上讯信息 SUNINFO | InforCube

AGILE DATA MANAGEMENT PLATFORM

敏捷数据管理平台

企业上中下游数据高效使用与安全管控综合解决方案

上讯信息技术股份有限公司
Suninfo Information Technology Co., Ltd.

产品介绍

前言

近年来，随着互联网、云计算等新兴技术被广泛使用，数据呈爆炸式增长，数据使用的场景也随之增多，常见的如本地测试环境、云端测试环境、测试分析环境，为保证众多使用场景的安全性，国内外相继出台各项法律法规规范数据使用流程，其中，由人大常委会通过的《中华人民共和国网络安全法》是我国第一部全面规范网络安全管理的基础性法律，为网络安全工作提供切实法律保障；中国银保监会推出的《银行业金融机构数据治理指引》规定依法合规采集、应用数据，明确数据访问和拷贝的权限并监控行为；国家卫生健康委员会印发的《国家健康医疗大数据标准、安全和服务管理办法》要求医疗健康大数据在数据采集、存储、传输、应用等业务场景，对数据使用的整个生命周期做到访问权限管控。

然而，在实际的数据使用场景中，的确逐渐暴露出存储资源浪费、数据交付效率低下、隐私数据泄露以及访问权限管控缺失等方面问题。如何做到对测试环境数据的采集、传输、存储、使用、流转等关键环节进行效率和安全的双重保障，兼具加强业务数据流的权限访问控制，成为当前企业关注的重点，由此面向企业上中下游数据的敏捷数据管理平台应运而生。

敏捷数据管理平台产品概述

敏捷数据管理平台（Agile Data Management），简称 ADM，是企业上中下游数据的高效使用与安全管控的综合解决方案，可确保在数据安全的前提下，提高数据使用效率、降低数据存储成本。

ADM 由生产数据管理、备份数据管理、敏感数据管理、测试数据管理以及数据访问管理五部分组成，各功能系统可独立运行，也可以灵活组合，并可以软件与硬件一体机两种方式部署。

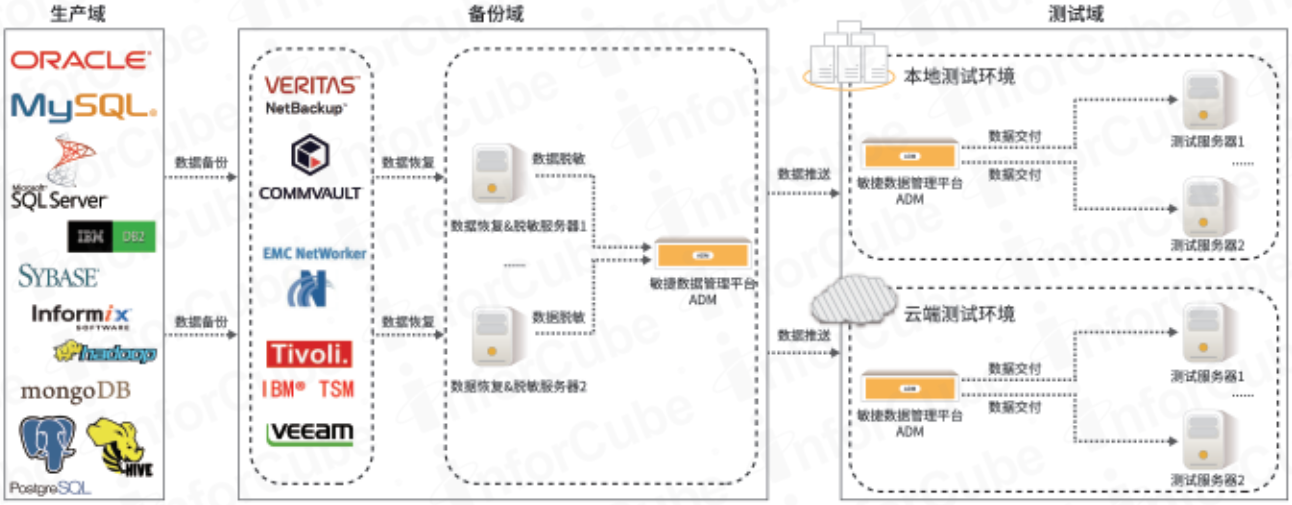
生产数据管理负责对生产业务数据库进行实时持续的数据备份与快速恢复。

备份数据管理负责自动恢复备份服务器中的备份数据，自动验证备份数据的有效性。

敏感数据管理负责对生产隐私数据进行敏感数据的静态脱敏，包括数据库与文件脱敏。

测试数据管理负责快速创建与交付测试数据库，提供给开发测试使用，属 CDM 产品。

数据访问管理负责对数据库访问行为进行权限管控，规范数据访问操作流程。



敏捷数据管理平台（ADM）产品功能示意图

生产数据管理

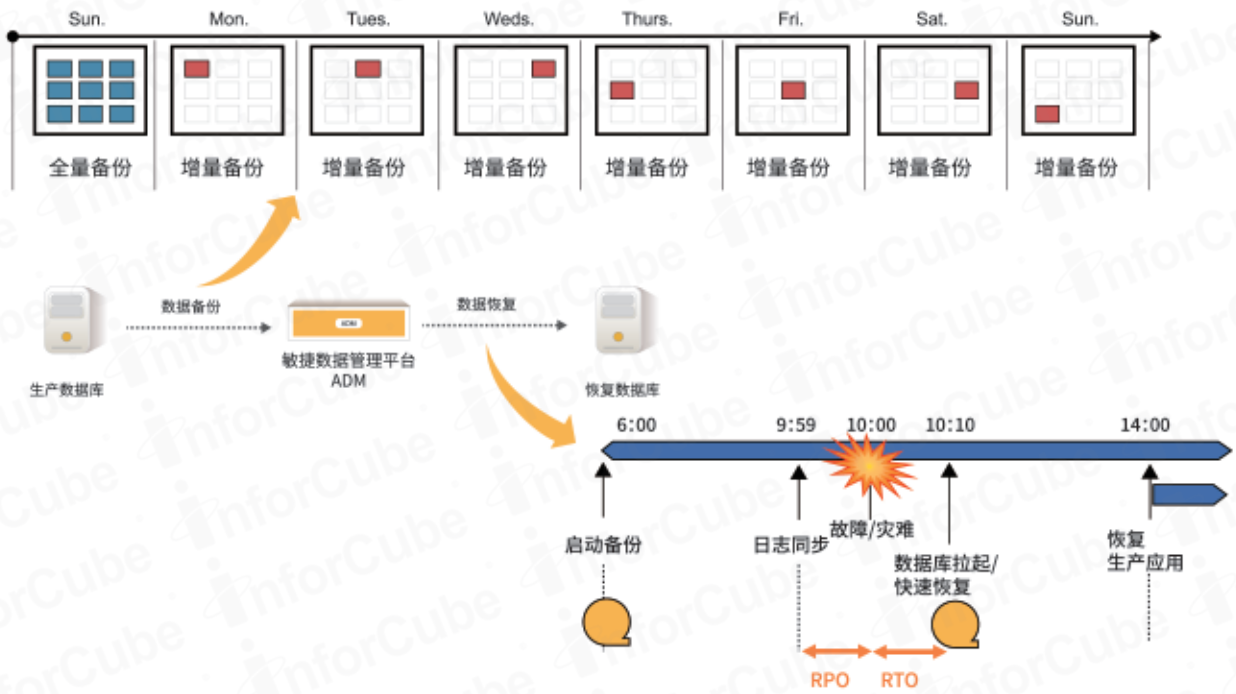
生产数据管理现状

近年来，企业为了防护数据丢失和保障业务持续，逐步加强数据库备份的 IT 建设，然而当前备份业务操作复杂、步骤繁琐，全量备份的方式导致备份恢复速度较慢，制约了企业备份恢复业务的有效运行。

因此，企业对备份产品提出了新的要求，不仅要保障数据安全，实现实时持续备份，还要求在灾难发生时，快速且不间断地恢复数据，做到数据库应急接管，同时对恢复的数据自动查验有效性。

生产数据管理解决方案

ADM 采用旁路式部署，实现对数据库的实时持续备份、快速恢复以及基于数据副本的恢复校验管理。通过首次全量，后续持续增量合成的备份方式，达到分钟级的恢复时间、秒级的恢复粒度，实现数据库的应用级保护与备份数据有效性的自动校验。



生产数据管理功能示意图

功能特点

- **持续增量备份**

通过结合数据库自身成熟备份方式，进行首次全量备份，持续性增量备份与全量快照合成，实时日志同步与日志校验技术，保证同步数据和生产数据的完整性和一致性。

- **快速秒级恢复**

支持数据恢复方式：本机和异机恢复，可选最近时间点快速拉起数据库，恢复时间可达分钟级、恢复粒度控制在秒级，实现生产业务的应急接管保证业务的连续性，待业务不繁忙时将数据库进行物理恢复，实现数据恢复业务 RTO 与 RPO 最少化。

备份数据管理

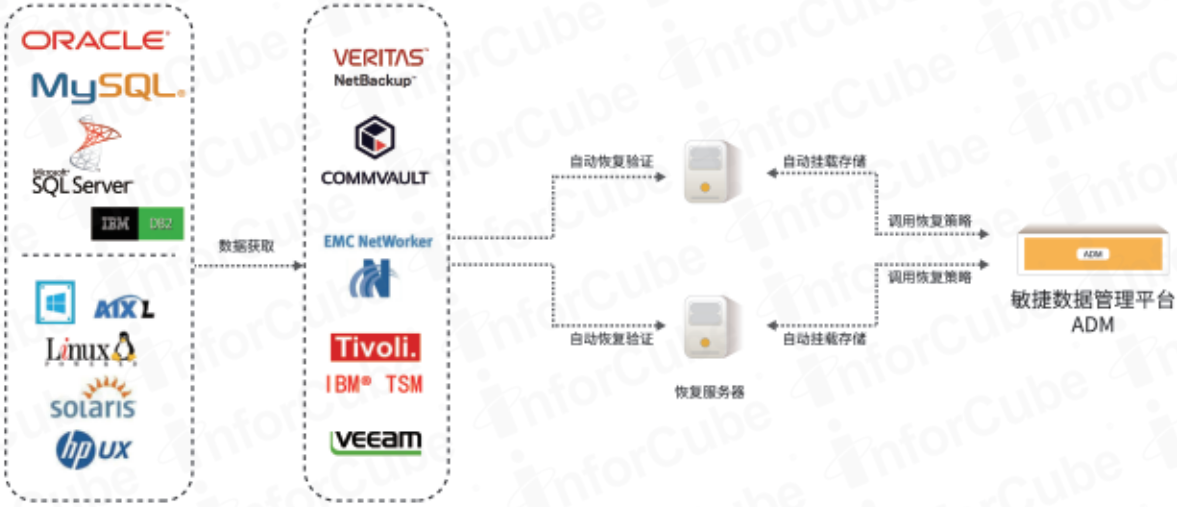
备份数据使用现状

2017 年以来，全球范围内爆发了大量的勒索病毒，遭遇攻击的服务器出现严重故障无法使用，导致备份数据无法恢复，因此企业急需对长期处于暗数据的备份数据进行恢复验证，保证其可用；与此同时，各行各业对备份恢复验证也提出，要求定期恢复验证以保证企业备份数据的有效性。

然而，企业对备份数据进行恢复验证的过程中，不仅需要投入大量的人力、设备以及存储资源搭建恢复环境，同时整个恢复流程均采用人工操作，过程繁琐复杂，耗时长，如需多次恢复则只能重复工作步骤，增加了备份验证工作的难度。

备份数据管理解决方案

ADM 通过集中管理存储资源、恢复服务器资源和恢复任务，实现存储空间、恢复服务器和恢复任务的自动调度，从而实现备份数据有效性验证的全自动化，并且根据验证结果生成详细的恢复验证报告。备份数据管理可以满足用户对当前备份数据的可恢复性验证、恢复后的完整性验证两方面的需求，且能够覆盖用户现有全部业务系统的备份数据，达到验证工作的高覆盖率，提高有效性验证的频率。



备份数据管理功能示意图

功能特点

- **恢复资源集中管控**

ADM 通过集中管理恢复服务器、恢复存储资源，实现闭环式集中数据管理流程，全程监控实现恢复数据的有效管理。

- **备份恢复验证自动化**

根据现有备份服务器的备份策略，ADM 统一调度恢复任务，设定任务计划，自动地将备份数据进行可恢复性验证与有效性验证，摆脱人工繁琐的恢复操作步骤，简化恢复流程，节省大量的人力成本和时间成本。

- **恢复存储成本节约**

ADM 自动恢复备份数据可充分盘活备份数据，实现对备份数据的二次利用；ADM 内置的高效压缩存储池，压缩比高达 4:1，大大降低了备份数据恢复的存储空间占用，显著节约了存储成本。

敏感数据管理

敏感数据使用现状

01 发现不彻底

敏感数据种类繁多，特征不一，人工识别易遗漏，数据库大表多，无法进行全面比对

02 灵活度不足

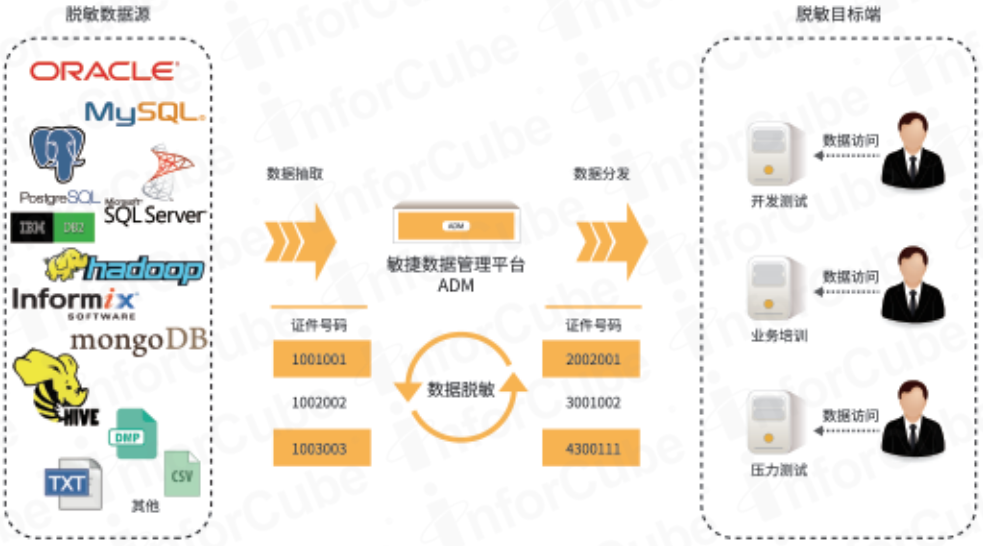
脚本脱敏算法单一，速度慢耗时长，敏感数据分布不均导致无法集中处理

03 脱敏不满足要求

脱敏后数据丢失业务属性，仿真度低，脱敏后打破原有业务数据关联，无法满足大量测试场景需求

敏感数据管理解决方案

敏感数据管理可以实现敏感数据的自动识别与敏感数据的仿真脱敏，针对敏感数据识别提供通用数据特征库、全库与子集自动扫描，包括数据内容、字段类型、约束关系均可以实现自动识别，并依据敏感类型特征加以分类；针对敏感数据的仿真脱敏，ADM 内置大量数据脱敏算法对敏感数据进行随机化、模糊化、高仿真度替换，保证脱敏后数据的完整性、仿真性以及数据间的关联关系保持不变。



敏感数据管理功能示意图

功能特点

- **敏感数据发现自动全面**

智能定义敏感数据类型，自动扫描敏感数据，包括数据类型、内容、约束关系，灵活排序减少人为筛选，全面精准定位敏感数据源。

- **脱敏算法丰富仿真度高**

丰富的脱敏算法与仿真的字典库相结合，保证脱敏后数据仍具有业务属性，数据表间关系仍具有业务一致性，不影响数据挖掘分析数据价值。

- **表级并发灵活异构脱敏**

支持数据库全库与子集的异构脱敏，支持库到库、库到文件、文件到库、文件到文件等多种数据脱敏转换方式，支持表级并发处理，提高数据脱敏效率；核心生产数据中间不落地，减少数据泄露风险。

测试数据管理

测试数据使用现状

测试数据交付周期长

测试环境从生产环境获取测试数据，《网络安全法》实施后申请流程愈发严格，加之测试环境准备繁琐复杂，延长了测试数据的交付时间，造成系统开发计划的推迟。

测试数据存储占用高

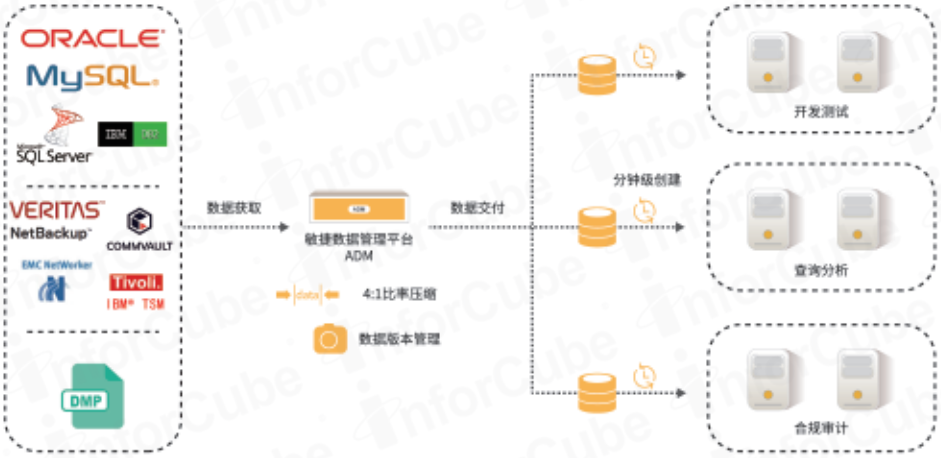
一旦有测试数据的新需求，需通过物理导出生产系统的数据，独立存放，长此以往测试环境形成了大量的数据孤岛，存储资源被过度占用。

测试数据版本管理难

测试数据更新较快，如需使用上一份测试数据，只能重新导出重复操作流程，目前无法对测试数据的版本进行保存和共享。

测试数据管理解决方案

测试数据管理是基于数据库虚拟化技术对生产数据进行获取、存储与使用的拷贝数据管理（CDM）产品，能够通过生产数据获取，数据副本存储，虚拟数据库挂载，达到快速交付测试数据，集中管理测试数据存储与流转的目标，是主要针对企业软件开发测试部门使用数据的实际需求，提供的一套完整的测试数据管理解决方案。



测试数据管理功能示意图

功能特点

- **存储成本节省 10 倍**

（1）ADM 内置独有的高效压缩存储池，压缩比高达 4:1，存储即压缩，显著降低了基础数据源获取的存储成本；

（2）ADM 的数据库虚拟化技术（专利申请号 201611227355.X），能够做到只需一份基础数据源，即可快速拉起多份虚拟数据库，拉起时不占用物理存储空间，节约了存储成本 10 倍以上；

- **数据交付效率提升 100 倍**

（1）通常情况下，ADM 将 TB 量级数据库拉起时间控制在分钟级，响应速度快，可满足开发测试、查询分析、合规审计、应急容灾等场景对数据交付效率的要求；

（2）数据库虚拟化技术的优势在于多份虚拟数据库读写操作独立，完全满足测试环境多场景同步测试的需求，ADM 内置的智能读写缓存机制，能够有效保障性能压力测试；

- **测试数据版本管理**

集中的数据使用流程，通过跟踪数据流向，识别虚拟数据库使用状态，实时拍摄快照，实现数据版本的保留，测试数据版本的快速回退，有助于对数据版本的良好管理。

数据访问管理

数据访问管理控制现状

01 权限控制分散

数据动态访问行为受限于数据特征预定的静态敏感策略，无法满足数据访问过程的随机性和灵活性，故当前数据库权限控制行为过于分散

02 特权账号共享

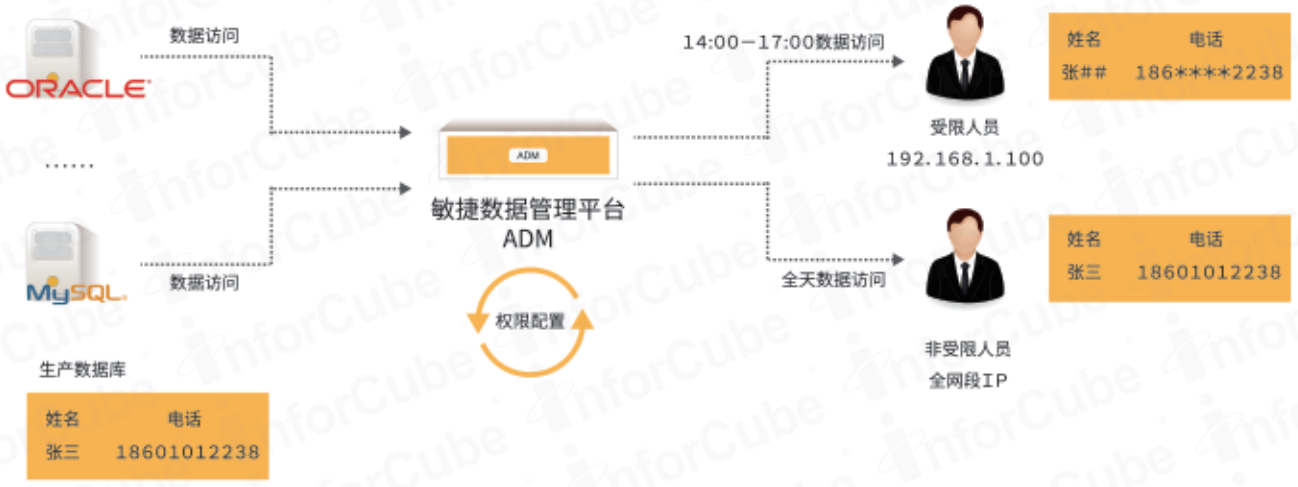
当前对业务数据库访问的特权账号存在共享的现象，一旦发生数据越权访问，难以确定访问主体，事后追责困难

03 事中控制薄弱

现有的数据访问控制措施粒度过大，访问对象控制在数据库级，无法覆盖数据权限控制的全部细节，导致管控环节的遗漏

数据访问管理解决方案

数据访问控制管理系统，采用基于虚拟账号的授权管理与行为控制，全面控制数据访问操作行为，规范数据申请审批流程，通过对用户角色、访问时间、终端 IP 以及数据库访问工具制定数据访问规则，达到强制数据安全管控的效果。



数据访问管理功能示意图

功能特点

- **采用虚拟账号，消除访问隐患**

ADM 内置权限匹配的功能，根据具体属性制定访问策略，做到事前控制、事中跟踪、事后识别全程记录访问者，严格控制访问行为

- **缩小访问粒度，管控访问细节**

所有 SQL 指令经过 ADM 过滤，扫描出所有的访问属性，首次将访问粒度缩小至数据库表级、数据库字段级，满足等保 2.0 对数据访问控制的客体要求

- **属性动态灵活，提高访问安全**

ADM 访问控制技术的优势在于能够动态识别客户端发出的所有访问行为，替换真值返回受限访问结果，不局限于数据自身特征预定的固定、静态的敏感策略，因此在保证数据安全访问的前提下，增加了数据访问的灵活性。

法律政策合规

《中华人民共和国网络安全法》

第四章第四十二条 网络信息安全

网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

《信息安全技术 网络安全等级保护基本要求》

第一部分：通用安全要求

应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

应禁止未授权访问和非法使用用户个人信息。

《金融行业信息系统信息安全等级保护测评指南》

第七部分：现场测评 系统运维管理

应定期对主要备份业务数据进行恢复验证，根据介质使用期限及时转储数据。

《银行业金融机构数据治理指引》

第三章第二十四条 数据管理 数据安全

银行业金融机构应当建立数据安全策略与标准，依法合规采集、应用数据，依法保护客户隐私，划分数据安全等级，明确访问权限，监控访问行为，完善数据安全技术，定期审计数据安全。

中华人民共和国
网络安全法

上讯信息技术股份有限公司

咨询热线：400 880 5062
服务热线：400 682 1599
传　　真：86-21-51905959
邮　　箱：market@suninfo.com
网　　址：www.suninfo.com
地　　址：上海市浦东新区郭守敬路498号20号楼

SUNINFO官网

SUNINFO公众微信