联软科技
LEAGSOFT

UniEDR终端检测与响应系统

一体化终端威胁检测与响应平台，助力企业完善端点安全保护

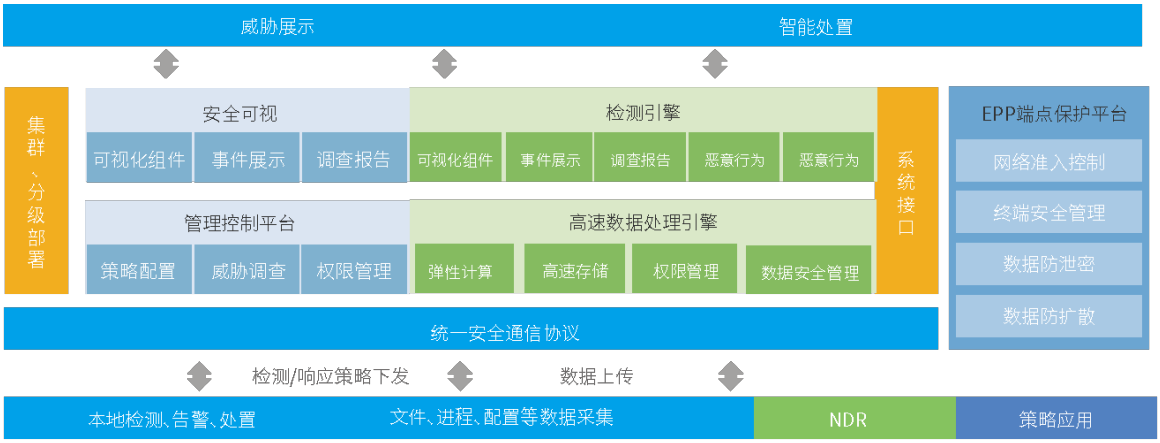
深圳市联软科技股份有限公司

UniEDR终端检测与响应系统

产品概述 Product overview

联软UniEDR终端检测与响应系统（简称：UniEDR）是联软科技基于Gartner提出EDR概念结合CARTA“持续自适应风险与信任”安全模型开发的，用于解决终端高级威胁攻击、威胁攻击溯源及协助企业持续化改进的终端安全管控平台。产品可通过现有联软EPP管控平台进行扩展，在统一管理平台统一客户端的基础上，实现安全能力互补，通过UniEDR系统发现威胁、分析威胁、处置威胁，联软EPP平台通过威胁追溯分析结果改进终端安全管理配置，使企业内部终端安全持续完善。

产品方案 Solutions



产品适用场景 Application scenarios

1、攻防演练中的攻击检测与快速响应

提供快速的检测定位与响应阻断能力。发现内网中爆破、提权等常见攻击工具，可以发现凭据获取、权限维持和提升、防御绕过、内网信息收集、隐藏命令控制通信等高级攻击手法，可以对内网横移手段中常用的域控攻击、漏洞利用、远程服务爆破等方式进行检测。可以对失陷终端进行快速隔离，同时将失陷情报上报后同步至机构所有关联终端，第一时间做到全网响应。

2、APT攻击的检测与溯源

能够从终端上抓取APT攻击检测所需的多种行为数据，包括进程注入、Playload反射加载、进程挖空等APT相关的高阶行为事件；此外依托威胁情报能力，可以主动将APT组织在其他同类目标的攻击线索、攻击手法、攻击技巧等转为检测脚本，实现反客为主式的检测与溯源。

3、高危安全事件的终端定位与分析

可以快速通过终端行为定位到威胁的进程源头，进而通过终端间的网络访问关系确定其关联影响的其他终端。安全管理者可据此快速下发响应策略，如隔离或修复。

4、安全产品联动

可提供丰富的端点数据采集信息供综合威胁检测平台分析和调查，溯源威胁主体的传播途径和攻击手段，对该威胁所造成的影响进行评估，确认影响终端范围，并针对性完善系统加固体系和应对措施。

产品功能 Functions

行为采集

- 对系统配置、启动项、系统日志、软硬件、补丁安装等系统静态数据，以及系统运行的日志、驱动变更信息、进程信息（进程创建、进程访问、进程篡改）、网络连接、文件读写、注册表读写、PowerShell&CMD命令、DNS请求、WMI、证书、LDAP请求、Pipe管道等数据进行全面采集。

威胁检测

- 基于专家级行为基线分析模型检测产生攻击告警；
- 通过MIRTRE ATT&CKTM攻击者战术知识库映射比对，定位与展示攻击阶段；
- 基于威胁情报库碰撞，快速发现威胁线索。

安全事件

- 对威胁行为特征进行综合判定，产生安全事件和告警信息；
- 自动化分类安全告警信息，结合多种方式快速通知告警；
- 安全事件关联攻击日志和原始日志，展示攻击链详情，清晰展示攻击事件关联，快速溯源分析。

威胁调查

- 支持多条件组合查询，多维度数据聚合，关键信息可便签标记，便签内容高亮展示；
- 进程事件树方式展示进程关系及相关详细进程行为信息；支持图关系查询，实时展示关联调查步骤关系；
- 调查对象、关联数据支持以时间流方式抽取记录，进行查询回溯，自主生成调查取证报告。

威胁处置

- 支持网络隔离、阻断，设备关机，进程权限限制、隔离，文件隔离、删除等多方位处置手段；
- 支持与UniNAC网络准入控制、UniAccess终端安全管理等多种安全管控平台深度结合联动。

产品特点 Features

- 提升终端安全管理的可见性，有效发现未知威胁。
- 能够基于统一的威胁检测框架，对威胁防御工作进行评估量化，自动对威胁进行识别，并通知安全人员。
- 威胁调查工具可对已识别的威胁进行研究并搜寻潜在的可疑活动。
- 通过有效、及时的处置手段，对威胁进行遏制、删除，保护企业资产。

方案优势 Advantages

全面精准的数据采集

- 数据采集针对不同类型信息针对性分类处理，性能占用低、数据采集全面，PE文件信息、底层硬件信息、文档内容等信息都可完整采集，数据关联信息以图的方式进行存储，方便查询。

快速的威胁检测

- 以MITER ATT＆CK™为基础，系统化对威胁检测策略规划，相比传统依赖已知案例专家规则，能够更全面地对威胁进行防御，发现未知潜在威胁；
- 独创的高速数据存储、处理引擎和图计算模型，大幅提升计算速度，有效提升威胁调查的速度，更快发现威胁。

更高ROI

- 整体性架构平台，同一Agent集成准入控制、桌管、防泄露功能，根据企业需求与业务发展快速无缝扩展；
- 1500万+Agent部署数量，良好的兼容性，系统资源占用更少，大幅节省终端硬件投入，提升员工使用体验；
- 与联软UniNID、UniCWPP（服务器侧的威胁检测）无缝联动，所有产品基于同一个威胁检测模型实现高效检测和更加全面的威胁处置。

HONORS AND QUALIFICATIONS

产品资质与荣誉

部分典型客户 Some Typical Customers

招联 | 财信金控 | WeBank 微众银行 | 南方基金 CHINA SOUTHERN FUND | ARN环新集团 | ZTE中兴

马上消费 | 大丰 | 东风 HONDA | DAIKIN（苏州） | 招商信诺资产管理有限公司 | 康正生物

张家口市人民政府 | 马鞍山市数据资源管理局（政务网络管理局） | 鹏龙汽车有限公司 | 中国移动（陕西） | 淮北市数据资源管理局 淮北市政务服务管理局 |

安徽省数据资源管理局 | 高邑县发展和改革局 | 东莞市政务服务数据管理局 | 东莞市城市管理和综合执法局 | 吴川市政务服务数据管理局 | 内蒙古自治区兴安盟行政公署

大金(中国)投资有限公司深圳研发分公司 | 陆家嘴信托 | FUHUA | 宜格美妆集团 | 上海市杨浦区中心医院 | Lontium

河北中烟工业有限责任公司 | 中广有线（温州） | 广州地铁 Guangzhou Metro

联软科技
LEAGSOFT

服务热线:400-6288-116
地　址:深圳市南山区粤海街道科兴科学园A2栋9层
邮　编:518057
电　话:0755-86219298
传　真:0755-86148550
网　址:https://www.leagsoft.com

获取专家支持

知晓最新资讯