天阵 TFP^2 威胁态势感知平台
白皮书

网址: http://www.secsmarts.com

地址:北京市海淀区西直门北大街 41 号天兆家园 3 号楼 b 单元 1902

电话: 010-62230132

传真: 010-62230132

北京同余科技有限公司

邮箱: service@secsmarts.com

邮编: 100876

■ 版权声明

■ 商标信息

版本修订：

编号	时间	修订模式	修订者	修订内容
1	20170105	新建	王占宾	全文
2	20170117	修改	王占宾	全文
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				

备注：修订模式包括新建、增加、删除、修改等

目录

一、 前言 5
二、 产品理念 6
2.1 知己知彼 6
2.2 智能安全 6
2.3 持续演进 6
三、 技术原理 7
3.1 全量日志采集 7
3.2 原始流量分析 7
3.3 载荷研判 8
3.4 威胁情报引入 8
3.5 大数据架构建模分析 8
3.6 机器学习 8
3.7 可视化 9
四、 产品价值 10
4.1 有效应急响应 10
4.2 未知威胁发现 10
4.3 完整证据链 10
4.4 安全业务定制 10
4.5 攻防可视化 11
五、 同余威胁态势感知平台 12
5.1 平台构成 12
5.2 平台架构 13
5.3 平台功能 15
六、 平台部署 17
6.1 集中部署 17
6.2 分布式部署 17
七、 公司简介 19

一、 前言

随着工业化和信息化深度融合，跨区业务量增加，生产控制区和管理信息区互联互通的信息交换量急剧增加，企业生产控制系统中的设备没有采取有力的技术和管理措施。

在特定工作中（如系统调试和维护时），通常需要本地或远程接入移动终端。而对这些接入的移动终端缺乏有效的安全监管，给企业生产带来巨大的安全风险。

随着新能源的发展和新技术的应用，“无人值班，少人值守”的远程监控管理模式快速发展，机组和远程集控中心通过网络进行数据及控制指令传输，使生产控制区受到攻击的风险大大增加。

近年来，关于 APT（Advanced Persistent Threats，高级持续性威胁）攻击的报道日益增多。APT 攻击主要目的就是窃取目标机器内的情报数据，一旦攻击获得成功，首先收集目标机器的相关信息，进一步会大量窃取目标机器的敏感数据，如果横向移动达到效果，则是窃取目标网络其他机器的敏感数据。

根据调研发现遭受攻击的受害者中几乎都是具备一定规模的企事业单位，而且都已经部署了大量的安全设备或系统。既然已经有了防御措施，为什么仍然会有部分威胁能绕过所有防护直达企业内部，对重要数据资产造成泄漏、损坏或篡改等严重损失？

经过分析主要由以下问题造成：

- 安全设备部署孤立，无法联合支撑判定准确的攻击行为。
- 业务系统日志未被使用，对攻击判断失去作用。
- 海量日志，分析处理困难，更无法进行智能的关联分析。
- 对绕过现有安全设备的威胁没有有效的检测手段。

二、 产品理念

2.1 知已知彼

在网络空间的战争中，同样需要做到知己知彼。通过大数据分析，感知内部情境为知己”，“知己”可以快速排查误报，进行异常检测，支撑事件响应活动；通过威胁情报，收集外部威胁情报为“知彼”，“知彼”可以应用这些数据来发现未知的恶意活动，以便定位到具体的攻击者。

2.2 智能安全

自适应安全，随着攻击技术、攻击手段的发展，防护手段如果一成不变那么就意味着总会被突破。通过多种系统的日志、原始流量和载荷的综合分析，发现新的威胁，动态调整防护策略使被突破的可能降性到最低。

2.3 持续演进

随着业务信息化的的快速发展，伴随而来的安全风险也在不断增加，黑客攻击技术在进步，并且攻击手段在不断完善。如果通过单一的不断增加安全产品来来应对是不现实的，因此需要一个一劳永逸的安全解决方案显得势在必行。采用大数据分析为核心，在未来出现更多的威胁时，通过升级大数据分析模型即可实现对新型威胁的识别和防护。

三、 技术优势

3.1 全量日志采集

采集的数据源包括：镜像流量数据、日志数据、威胁情报数据。平台使用大数据采集架构，其部署和应用均较简单，有较好的容错性和扩展性。

- **镜像流量数据**

平台采用独立的流量采集设备对原始镜像流量进行预处理，该设备使用多核并行化处理手段对大流量的网络原始数据进行解析、还原、范式化、分析等工作。

- **日志数据**

平台使用成熟的事件采集设备对各业务应用系统、服务器、安全设备、中间件、终端等设备通过主动采集或被动接收的方式对日志进行采集。

- **威胁情报数据**

平台通过同步云服务器或升级包的方式对威胁情报库进行定期更新，并将威胁情报数据存储在系统内存中，供数据处理及分析时使用。

3.2 原始流量分析

采取分光器镜像网络出入口上下行数据，输入到流量采集设备上做相关分析。流量采集和分析模块使用自定义的高性能内核和驱动程序，使用独立部署模式，单台可以支持最高 40Gbps，集群部署模式可以支持高达 10Tbps 的线速流量采集。

流量分析和数据还原模块，可以在 IPv4/IPv6 网络环境下，支持 HTTP、FTP、SMTP、POP3 等主流协议的高性能分析。

流量的还原当中使用了多种技术，包括端口匹配、流量特征检测、自动连接关联和规则分析。

3.3 载荷研判

采用的分布式载荷研判方法，可以对样本进行已知威胁的检测和防护；对客户端应用中已知漏洞和未知 0day 漏洞的威胁利用进行检测，发现主流客户端应用程序的可疑威胁；利用代码的行为对代码进行检测，在没有提前预知恶意代码特征的情况下发现代码中的未知威胁。因为代码中的未知威胁是 APT 攻击的核心步骤，因此对代码中未知威胁的有效检测，是 APT 攻击发现过程的一个重要环节。

3.4 威胁情报引入

威胁情报，是面向新的威胁形式，防御思路从过去的基于漏洞为中心的方法，进化成基于威胁为中心的方法的必然结果，它和大数据安全分析、基于攻击链的纵深防御等思想正在形成新一代的防御体系的基石。

3.5 大数据架构建模分析

平台采用 Spark 框架，Spark 框架自身是一个分布式的架构，支持水平扩展，通过增加集群节点即可提高集群的并发处理能力。Spark 还具有自动容错机制，可自动处理进程、机器以及网络异常，保证事件处理流程的稳定运行。在处理数据时，由于数据不写入磁盘，均是缓存在各个节点的内存中，因此 Spark 具有延迟低，实时性强的特点，通过预先设定的 Spark 事件处理拓扑，可以快速的对事件处理流程进行搭建，可根据不同的处理要求构建相应的事件处理拓扑模型，满足业务需求。

3.6 机器学习

机器学习能够自动完成数据分析师所做的工作，甚至能做得更好。基于机器

学习的方法进行大数据建模比传统通过配置的方式更能准确的发现未知威胁。把机器学习与大量的训练数据相结合，就能击败基于特征码的传统安全分析手段。拥有的训练数据越多，用来训练机器学习后得到的模型越多，那么在威胁发现上的优势就会越明显。

3.7 可视化

通过可视化技术，将原本碎片化的威胁信息、异常行为信息等数据结构化，形成高维度的可视化方案，以便于理解。大数据的存储与实时运算能力保证了数据的实时推送，配以可以实时交互的 3D 可视化界面。

四、 产品价值

4.1 有效应急响应

将大数据技术应用到本地，建立本地大数据分析平台，使用户能将全量的网络行为日志、主机行为日志、流量日志、设备日志和应用日志进行存储，通过用户数据的行为分析出违规行为，为应急响应提供参考依据。

4.2 未知威胁发现

通过海量数据的流式计算的高效关联分析引擎，实现对所采集数据的实时关联分析，动态发现未知威胁；通过基于代码行为的检测手段发现代码样本中的恶意代码，进而实现对 APT 攻击的预警。

4.3 完整证据链

通过事件溯源分析模块，安全分析人员可以方便、快速地对攻击事件和可疑网络访问行为进行溯源分析。基于发现、取证、溯源的安全业务设计，提供全生命周期的威胁发现过程。

4.4 安全业务定制

通过规则配置、机器学习、升级大数据模型等方式实现专属场景的配置展现，发现未知威胁和违规行为。而不需要等到安全事件已经发生后，再通过购买安全设备实现安全。

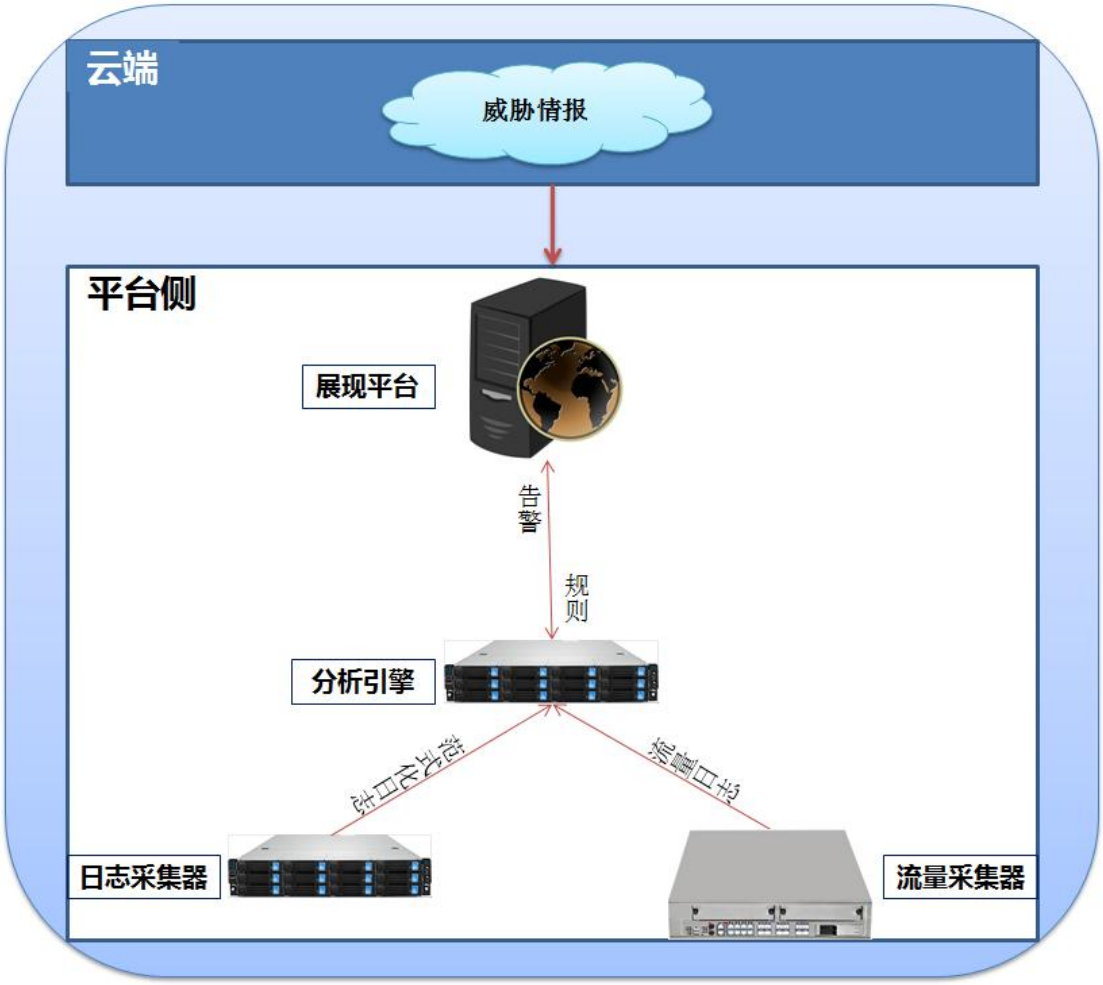
4.5 攻防可视化

通过可视化技术为用户提供基于网络威胁和相关统计的整体安全态势大屏，使得用户的业务管理和决策者能通过大屏总览其网络的威胁来源和态势，有利于帮助业务管理者迅速判断做出决策。

五、 同余威胁态势感知平台

5.1 平台构成

同余威胁态势感知平台主要包括流量采集器、日志采集器、分析引擎和展示平台四个硬件模块和云端威胁情报组成。如下图所示：



- **流量采集器**

流量采集器通常部署在网络出口交换机旁，或者其他需要监听流量的网络节点旁。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，还原后的流量日志加密传输给分析引擎。

- **日志采集器**

日志采集器主要负责对网络内各业务应用系统、安全设备、中间件、服务器、终端等设备通过主动采集或被动接收等方式对日志进行采集。解析、范式化后的

日志加密传输给分析引擎。

- **分析引擎**

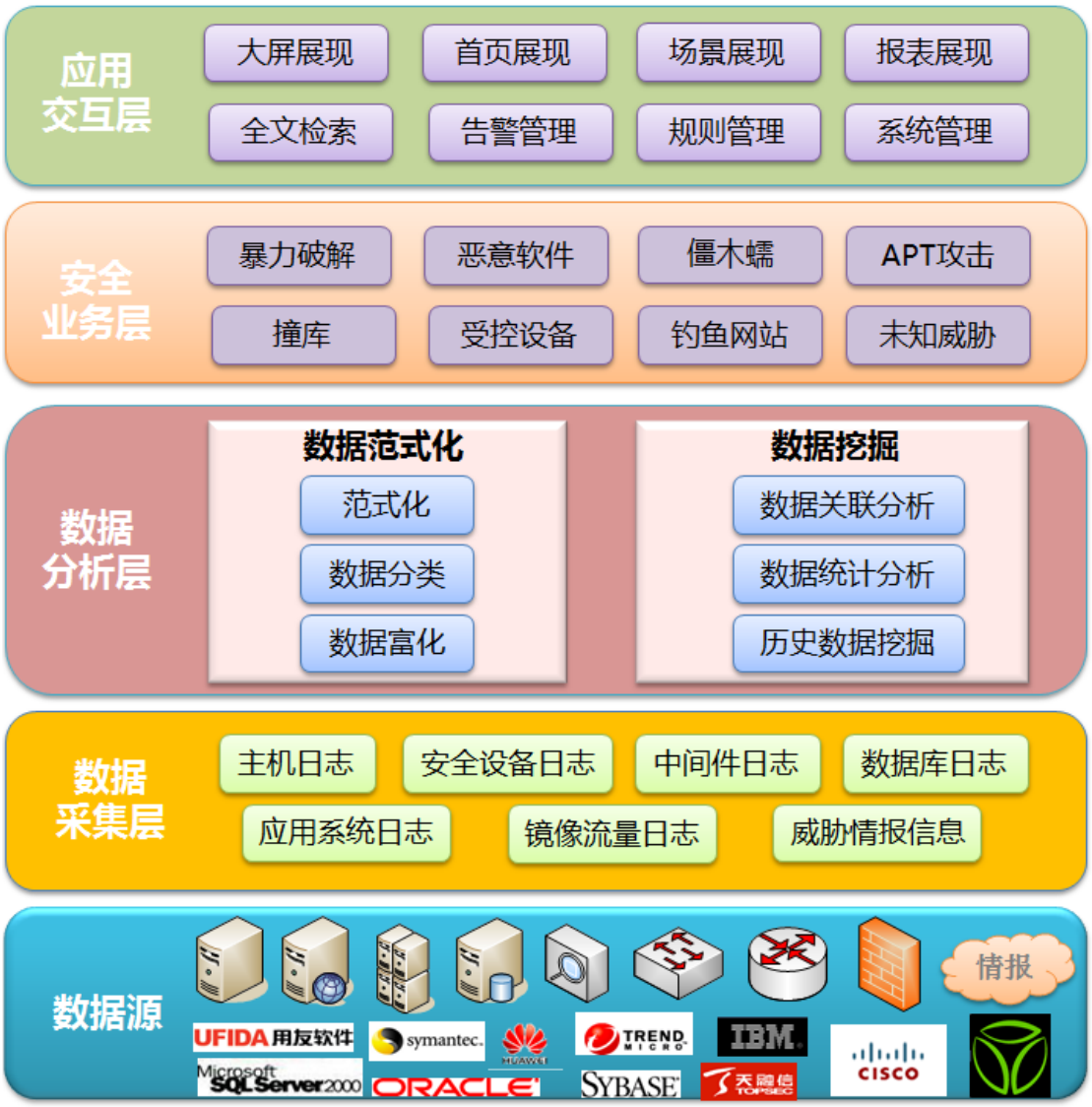
分析引擎主要负责对大量数据信息进行实时流分析，并匹配关联规则，对异常行为产生关联告警。分析引擎底层的数据检索模块采用了分布式计算和搜索引擎技术对所有数据进行处理，可通过多台设备建立集群以保证存储空间和计算能力的供应。

- **展现平台**

展现平台用于提供应用交互界面。利用可视化技术直观的对海量数据进行展现。为用户提供易于操作的数据分析功能。

5.2 平台架构

同余威胁态势感知平台功能架构分为：数据采集层、数据分析层、安全业务层、应用交互层，如下图所示：



- **数据采集层**

数据采集层由流量采集器和日志采集器两个硬件组成。其中流量采集器的主要功能是接收来自内网的镜像流量，将网络原始数据进行解析、还原。日志采集器的主要功能是对内网各业务应用系统、安全设备、中间件、服务器、终端等设备日志进行采集、解析、范式化。

- **数据分析层**

数据分析层主要是将采集到的数据进行分布式存储和索引，以便上层应用根据需求随时调用。同时本层还包括多种数据处理引擎，包括：规则引擎、数据搜索引擎、关联分析引擎、统计分析引擎、机器学习引擎等。这些引擎分别提供各种功能接口，上层应用通过接口调用这些工具引擎对采集到的数据进行关联统计分析和处理。

- **应用交互层**

应用交互层根据行为发现、证据固化、攻击回溯、深度分析、事件溯源等威胁处置的不同过程，将产品功能按照威胁处置的不同应用场景分成了大屏展示、首页展示、场景展示、报表展示、全文检索、告警管理、规则管理、系统管理等多个功能模块。

5.3 平台功能

同余威胁态势感平台主要实现以下功能：

- **大屏展现**

大屏展现分别提供攻击和病毒情况的态势监控界面：攻击态势、僵木蠕安全态势。并对攻击、病毒情况的源和目标进行统计展现。

- **首页展现**

首页展现利用系统采集的海量数据，并根据用户不同的安全分析应用场景，精心定义了四类不同维度的展现，分别为告警趋势图、重要的告警信息监控视图、内网互联聚合视图、内外网互联攻击和病毒情况视图。

- **场景展现**

场景展现通过用户自定义，通过仪表盘、列表、告警等展现方式多维度让用户最直观的看到其所关心的数据。

- **报表展现**

报表展现提供丰富的报表管理功能；根据时间、数据类型等定期自动生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为 HTML、EXCEL、文本、PDF、WORD、PNG 等多种格式，提供报表模版的导入、导出功能，用户可根据需求自定义相关报表模版进行数据的导入、导出。

- **全文检索**

全文检索的主要功能是对采集到的全量原始日志进行快速检索，可实现千亿条日志秒级检索的性能。

- **告警管理**

告警管理的主要功能是对告警信息的可视化展现，对告警产生的过程进行追踪溯源。

- **规则管理**

同余威胁态势感平台采集的数据维度较多，太多的日志和告警反而让安全管理员无从下手。通过规则管理，安全管理员可将多个不同维度的数据进行关联重定义，这样可大大减少有效告警数量，提升安全管理效率。在规则管理中，安全管理员可将潜在的威胁的判定逻辑做成关联规则，定义成告警并下发。

- **系统管理**

系统管理主要功能为用户管理、角色管理、权限管理、菜单管理、字典管理、操作审计、自身状态监控等功能。

- **威胁情报查询**

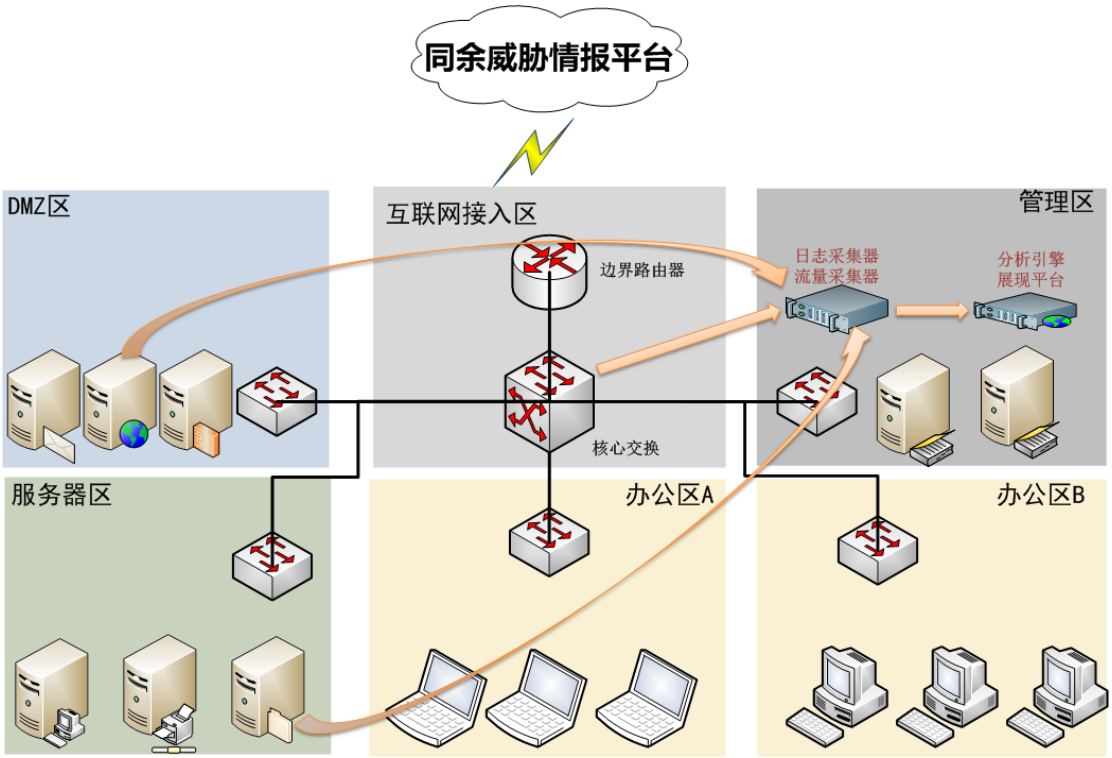
威胁情报信息通过从同余云端平台获取（在线查询、云端推送或离线拷贝）威胁情报，本地系统可自动创建分析规则，对本地网络中采集的数据进行实时比对，发现可疑的连接行为。

六、 平台部署

日志采集器对设备日志进行采集。流量采集器对核心交换机镜像流量进行采集。分析引擎通过对本地的设备日志、流量日志、本地的安全规则和云端威胁情报进行自动化关联分析，可有效发现本地威胁和异常。威胁情报采取单向推送的方式传给部署在本地的分析平台，不会造成本地数据的泄漏。展现平台可采用在线或离线模式获取威胁情报升级包。分析引擎可轻松进行水平扩展。

6.1 集中部署

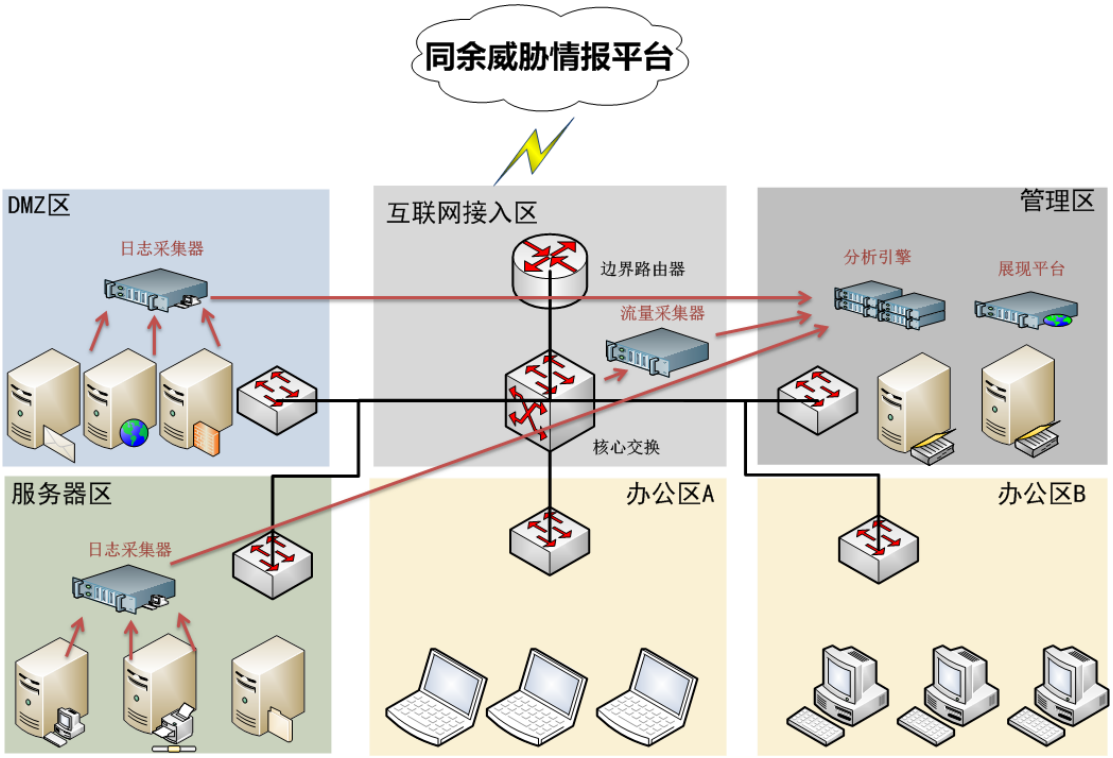
主要针对设备数量较少、设备分布集中、网络拓扑比较简单的中、小型网络。日志采集器和流量采集器部署到同一台设备，分析引擎和展现平台部署到同一台设备，两台设备组成一个独立网络，不和用户本身的网络产生交集。



6.2 分布式部署

主要针对设备数量众多、设备分布零散、网络拓扑比较复杂的大型、级联网

络。日志采集器分布式部署到各个域里面，流量采集器旁通过核心交换机的镜像端口采集进出口流量，分析引擎和展现平台部署到同一区域。分析引擎支持水平扩展。



七、 公司简介

北京同余科技有限公司（以下简称：同余科技）是一家业界领先的智能设备体系安全服务提供商。公司提供的安全体系规划咨询、攻防验证、安全建设监理、安全产品支撑和安全运营咨询等安全服务，正支撑着业界主流厂商的智慧云平台上数千万智能设备的安全运行。

同余科技核心技术源自于北京邮电大学信息安全实验室，实验室在移动 APP 和智能设备安全分析、漏洞挖掘、安全加固、密码破译，以及大数据威胁感知方面积累了大量的人才、技术、产品和服务经验。

公司核心技术团队由来自于甲骨文、启明星辰、天融信、网神和国美在线等国内外知名公司的资深工程师组成，具有丰富的网络安全、大数据分析、移动应用和嵌入式系统研究、开发和服务经验。

公司研发了智能设备安全防护组件、智能设备安全传输组件、智能设备密钥分发管理系统、智能设备体系大数据威胁感知平台和智能设备威胁情报云等一系列针对智能设备体系的安全产品，覆盖了智能设备体系数据采集、传输、存储、使用和共享的整个生命周期。

同余科技依托“信任”文化，践行“服务致信、共创未来”的使命，为实现“守望智能安全，共享智慧生活”的愿景，以专业、专注、真诚的安全服务赢得客户的信任，共同为广大民众打造安全有保障、隐私有保护、健康有依托的智能生活环境，力争成为值得社会信赖的信息安全服务企业。