某医院网络建设解决方案

北京一实天勤科技有限公司

2023 年 5 月

目录

第 1 章 背景介绍 2
第 2 章 技术应答 3
2.1 出口防火墙解决方案介绍 3
2.2 内网防火墙解决方案介绍 4
2.3 内网 EDR 解决方案介绍 5
2.4 上网行为管理解决方案介绍 6
2.5 态势感知系统解决方案介绍 7
2.6 终端准入系统解决方案介绍 9
2.7 堡垒机系统解决方案介绍 10
2.8 日志审计解决方案介绍 11
2.9 漏洞扫描解决方案介绍 12
第 3 章 北京一实天勤科技有限公司简介 15

第 1 章 背景介绍

某医院现网中目前两台 CP 设备已到维保期，为保证某医院网络安全建设顺利进展，提出如下建议，以目前现状为基础，并考虑后期发展要求，以便对网络安全做出优化。

第 2 章 技术应答

2.1 出口防火墙解决方案介绍

在如今的网络环境中，部分有安全隐患的终端可以肆意上网，易感染威胁，病毒等恶意内容在内部扩散，员工随意的访问网页，却可能因此感染木马，恶意插件；僵尸终端恶意外联或对外 Dos 攻击，各种类型的网络应用层入侵风险层出不穷。

究其原因，企业缺乏有效的安全技术保障导致执行效果差，而传统的安全设备防护割裂不完整，与此同时互联网威胁越来越多，隐蔽和感染技术越来越先进。而普通终端用户安全意识参差不齐，间接的放大了互联网威胁。

企业网络问题体现在以下方面：

在事前体现为难以看清风险，防护缺乏针对性，因此要求事前洞悉资产风险，确保防护有效性事前自动梳理资产，发现资产风险和新增资产，确保防护策略的全面、有效、准确，。

在事中体现为难以防护成功，威胁快速更新迭代导致攻防失衡。要求事中融合防护能力，确保防护的完整性事中防护能力需要涵盖网络层防护能力和应用层防护能力，具备边界防护的完整功能。

在事后体现为发现滞后，响应迟缓，导致损失扩大。事后持续监测已入侵威胁，要求快速止损事后能够实时监测内部异常外联行为，及时察觉并定位已入侵威胁，快速处理减少损失。

典型的传统防火墙的能力包括：数据包过滤、网络地址和端口地址转换、状态检查以及虚拟专用网络（VPN）支持。典型的入侵防御系统的能力包括：面向漏洞的和面向威胁的签名以及启发式处理。

新一代防火墙的关键能力在于，除了传统防火墙具备的一切能力外，它还具备一些整合了创新型识别技术、高性能以及其它基础特征的高级能力，能够形成企业级解决方案。

主动应用程序识别功能是位于新一代防火墙核心位置的通信流分类引擎。该功能要求采取多方位手段，确认网络上应用程序的身份，并且不分端口、协议、加密或规避技术。

用户识别技术将 IP 地址与特定的用户身份相联系，实现对单个用户网络活动的检视和控制。

新一代防火墙提供了强化可视性和控制力，让企业能够把重心放在业务元素上，同时又不必依靠那些模糊的、具有误导作用的端口和协议等属性。可以针对所有位置的全体用户，提供一套统一的保护和启用能力，实现全面覆盖。

2.2 内网防火墙解决方案介绍

内网防火墙位于企业内部，依照不同的功能部署在不同的位置点上，例如部署在服务器区前面，等保区域前方。

功能与外网防火墙类似，但单纯的外网防火墙无法阻挡内部的横向攻击，员工在不知情的情况下携带含有病毒木马的终端设备，连入内网之后，如果没有对关键位置的防护，很容易被内部横向传播，继而攻击重要服务器，引起重大的安全隐患。

内网防火墙与外网防火墙相比，与硬件上存在不同的要求，内网中横向流量接口较多，吞吐量较大，要求防火墙有着合适的性能与板卡。

在功能方面，典型的传统防火墙的能力包括：数据包过滤、网络地址和端口地址转换、状态检查以及虚拟专用网络（VPN）支持。典型的入侵防御系统的能力包括：面向漏洞的和面向威胁的签名以及启发式处理。

新一代防火墙的关键能力在于，除了传统防火墙具备的一切能力外，它还具备一些整合了创新型识别技术、高性能以及其它基础特征的高级能力，能够形成企业级解决方案。

主动应用程序识别功能是位于新一代防火墙核心位置的通信流分类引擎。该功能要求采取多方位手段，确认网络上应用程序的身份，并且不分端口、协议、加密或规避技术。

用户识别技术将 IP 地址与特定的用户身份相联系，实现对单个用户网络活动的检视和控制。

新一代防火墙提供了强化可视性和控制力，让企业能够把重心放在业务元素上，同时又不必依靠那些模糊的、具有误导作用的端口和协议等属性。可以针对所有位置的全体用户，提供一套统一的保护和启用能力，实现全面覆盖。

2.3 内网 EDR 解决方案介绍

从近年来的安全事件我们可以看到,攻击者从以破坏为主的攻击逐渐转变为以特定的政治或经济目的为主的高级可持续攻击。无论从著名的 Lockheed Martin Cyber Kill Chain（洛克希德-马丁公司提出的网络攻击杀伤链），还是近年名声大噪的勒索病毒、挖矿病毒，这些攻击都有一些显著特点，一旦边界的防线被攻破或绕过，攻击者就可以在数据中心内部横向移动，而中心内部基本没有安全控制的手段可以阻止攻击。这也突出了传统安全的一个主要弱点，复杂的安全策略、巨大的资金和技术都用于了边界防护，而同样的安全级别并不存在于内部。

安全体系的建设应呈现一体化形态，各安全设备分散应用、各自为战，无法有效实现安全防护工作的进一步增值，病毒威胁一旦感染至终端，前期所做一切工作将形同虚设。

通过 EDR 的全面部署应用，提供全网终端病毒、木马、入侵攻击等威胁防御能力，通过 EDR 人工智能 SAVE 引擎、全网信誉库、云查引擎、行为分析等技术，全面应对威胁，有效防御新型未知病毒的感染与传播，解决现有信息系统安全问题，构建百分百多维度威胁防御体系。

系统主要由基础平台、核心引擎、系统功能三部分组成：

基础平台：

由主机代理、恶意文件查杀引擎、WEB 控制台三部分组成，该平台提供 EDR 系统良好运行的基础支撑，提供终端安全防护功能的基本运行环境，负责功能指令以及消息的接收、发送、执行；

核心引擎：

由人工智能 SAVE 引擎、云端威胁情报、第三方引擎所组成，用以实现病毒有效检测以及快速响应功能。

系统功能：

系统功能展现则由预防、防御、检测、响应四部分组成，通过上述四部分功能对终端赋予加固措施，有效抵御病毒木马等威胁，实现安全有效的终端防护效果。

通过对全网终端资产的全面盘点，包含业务服务器的终端和用户 PC 的终端。盘点每台终端设备的名称、IP 地址、MAC 地址、所属组织、责任人、资产编号、

资产位置等。每一台的终端上的资产信息清晰，每一个安全事件责任到人，使得安全管理能落实到位。

通过对终端安全的合规检查，对身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范等策略进行合规性审查，满足企业建设等级保护系统的主机安全要求。

2.4 上网行为管理解决方案介绍

传统的网络安全设备可以有效地阻挡来自行业外部的攻击，但对于内部原因，特别是由于员工上网行为不当引起的安全问题却无能为力。据调查，大部分金融安全问题是由于内部监控和风险管理欠缺引起的。许多公司可能认为员工是最不需要进行安全管理的一部分，但是，内部员工有意或无意的不当上网行为往往对信息安全造成更大的损害。这些行为表现为：

敏感信息泄漏

员工掌握着大量敏感数据，如果不对员工的外发信息进行严格控制与监控审计，这些重要信息可“轻易而快速”地传递到外部，造成重大损失。

安全事件频发

由于内部员工不安全的互联网访问而造成的病毒传播与黑客入侵，成为网络安全的最大黑洞。

工作效率降低

未加管理的互联网应用可能会大大降低员工的工作效率。据一项调查显示，普通企业员工每天的互联网访问活动中 40%与工作无关。人力资源在无形中浪费巨大，企业运行效率也因此大大降低。

带宽资源浪费

企业为了业务发展进行了大量的 IT 设备与带宽资源投资。而宝贵的带宽资源超过 70%被音乐、视频下载等占用，尽管带宽一扩再扩，却总是被 BT、电驴、迅雷等 P2P 应用挤占。这不仅造成带宽资源被大量浪费，还使得企业正常业务得不到应有的带宽保证。

导致法律风险

对于互联网资源的非法访问，比如访问色情、赌博、犯罪网站、发表反动言论、泄露重大机密等，都会触犯相关法律，给 XX 行业带来法律风险。

何为上网行为管理？简单地讲，就是对员工主体的基于内容的网络访问行为进行管理，包含如下几个要素：

第一、上网的人是谁（Who：哪个部门哪个员工）；

第二、上网的时间（When：工作日/周末，上班时间/午间休息/夜间，上午/下午）；

第三、上网做了什么事（How：浏览网页、下载文件、聊天、游戏、等等）；

第四、具体内容是什么（What：网页的内容、聊天的内容、邮件的内容）；

第五、占用的带宽和流量是多大（How much），等等。

与传统的安全防护方式不同，上网行为管理产品基于用户、时间、网络应用、带宽等元素对员工的上网行为进行灵活的策略设置，把网络风险管理从“被动式响应管理”提升为“主动式预警管理”，从“防范管理”提升为“控制管理”。为了实现真正安全的网络环境，企业需要“内外兼修”，除了阻挡外部攻击外，还应该转换视角，大力加强对内的管理，对员工的上网行为进行规范管理是十分必要的。

可靠的上网行为管理，可以满足以下要求：

1. 可靠高效的硬件系统和智能容错旁路技术
2. 灵活安全的设备管理方式
3. 专业级的应用识别和分类，层次清晰的结构化管理
4. 迅速准确的协议跟踪识别
5. 细致的用户组织结构管理
6. 灵活精细的带宽管理策略
7. 异常流量防护报警，保障出口线路的稳定
8. 先进的内容过滤技术，构建文明健康的企业网络
9. 外发信息控制管理
10. 强大的内置流量分析和行为统计报告

2.5 态势感知系统解决方案介绍

目前，企业中均设立网络与信息安全相关部门，并在网络中的不同位置部署了大量安全设备，但关键信息基础设施和重要数据仍然面临着各种安全风险。由

于缺乏必要的威胁感知能力，企业很难及时发现潜藏在网络中的安全威胁，对恶意行为无法实现早期快速发现，对受害目标及攻击源头无法进行精准定位，对入侵途径及攻击者背景的研判与溯源更是无从谈起。

解决方案通过构建基于全流量与沙箱检测技术的威胁监测、预警、处置响应及溯源平台，帮助企业提升对网络与系统重要出入口、高风险网络节点的监控能力，对有组织网络攻击、未知威胁、ODay、隐蔽隧道等高级安全事件的发现能力，对已失陷系统的发现与溯源处置能力，使得企业能够有效应对网络空间安全压力、实战化安全攻防压力和重大安全保障压力。

方案架构

通过部署在客户本地的软、硬件设备，能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源。本方案主要包括威胁情报、分析平台、流量传感器和文件威胁鉴定器四个模块。

在安全服务内容全面，不仅能应用企业自身新技术新业务的发展，还能够协助企业在等保等合规领域开展安全服务。

威胁情报

威胁情报来自云端的分析成果，可对 APT 攻击、新型木马、特种免杀木马进行规则化描述。

分析平台

分析平台用于存储传感器提交的流量日志和文件威胁鉴定器提交的告警日志，可对所有数据进行快速处理，并为检索提供支持，还可以与威胁情报或其他告警进行关联，帮助进一步分析，对攻击进行准确回溯定位。

流量传感器

流量传感器主要负责对网络流量的镜像文件进行采集并还原，还原后的流量日志会加密传输给分析平台。传感器通过对网络流量进行解码还原出真实流量，提取网络层、传输层和应用层的头部信息，甚至是重要负载信息，这些信息将通过加密通道传送到分析平台进行统一处理。

文件威胁鉴定器

文件威胁鉴定器主要负责对传感器还原后的文件进行沙箱检测、静态检测与动态检测等多种检测，及时发现有恶意行为的文件并告警，告警日志可传给威胁

态势感知分析平台供统一分析。

2.6 终端准入系统解决方案介绍

企业网络为大量的传统和非传统设备和其他端点服务 - 从 PC、平板电脑和智能手机到工业控制器、虚拟服务器、无线接入点和基于云的应用程序，无所不包。毫无疑问，设备相关的挑战的范围将随着 BYOD*、IoT*、混合 IT 环境和黑客复杂化而继续增大。因此，您的网络访问控制 (NAC) 解决方案必须管理您了解的公司和员工拥有的设备，以及您所不知道的数目不断增多的未授权、“未引起注意的”设备。

以下是对于全面、高度智能的 NAC 安全解决方案的需求增大的数个事实：

- 到 2020 年，投入使用的互连和联网设备数目将达到 260 亿。
- 75% 的移动应用程序将无法通过基本安全测试。
- 在 2014 年，98.7% 的威胁记录来自外部黑客行为。

可见性受限导致安全盲点。大多数端点安全系统需要每台设备上有最新的代理，以对它们进行查看和管理。IT 管理者通常对于未受管自带设备端点的存在与否以及每天在网络上数目不断增多的 IoT 设备没有可见性。但是，您必须知道尝试访问您的网络或者已经登录的设备和系统是否符合您组织的安全标准。

一旦设备访问网络，我们需要根据设备的实时可见性提供全面的 NAC 功能等。它持续扫描网络并监控未知、公司拥有的设备以及未知的设备，例如个人拥有的以及未授权端点。并且它可让您自动执行基于策略的网络访问控制、端点合规性以及移动设备安全保护。我们需要提供广泛的自动控制措施，保证用户体验不变并让业务以最大效率运转。

NAC 设备通过收集有关端点、其位置、其拥有者以及其上内容的丰富上下文深刻见解。

它可确保：

- 杜绝未经授权的设备和未获许可的应用程序进入您的网络
- 得到授权的设备配备最新的操作系统，已经安装并运行最新的防病毒软件，并且安全漏洞得到正确修补
- 加密和数据丢失预防代理正常工作
- 用户无法在网络上运行未经授权的应用程序或周边设备

如果端点不符合组织的标准，设备将会自动采取一项或多项基于策略的执行和修复措施 – 从不合规情况的电子邮件通知到必要的修复（例如软件更新）再到完全隔离或阻止访问。无需和管理访客访问、确定系统以及打开或关闭网络端口相关的人为干预或手动操作。根据策略对网络访问进行控制。

2.7 堡垒机系统解决方案介绍

堡垒机是用于解决“运维混乱”的。当公司的运维人员越来越多，当需要运维的设备越来越多，当参与运维的岗位越来越多样性，如果没有一套好的机制，就会产生运维混乱。具体而言，你很想知道“哪些人允许以哪些身份访问哪些设备”而不可得。

当前环境中，随着企业规模的不断扩大，各种安全设备和网络设备，在各类产品提供安全保障，方便我们对网络安全进行管理的时候，他们本身却可以隐藏一些安全隐患，现网中，以下问题随着规模扩大，都会成为管理者急需解决的问题。

1. 账号缺乏管理：账号管理混乱，缺乏对资源账号统一管理和统一认证。
2. 权限细粒度不够：采用粗放式的权限管理，授权工作量大，缺乏统一的授权策略。
3. 操作无法审计：系统账号管理与授权审计缺乏，用户操作无法审计。
4. 造成事故无法定位：日志记录不全面，无法实名制审计，事后无法追责。

从功能上讲，堡垒机系统综合了核心系统运维和安全审计管控两大主干功能，从技术实现上讲，它通过切断终端计算机对网络和服务器资源的直接访问，而采用协议代理的方式，接管了终端计算机对网络和服务器的访问。

在账号管理方面：包括主账号和从账号管理，主账号为用户账号，从账号为原 IT 系统帐号。通过主从账号的方式，将身份和授权分离开来，增强身份认证和系统授权的可靠性，从本质上解决帐号管理混乱问题，为认证、授权、审计提供保障。

在身份认证方面：为提高访问安全性，系统提供高强度身份认证功能，支持本地认证与第三方认证服务器对接，如 AD 域、LDAP、Radius 等，另外支持 OTP 动态令牌、短信、UsbKey、数字证书、人脸识别等多种认证方式进行双因子强认

证，保证身份可靠性。

在集中授权方面：强调的“集中”是逻辑上的集中，而不是物理上的。系统提供统一的授权界面，不但可以做到基于应用边界的粗粒度授权，例如授权用户可以访问哪些资产，还可以做到基于应用内部的细粒度授权，例如限制用户的操作行为。

在操作方面：将人员的操作记录为日志，管理人员可以在系统中查看相关的审计日志。操作审计主要审计人员的帐号管理、认证、账号分配情况、权限分配情况、账号使用（登录、资源访问、操作行为）等情况，所有操作有据可查。

通过严格的堡垒机部署，使得所有密码集中管理，公司获得对关键系统特权账号的掌控权。

确保所有系统能够执行公司密码安全策略：复杂度，定期更改，一次性密码，确保对所有系统的“合法”访问： 合适的人，合适的时间，合适的地点，做合适的事情。

确保公司对所有行为的完全的审计行为。使得企业有更高的信息系统可管理性和安全性。

2.8 日志审计解决方案介绍

完整的日志分析系统建设，涉及日志的结构规划、采集存储、过滤关联、统计分析、数据挖掘、图表报告以及管理章程等各个方面。几乎每个方面，都有着足够的技术深度和难点等待人们一一克服。常见的来说，公司的日志分散在各台服务器上，每次查找日志都要登录到各台服务器，效率低下。这些公司首先需要统一管理日志，在一个界面上查看所有日志，大大提高运维效率。公司的日志由各业务部门分别处理，导致了日志数据及分析结果的碎片化。日志是一家公司运营情况的真实数据，不同业务部门的日志往往互相关联。在公司层面统一处理、分析日志，可以把不同来源的日志对照关联分析，去除噪音，反应真实情况。

此外，黑客在入侵服务器或网络设备时，往往会删掉日志，抹除作案证据。统一上传、管理日志，可及时发现入侵行为，监控告警，也可以长期保存日志，方便事后安全审计。

现有的日志分析技术在多年的发展中，已经经过了几代的发展，涌现了各种不同的技术手段和工具。这些工具在解决一些问题的同时，也都还带有一定的局限性。

作为通用的日志分析技术平台，可以在各种不同的 IT 场景上发挥重要作用。

端到端的全链路性能监控

- 通过日志或客户端埋点数据对接方案，如开源的 count.ly 方案，进行最终用户监控(Real User Monitor)

- 通过日志或服务端埋点、JVM 探针数据对接方案，如开源的 zipkin、skywalking 方案，进行应用性能监控(Application Performance Monitor)

- 关联不同系统或模块的日志，进行端到端的服务监控和故障排查

安全信息与事件管理（Security Information and Event Management）

- 通过服务器日志发现端口扫描和非法入侵
- 防火墙、网络设备、服务器日志安全跟踪分析
- 用户及端点行为分析审计(User & Entity Behivour Analysis)

- 安全编排和自动响应(Security Orchestration, Automation & Response)

业务统计分析

- 网站用户及手机用户访问统计及留存分析
- 社交、视频、电商、游戏网站用户行为及交易路径分析
- 客户端设备、操作系统、浏览器统计

运维故障和程序 Bug 分析

- 通过日志对网络设备、服务器及应用程序状态实时监控，迅速定位问题根源
- 快速关联分析大规模分布式系统各个模块产生的大量 Debug 日志

2.9 漏洞扫描解决方案介绍

无论是从权威机构的调研结果，还是从近几年发生的重大安全事件的直观感受中，可以了解到已知安全漏洞但发现与补救不力是出现安全事故的主要原因。例如，知名咨询公司 Gartner 的专家表示说“到 2020 年，可利用的漏洞中有

99%仍是安全和 IT 专家们已知的、存在至少 1 年以上的漏洞。”，最有力佐证是 2017 年由永恒之蓝系列漏洞导致的全球大规模勒索软件事件（WannaCry）等，造成全球多国重大经济损失。

脆弱性扫描与管理系统在构建完善的信息安全防御体系中，是必不可少的基础设施系统。随着安全形势越来越严峻，并且信息化在各行各业的应用越来越深入，脆弱性扫描产品面临着多重新的挑战。

首先，随着时间推移各种安全漏洞总数也成倍数增加，修复难度和复杂度也在增加。也因此漏洞扫描器需要高扫描覆盖率、高更新频率、更有效的风险评级机制及更详细有效的修复建议等。为漏洞的扫描和修复争取时间。

其次，由于企业单位等信息化程度提高，IT 资产规模也飞速增加，对漏洞扫描与管理产品的精确度提出了更高的要求。低误报率和漏报率的产品会给企业单位节约更多成本的同时，同样的时间和人力成本投入下取得更好的安全防护效果。

另外，当系统环境变的越来越复杂时只有智能化的漏洞管理系统能带来最大的收益，包括为安全运维人员节省时间，为管理层提供决策辅助，避免任何人为带来的疏忽等等。

漏洞扫描与管理系统在构建完善的信息安全防御体系中，是必不可少的基础设施之一。信息技术（IT）是一个非常复杂和混沌的领域，充斥着各种已经半死不活的过时技术和数量更多的新系统、新软件和新协议。随着时间推移，安全漏洞数量成倍增加，对漏洞扫描与管理系统也提出了新的挑战。

一是智能化，减少人工操作干预程度；

二是高效率，更有效的风险评级机制及更详细有效的修复建议等；

三是准确性，低误报率和漏报率。

而漏洞管理有效的关键在于，

自动化：系统可以自动开启的周期性漏洞评估任务和策略、自动生成发送报告。

风险量化：系统可以基于 CVSS、真实攻击风险、病毒利用风险的自动风险量化和漏洞筛选，聚焦高危漏洞。

整合性：可以通过物理设备，虚拟机等多种部署方式，漏洞管理的一站式平台。

漏洞管理不是无休止地发起扫描并发现漏洞，更重要的是全面且准确的扫描，并对得到的数据进行智能有效的分析，确保关键的安全风险能优先处理，并满足多种合规和报告需求。一个优秀的漏扫系统，可以做到如下内容：

资产自动发现和识别

强大的漏洞扫描评估

准确的漏洞风险量化

漏洞、资产信息快速查询

完善的漏洞修补建议

合规检测模版及多样化报告

全功能、全开放 API

第 3 章 北京一实天勤科技有限公司简介

北京一实天勤科技有限公司（以下简称“一实科技”），可信的大数据安全、数据优化综合服务商，专注于为您提供基于可视架构的智慧解决方案和全生命周期的可视化服务，让一实科技创造更多价值。

一实科技以大数据分析、云计算等创新技术为基础，通过基础网络、安全合规、性能优化、混合 IT、数字化云等领域的专业技术积累，结合卓越的大数据综合服务能力，为客户提供定制化可视化解决方案与全生命周期的新 IT 服务。公司拥有多年的安全咨询、安全分析、安全测试和专业服务行业经验，在金融、电信、互联网、 制造、零售、能源等领域具备广泛的客户基础，自 2009 年成立以来公司业务始终保持高速稳定的增长。公司拥有领先的专业技术和权威的资质认证。公司总部设在中国北京，在北京、上海、广州、成都等多个城市设有分公司和办事处。一实提供的主要服务如下：

WEB 应用安全分析服务:一实科技提供的安全分析服务在系统发现和阻断的安全事件均为防火墙、IPS 等传统安全解决方案没有侦测和阻拦的网页应用攻击。在应对网页应用安全上的成效是传统安全解决方案所不能比拟的。

全网性能可视故障回溯分析服务:一实科技提供的全网性能可视化分析服务，从多种应用维度，覆盖所有端到端的应用，适用于不同场景，进行全网可视化性能分析服务。

APT 攻击检测与取证服务:一实科技提供的 APT 攻击检测与取证服务服务，从不同维度发现并阻止 APT 带来的巨大资金，声誉上的损失隐患，为企业安全治理，安全运营打下坚实的基础。

资产与漏洞风险评估管理服务:一实科技提供动态发现资产和漏洞，覆盖所有最新的安全风险。如果你不能发现、区别和验证弱点，就不可能降低风险。此项服务为信息安全风险管理提供主要分析参考。

安全系统压力测试服务:一实科技进行全面的网络性能和安全测试，能够全面了解新兴威胁和应用以及 IT 基础架构在实际运营和恶意攻击下的弹性。此项服务为安全项目管理中的质量管理提供依据。

一实科技维保高级服务: 一实科技设立服务与支持中心将在项目验收完成

后专门司职用户售后服务工作的统一接口工作。