BEYOND
TECHNOLOGY

SaCa® IAM 身份与访问控制管理平台产品白皮书

此处标注东软信息安全密级

Neusoft

一、前言

1.1 多应用身份管理面临的问题

随着云、互联网的快速发展，企业规模不断壮大，集中表现在企业应用系统数量和企业用户数量不断增多、企业网络规模不断扩大，与之带来的安全问题日益突出。然而当前企业各个应用系统独立，各自实现系统内的身份管理、认证、授权和审计工作，已远远不能满足企业发展的需要，存在的问题主要表现在以下几个方面。

1.1.1 企业用户面临的问题

随着企业应用系统的增多，用户需要登陆的系统随之增多，比如财务系统、人力系统、CRM系统等。用户经常需要在多个系统之间进行切换，每次从一个系统到另一个系统的切换都需要输入账号密码来进行登陆，这样的操作行为给用户带来了诸多不便，影响了用户的工作效率。

在此基础上，很多用户为了快捷使用，通常采取将系统账号密码设置为简单密码的方式来方便记忆，或者将多个系统采用同一账号密码来进行登陆。这种方式给系统带来了潜在的危险。

此外，用户缺乏一个统一的视图来知晓自身可以访问哪些应用，当涉及到多个系统共同完成一个完整的业务工作时，缺乏可定制的个性化页面来集中流畅地完成跨多应用的复杂业务处理。

1.1.2 企业管理员面临的问题

对于企业系统管理员来说，需要完成多个应用系统上用户账号、认证、授权和审计方面的管理工作。在这个过程中，管理员面临着多个方面的压力。

1) 管理工作量日益巨大。

企业管理员需要完成多个应用系统上用户、认证、授权和审计方面的管理工作，并随着企业应用系统数量和企业用户数量的增多，工作量呈现指数级增长。

2) 管理难度日益扩大。

企业应用系统设计标准不一，对于账户信息，账户所在组织机构信息表达方式各异，经常出现各系统间账户信息不一致问题。当新增用户时，管理人员需要同步增加符合该用户的应用系统的用户信息；当删除用户时，管理人员需要同步删除各个系统中的用户信息，对管理人员来说管理难度越来越大。

3) 管理常常不合理。

在用户授权过程中，管理员难以完全遵照最小权限原则来进行用户权限的分配，导致用户权限分配缺乏正确的边界。

4) 人工管理无法保障企业安全。

有些账号信息多人共用，当安全事故发生时，无法确定账号的使用者，人工管理无法准确定位问题根源。

1.1.3 企业 IT 建设面临的问题

不同的应用系统，各有一套独立的用户管理、认证、授权和审计机制，造成系统重复开发的成本。除了成本问题以外，更严重的是安全问题：由于各个系统各自为政，在身份认证上缺乏统一、严格、安全的认证机制；在访问控制上缺乏集中统一的资源授权管理机制，无法严格分配权限，不能达到系统只授予用户必要的权限的要求；在安全审计上各个系统单独审计，缺乏集中统一的系统访问审计，无法对支撑系统进行综合分析，不能及时发现入侵行为。

1.2 企业对多应用身份管理的诉求

伴随着企业业务不断发展而来的越来越多的安全孤岛，帐号多，认证多，授权复杂，审计分散等问题的出现，企业对多应用系统的身份管理和访问控制逐渐有了新的要求。具体体现在三个方面。

1) 降低企业管理复杂度

- 实现应用系统用户信息的全生命周期管理，均可在一个平台上完成。
- 轻松发现未经授权的信息资源访问、权限滥用和非法入侵企图等。

2) 提升企业用户使用体验

- 实现企业用户一次登录便可访问所有授权的应用系统，提升用户的工作效率。
- 提供统一的视图展示所有可访问的应用，轻松在多个应用间切换。

3) 保障企业信息安全

- 完成账号、认证、授权的统一管理，实现不同权限级别的账号拥有不同的安全策略
- 完成安全审计的统一管理，实现对所有系统的综合分析，及时发现系统中存在的安全问题和各种

入侵企图。

二、SaCa IAM 身份与访问控制管理平台

2.1 简介

SaCa IAM（Identity and Access Management）是一款安全、灵活、稳定和可扩展的企业级身份与访问控制管理平台，旨在生产环境下将分散、重复的用户身份信息进行整合，提供统一的门户入口，并方便门户的个性化定制，提供标准身份信息读取和查询方式，统一管理用户身份的生命周期，统一企业内部身份安全策略管理和权限管理，为应用系统提供标准访问接口，最终达到保障应用安全访问、减轻系统压力、提高工作效率、提升用户体验的效果目标。

2.2 为什么选择 SaCa IAM

SaCa IAM 能够以统一、安全、可靠、合规的方式对承载企业数据资产（包括数据、应用软件、数字化资产等）的信息系统访问者进行授权管理。也即是让可信任的人提供可信任的身份从统一的门户入口访问已授权的数据资产，在整个访问周期内对关键行为实现对应的风险识别与控制，从而保护企业应用系统免受内外部的攻击威胁，确保企业数据资产的完整和安全，并且提供及时、可信的审计和报告。具体来说，SaCa IAM 的关键价值体现如下：

2.2.1 大幅度提升企业运作效率

企业普遍存在大量的应用系统，且复杂业务常跨越多应用。SaCa IAM 提供优质的单点登录，助力用户快捷登录多应用，同时提供统一门户，帮助用户在统一视图集中流畅地完成跨多应用的复杂业务处理，极大提升企业整体的运作效率。

2.2.2 节约开发成本 降低管理难度

为避免企业快速建设中，对多个既有共通又有个性差异的应用系统重复开发和维护多套用户管理、身份认证体系，SaCa IAM 高度可扩展的统一用户与身份认证帮助企业集中式管理，节约大量开发成本，解放管理人员。

2.2.3 超强认证支持 保障信息安全

随着企业对信息资产安全重视度的提高，SaCa IAM 提供多种强认证手段，支持多重认证防护，高可扩展认证能力，帮助企业轻松实现全网统一的信任服务体系，有效抵挡潜在安全威胁，将安全风险降到最低，有力保障信息安全。

三、关键特性

3.1 单点登陆机制

SaCa IAM 具有完善的单点登录体系，可安全地在应用系统之间传递或共享用户身份认证凭证，用户不必重复输入凭证来确定身份。不仅带来了更好的用户体验，更重要的是降低了安全的风险和管理的消耗。

与单点登录相对应，单点退出功能可以解决“单点登录”功能在方便用户的同时留下的安全隐患，用户主动下线或超时下线时，SaCa IAM 会向业务系统发起用户下线通知，告知业务系统，某用户已经下线，请销毁相关 Session 会话。

3.2 统一用户管理

SaCa IAM 的用户管理模型是一个高度可扩展的模型，能够满足绝大部分企业不同场景下的需求。用户管理模型主要包含的特性如下：支持多维度管理；提供组织单元、用户管理以及属性扩展，同时支持组织机构快速定位、拖拽功能；用户密码修改。此外，SaCa IAM 用户管理模型支持组织机构核心管理接口的回调功能，支持二次开发改变或扩展原有功能等特性实现。

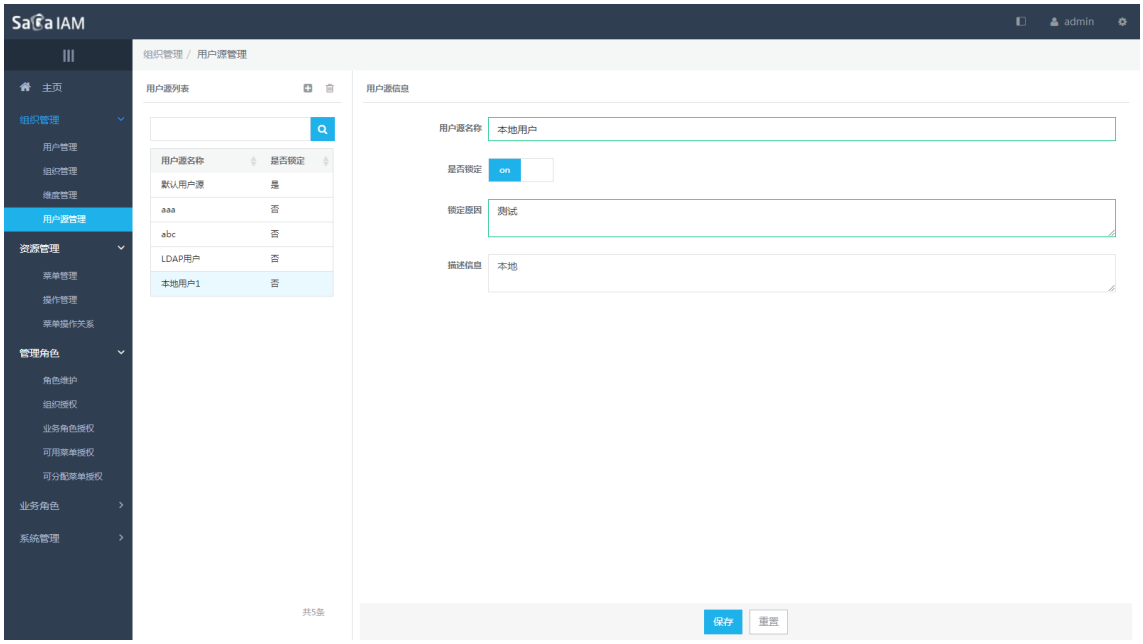

图 用户源管理

3.3 统一认证管理

SaCa IAM 利用领先的身份认证功能，将用户的身份认证与企业的管理技术和业务流程密切结合，保证系统中的数据资源只能被有权限的用户访问，未经授权的用户无法访问数据；防止伪造身份认证手段、访问者身份等非法措施，从而有效保护信息资源的安全。

3.3.1 多手段融合的高级安全认证体系

传统身份认证只采用一种身份识别用户身份，因此认证很容易被仿冒或攻击。而 SaCa IAM 支持对多种身份认证方式的组合使用，比如用户名/密码认证、短信验证码认证和 OpenID Connect 等，有效提高身份认证的安全性。此外，SaCa IAM 支持强制认证方式，即用户使用其他认证方式登录进入系统，对需要进行强制认证的系统或应用场景依然需要二次强制认证，可以充分保证系统的运行安全和操作维护安全。

3.3.2 灵活便捷的认证扩展机制

SaCa IAM 认证扩展的机制是基于插件实现的，任何一种新的认证方式都可轻松通过我们的插件体系进行灵活支持。通过自定义的插件扩展，结合强认证的认证方式，实现更加符合企业需求、更加安全可靠的安全策略。

3.4 统一权限管理

SaCa IAM 为企业用户提供了两种灵活的授权方式：角色授权和组织机构授权。在 SaCa IAM 中可以同时为某个系统分别按照用户角色和用户组织授权，如 HR 系统只有人事部门可以访问，并且部门经理及以上级别可以访问。这种按照用户组织机构与用户角色结合的授权方式不仅更为灵活，同时也更符合实际成产生活的需求。

SaCa IAM 将角色分为业务类角色和管理类角色。其中管理类角色又分为超级管理角色、安全管理角色、组织管理角色及审计管理角色。这样分类最主要的目的就是确保对业务用户维护、授权和审计等操作不被同一个管理人员拥有（当然也可以配置是否采用这种安全策略）。对于管理类角色，提供了分级管理功能，能够支持上级角色给下级分配可用菜单、组织和业务角色，做到权限的分级授权以及级联回收功能。

SaCa IAM 中的组织是组织机构的组成单元，一个组织机构是由多个组织通过上下级关联构成的一棵组织树。组织单元支持分级管理，管理角色可管理的组织单元可以级联下级。SaCa IAM 中的维度反映组织上下级关系的一个视角，不同维度下组织单元的上下级关系可能不同。操作人员登录系统后有且只有一个默认维度。对于比较复杂的业务系统组织机构，可以根据需要定义任意多个维度，例如行政维度、财务维度、地域维度等。

3.5 统一门户管理

SaCa IAM 提供一个可扩展的门户框架，将企业信息系统分散的功能等有机的整合到统一的界面中，比如通过门户实现统一权限管理、统一应用功能管理等功能。前端展现采用 HTML5 的技术，风格样式满足当前最流行的互联网 UI 风格展现要求。

SaCa IAM 提供三种门户展现的方式：门户应用列表，门户菜单集成和服务集成，默认方式是门户应用列表。其中门户应用列表是指用户通过单点登陆成功后看到的页面信息，展示的是用户可访问的所有应用；门户菜单集成实现的是将所有可访问的应用中的菜单展示在门户中，用户无需访问各个应用即可完成相应的工作；服务集成是能够以 Widget 的形式来对多个系统的功能统一的集成起来，方便用户在统一的页面下完成多应用的操作。

图 多应用列表

图 widget 服务集成

SaCa IAM 对于服务集成的方式满足运行期页面个性化定制，用户能够针对实际使用情况完成首页 Widget 的个性化配置工作，Widget 设置支持：1、登录用户首页可视化配置，方便用户操作；2、支持布局调整，方便根据展现 Widget 的实际内容设置；3、支持 Widget 的排序设置，用户可以根据自身的操作习惯设置。此外，SaCa IAM 实现多套 UI 皮肤并支持运行期皮肤切换。用户登录成功后，可以通过皮肤切换按钮完成皮肤切换。门户会帮助记录换肤动作，用户在下次登录时，会按照最后一次换肤的风格展示。

3.6 安全审计

SaCa IAM 记录系统范围内的安全和系统审计信息，有效地分析整个系统的日常操作与安全事件数据，通过归类、合并、关联、优化、直观呈现等方法，使管理员轻松识别应用系统环境中潜在的恶意威胁活动，可帮助用户明显地降低受到来自外界和内部的恶意侵袭的风险。

SaCa IAM 具有实时监控功能，能够随时了解用户当前操作的内容、监控用户的操作，及时发现潜在的危险操作或者违法行为，以便第一时间处理。在 SaCa IAM 中发生的关键事件可以得到过滤、标记，并被发送给指定的接收对象。这种能力可以使管理员接近实时地发现重要的事件，同时还可以实现 Email 告警、短信告警或其他形式的操作。

SaCa IAM 内置了大量报表和图表功能，使管理员方便地制作多种类型的报告，可以细化到每个字段。报告功能可提供多种格式的报表，包括便于 web 浏览和分发的 HTML 格式。

另外，对于 SaCa IAM 采用三权分立的授权机制，管理员对 SaCa IAM 所作的所有修改和系统自身发生的情况都会被记入日志中，并且只有日志审计管理员才可对日志进行操作。

四、应用场景

4.1 优质的单点登录，助力用户快捷登录多应用

背景：很多政企已建设多个应用、每个应用都有各自的登录账号，用户经常需要在多个系统之间进行切换，缺乏系统登录统一入口。

解决方案：通过 SaCa IAM 的统一用户的功能，解决了各个应用系统需各自维护用户的问题，由 SaCa IAM 实现用户统一化。通过 SaCa IAM 的统一认证的功能，解决了各个应用系统认证方式不一致、认证强度不足的问题，由 SaCa IAM 实现了多方式、多终端的统一认证支持。基于统一用户和统一认证来实现一处登录处处访问的单点登录效果，包括提供统一的登录入口和提供应用列表的门户界面等，使得用户维护一套用户名密码即可快捷访问企业所有应用系统，大大提高了企业用户的工作效率。

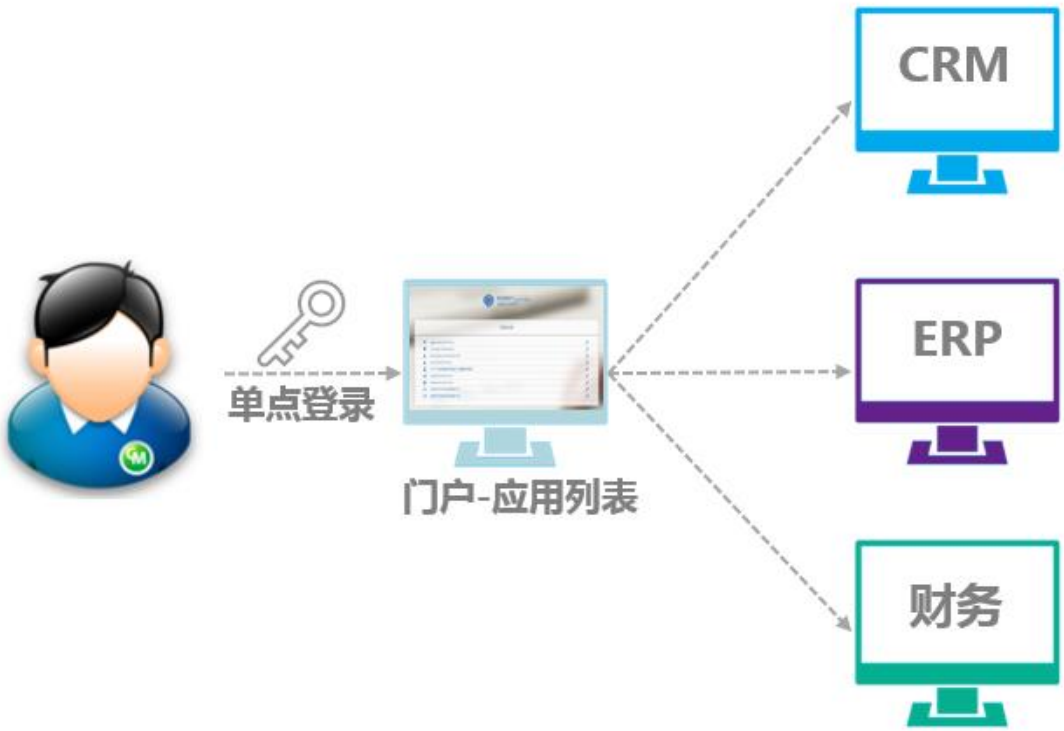

图 多应用单点登录示意图

4.2 灵活的权限控制，实现多应用菜单集成

背景：在满足基本的单点登录需求上，用户希望能够集中访问所有的应用功能，而非跳转到各个应用去操作。

解决方案：通过 SaCa IAM 的统一权限功能，能够方便地维护各个业务系统的菜单、角色，并完成用户、角色、菜单的权限设置操作。通过菜单管理与授权，门户中能够展现登录用户可访问的所有应用下的菜单列表。用户通过门户直接访问所有的应用的菜单，而不再需要通过点击应用超链接跳转到各个应用中。

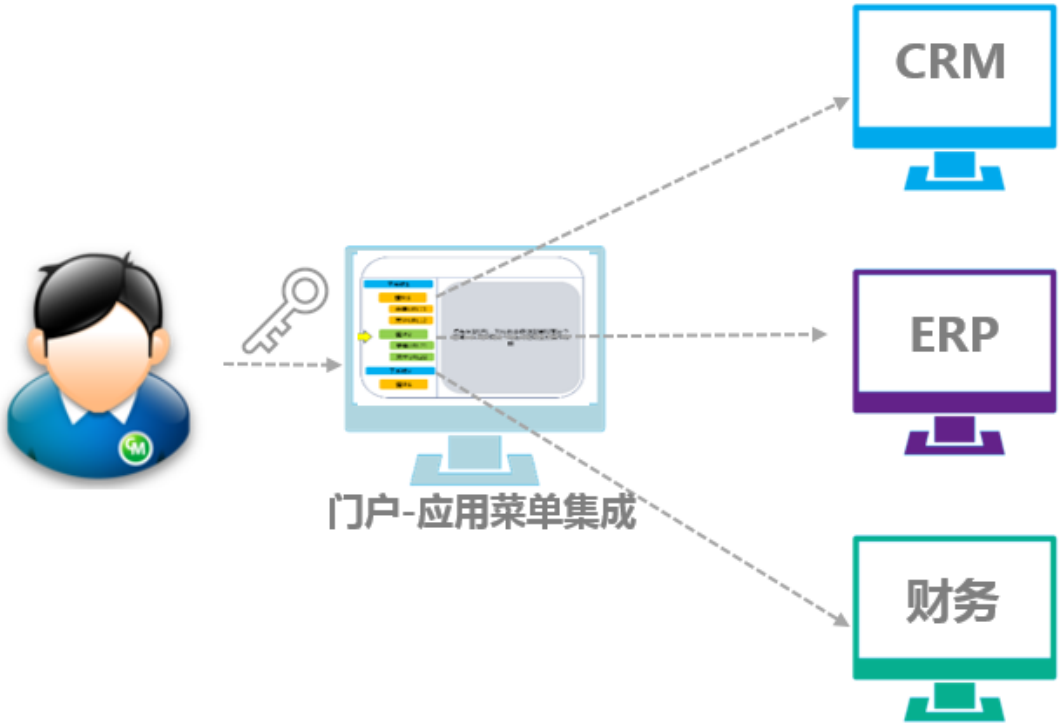

图 基于统一权限实现的菜单集成示意图

4.3 个性化的门户定制，结合 API 完成能力开放与集成

背景：在 4.1 和 4.2 场景中，在实现单点登录和权限控制的基础上，分别提供了应用列表和全部应用菜单的门户页面。除此之外，一部分用户希望能够个性化的定制属于自己的门户页面，页面中能够包含很多模块，每个模块是自己常用应用的功能，那么用户可以在自定义的页面中查看和操作多个应用的多个功能模块。

解决方案：通过 SaCa IAM 提供的自定义门户框架，基于 Widget 开发模式，每个 Widget 会调用集成应用的 API，引入 API 管理平台能够很好地实现 API 的接入和开放。SaCa IAM 管理员能够进行 Widget 的创建与发布、管理与授权，企业用户能够在首页通过 Widget 的添加、布局、删除等操作来定制自己的页面，将各个业务系统最常用的功能统一在首页上操作，更大程度上提升了使用体验和工作效率。

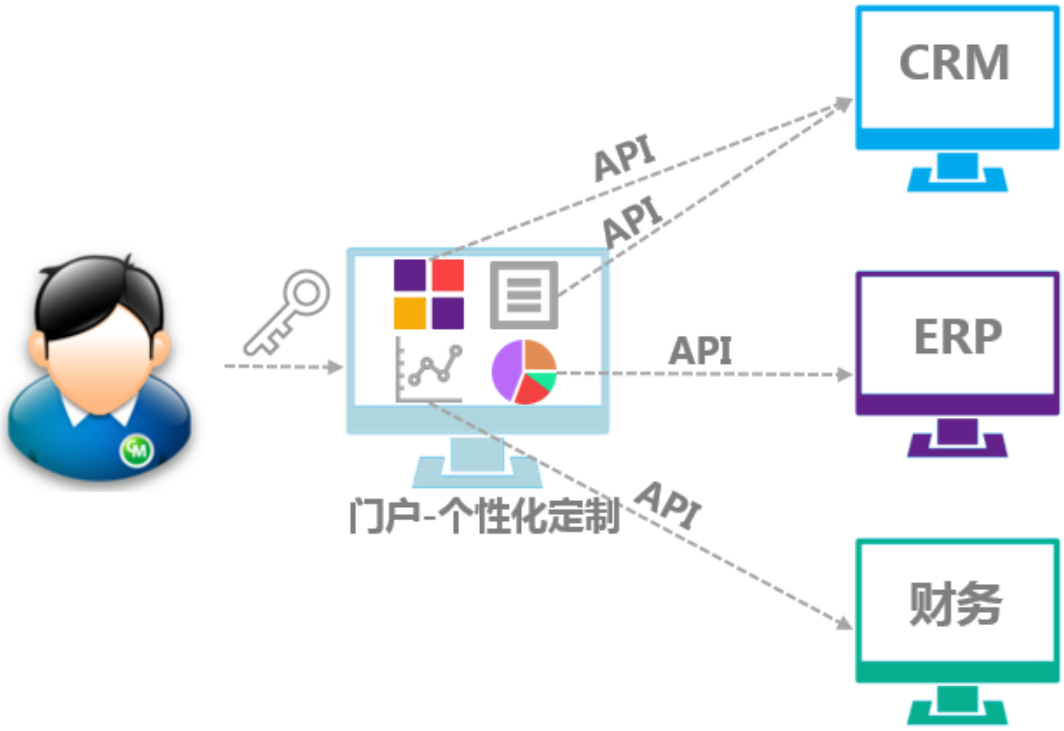

图 基于个性化门户框架实现的能力开放与集成示意图

五、关于东软

东软创立于 1991 年，是中国领先的 IT 解决方案和服务提供商。公司主营业务覆盖软件产品与平台、行业解决方案、产品工程解决方案和服务四个领域。目前，东软拥有员工 13000 余名，在中国建立了 8 个区域总部、16 个软件开发与技术支持中心，5 个软件研发基地，在 40 多个城市建立营销与服务网络，在大连、南海、成都和沈阳建立了 3 所东软信息学院和 1 所生物医学与信息工程学院；在美国、日本、香港、阿联酋、匈牙利和印度设有子公司。

东软是中国第一家上市的软件企业，是第一家通过 CMM5 和 CMMI（V1.2）5 级认证的软件企业，是中国最大的离岸软件外包提供商。2007 年，公司主营业务收入为 33.5 亿元人民币。

东软的 IT 解决方案广泛地应用于电信、电力、社保、金融、税务、交通、教育、医疗、制造业以及电子政务等几十个重点行业和领域，在中国市场，拥有客户达 15000 家，其中在社保行业占有 50%以上的市场份额，在电信行业占有 30%的市场份额，在电力行业占有 10%的市场份额，在网络安全领域拥有 15%以上的市场份额。 在离岸软件外包方面，东软已经与日本、美国、芬兰、荷兰、德国等国家的跨国企业建立战略合作伙伴关系，拥有 50 多家国际软件外包客户。 2007 年，东软被美国国际外包专业委员会（IAOP）评为全球 25 家最优秀的外包提供商之一。

东软致力于成为最受社会、客户、投资者和员工尊敬的公司，并通过过程与方法的不断改进，领导力与员工竞争力的发展，持续和开放的创新，使公司成为全球优秀的 IT 解决方案和服务提供者。

产品网站：http://platform.neusoft.com

技术社区：http://plus.neusoft.com

电话：400 655 6789

邮箱：platform@neusoft.com

微信：东软平台产品