杭州融至兴科技有限公司

安全威胁盾

（安全运维审计系统）

白皮书

2023 年 7 月

【公司介绍】

杭州融至兴科技有限公司，是一家专业的软件开发公司，致力于为客户提供高质量的定制化软件解决方案。本部位于杭州市西湖区，2014 年起成立南京、宁波、台州、嘉兴、金华、衢州等分公司。公司经营范围包括: 软件产品研发，系统设计服务、定制化开发、技术服务、网络安全服务、网络系统，计算机软硬件，通讯设备，计算机系统集成的设计、安装等；获得了华为、H3C、深信服、安恒、DELL EMC、IBM、宏杉、海康威视、大华、洲明、科达、华平等国内外著名厂家的鼎力支持和全力合作。

公司自成立以来，秉承开拓、进取、创新的创业精神，在完善已有成绩的同时，不断拓宽自己的市场，发展成集计算机网络技术研发、专业化系统集成服务、网络产品销售于一体，在国内计算机网络行业具有重要地位的公司。

企业资质

合作伙伴

HUAWEI　H3C　SANGFOR 深信服科技　安恒信息　DELL EMC　IBM

宏杉科技 macrosan　海康威视 HIKVISION　alhua TECHNOLOGY　Unilumin 洲明　KEDACOM　EISOO 爱数

AVCON　TE connectivity　CISCO　NSFOCUS　lenovo 联想　hp

ORACLE　亚信安全 AsiaInfo　启明星辰　JUNIPER NETWORKS　vmware　Microsoft

SUNINFO 上讯信息　CITRIX　f5　Ruijie 锐捷 Networks　COMMSCOPE　Symantec

目录

1 产品发展背景

随着网络技术的快速发展和信息化进程的日渐深入，计算机网络已成为企业高效运营的重要支撑。工作效率的提高、企业信誉的提升、利润来源的拓展都依赖于稳定、高效、安全的网络环境。但是，各种网络攻击技术也变得越来越先进、越来越普及化，企业的网络系统面临着随时被攻击的危险，经常遭受不同程度的入侵和破坏，严重干扰了企业网络的正常运行。

日益严峻的安全威胁迫使企业不得不加强对网络系统的安全防护，不断追求多层次、立体化的安全防御体系，逐步引入了防病毒、防火墙、IDS、VPN、AAA等大量异构的单点安全防御技术。然而，现有网络安全防御体系还是以孤立的单点防御为主，彼此间缺乏有效的协作，从而形成了一个个的安全“孤岛”，使得网络安全不得不面对新的挑战。

1.1 现阶段的挑战和问题分析

1） 维护使用问题

分散的安全设备管理意味着安全管理员需要登录到每个设备来进行配置、监控和维护。这样的操作方式非常繁琐和耗时，对管理员的工作效率提出了挑战。此外，不同安全设备的管理界面和操作方式可能不一致，使得管理员需要学习和掌握多个不同的管理系统。

2） 策略配置问题

分散的安全设备管理容易导致配置不一致性和安全漏洞。由于不同设备的配置是分开进行的，可能存在配置错误或遗漏的情况，进而造成安全缺陷或漏洞。这给黑客攻击提供了机会，使得整个网络系统容易受到威胁。

3） 事件分析问题

分散的管理方式使得安全事件的检测和响应变得困难。当发生安全事件时，

管理员需要手动搜索并分析多个设备的日志，这不仅费时费力，还容易错过重要的安全信息。对于快速检测和应对威胁而言，反应时间往往十分关键。

4） 风险响应问题

孤立的安全防御体系中，安全防护、安全检测、安全响应没有形成高效的闭环，各安全子系统的响应手段单一，安全部件、网络设备、用户终端和管理员之间缺乏协同与联动，导致企业网络对安全事件的响应能力低下，难以做到及时、准确的整体防御。

2 产品介绍

安全威胁盾对企业网络中的各类安全产品及多方安全威胁事件进行集中化管控。对市场上主流品牌的安全设备（防火墙态势感知、、IPS、WAF、EDR 等）的对接和事件分析。整合企业内部的设备资产、网络流量、安全漏洞、安全配置、安全日志、设备运行状态、业务故障日志、安服信息、护网综合分析日志等信息，通过智能关联分析获取企业的安全风险和态势，指导网络中的安全事件、网络监测、入侵识别，实现安全策略的统一配置、运行状况的全面监控、安全事件的实时告警、威胁信号的准确处置，同时基于诱捕防御系统指纹识别技术实现网络的脆弱性识别，帮助企业用户掌握网络的安全现状，降低运维成本，提高安全事件响应效率。

2.1 市场定位

1） 市场分析

随着网络安全的威胁来源和攻击手段不断变化，分析日益复杂的网络环境、不断增长的网络安全威胁、合规要求的增加，我们发现仅采购和部署几类安全产品无法完全保障网络长期、系统的安全，而对网络进行系统规划、构建全面的安全防护体系、制定完善的安全管理策略落实日常专业的安全管理显得尤为重要。

接下来几年，不管是企业还是个人用户都急需一类能融合所有功能、开启全

部功能后仍然保持较高性能的产品，从而有效降低用户运维管理的复杂度，多功能融合的安全产品需求日益强烈，相关产品将会加速发展。

2） 网络信息安全人才匮乏

权威数据显示，最近 3 年，我国高校学历教育培养的信息安全专业人才仅有 3 万余人，不足 70 万需求的 5%。预计到 2020 年，需求量将达到 140 万人，而现在每年培养的人数，尚不足 1.5 万人。其中一部分原因是由于薪酬和福利等吸引人才的条件不足，传统安全企业的大量人才流入国外企业或者大型互联网公司，同时顶尖安全专家日益匮乏。

2.2 目标客户群体

1） 单位缺乏专业的信息安全技术人员

安全设备通常需要专业的技术人员进行配置、安装和维护。如果客户缺乏具备相关技能和经验的工作人员，可能会导致设备无法正常投入使用。安全设备可能具有复杂的操作界面和功能设置。如果技术人员不熟悉设备的操作和功能，可能会导致无法正确使用。

2） 政策落实护网频率高

政府或相关机构应制定明确的网络安全政策目标，并将护网频率作为其中一个重要指标。那么政府在网络安全方面应当招募和培养网络安全专业人员，购买和更新网络安全设备，加强网络监测和响应能力等。需要投入足够的人力、物力和财力资源，对于小型企事业单位来说，是一笔不小的开支。

3） 各类安全设备资料零散不齐

安全设备的资料可能来自于不同的渠道，例如大型护网行动、定期安全服务、日常维护操作等场景，会生成不同类型的安全分析报告和解决建议梳理。这些资料往往以不同的形式存在，可能存在于多个不同类型的安全设备源头，导致资料的分散存储和管理困难。

3 产品属性

3.1 产品迭代

迭代版本	版本说明
迭代 1.0（目前）	全面将安全设备使用起来，数据统一输出、异常统一处置、行为统一记录；

4 产品体系架构

4.1 系统架构图

4.2 技术原理

1） 统一数据模型与接口：

在各个系统在数据结构和接口设计上进行适配，通过定义统一的数据模型和接口规范，使不同系统之间能够进行数据交换和共享。

2） 集成技术和中间件：

使用集成技术和中间件提供数据转换、消息传递、事务处理等功能，实现不同系统之间的连接和数据传输，使各个系统能够进行有效的通信和协同工作。

3） 服务导向架构：

采用服务导向架构，通过标准化的接口进行调用和组合，将各个系统和应用程序拆分为可重用的服，实现跨系统的业务流程集成和功能共享。

4） 中央控制和管理：

建设中央控制和管理模块，以提供统一的权限管理、数据监控、错误处理等功能，用于监控和管理各个系统的运行状态和数据交互，确保各个系统的正常运行和数据的安全性。

5 产品功能

5.1 多元交互

5.1.1 多品牌汇集

不同品牌的安全设备可能具有各自独特的功能和特点，将来自不同厂商或品牌的安全设备，通过专业的集成手段连接起来进行整合和协作，使得不同品牌的安全设备可以共享信息、协同执行任务，提供更强大、全面的安全保护，共同应对威胁和安全事件，以提高整体的安全防护能力。

5.1.2 多类型涵盖

不同类型的安全设备可能专注于不同领域或层面的安全防护，将来自不同类别或种类的安全设备进行集成和协同工作。通过整合这些不同类型的安全设备，以提供综合性、全面性的安全解决方案，可以构建一个综合性的安全生态系统，以更好地应对多样化的威胁和风险。

1）网络安全设备

防火墙、入侵检测与防御系统（IDS/IPS）、虚拟专用网络（VPN）、态势感知等，用于保护网络资源和数据的安全。

2）物理安全设备

视频监控系统、门禁系统、安全闸机等，用于保护物理空间和设施的安全。

3）终端安全设备

防病毒软件、终端加密、数据备份与恢复、终端安全管理等，用于保护终端设备和数据的安全。

4）应用安全设备

Web 应用防火墙（WAF）、应用程序审计工具、漏洞扫描工具、诱捕防御系统等，用于保护应用程序的安全。

5）数据安全设备

数据加密设备、数据遗失防护（DLP）系统、数据库防水坝、数据库防火墙等，用于保护数据的机密性和完整性。

5.1.3 多数据整合

对于有全局统一模式的安全威胁盾平台，通过数据整合方式访问组织外安全设备的事件分析信息，通过建立局部分析模式、全局分析模式，可以访问集成系统中的其他安全数据信息；对于集合式安全系统，可以通过定义策略、定义数据分析模式，进行各集合式系统之间的威胁访问。

1）威胁情报数据：

来自公共情报平台、专业安全团队或第三方供应商的威胁情报，包括恶意软件样本、IP 地址黑名单、漏洞信息等。

2）行为分析数据：

通过对网络和终端设备上的行为进行分析，提取异常活动、潜在威胁、网络流量、终端行为、威胁情报等，进行全面的安全分析和威胁检测。

3）安全事件响应数据：

包括安全事件的响应记录、处置过程中产生的数据，以及跟踪调查过程中的相关信息。

5.1.4 多层次堆叠

通过不同层次的安全防护，提供多重防线和综合保护，以增强网络的安全性和防御能力。在系统内合理地配置和整合多元化的安全设备，并综合使用安全策略、安全事件管理和持续监测，可以有效地减少潜在的安全威胁和风险，从而帮助组织更好地应对安全威胁和风险。

1） 边界安全设备层：位于网络边界处，保护内部网络与外部网络之间的通信。

- 防火墙：监控和过滤进出网络的数据流量，实施访问控制和流量策略。
- 入侵防御系统：检测和阻止网络入侵行为，如恶意流量、攻击、漏洞利用等。
- 传输层安全协议加密设备：提供加密和认证功能，保护网络通信的机密性和完整性。

2) 网络安全监测与分析层：用于实时监测网络流量、检测异常行为和威胁，并进行网络安全事件分析。
   - 入侵检测系统：监测网络中的异常流量和攻击行为，并生成警报。
   - 安全信息与事件管理系统：收集和分析来自各种安全设备的日志和事件，并提供综合的安全事件管理和报告功能。
   - 威胁情报平台：整合和分析来自内部和外部的威胁情报，以获得关于已知和未知威胁的实时情报。
3) 终端安全层：保护终端设备免受恶意软件、数据泄露和其他威胁的攻击。主要包括以下设备和措施：
   - 终端防病毒软件和安全补丁：提供实时防病毒和恶意软件检测，并及时应用安全补丁来修复漏洞。
   - 终端加密和数据保护：使用全盘加密、数据分类和访问控制等措施，保护终端设备上的敏感数据。
   - 移动设备管理（Mobile Device Management, MDM）：对移动设备进行集中管理和安全策略强制执行，保护企业数据的安全性。
4) 应用安全层：保护特定应用或服务免受攻击和漏洞利用。
   - Web 应用防火墙（Web Application Firewall, WAF）：针对 Web 应用的攻击进行检测和防护，保护 Web 应用免受漏洞利用。
   - 访问控制和身份认证：强化对应用和服务的访问控制，采用多因素身份认证等措施，确保合法用户的身份和权限。

5.2 风险威胁

5.2.1 网络威胁

通过各种基于统计和规则的关联分析算法，结合安全事件产生的网络环境、资产重要程度、系统漏洞级别，对安全事件进行深度分析，可以有效提高安全事件的响应力，减少告警日志数量而不丢失重要信息，为安全事件审计和风险响应提供更准确的决策支持。

- 网络入侵
- 病毒和恶意软件
- 垃圾邮件
- 弱口令
- 数据泄露类型
- 无线网络攻击

5.2.2 攻击事件威胁

收集和分析来自内部和外部的威胁情报，对网络、系统或应用程序遭受的安全攻击进行深入分析和研究。针对已识别的安全事件，进行风险评估和威胁分析，更好地了解当前的威胁趋势和攻击方法，以及采取相应的防御措施。

- 攻击技术
- 攻击水平
- 攻击手段
- 攻击目的
- 威胁严重性
- 潜在影响

5.2.3 漏洞威胁

采集漏洞扫描系统内通过对系统、应用程序或网络中存在的漏洞进行扫描的出来的报告数据，进行深入研究和分析，及时发现和识别系统中的安全弱点，并采取适当的措施加以修复。提高企业网络环境的安全性和抵御潜在的攻击威胁。

- 收集漏洞脆弱性态势分析
- 收集安全设备的高、中、低危漏洞的数量
- 收集/识别漏洞级别的分布
- 资产配置核查中发现的弱点分析

5.2.4 故障威胁

构建了开放的、检测和响应等不同生命周期的各个安全环节进行基于策略的

管理，将各种异构的安全产品、网络设备、用户终端和管理员有机的连接起来，构成了一个智能的、联动的闭环响应体系，网络环境种的安全设备出现异常情况时，能够迅速察觉、准确定位，可持续演进的网络安全管理平台，有效应对现有的安全威胁，保障企业基础业务的正常运作。

- 设备无法启动或无法正常运行
- 失去连接或网络中断
- 错误或警报消息
- 数据丢失或损坏
- 更新或升级失败

5.3 安全事件响应

5.3.1 威胁感知响应

解决安全服务局限性。系统配备了数十种安全服务相关脚本内容，由我司专业安全技术团队一手打造的安全服务服务项脚本库，打造智能、全面、灵活的安全服务自动化模式，帮助企业找到资产面临的威胁，全面预判识别安全事件风险，提出有针对性的抵御威胁的防护对策和加固整改措施。

- 渗透测试、漏洞扫描
- 风险识别、风险评估
- 安全排查、安全加固
- 安全监测、安全测试、安全规划设计
- 自定义/新增脚本内容

5.3.2 安全盾牌响应

与各类防火墙做对接，实现对防火墙的智能联动，平台集成了各种安全设备和日志源的综合安全管理平台，实现对防火墙日志和事件的集中管理、监控和分析。通过配置协议实现对防火墙的远程管理和监控。同时基于用户网络安全考虑，使用加密技术对防火墙的连接进行身份验证和授权，以确保只有合法的用户能够访问和操作防火墙。

5.3.3 漏洞失活

监管单位定期进行漏洞扫描，扫出漏洞进行通报并要求限期修复。通过一系列的专业措施和技术，对系统或应用程序中的漏洞做封禁处理，用户可以自定义配置需要保护的漏洞信息。本系统一旦检测到有攻击流量针对“被保护的目标漏洞”时，会向交换机发送阻断报文，中断相应漏洞攻击链接，而不影响其他正常的通讯，从而阻止攻击者利用这些漏洞进行恶意活动。漏洞失活的目标是减少系统或应用程序的攻击面，提高其安全性。

5.3.4 事件处理流程

单位能够事先在系统内建立自动式工单流程管理，当系统捕捉到设备或软件发生异常或超出预警指标时会触发相关的事件，同时触发相关工单处理流程，单位管理员能够自定义安全运维人员，并进行及时维护处理。异常工单维护完成后，可以由运维人员确定目标工单的异常内容、处理说明、处理情况等，形成附件上传至系统工单存档空间内，形成闭环响应链路，便于运维人员后期对设备维护和管理，以提高运维响应的效率。

5.4 丰富报表

5.4.1 操作审计

平台配备日志审计工具、程序，启用详细的日志记录功能，确保将所需的操作事件记录到日志文件中。对日志进行实时监控和分析，支持设定关键事件的报警规则，以及异常活动的检测和报警机制，实现快速识别潜在的安全问题或违规行为。为了确保审计日志的可靠性和完整性，采取加密技术对日志进行加密，保证日志的完整性，防止对日志文件的篡改或删除。

5.4.2 安全事件评估

1) 提供关于安全评估的目的、范围和背景的简要说明，描述评估的系统或应用程序的基本情况和重要性。

2) 描述安全评估的方法和技术，包括使用的工具、测试方法、采集的数据等，使管理者了解评估的可靠性和有效性。
3) 报告总结评估发现的主要结果和发现的风险，明确列出发现的漏洞、弱点和存在的威胁。
4) 对每个发现的漏洞或弱点进行详细分析，并评估其对系统安全的风险程度。描述漏洞的影响、可能的利用方式以及潜在的风险后果。

5.4.3 异常分析

收集与异常事件相关的日志、报警记录和其他相关信息。整理这些信息，并确保记录涵盖事件发生的时间、地点、受影响系统或服务。基于分析结果提出必要的修复措施和恢复计划，以避免类似事件再次发生。编写详细报告，对异常事件的分析过程、结果和建议进行总结，支持后期实现发生调取溯源记录。

5.4.4 护网报告

生成关于网络安全保护工作的综合性文档，总结和记录网络安全保护的情况、发现的问题以及提供改进和加固措施的建议。

1) 对报告的目的、范围和背景进行简要介绍，说明对网络进行了哪些方面的保护和评估。
2) 列出进行的漏洞扫描和弱点评估的结果，包括发现的漏洞、弱点和存在的风险等级。对每个漏洞进行详细描述，包括其影响范围和可能的攻击方式。
3) 总结安全事件和攻击活动的情况，包括入侵日志、异常报警和监测结果。分析攻击类型、目标和影响范围，以及响应措施和恢复过程。
4) 提供针对网络和系统的最新威胁情报，包括常见的攻击方式、新型威胁和相关漏洞等。进行风险评估，确定事件对业务的潜在损害程度。
5) 对整体网络安全保护情况进行总结，并强调需要重点关注的问题和改进方向。提供关于未来改进措施和网络安全发展方向的建议。

5.4.5 安服报告

由我司安全服务团队专业技术人员配合执行脚本后，向客户提供的一份文件，

旨在总结和记录所提供的安全服务的情况、成果和建议。详细描述在安全服务期间发生的安全事件和威胁活动的情况。提供最新的威胁情报和安全趋势分析，包括常见攻击类型、新型威胁和漏洞信息等。帮助客户了解当前的安全态势并采取相应的防护措施。对提供的安全服务进行总结，并强调需要重点关注的问题和改进方向。

5.5 云维护

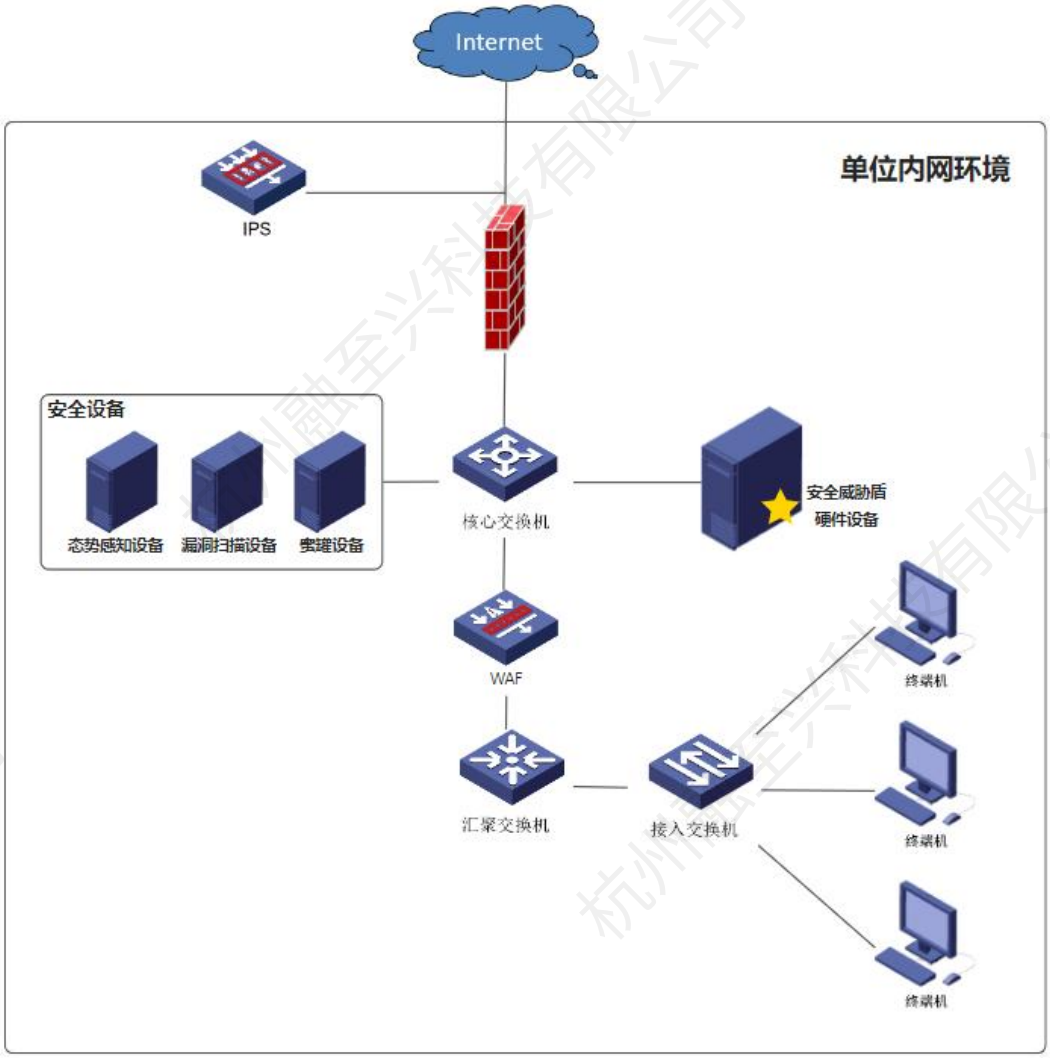
解决现场维护的弊端。多方数据对接，支持 5G、4G、WiFi、VPN、有线以太网等各种联网接入方式，支持网口、串口设备远程维护，无需配备服务器。工程师可随时随地远程到现场设备、一键式快速维护，提高工作效率。现场设备的远程运营管理和通过大数据分析，为客户提供各种便捷高效服务，推动企业提升创新能力，提高研发水平，开拓市场。

6 产品后台

6.1 运行环境

序号	设施	环境参数
1	虚拟机	Linux 操作系统； CPU：8 核；内存：24G 或以上；存储：500G 以上；
2	服务器	Linux 操作系统； CPU：10 核；内存：64G；存储：10T

6.2 部署方式



7 产品价值

1） 改善生产力

安全人员可以在一个平台上查看整个网络和系统的安全状态，全面了解安全事件的发展趋势、相关性和影响程度。减轻技术人员重复查看安全设备的工作量，节省人员时间。

2） 降低企业成本

将安全服务和安全设备的日常数据维护工作分担给安全威胁盾平台，从而降低人员技术能力低下导致的内部运营成本和风险，减少护网/安全服务费用、降低风险和损失等。

3） 提高响应时效

及时发现入侵行为、异常活动和其他安全事件，帮助运维人员快速定位问题、采取行动并恢复业务正常运行，从而减少潜在的安全风险和损失。

4） 数据准确可靠

消除由数据孤岛和信息孤岛所带来的种种问题。构建一个全面、综合的安全解决方案，以高度准确性和可靠性执行任务，减少了人为错误和数据不一致的风险。提高工作质量和精度，减少错误带来的损失。

5） 降低技术人员门槛

平台一键管理和分析，减少复杂性和繁琐的操作步骤，优化工作流程，降低对员工技术的依赖程度。通过简化工作流程，使得任务更容易理解和完成，降低对员工技术水平的要求，降低护网行为、护网人员的技术门槛。