选择合适的工具或模块建立态势感知平台，不要盲目投入 SIEM 平台，以免达到反面的效果。

中小型金融机构因其人员和资金限制，需求直接定义为能够发现问题、实现安全设备联动、减少人工投入、能够辅助分析安全威胁的工具，该种需求基本定义为以流量分析为主平台，再根据其自身情况选择是否投入 SIEM 平台。简单有效是主要选择，而流量分析是最直接也是有效的安全威胁分析方式，但因其自身特点，中小用户走向安全运营中心的路还很长。

“态势感知”不仅可以赋能金融机构建立防御体系，还可以赋能监管部门实现检测通报预警能力。未来，随着态势感知系统更加广泛的应用，或将成为金融行业安全防护的“大脑”，为金融机构更好地加强纵深防御，实现主动防御、持续检测、应急响应、溯源取证、风险预警等安全能力，为保障网络信息安全发挥出更大效能。深信服也将继续跟紧金融行业发展动向，围绕网络安全的重点领域深入研究，积极助力金融行业网络安全体系建设。

扩容难、性能低、成本高，医院数据存储“疑难杂症”如何根治？

医院，医学影像科。

堪称“火眼金睛”的现代医疗影像设备正在运行——光不可见，声不可闻，人体内部世界便“跃然纸上”，透过医疗影像资料，医生们扮演着人体内部世界的福尔摩斯。从暗室中的手动冲洗胶片到 PACS 系统的广泛应用，一张张医学影像记录着医学影像技术的变迁。

随着医学技术的进化，影像设备的激增，医学影像的数据量也迎来了滚雪球式增长，对医院的数据存储及处理都提出了挑战。更进一步来说，PACS 能否高效运转，医院能否为患者提供更好的服务，很大程度上取决于是否选择了较好的存储方案和优化的存储工作流。

片子铺天盖地，PACS 面临存储“疑难杂症”

目前，医院存储的数据 80%-85% 来自于影像数据，据统计一家三甲医院每天需要几十个 G 的空间用于存储海量的 PACS 数据，而对于这些数字化影像，既要实现短时间内的迅速调取，同时也要保障长时间的妥善存储（按相关规定，医学影像保存时间必须大于 15 年）。简而言之便是，空间要可扩，读写要顺畅，在此基础之上成本也要可控。

- **影像数据持续增长下的扩容难题：**

由于大量医疗设备的引入，PACS 系统所收集的 B 超、X 射线、CT、核磁等影像数据飙升，对于磁盘阵列的存储空间提出挑战，这就需要存储具备按需扩容的能力，并保障数据的自动迁移。

- **影像数据对设备性能的高要求：**

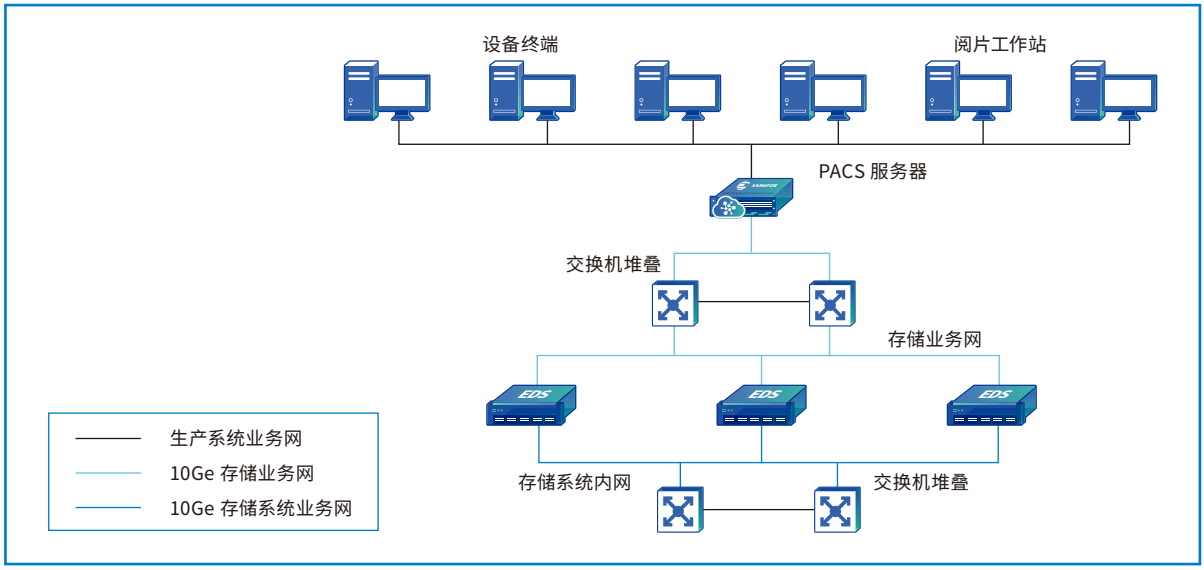
在医院业务快速增长的环境下，存储设备同样面临运行压力，只有持续正常运转不宕机才能保障业务连续性。同时要能够适应 PACS 场景下数据的高速写入以及低时延访问，保障影像医生和临床医生有好的阅片体验以便提高医生的工作效率。

- **采购、管理等成本的持续上升：**

在扩容过程中，医院往往会购入多套不同型号存储，会造成管理成本的增加；而为了保持高性能运转并保障及时的故障修复，同样会耗费大量的时间和人力，日积月累的各种成本问题亟待解决。持续扩大存储空间以及提升存储性能，医院必然面临采购成本的飙升。

医疗影像存储需求繁杂，EDS“对症下药”

面对医疗 PACS 的诸多存储诉求，深信服企业级分布式存储 EDS，基于分布式存储按需线性扩容的特性满足医疗 PACS 对存储空间的需求，以激发硬件潜能的方式最大化提升存储性能，同时实现对成本的有效控制。



▲ EDS 医疗 PACS 场景解决方案

按需扩容，高效迁移：

以天津市某三甲医院为例，通过深信服 EDS，扩容变得极为简单。只需要通过加入新的硬盘或者服务器即可实现扩容，并支持设备内增加任意数量的硬盘，数据的迁移通过集群内部高效率的完成，用最少的操作步骤将业务影响程度降到了最低。

激发潜能，性能拔高：

影响数据时延的两个关键因素便是硬件和网络。深信服 EDS 将最新的 NVMe SSD 和 RDMA 网络这两项核心高性能技术进行深度融合，使得单次通信时延降低至 50us 之内。这一高性能保障会直接提升医生的工作效率。目前从某医院存储系统整体性能表现来看，在应用了 EDS 后系统的数据时延已至少降低 3 倍以上，医生的阅片效率至少提高 2 倍。

在数据处理上，医疗影像热数据要求迅速读取，当热数据冷却后虽然极少访问却需要长期保存。深信服 EDS 利用自研的分层存储技术满足了对热数据和冷数据的处理需求。就好比我们的个人衣柜，衣服虽多，但是不同时段需要经常穿的就那么几件。日常的穿着衣物我们会挂在最便于拿取的位置，相当于存储的 SSD 层，为热数据提供低时延访问，据统计应用 EDS 后单张影像的读取速率不超过 1ms；而不合时令的衣物则往往被存放在收纳箱，相当于 HDD 区用于冷数据的长期存储。深信服 EDS 实现了基于现有硬件条件下的高性能需求。

- **高效运维，成本可控：**

其实以目前分布式存储技术，单纯实现扩容或通过硬件堆积提升性能并非难事，但是满足扩容需求和高性能前提下还能保证成本可控，对于研发团队来说就有了更高的挑战，那便是要在现有的条件下激发硬件潜能，实现高性能与低成本的兼得。在深信服 EDS 按需扩容的特性下，医院只需要加入新的硬盘或者服务器即可实现扩容，降低采购以及机房空间成本；高性能 NVMe SSD 和 RDMA 网络极大的释放了存储系统对 CPU 的负担和消耗，发挥硬件协同综合性能，使得整机硬件具备更高性价比；并通过 AI 深度学习形成精准模型，对硬盘故障进行实时预测，能够提前 15 天预测故障同准确率达到 98.5%，有效控制了管理维护成本。

目前，深信服 EDS 已经成功为天津市中心妇产医院、深圳市眼科医院、襄阳市襄州区人民医院等提供数据存储解决方案。

从 1895 年 X 射线发现，到今天医学影像技术已经成为了医疗的重要部分，不过无论是当下的实际应用还是未来的进一步演化，都离不开海量影像数据的支撑。对于各大医院面临数据存储挑战，深信服 EDS 也将继续行走在存储的前沿，为医疗行业提供坚实的数据存储保障。

这一杯酒：是瓶中方寸千年香 也是智慧化的未来

酱香突出、醇香馥郁、幽雅细腻、入口柔绵、清冽甘爽……是世人对茅台酒香味的美评，这种香味流传至今，不曾改变。如果要选一款酒与时光同饮，非茅台莫属，毕竟用一口酒就能尝尽数十载光阴。

当经济发展由高速增长阶段转向高质量发展阶段，数字技术由消费领域向生产领域、由虚拟经济向实体经济延伸，数字化正在成为一种新型生产方式，全面数字化转型也正成为各行各业实现高质量发展的趋势性选择。对于贵州茅台集团而言，与时俱进地借力数字化东风，布局智慧发展的未来，正是他们当下最重要的议程之一。

定位信息化建设需求，备战数字化转型

正如茅台酒的酿造要经历重阳下沙、端午踩曲、长期贮存等工艺环节的淬炼准备，茅台集团的数字化转型也有着一个持续的准备过程。

茅台集团虽然是传统的制造企业，在识别发展机遇时却反应敏捷，早在 2017 年就已开始数字化转型，着力推动“智慧茅台”建设。随着数字化转型推进，IT 信息系统不断推陈出新，给 IT 基础设施带来了挑战：

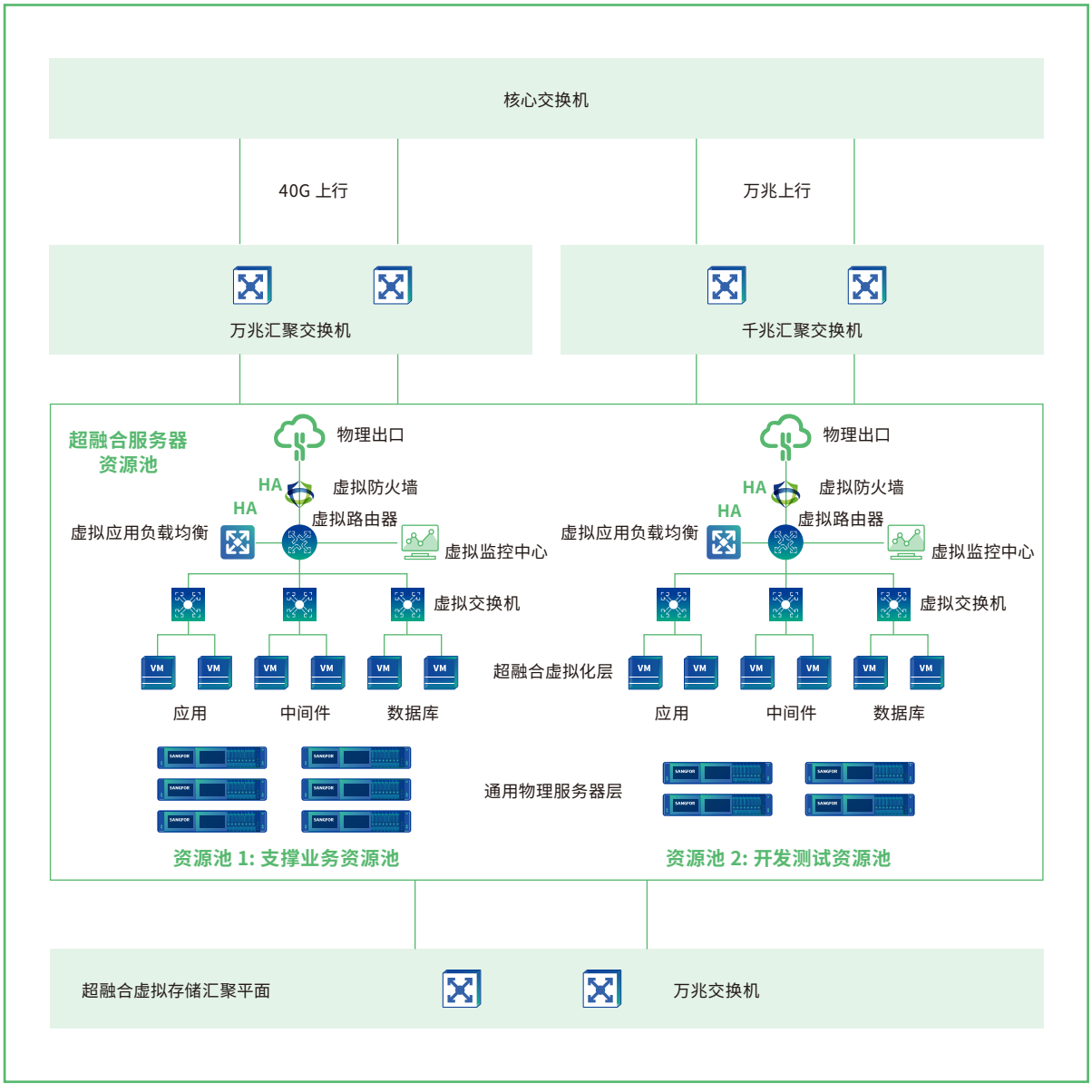
- 现有服务器和存储资源已经不足以承载大型的业务系统，亟需一个高效、可靠的 IT 基础设施资源池。
- 随着新业务的不断上线，开发测试环节不可或缺，开发测试周期内对计算、存储等 IT 基础设施的需求和生产环境既要保持一致，又要相互独立。
- 网络安全一直以来缺乏体系化的建设，随着内、外部安全形势的变化，需要构建一套可视化、能联动、多纵深的综合安全防护体系。

构建超融合服务器资源池及网络安全体系，加速“智慧茅台”落地

为确保安全、有序地推进茅台集团“6+N”全产业链大数据平台建设，加速“智慧茅台”的实现，满足所有围绕“智慧茅台”的新应用系统迅速上线，贵州茅台通过考察各种技术解决方案，并进行优劣分析后，选择在现有数据机房建设基于超融合架构的服务器资源池。这一方案采用分布式架构具备高 IO 和高吞吐量的特性，可有效解决现在业务系统卡、慢问题，并划分开发测试资源池为公司未来的软件开发和测试提供足够的资源支撑。

1 深信服超融合助力实现软件定义数据中心

通过构建极简化的大二层网络结构，满足现阶段财务系统、OA 系统、原料基地平台、全面预算系统等 50 多个核心业务系统的高效运行。同时，超融合资源池的横向可扩展特性可为业务高速发展提供可靠的基础架构，以及实现开发测试环境的按需快速搭建和灵活调配。



2 深信服整体网络安全解决方案为茅台赋能

通过赋予茅台数据中心安全可视、持续检测、协同防御的能力，在保障业务持续性的同时，结合信息系统纵深防御、网络结构整体安全等方面进行设计，切实提高公司的网络安全防御、监测、响应的能力，并满足国家《网络安全法》以及等级保护建设的要求。同时，大幅度降低网络故障排查的难度以及安全运维的工作量，对核心业务进行重点防护，实现“业务驱动安全”。

筑牢信息化基石 布局“智造”未来

实践证明，通过超融合服务器资源池及网络安全体系建设方案的实施，茅台在信息化建设层面实现了三大突破。

1 高效运行，降低能耗

茅台超融合资源池建成后，硬件仅需由通用 X86 服务器和通用汇聚交换机组成。实现 20+ 台物理服务器高效运行近 500 台虚拟服务器，同时纳管第三方虚拟服务器 200 多台，逐渐替换上一代数据中心的多台服务器和若干共享存储设备的传统 IT 架构，仅机房空间和能耗一项就降低了 85%。

2 无限扩容，降低成本

采用分布式的虚拟存储架构，打破了常规数据中心存储堆叠共享的建设模式，可以实现无上限的横向线性扩容，成本比传统共享存储方案降低至少 20%。此外，通过 SSD+HDD 混合冷热分层存储模式，使超融合资源池 IOPS 高达 200 万以上，吞吐性能高达 20GB/S 以上，性能是原来传统架构的 5 倍。有效提高了财务、OA、全面预算等茅台集团大型应用系统的访问效率，用户体验也得到提高。

3 策略联动，简化运维

一方面，网络安全建设使公司网络内部的各个安全域之间的安全防护策略能够实现集中信息共享和策略联动，解决了以往安全设备防护孤立、安全难以形成有效纵深的问题。另一方面，通过全 Web 化的云管理平台简化运维，业务逻辑编排“所画即所得”，业务运行状态可通过云平台内嵌的应用性能监控模块实现实时监控，运维人员节省 2 人，业务上线时间由原来的一周缩短到 1 天，开发测试环境搭建由 1 天缩短到 30 分钟。

与此同时，人工运维的工作量和工作复杂度也大大降低，直接节约的网络安全运维时间成本达 40% 以上，提升了信息化部门业务运作效率，为公司数字化转型提供了安全、稳定的保障。

综合来看，深信服超融合服务器资源池及网络安全防御的有效运行正在不断助力茅台集团的数字化转型。事实上，除了深信服，茅台集团还通过与阿里巴巴、华为、京东等不同科技企业的深度合作，启动集团的全产业链数字化平台建设，打造包括茅台云、茅台数据湖两个基础型平台，“智慧茅台”应用中心，原料基地平台，质量和食品安全管控平台三个应用型平台，在生产、销售、管理、溯源等方面全面进行信息化建设。

深信服作为专注于企业级安全、云计算与基础架构的产品和服务供应商，未来还将继续秉承“让 IT 更简单、更安全、更有价值”的使命，积极参与和推动制造业的信息化建设，通过构建安全的网络环境，助力云计算、5G、AI 等数字信息技术与制造业的生产、管理、销售等全产业链环节的深度融合，为更多像茅台集团一样的企业构筑安全、稳固的数字化基石，加快推动“中国制造”向“中国智造”的转型。

一

打破束缚，云化升级
看中国传媒大学数据中心
云化升级之路

提起中国传媒大学（简称“中传”），很多人的第一印象就是中国传媒事业的圣地，2018 年起，深信服开始助力中传建设云化数据中心。

▲ 中传校区景色

2018 年《教育信息化 2.0 行动计划》启动，中传为了不断推进教育信息化 2.0 落地，梳理了学校底层 IT 架构及分散的信息化建设情况面临的三大挑战：

- **其一，系统运维困难：**

学校业务系统采用分散的建设架构，IT 资源（计算、存储、网络）无法统一调度、统一管理。此外，系统的单点故障等运维问题消磨了信息中心业务创新能力。

- **其二，业务上线速度慢：**

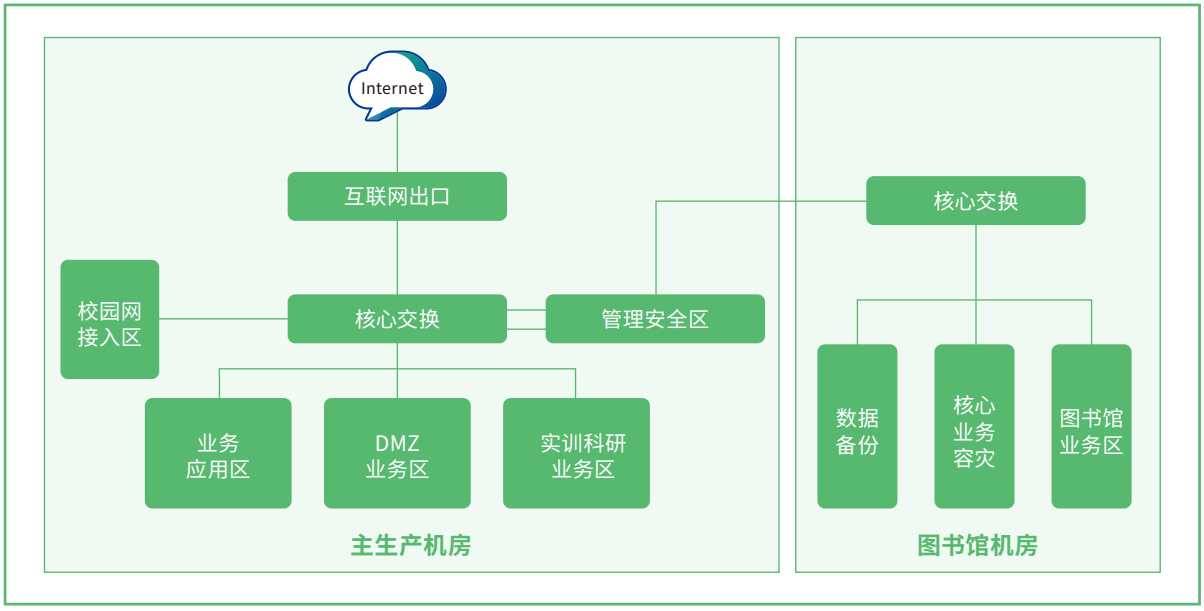
新业务部署上线需要经过调研、采购、部署、测试、上线，学校传统的虚拟化 + 外置存储架构使得 IT 交付过程漫长、繁琐，无法适应智慧校园建设大规模业务上线的需求。

其三，IT 架构缺少弹性：

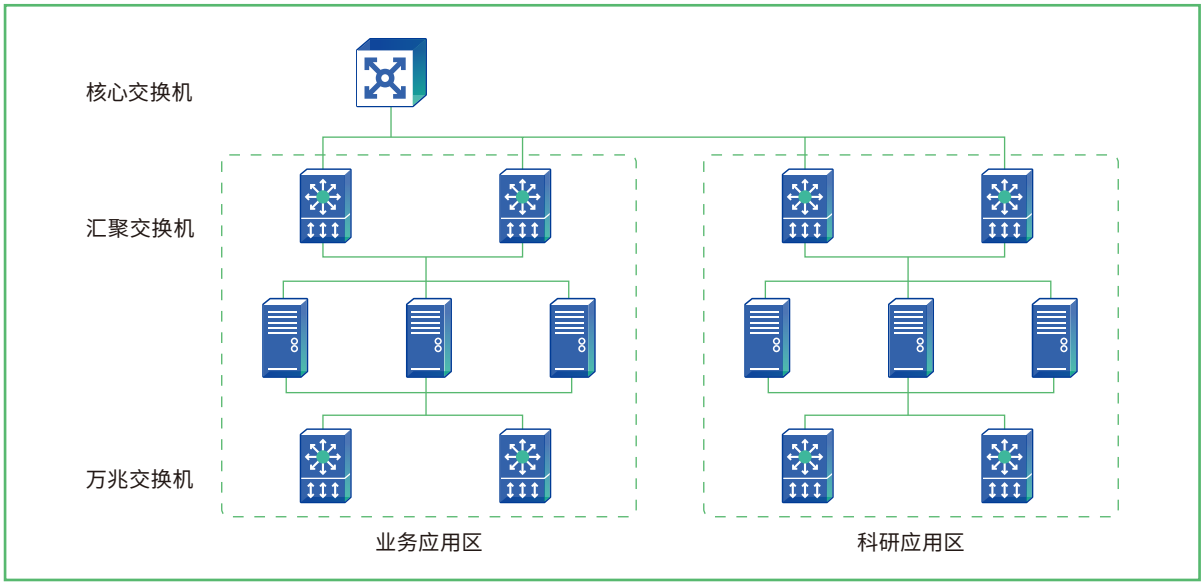
随着学校“大数据”业务的开展，不同学院的信息化业务逐步收归到学校的信息中心统一管理，以达到数据资源集中化，进一步挖掘数据价值，为师生提供更好的服务体验，但现有平台无法应对学校数据的急速扩张和高效利用。

打破束缚，云化升级

中传在 2018 年开展多轮调研，协调内外部专家，结合各个厂商的解决方案反复论证，最终确定采用深信服的私有云平台建设方案。方案具体部署如下：



▲ 中传云平台整体规划



▲ 中传业务拓扑（一期）

在业务应用区：

通过 9 台服务器（3 台深信服超融合一体机、6 台原有服务器），实现资源与授权，承载苏迪网站群、迪科一卡通系统、办事大厅应用平台、教务系统（含选课模块）、易普拉格管理系统等业务。

在科研业务区：

通过一期 6 台服务器（2 台深信服一体机、4 台原有服务器），承载智能影库大数据分析查询系统，包含组件 Hadoop（HDFS）、Neo4j（图数据库）、TensorFlow（人工智能计算框架）及 Web 查询平台，该平台将利用云平台租户隔离、弹性伸缩的独特优势，为科研、毕业课题研究等业务提供计算和存储资源。云平台一期为小规模集群部署，后续业务稳定运行后，云平台会持续扩容，并以此为基础打造广电影视大数据平台，用来服务全国地市电视台及社会媒体制作公司。

▲ 中传云平台界面展示

创新技术，量身打造

部署完深信服私有云平台建设方案方案后，中传的云平台整体架构变得非常清晰，并具备五大功能：

1 平滑演进

深信服云计算平台以超融合为底层架构，上层搭建云管理平台，不仅能提供数据中心 IaaS 层服务，还具有丰富的 PaaS 层服务，并为学校提供后续容灾备份、多云管理等不同场景的精细化演进方案，助力学校信息化发展。

2 稳定承载

中传云平台通过分布式存储技术，打造高性能、高可用、高扩展存储，承载学校关键应用和关键数据库。其中，关键应用包括选课系统、一卡通系统等，关键数据库如当前流行图数据库 Neo4j 等。与此同时，云平台还能利用 CDP 备份实现关键业务秒级 RPO 容灾要求。

3 安全合规

平台集成深信服优势安全组件（防火墙、负载均衡、全网行为管理等），组件支持模块化部署，简单、易用、有效。

4 简化运维

通过云管平台的 IaaS 层服务，提供租户资源自动化审批流程，简化信息中心业务上线方式，提高办事效率。

5 节约成本

利用平台高兼容性特点，充分利旧用户现有资源，并实现轻松上云，节约用户成本。

深信服作为专注于企业级安全、云计算与基础架构的产品和服务供应商，深耕教育行业二十载，已经为全国 80% 以上的高校、70% 以上的职业院校（含 85% 以上的国家级示范院校）和 60% 以上的市县区教育局、电教馆、重点中小学提供产品与技术服务。未来，深信服将继续秉承“让 IT 更简单、更安全、更有价值”的使命，扎根教育行业，积极参与和推动教育信息化的建设，通过构建安全的网络环境，助力教育信息技术和教育教学的深度融合，加快推动教育服务模式和学习方式的新变革。

中国传媒大学简介

中国传媒大学（Communication University of China）简称“中传”，位于首都北京，是中华人民共和国教育部直属的“一流学科建设高校”，“211 工程”重点建设大学，“985 优势学科创新平台”重点建设高校。

康辰药业：拒绝信息化建设滞后 成为创新发展的“拦路虎”

研制特效药，是对抗流行性传染疾病的一大利器，而打造中国自身的新药研发硬实力，则需要更多拥有创新研发能力的医药企业。有这样一家药企——研制出了已上市的国家一类新药：苏灵，同时拥有 CX1026、CX1003、KC1036 等多个在研的国家一类新药和 45 项国家、国际发明专利，获得国家 863 计划、国家火炬计划、中国专利优秀奖等多项中国顶级荣誉。这家走在创新前列的医药企业，名为康辰药业。

▲ 康辰药业使命担当（图片来源于康辰药业官网）

北京康辰药业股份有限公司始创于 2003 年，秉承“用生命科学呵护人类健康”的核心使命，现已发展成为集研发、生产、营销于一体的高新医药企业，并于 2018 年 8 月在上海证券交易所挂牌上市。

十六年来，康辰药业都在新药创制上矢志不渝，创新发展之路，离不开公司内部各系统的全力配合支持。随着公司发展日趋加速，短期内业务系统大量增加，而公司原本的服务器使用年限久，性能较低，每当面对系统扩容与新应用上线都略显疲态。

初次和康辰药业信息部总监李博交流时，对于目前公司 IT 建设的现状，他希望能够有所改善，却又不可避免陷入困境。李总无奈地表示到：“目前公司整体计算机资源利用率并不高，我们信息部门很难去实现统一规划与共享；IT 架构没有云化，系统缺乏弹性和稳定性；当前的数据安全和平台安全都让大家心里没底，一旦边界防护体系被攻破，将会对内网的业务和系统造成不可预估的损害。这些都是公司在创新发展道路上的‘拦路虎’啊！”

想要破解当前的信息化建设困局，实施一套切实可行的解决方案刻不容缓。深信服决定从两大方向入手，为康辰药业重塑架构，护航安全。

“刮骨疗伤”重构 IT 基础平台

当前公司的 IT 架构存在较大的发展阻力，要想真正能够实现业务高速发展，需要来一场“刮骨疗伤”。深信服通过对多种技术路径调研，选用当前较为成熟且起步门槛低的超融合架构作为 IT 基础平台的替代。通过对架构的深度优化和解耦，让康辰药业云平台建设可以三台起步，平滑扩容，不仅简化了运维管理，更从业务和战略角度简化了康辰药业日后的 IT 建设规划，让相关业务可以一次上云，持续演进。

除此之外，可视化的可靠性中心，能够让系统自动发现端到端的可靠性问题和潜在风险，配合深信服延伸双活集群技术，以及底层磁盘亚健康检测和自动隔离修复技术，持续守护业务系统稳定运行。

“查缺补漏”深化安全防护体系

考虑到康辰药业的安全体系建设还主要停留在传统的边界防护上，缺乏拥有内网检测能力的纵深防御体系建设，经过分析讨论，决定匹配“安全云脑 + 下一代防火墙 AF+安全感知平台 SIP+终端检测响应平台 EDR”的整体安全解决方案，为康辰药业构建新一代威胁防护架构。

这套安全架构通过内网威胁检测叠加边界安全加固，帮助构建闭环安全体系，从之前的“被动防御+应急响应”到现在的“积极防御 + 持续响应”，以此来实现事前风险预知、事中积极防护、事后持续检测及响应，持续保障公司业务系统安全运行。

迄今为止，深信服整体解决方案已经交付予康辰药业两年时间了。在近日的沟通交流中，康辰药业信息部李总表示，这两年来，公司信息化建设在重塑 IT 架构和构建安全体系两方面升级改造下，解决了一直以来的困扰，信息系统的运作已然步入正轨，使用起来愈发顺心了。

“早期我们业务系统面临的弹性和稳定性弱的问题，通过超融合架构都有效解决了。当需要扩容时，只添加深信服超融合一体机就能实现，解决了短期的资源问题，未来逐步将更多业务迁移上云，直至实现全业务云化。

有超融合的架构在，短期出现服务器故障或硬盘故障后，都能快速恢复业务系统。原先无法发现的安全问题，也在网端云安全架构多方位监测下无处遁形。多块大屏直观展示网络安全状况，看得见的放心。

综合来说，使用这套解决方案，在整体投资成本较低的情况下，有效地满足了 IT 建设需求，产生了很高的投资收益，让我们也能够更加无忧地将精力集中到新药研发上，加速了公司的创新发展进程。”李总这样说到。

一个好的信息化架构能够为一家公司带来新的内生动力，康辰药业依托全新的 IT 建设架构，完善的安全防护体系，坚守经营核心——“用生命科学呵护人类健康”，在医药创新的道路上持续迈步前行。而深信服也将继续秉承初心，以用户需求为导向，切实打造贴合用户的解决方案，持续助力用户的信息化转型。

探秘“新世界七大奇迹”港珠澳大桥的珠海口岸如何打造云数据中心

近日，由深信服发起的“走进港珠澳大桥珠海口岸，看云数据中心如何乘风破浪”CIO 研讨会在珠海圆满落下帷幕。来自上海、深圳、广州、南京、东莞等全国各地 40 余家企业 CIO 及信息化负责人齐聚港珠澳大桥珠海口岸，实地了解珠海智慧口岸云平台的建设效果，共同探讨新基建形势下数据中心的建设与创新。

港珠澳大桥珠海口岸信息化建设

港珠澳大桥是一项举世瞩目的超级工程，创造了多项“世界之最”记录。伶仃洋中宛若游龙的大桥飞架三地，连接广东珠海、香港和澳门。

其中，港珠澳大桥珠海公路口岸位于港珠澳大桥珠澳口岸人工岛上，占地面积 107.33 万平方米，是我国唯一的三地互通、客货兼重的陆路口岸，主要负责对香港、澳门、珠海的出入境客、货车及经三地过境的旅客进行通关查验和旅客运输。由珠海创投港珠澳大桥珠海公路口岸运营管理有限公司（简称口岸运营公司）进行运营。

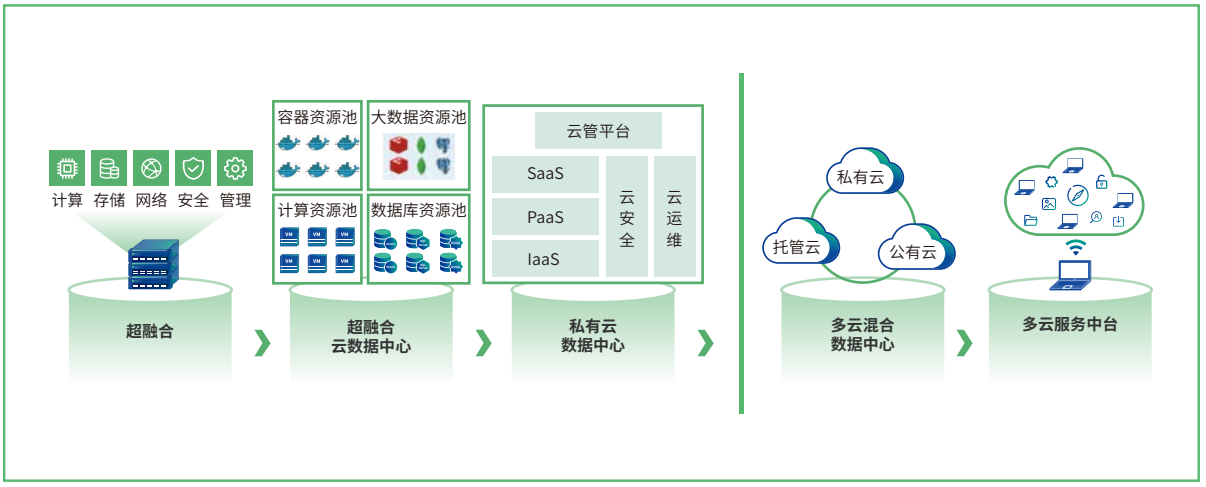
口岸运营公司按照统一规划、统一建设、统一经营、统筹管理的原则，对旅检大楼、交通站场、配套商业等项目进行管理，致力于将其打造成为粤港澳大湾区商业新中心，在信息化建设上，积极推进通关模式创新，建设“建设现代化、通关电子化、信息网络化”的智慧口岸。

基于珠海口岸人工岛上的业务特征，港珠澳大桥珠海口岸联合深信服构建了一个平台功能完整（含 IaaS、PaaS 资源、安全合规、丰富的服务目录）、管理运营简单、支持平滑弹性生长、具备一站式服务的分布式云数据中心。岛上的数据中心采用超融合基础设施搭建，承载全部核心业务，如口岸的智慧物业、智能商业、智能站场管理、票务平台、支付平台、无感服务、AI 机器人等智慧运营系统；自港珠澳大桥珠海口岸开放近两年来，云数据中心稳定运行零故障。

云化赋予业务创新更多可能

会上，口岸运营公司信息中心主任汤建先生提到：智慧口岸数字化云平台的建成，为港珠澳大桥珠海口岸开展沉浸式观光游览、“一站式”通关体验、便捷出行服务、口岸人工岛运维管理等应用提供了稳定可靠的运营基础。

不仅如此，考虑到数十套不同系统之间的数据治理需求，港珠澳大桥珠海口岸基于超融合架构的开放性与灵活扩展性，可以随时在智慧口岸云平台基础上横向扩容，通过云平台提供的高性能分布式计算、大数据计算和深度学习计算服务，将口岸各个业务单元进行数字化，从数字反映出口岸的运营情况，帮助口岸更全面、更准确的掌握口岸运营情况。通过各个角度对内部管控、流程优化提供数据的支持，有力支撑通关模式创新及商业运营模式创新。



▲ 珠海口岸信息化 -- 数据中心云化演进路径

信服云运营专家方骅懋在交流中提出：“新基建”时代，用户的数字化转型在不同阶段会产生不同的需求，如何满足数据中心在各个阶段的不同需求是深信服关注的重点。深信服为用户设计的云化演进之路既保证稳态的内部应用，又适应敏态的创新应用。

在本次项目中，信服云平台创新的架构将持续助力港珠澳大桥智慧口岸从提升管理向卓越运营转型。信服云前期提供专业的云咨询规划服务（云部署的战略选择、迁移策略制定等），帮助用户制定云上安全体系建设、容灾备份建设、场景化应用改造等解决方案，后期的服务交付还涵盖了员工知识体系重构、流程改造的管理和成本优化等长期的运营运维内容。

短短半天的沙龙分享，与会 CIO/ 技术专家们不仅聆听了港珠澳大桥珠海口岸的建设成果，会后大家还进行了热烈的技术方案探讨，收获颇丰。目前，信服云已稳定交付上万家用户，助力传统数据中心云化演进。未来，信服云将持续为社会和企业创造更大价值。

看深信服与中控信息
如何为城市交通“舒筋活络”

繁华的城市主干道上，汽笛轰鸣，车水马龙。

在城市交通中，每天有数以百万计的车辆行驶在城市道路上，只有合理地进行规划和管控，才能保障城市的正常运行，而中控信息（浙江浙大中控信息技术有限公司，简称中控信息）在城市交通系统中扮演着重要的角色。

作为中国智慧城市建设先驱，中控信息长久以来为城市智能交通提供规划、实施、运营服务一体化的整体解决方案。日前，深信服与中控信息达成合作，完成深信服企业级分布式存储 EDS 与交警集成管控平台的兼容性认证，双方将发力智能交通领域，携手满足用户多样性的数据存储要求。

这次兼容性测试全面涵盖了稳定性、性能等方面，测试周期长达半年。在测试表现中，交警集成管理平台能够在 EDS 平台实现快速调用，稳定运行。同时 EDS 性能表现优异，指挥平台对 EDS 发起了超过千万的访问请求，图片调取平均时延为 53ms，充分发挥了 EDS 在海量图片数据存储下的优异性能。


产品认证
PRODUCT CERTIFICATION
认证日期：2020 年 04 月 21 日
认证结论：
经过深信服科技股份有限公司和浙江浙大中控信息技术有限公司共同严格测试：交警集成管控指挥平台能够在深信服分布式存储EDS平台中实现快速调用，稳定运行，双方相互兼容，性能表现优异，有效降低运维难度，共同为交通行业用户提供一体化解决方案。
测试内容：
● 功能完整性测试
● 可视化界面运维测试
● 高压力环境性能测试
SANGFOR 深信服科技
深信服科技股份有限公司（盖章）
中控·SUPCON
浙江浙大中控信息技术有限公司（盖章）

▲ 中控信息 & 深信服 EDS 产品测试认证

智能交通管理的“木桶效应”

大数据时代的来临，让智能交通管理模式成为了城市的必然选择，但是机动车和非机动车数量的暴增带来愈发庞大的交通压力依然是客观事实。中控信息在交通监控等方面不断丰富功能，以提高交通运输效率，实现更妥善更清晰的道路管制。不过，对于中控信息而言，交通管理业务依然存在着“木桶效应”，如果没有强有力的存储技术作为支撑，数据处理便会成为整体系统的那一块短板，比如——

1 无法及时向每个平台提供历史数据

在交警管控指挥平台中，不管是即时业务处理，还是事后查找回溯，都需要对图片进行大量的调用，这就对存储读取的即时性提出要求。然而，大多数早期存储系统的响应速度很慢，直接造成整体效率低下。

2 大量交通管理数据缺乏有效的防护

由于人为误删或者恶意攻击造成的文件数据丢失时有发生，系统要具备高效可靠的实时数据恢复能力保障业务的连续。

3 海量交通数据需要定期管理，存储设备需要维护

道路监控数据日积月累，既需要实时保存又需要定期处理，而长期运行的存储设备又难免出现性能故障，有些甚至需要人为检测，这为工作人员带来极大的运维管理压力。

交通数据存储支持“一个都不能少”

面对复杂的数据存储需求，中控信息最终选择了深信服 EDS 承接交警集成管控平台业务，在 EDS 高性能读写、数据安全保障、智能管理等特性加持下，双方将携手为用户提供更好的管理体验。同时，EDS 还通过激发硬件潜能的方式同时实现低成本和高性能。

1 解决交通管理系统时延问题

针对套牌车的以图搜图功能，需要及时读取历史图片做碰撞比对。在深信服 EDS 的高性能支持下，管理平台整体效率将大幅提高：通过三节点提供对象存储有效支持百亿级文件数量，并使用自研 PhxKV 分布式数据库满足海量小文件的快速检索需求，同时通过对小文件的聚合处理以提高随机读写速度，前端监控摄像机采集到车辆图片信息后，工作人员便能第一时间进行分析处理。

2 解决存储安全问题

为符合法律法规合规性要求，当共享文件服务被恶意攻击时，管理平台要具备追溯攻击源的能力并提供电子取证凭据。深信服 EDS 将为管理系统提供“回收站”恢复用户临时删除的文档资料，为误删除提供“后悔药”。在恢复速度上，1TB 的数据恢复不超过半个小时，数据丢失和业务中断的风险便大幅降低。

3 解决存储自动化运维问题

在道路卡口，交通管理平台每天会产生大量的车辆通行图片，图片要求保存周期为一年，文件管理任务繁杂。平台可通过深信服 EDS 配置生命周期规则，超过一年的图片将会被自动删除，这样用户就能更高效地管理数据并节省存储成本。此外，平台用户还可以通过深信服 EDS 的一键检测功能自行检测包括 CPU、内存、硬盘在内的系统健康状态，深信服内置 AI 系统可以提前 15 天发现亚健康状态的硬盘并提前提醒更换，预测准确率可达到 98.5% 以上，这种更加智能的管理方式同样有效降低了人力成本。

未来，深信服将会与中控信息加深合作，建立全方位、多层次的伙伴关系。双方将对解决方案进一步整合，在城市交通、轨道交通、公路交通、智慧水务、新型智慧城市等领域加大投入，携手为用户提供更高性能、更可靠、更智能的产品和服务，为智慧城市的建设贡献力量。

深信服 & 星环科技：以存储进一步挖掘数据价值

曾经离我们很远的大数据如今已经时刻服务于我们的日常生活，这些服务得益于大数据领域日益精进的平台服务，星环科技便是其中的一员。

多年以来星环科技致力于大数据和人工智能核心平台的产品研发，目前，星环科技已经与深信服企业级分布式存储 EDS 达成战略合作，双方就深度兼容性、功能完整性、性能、稳定性等方面进行了严格测试，结果表明星环大数据平台能够完美对接 EDS，双方相互兼容且性能表现优异，能够有效降低运维难度。

Hadoop 原生的 HDFS 大数据存储采用的是和计算分析平台的融合部署，这种方式带来了扩容、数据互通、可靠性等方面的难题。星环科技与深信服 EDS 联手，打造更强大的数据服务平台，在 EDS 按需扩容、多协议互通、高可靠高性能等特性的加持下，双方将为用户提供更完备的数据服务。


产品认证
PRODUCT CERTIFICATION
认证日期： 2020 年 6 月 20 日
认证结论：
经过深信服科技股份有限公司和星环信息科技（上海）有限公司共同严格测试：星环大数据平台TDH6.0能够对接深信服EDS3.0企业级分布式存储，实现稳定运行，双方相互兼容，性能表现优异，有效降低运维难度，共同为企业用户提供一体化解决方案。
测试内容：
- 深度兼容性测试
- 功能完整性测试
- 性能测试
- 稳定性测试
SANGFOR
深信服科技股份有限公司（盖章）
TRANSWARP
星环信息科技（上海）有限公司（盖章）

▲ 星环科技 & 深信服 EDS 产品测试认证

“存算分离”实现按需扩容

为提高性能，Hadoop 最初设计采用了计算和存储融合的“存算一体”架构，但存储空间的需求增长速度往往高于计算的需求增长，而扩容的时候必须按照两者的最大需求去进行扩容，导致计算资源大量的过剩和浪费，存储计算耦合也导致系统无法平滑向云过渡。

通过多年深耕，星环科技在大数据和人工智能领域拥有了强大技术优势，为了让扩容空间得到更高效的利用，星环科技通过联手 EDS 以支持大数据存算分离部署，计算和存储分别云化，实现资源的动态分配，按需扩容。星环科技与深信服 EDS 的优势互补，既保障了整体性能，也为用户节省了扩容成本。

多协议互通实现数据轻松导入

根据业务需求，数据往往存储于不同平台，极大地增加了管理难度，并且不同平台之间的协议又各有不同，一旦涉及不同平台之间的数据导入，将耗费大量时间和精力。不同平台存储的重复建设也大大增加了 TCO。

在星环科技与深信服 EDS 的通力合作下，数据平台可以通过一套存储实现 CIFS、NFS、FTP、HDFS 多协议互通。双方共同构建跨多个平台的业务处理管线的应用场景，帮助用户实现对业务数据就地分析，数据的互通大幅提高了业务处理效率。

保障数据可靠性及整体性能

由于 Hadoop 本身是个开源项目，在数据安全方面，HDFS 仅仅考虑了硬盘、服务器故障的保护机制，没有考虑到误删除、病毒、硬件亚健康等其他方面带来的可靠性隐患；在性能方面，当文件数量到达亿级别后 Hadoop hdfs 会出现严重的性能下降甚至更严重的系统问题。

星环科技结合深信服 EDS 自主研发的分布式数据库 PhxKV，满足亿级小文件规模承载且性能波动小于 5%。在数据保护方面，星环科技充分结合深信服 EDS 的纠删码、快照恢复、硬盘亚健康监测等可靠性机制，进一步提升大数据平台的容灾能力。用户也可以根据业务需求自行配置纠删码或副本模式，最大化地实现可靠性与经济性的平衡。

随着大数据对全行业各个领域的渗透，数据应用场景变得更加丰富，数据的价值将被进一步挖掘、放大。此次星环科技与深信服 EDS 的战略合作，为用户的大数据解决方案注入了更强大的数据整合及管理能力，未来，双方将继续以数据为驱动，为不同领域的业务持续赋能。

动态新闻一览

深信服重磅发布国内首批云安全访问服务，拥抱SASE新趋势

9 月 10 日，深信服基于多年的云安全研究技术及安全产品研发能力重磅发布国内首批 SASE 安全产品「云安全访问服务 Sangfor Access」，深信服将全面进入安全能力的云化交付时代。

深信服云安全访问服务是一个以 SASE 模型为核心的安全服务平台，通过集成“SD-WAN 接入服务 + 完整的云交付安全产品栈”以及部署在全球的多个 POP 节点，为海内外用户提供更灵活、更稳定、更有效的端到端网络及安全服务。

信服云品牌全新亮相：新定位、新形势、新能力、新方案

深信服将云计算品牌重磅升级为信服云，并发布新的 Slogan：助力数据中心云化演进，表示云计算业务致力于为用户交付省时省事、平滑弹性、安全可靠、业务承载丰富的云化数据中心，匹配数字化转型过程中用户在不同阶段的不同需求。

深信服亚太区巡展火热启动，珠海首站旗开得胜！

2020 年 8 月 26 日，“立数字基石，赢剧变时代”2020 年深信服亚太区巡展珠海首站旗开得胜！超过 300 位 IT 领域专家、学者、CIO 等齐聚珠海，针对网络安全、业务上云、敏捷 IT 架构建设多维度视角深入交流，展会现场，精彩纷呈。

作为深信服倾力打造、规模最大、覆盖面最广的年度盛会，本次巡展将陆续覆盖亚太 180 个城市地区，将结合外部环境剧变，紧紧围绕用户实际需求，从 IT 建设规划演进到前沿技术产品解析，与参会者共同探析如何做好数字化转型的基石性工作，在时代剧变的当下及未来，为业务注入持续发展的动力。

践行“四个坚持”，深信服联动21省市开展网络安全周活动

9 月 14 日，2020 年国家网络安全宣传周在河南省郑州市拉开帷幕。深信服 CEO 何朝曦应邀出席高峰论坛主论坛并发表主题演讲，针对网络安全厂商如何践行“四个坚持”进行探讨分享。此次深信服网络安全周宣传活动在广东、浙江、福建、湖北、重庆、山东、河北、青海等超过 21 个省份和地区同步开展，遍布大江南北。

深信服斩获中国网络安全产业联盟CCIA双料大奖

中国网络安全产业联盟（CCIA）组织开展了“2020 年优秀网络安全解决方案和网络安全创新产品评选活动”，经过专家评选、用户线上投票、复审答辩等多个环节，最终深信服安全运营中心解决方案和全网行为管理 AC 分别荣获“2020 年网络安全解决方案优秀奖”和“2020 年网络安全创新产品优秀奖”双料大奖，成为极少数荣获双项大奖的企业之一。

信服云荣获“鲲鹏应用创新大赛2020”奖项

在华为“鲲鹏应用创新大赛 2020”上，深信服“信服云 sCloud”解决方案在 13 个赛区近 1000 支队伍中脱颖而出，荣获“ARM 原生应用”赛道银奖。

信服云 sCloud 底层能够适配华为鲲鹏高性能服务器及欧拉操作系统，以虚拟化技术为核心，利用计算虚拟化、存储虚拟化、网络虚拟化、安全虚拟化等组件，将计算、存储、网络、安全等虚拟资源融合到 ARM 架构服务器中，信服云 sCloud 平台是面向下一代数据中心的、软件定义的、灵活起步、灵活扩容的基础架构。

深化金融科技创新应用，深信服与深交所达成战略合作

8 月 24 日，证券基金行业信息技术应用创新中心启动仪式暨信创工作研讨会在深圳证券交易所（以下简称深交所）举行。会议上，深交所与深信服正式签署了战略合作协议，这也标志着双方建立起长期、稳定、共赢的战略合作关系。未来，双方将发挥各自在信息技术资源和行业科技引领的优势，合力推动金融科技的研究与应用。

SANGFOR
深信服科技

让每个用户的数字化更简单、更安全

深圳市南山区学苑大道1001号南山智园A1栋
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

深信服官方微信

深信服移动官网