未来智安
XDR SEC

NDR 网络威胁检测响应系统

产品技术白皮书

北京未来智安科技有限公司

2022.6

目 录

1. 引言

1.1 安全趋势

当前全球网络安全形势严峻，网络安全面临着各种新的挑战，网络攻击层出不穷，且攻击来源、攻击目的、攻击方法以及攻击规模都在发生着巨大的变化。与此同时，伴随我国信息化发展进入新阶段，云计算、大数据、物联网、移动办公等新技术新应用已经日趋成熟，并开始大规模应用，而新技术是一把双刃剑，在促进信息化发展的同时也带来新的安全风险，原有安全防护体系的适应性和防护能力已经不能解决信息安全工作面临的新风险新问题。

为应对网络安全面临的全新形势和挑战，我国网络安全制度体系建设和组织机制建设也进入了快车道，2016 年 11 月 7 日，《中华人民共和国网络安全法》发布，并于 2017 年 6 月 1 日起正式施行，这是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，网络安全法进一步明确了信息化发展与网络安全并重的原则，指出“国家实行网络安全等级保护制度”，“对关键信息基础设施在网络安全等级保护制度的基础上，实行重点保护”，并“保证安全技术措施同步规划、同步建设、同步使用”。

随着《网络安全法》的发布施行，国家网络安全保障制度和标准体系也在快速制定和完善中，2018 年 6 月，由公安部牵头制定的《网络安全等级保护条例》发布征求意见稿，2019 年 5 月 13 日，新 2.0 版本《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)及扩展要求正式发布，与此同时针对关键信息基础设施的相关制度和标准也在加紧制定中，由此可见国家对国产化进程的推进力度及网络信息安全发展的决心。

1.2 项目背景

随着网络信息化发展的不断应用和普及，网络应用向多层次、立体化、空间化方向发展，网络空间信息的安全问题越来越突出，给数字化的安全管理带来很大挑战。网络空间安全通常被认为是计算机网络上的信息安全，是指网络系统的硬件如骨干网设备、线路、辅助设备等）、软件（如操作系统、应用系统、用户系统等），及其系统中运行的数据、提供的应用服务不因偶然的、恶意的原因而遭到破坏、篡改、泄露和失控。

首先，对网络信息系统而言，当 DDos 攻击、身份伪造、主动入侵、漏洞利用、勒索病毒、未知威胁、非法接入、违规操作、信息泄密、存储介质随意使用，以及国外势力电子信息战等越来越严重的影响到单位利益和国家利益的时候，网络空间安全 (Cyberspace Security) 也继国防安全、政治安全、经济安全、金融安全之后成为了国家安全体系中的一项重要内容，受到包括美国、欧洲和中国政府的高度关注。

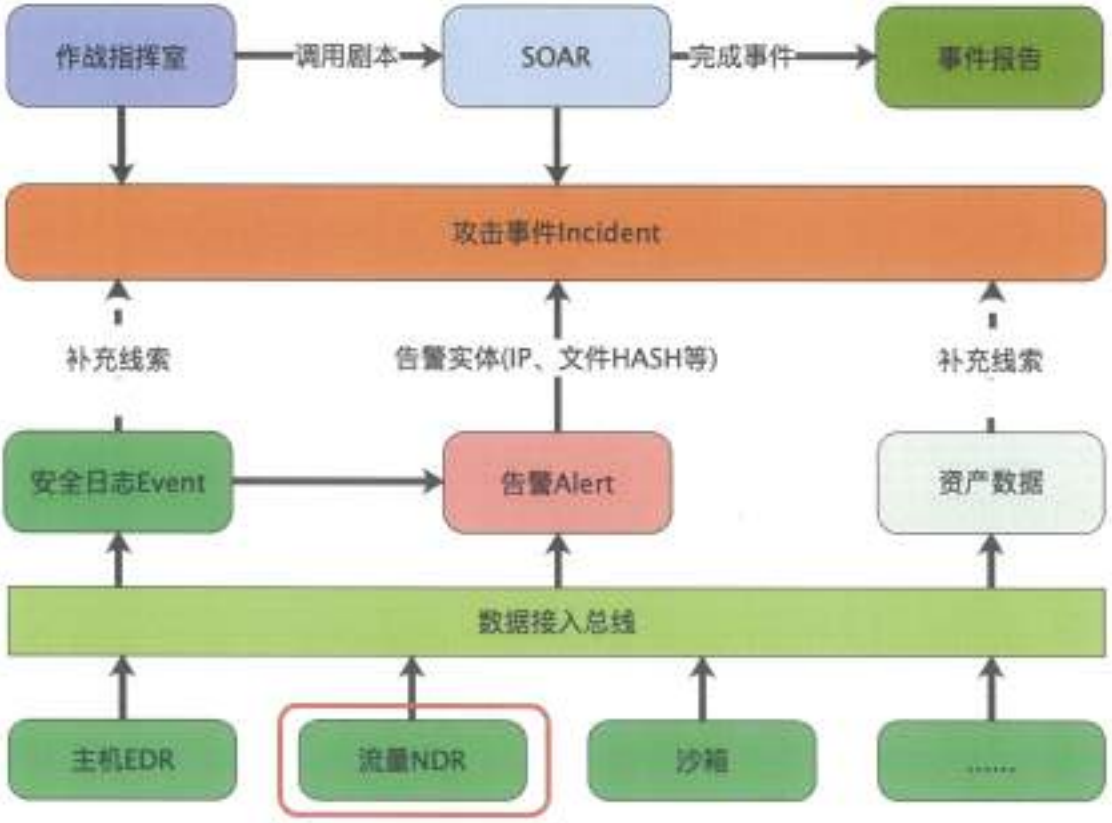
其次，在国家行业信息化推进的大环境下，行业专网的运营安全在国民经济建设中日益显得举足轻重。特别是在政府机关网络中，工作秘密的泄露会使政府机关工作遭受损失，带来不必要的被动；而国家秘密的泄露会使国家的安全和利益遭到严重损害，而泄密者受到降职、降衔的严肃处理，甚至移交司法机关处理。

综上，如何应对上述安全问题，减少直至杜绝内部各种各样安全威胁，实现单位内建设面向网络空间的、安全和谐网络环境，则成为了安全工作的重中之重。

2. 产品介绍

未来智安NDR网络威胁检测与响应系统(以下简称"NDR") 通过部署在系统中的核心网络节点上，采用侦听网络数据包的方法将网络流量捕获并进行协议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及流量中重要的负载信息。支持常 IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN 的数据包解码；支持 HTTP, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, Modbus, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP 等几十种协议解析还原能力。支持 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为、IM 通信等行为描述。

未来智安 NDR 通过结合自研或第三方的 EDR、SOAR、作战指挥室、SIEM、SOC、XDR 等网络安全产品，为用户提供全方位立体化的威胁检测与响应能力。如下图所示：



2.1. 产品设计目标

2.1.1. 解决网络攻击分析溯源难问题

“猫捉老鼠”常被用来形容网络攻防中攻防二端的动态博弈，攻击者不断变化攻击手法、攻击载体，防守端需耗费大量的精力来抵御攻击,据研究资料表明攻击者在真正暴露前的潜伏平均时间长达 146 天，在这段时间内，驻留在网络上的攻击者可能已经秘密地窃取和泄露机密等重要信息，或者对客户数据资产进行破坏，当前大部分的网络安全产品在应对安全事件的检测分析及溯源层面基本围绕安全设备的告警日志，且大部分告警数据缺乏上下文关联关系，基本都是围绕单一产品视角进行数据关联，如主机侧安全产品围绕自身数据进行分析

溯源、网络侧安全产品同样围绕自身流量侧进行分析溯源，不同安全产品间存在的分析检测和溯源的盲点。

2.1.2. 解决网络攻击事件处置效率低问题

在网络安全形势日趋严峻当下,特别是攻击进入实战化阶段，攻击方式层现有组织有体系的特点，能够在第一时间完成响应处置对网络攻击防御显得尤为重要。目前市面上大部分的网络安全产品都依靠人工进行告警分析、调查、核实并利用其它安全设备进行响应如防火墙断网等等操作，需要在不同安全设备间来回跳转、切换，极大的增加操作的复杂度和操作时间长，不及时处置等原因造成更大的安全后果，另外目前的安全状态是安全产品单点多，步骤多、方式多、全局监控和实时性要求高，缺乏行之有效的防御和检测及响应处置能力，

2.1.3. 解决资产清晰度差问题

网络安全本质是信息安全，从一个侧面看信息安全就是风险管理，风险管理最核心是资产、威胁和脆弱性这三要素，这三要素都是以资产管理为基础。目前，资产的管理的粒度太粗，无法进行有效的资产统计和感知，有哪些资产，未来智安 NDR 支持从流量数据包中自动识别资产信息，具备新增资产及资产统计分析能力，包括资产总数、今日添加资产数、服务器资产数、终端资产数;支持资产分类占比、

资产来源占比、资产分组占比、操作系统占比、操作系统发布、资产标签占比等可视化呈现能力。

2.2. 产品价值

2.2.1. 针对流量数据的有效治理

未来智安 NDR 数据治理模块支持异构数据的接入，支持利用统一数据接入总线完成数据源管理、数据字典、数据结构及接入策略定义，支持多元异构数据的统一展示、分析、检索及利用治理后的数据进行攻击检测、告警及攻击事件的关联分析。

2.2.2. 针对告警多,误报多的有效治理

未来智安 NDR 告警治理引擎从核实告警、降告警、提升告警质量、降低告警误报率出发利用资产关联、不同安全设备间的数据进行告警的数据互补、互纠完成告警核实、告警 Alert 到攻击事件 Incident 的提升，降低告警的数量。同时利用 SOAR 技术针对不同类型的威胁告警进行告警的自动化分析核实及告警的归并，从而有效的降低告警量、降低告警的误报率。

2.2.3. 针对网络攻击分析溯源能力的提升

针对网络攻击分析溯源难问题，未来智安 NDR 基于自研的告警治理引擎，利用流量侧 NDR 及相关资产数据围绕攻击链完成攻击事件回溯。基于攻击事件 Incident 出发进行攻击事件的调查分析，攻击事件 Incident 提供了多纬度的攻击线索，可围绕攻击线索进行攻击行为上下文分析、进程链分析等操作大大提高了攻击溯源效率和溯源难的问题。

2.2.4. 针对网络攻击事件的处置效率提升

未来智安 NDR 针对网络攻击处置效率低问题，除了利用告警治理引擎实现告警的核实、降低告警的误报之外，还提供了基于 SOAR 的安排编排与自动化响应处置能力，可利用 SOAR 完成不同攻击类型、不同攻击场景的告警及攻击事件的应急预案，通过任务编排的方式以自动化或半自动化的运行，提高攻击事件的处置效率。

2.3. 产品组成与架构

2.3.1. NDR

未来智安 NDR 网络威胁检测及响应组件通过部署在系统中的核心网络节点上，采用侦听网络数据包的方法将网络流量捕获同时对网

络流量进行协议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及流量中重要的负载信息。

支持常见数据包解码包括 IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ, MPLS, ERSPAN, VXLAN；支持常见应用层协议解码包括 HTTP, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, Modbus, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP 等几十种协议解析还原能力。

支持 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为、IM 通信等行为描述；

网络流量采集模块可以支持 IPv4/IPV6，同时提供 IPv4 网络和 IPv6网网络的监听能力；支持 Overlay 网络流量支持，如 GRE, VLAN, QINQ，VxLAN，IPv4 in IPv4，IPv6 in Ipv6，Teredo，MPLS 等。

协议解析之后的元数据支持通过加密通道传送到上游 XDR 平台或其他 SIEM 平台进行处理。

2.3.2. XDR 分析平台

未来智安 XDR 平台通过异构数据接入及多元数据治理技术存储来自 EDR 平台、NDR 平台上报的主机日志、主机审计日志、流量日志及告警并进行存储，未来智安 XDR 平台存储组件基于分布式存储

架构，可以对所有接入的异构数据进行搜索、展示和分析，同时依托经过标准化治理之后的数据进行关联分析、威胁情报检测等威胁发现。未来智安 NDR 还可以通过威胁告警及异构数据关联建模回溯完整攻击事件,基于完整攻击事件分析、提取攻击线索、评估攻击事件的影响面等。总体而言未来智安 NDR 平台聚焦流量侧的威胁检测与响应，是一个基于安全中台构建的开放可扩展的平台，可连接生态中的安全组件数据，通过可插拔的能力模块和技术，实现跨网络、终端的统一可视、威胁发现，自动化分析溯源，统一作战指挥和协同响应处置。

2.4. 产品功能规格说明

功能类别		招标要求
流量采集	协议解析	AJP13，BGP，DB2，DHCP，DNS，FTP，HTTP，ICMP，ICMPv6，IMAP，Krb5，LDAP，MMS，MongoDB，MySQL，NetBIOS，NetFlow（V9/V7/V5 三个版本），NFS，NTP，OICQ，ONC-RPC，OSPF，POP3，Postgresql，RADIUS，RDP，RESP，RIP，RLogin，RSH，RTCP，RTP，RTSP，sFlow，SMB，SMTP，SOAP，SSH，SSL，Sybase，TFTP，TDS，Telnet，TNS，VNC，反弹 shell 场景
	流量传输内容	流量传输的内容包括：1、TCP 会话信息，包括源、目的 IP 及 mac，端口、开始及终止时间、会话上下行数据量 2、DNS 查询记录 3、邮件传输记录 4、Web 上网记录 5、SQL 命令执行记录 6、文件传输记录
	流量传输内容配置	采集信息内容可以配置
	流量传输接口配置	定义采集信息的传输目的 IP

	IPv4/IPV6	同时提供 IPv4 网络和 IPv6网网络的监听能力
	Overlay 网络流量支持	GRE，VLAN，QINQ，VxLAN，IPv6 in IPv4，IPv4 in IPv4，IPv6 in Ipv6，Teredo，MPLS
	流量抓包导出 pcap	界面配置 IP、端口或协议，抓去指定时间（限制 max）流量，导出为 PCAP
文件采集	流量类型	HTTP，FTP，NFS，SMB，SMTP，POP3，IMAP，TFTP，WebMail 流量标记
	文件还原	压缩文件：rar/zip/gz/bz2/tar/tgz 文档：doc/docx/xls/xlsx/ppt/pptx/wps/pdf 脚本：sh/bat/php/jsp/asp/aspx 程序：exe/jar/war/class/swf
	文件解压缩	支持对常见压缩格式的解压缩：RAR、ZIP、GZ、7Z
	文件还原配置	可配置还原文件类型，最大还原文文件大小,以及文件还原功能开关
	文件传输配置	可以定义还原后文文件的传输目的 IP 地址
攻击检测	网络扫描	主机扫描，端口扫描
	Flood	SYN Flood/ACK Flood/FIN Flood/DUP Flood/PING Flood/应用 Flood
	IP 分片攻击	
	ARP 欺骗	freeARP 频率检测，以及内网 IP 冲突报警
	WEB 攻击检测	供基于攻击原理的签名，检测此类攻击
	WEB 漏洞发现	可以通过听包方式，判断服务器是否存在相应的攻击漏洞，此信息和攻击检测信息一起显示

	SQL 高危命令	针对不常用且危险的 SQL 命令，直接进行告警
	SQL 命令检测	基于 SQL 命令，检测是否存在注入攻击，需要考虑针对不同后台的特殊注入方式，包括 MySQL、MSSQL、ORACLE
	木马心跳检测	检测网络中存在的心跳流量，以查找可能存在的木马
	常见木马蠕虫检测	常见蠕虫木马的网络特征检测
	抗逃避能力	提供针对数据包、TCP 流及 HTTP 协议的乱序、编码等逃避机制的 防御能力
	检测策略配置	提供检测的开关选项，并提供检测地址范围及白名单功能
	告警传输配置	定义攻击检测报警的目的 IP 地址
管理能力	管理接口配置	系统预置管理口（IPv4 及 IPv6），并可配置 IP、子网掩码及网关、 DNS
	监听接口配置	可启停监听接口，并指定监听白名单
	接口工作模式	可定义以上接口的工作模式，自动协商或手动配置
	时间配置	可指定时间和时区，提供 NTP 方式，预置 NTP 并可配置
	SNMP	支持 SNMP 管理，可以提供主机名、CPU、内存、存储信息
	syslog	网络报警信息可以通过 syslog 方式发送到第三方主机
	证书管理	提供独立的 license 管理机制，以证书导入时间为基准，证书到期后 签名库不再升级
	设备升级	提供设备自身的软件升级机制
	签名升级	提供在线的自动、手动升级机制，同时提供手动升级包方

		式
	用户管理	提供管理员帐号，可以修改密码
	用户安全	提供验证码登录机制、提供超时机制
	串口管理	提供串口命令行，可以修改管理口配置及审计管理员密码，提供基本的网络层 debug 命令
设备监控	系统配置	软件版本、规则库版本、license 信息、设备序列号
	系统状态	CPU、内存、磁盘、关键组件状态、uptime
	网络流量	24 小时、一周趋势：不同监听接口的网络流量总和及分网口的流量
	协议流量统计	24 小时、一周趋势：不同网络协议的流量大小
	文件数量统计	24 小时、一周趋势：不同文件类型的趋势图
	日志外发统计	24 小时、一周趋势：不同文件类型的趋势图
	网卡状态	不同的网卡当前工作状态，包括底层统计数据
安全性及其他	外发流量认证/加密	接口外发流量采用认证及加密
	磁盘文件加密	提供加密磁盘保护机制
	系统固化	设备接口进行系统漏洞扫描，不应发现内置服务版本及发现漏洞
	登录次数限制	鉴别失败超过设定值，锁定源 IP 5-10 分钟
	审计日志	审计用户登录、策略配置更改、管理员增删改、对审计日志的操作 等！只允许用户管理员查看，提供查询和导出功能。

	设备日志	设备运行状态及 debug 需要的日志信息提供导出功能
	旁路阻断	支持旁路阻断

3. 产品核心功能

3.1. 威胁检测

未来智安 NDR 具备完整的网络威胁检测能力，基于流量侧检测能力包括针对 APT 攻击、勒索软件、远控木马、僵尸网络、窃密木马、间谍软件、网络蠕虫、邮件钓鱼等高级攻击的检测覆盖。

3.2. 攻击事件回溯

未来智安 NDR 具备完整的攻击事件溯源能力，针对目前安全产品普遍存在的告警多的难题，基于自研的告警治理引擎，有效的降低告警的数量，挖掘更多的攻击线索，评估攻击影响面等多纬度数据来提高攻击事件的运营分析及响应效率。

3.3. 攻击事件调查分析

基于未来智安 NDR 的告警治理引擎通过自动化的威胁告警治理后提取出攻击事件 Incident，安全分析师或安全运维人员可围绕攻击事件 Incident 进行攻击事件的深度调查和分析,每条完整的攻击事件 Incident 包括攻击的关键线索、攻击事件所影响或覆盖的资产数量及

资产信息。其中攻击线索包括当前攻击事件所涉及到的如异常进程的md5、攻击 IP 等，并基于攻击线索进行对应告警关联、对应进程的文件操作行为、对应进程的启停信息、注册表及动态库加载信息等。同时也提供针对线索的信息孵化和分析如进程文件的威胁等级、攻击 IP 来源、攻击 IP 的威胁情报信息等。未来智安 NDR 攻击事件调查分析模块可以让安全分析师或安全运维人员围绕一个完整攻击事件进行调查分析而不是面对大量的告警、大量零散的告警进行威胁运维工作，提高安全运维效率。

3.4. 响应处置

响应处置能力是安全运营工作至关重要的环节，精准、高效、快速的响应处置能力对有效阻止网络攻击极其重要，响应处置能力决定了应对网络攻击所带来的破坏和损失的程度。未来智安 XDR 响应处置模块可基于 SOAR 的安全编排能力实现做好应急响应预案，也可针对告警或攻击事件在第一时间半自动化的调用对应的响应处置能力。未来智安 XDR 主机侧的处置能力包括访问控制、扫描防护、进程隔离、进程查杀、病毒查杀、及快速的取证溯源。同时在流量侧支持进行旁路阻断。未来智安 XDR 响应处置模块可针对不同的攻击类型、不同攻击场景定制有针对性的处置剧本 Playbook，可自动化、半自动化以及阶段性任务的方式编排剧本的执行策略。

3.5. SOAR

未来智安 SOAR 模块为客户提供安全编排和处置能力，能够依据安全管理需求场景或预案，制定执行计划和执行脚本，并具备自动、半自动和手动执行的能力。未来智安 SOAR 模块提供制定的编排预案协助客户梳理日常安全运维工作简化和提高安全运维工作效率。SOAR 模块除了内置的 APP 还支持在线导入和增加相关安全能力、安全运维过程中所需的工具、接口及企业现存的信息化系统的对接能力,SOAR 核心功能包括如下 ：

3.5.1. Playbook/编排

提供一种流程编写方式具备控制能力、流转方式、流嵌套、扩展性、编排性等实现对安全管理需求的快速响应、运维。例如 Agent 采集的数据触发了告警安全基线则可以通过 Playbook 编排出自动触发邮件告警的流程。

3.5.2. 安全能力脚本

安全能力脚本提供一种在线编程的能力。例如实现对接 OA 系统的脚本能力、对接发邮件的能力等。安全能力脚本提供给 Playbook 进行能力编排。

3.5.3. 联动管理

联动管理是对联动设备的接入管理配置，联动设备如 OA 系统、相关安全设备等。

3.6. 威胁狩猎

目前大多数的安全运维工作都是基于各类安全设备产生的告警，以告警作为线头逐个进行调查分析工作，缺乏对告警的完整的攻击描述、无完整的攻击上下文信息，更无有效的手段和没有充分利用安全日志 Event 及告警 Alert 进行回溯和构建攻击链条，另外不同安全产品间缺乏数据联动性，如 EDR 的终端数据无法结合流量侧的 NDR 进行数据间的关联分析，未来智安 XDR 威胁狩猎模块基于不同攻击线索、ATT&CK 等多维度关联分析技术，打通 EDR、NDR 之间的数据孤岛，可以任意类型告警 Alert 或安全日志 Event 作为线头输入或人工圈定攻击假设进行威胁分析、可视拓线，分析和挖掘企业侧网络攻击事件。

3.7. 旁路解密

针对 https 等加密流量，未来智安 NDR 提供基于旁路非代理方式的解密 Https 流量，只需在 NDR 管理平台导入对应的私钥，NDR 内

置旁路解密引擎依据对应私钥还原出标准 HTTP 协议便可进行威胁检测。

3.8. 日志检索

未来智安日志检索模块基于搜索引擎技术构建，可检索主机侧的安全事件日志、流量日志、告警及第三方接入的多元异构数据。同时日志检索模块还内置了针对不同威胁分析和检测场景的快捷搜索语句以提高威胁分析检索的效率。日志检索模块还可以依据搜索结果以时间纬度呈现数据或流量的趋势统计，以趋势图可视化的呈现方式数据或流量变化。

3.9. 数据治理

未来智安 XDR 平台支持通过异构安全设备及多元异构数据接入，数据治理模块包括数据源、数据字典、数据结构、数据模型及接入策略五部分组成。XDR 数据治理模块采用无码化数据接入支持的数据源包括 kafka、syslog、redis 等,数据字典从数据标准化角度出发梳理和定义出符合如 RFC 等标准化的元数据描述，为后续的攻击检测和溯源分析等构建标准化数据做好铺垫,另外数据字典有利于企业梳理数据资产，掌握企业内部的数据纬度。数据结构基于领域描述基础上构建符合标准的数据对象如 RFC 中的 http 协议元数据定义等,避免数据对象的各自表述。数据模型为多元预购数据提供在线建模，定义

字段提取规则，支持利用正则解码、GROK 解码、AES 解码、MsgPack 解码、CSV 解码以及自定义解析脚本等方式依据输入的数据样本构建数据消费模型。接入策略包括输入配置和存储配置，输入配置选择定义好的数据源及数据模型，输出配置选择存储策略例如存储到 ES、Postgres 等。

3.10. 报表管理

报表可以纵观全网安全数据、安全趋势，包括主机资产报表、运行软件报表、漏洞数据等，对全网安全风险做到量化观测，高效管理，全面监控等。

3.11. 报告/报告导出

通过基于输入的报告模板导出安全状态报告，支持自定义的导入报告模板，也可以基于默认的报告模板导出报告。

3.12. 应用服务

未来智安 XDR 应用服务模块支持以其他模块或安全应用以 APP 的方式接入未来智安 XDR 平台。XDR 应用服务通过 APP 式应用接入实现安全能力、安全运营能力的可扩展。

4. 产品详述

4.1. 设计目标/产品价值

未来智安 NDR 模块支持对客户内网的未知威胁检查和发现，通过旁路部署方式采集网络流量并对网络流量进行协议解码和协议还原，提取网络层、传输层和应用层的头部信息及流量中重要的负载信息进行威胁检测，同时支持还原流量中的 pe、非 pe 文件通过沙箱进行未知威胁检测。未来智安 NDR 协议解码能力覆盖 AJP13，BGP，DB2，DHCP，DNS，FTP，HTTP，ICMP，ICMPv6，IMAP，Krb5，LDAP，MMS，MongoDB，MySQL，NetBIOS，NetFlow（V9/V7/V5 三个版本），NFS，NTP，OICQ，ONC-RPC，OSPF，POP3，Postgresql，RADIUS，RDP，RESP，RIP，RLogin，RSH，RTCP，RTP，RTSP，sFlow，SMB，SMTP，SOAP，SSH，SSL，Sybase，TFTP，TDS，Telnet，TNS，VNC 等几十种，攻击检测能力覆盖网络扫描、Flood、IP 分片攻击、ARP 欺骗、WEB 攻击检测、WEB 漏洞发现、SQL 高危命令、SQL 命令检测、木马心跳检测、常见木马蠕虫检测等，支持将流量日志及告警发送到上游的xdr或其他管理平台进行进一步的分析。

4.2. 详细功能介绍

功能类别	招标要求

流量采集	协议解析	AJP13，BGP，DB2，DHCP，DNS，FTP，HTTP，ICMP，ICMPv6，IMAP，Krb5，LDAP，MMS，MongoDB，MySQL，NetBIOS，NetFlow（V9/V7/V5 三个版本），NFS，NTP，OICQ，ONC-RPC，OSPF，POP3，Postgresql，RADIUS，RDP，RESP，RIP，RLogin，RSH，RTCP，RTP，RTSP，sFlow，SMB，SMTP，SOAP，SSH，SSL，Sybase，TFTP，TDS，Telnet，TNS，VNC，反弹 shell 场景
	流量传输内容	流量传输的内容包括：1、TCP 会话信息，包括源、目的 IP 及 mac，端口、开始及终止时间、会话上下行数据量 2、DNS 查询记录 3、邮件传输记录 4、Web 上网记录 5、SQL 命令执行记录 6、文件传输记录
	流量传输内容配置	采集信息内容可以配置
	流量传输接口配置	定义采集信息的传输目的 IP
	IPv4/IPV6	同时提供 IPv4 网络和 IPv6网网络的监听能力
	Overlay 网络流量支持	GRE，VLAN，QINQ，VxLAN、IPv4 in IPv4，IPv6 in Ipv6，Teredo，MPLS
	流量抓包导出 pcap	界面配置 IP、端口或协议，抓去指定时间（限制 max）流量，导出为 PCAP
文件采集	流量类型	HTTP，FTP，NFS，SMB，SMTP，POP3，IMAP，TFTP，WebMail 流量标记
	文件还原	压缩文件：rar/zip/gz/bz2/tar/tgz 文档：doc/docx/xls/xlsx/ppt/pptx/wps/pdf 脚本：sh/bat/php/jsp/asp/aspx 程序：exe/jar/war/class/swf
	文件解压缩	支持对常见压缩格式的解压缩：RAR、ZIP、GZ、7Z

	文件还原配置	可配置还原文件类型，最大还原文文件大小,以及文件还原功能开关
	文件传输配置	可以定义还原后文文件的传输目的 IP 地址
攻击检测	网络扫描	主机扫描，端口扫描
	Flood	SYN Flood/ACK Flood/FIN Flood/DUP Flood/PING Flood/应用 Flood
	IP 分片攻击	
	ARP 欺骗	freeARP 频率检测，以及内网 IP 冲突报警
	WEB 攻击检测	供基于攻击原理的签名，检测此类攻击
	WEB 漏洞发现	可以通过听包方式，判断服务器是否存在相应的攻击漏洞，此信息和攻击检测信息一起显示
	SQL 高危命令	针对不常用且危险的 SQL 命令，直接进行告警
	SQL 命令检测	基于 SQL 命令，检测是否存在注入攻击，需要考虑针对不同后台的特殊注入方式，包括 MySQL、MSSQL、ORACLE
	木马心跳检测	检测网络中存在的心跳流量，以查找可能存在的木马
	常见木马蠕虫检测	常见蠕虫木马的网络特征检测
	抗逃避能力	提供针对数据包、TCP 流及 HTTP 协议的乱序、编码等逃避机制的 防御能力
	检测策略配置	提供检测的开关选项，并提供检测地址范围及白名单功能
	告警传输配置	定义攻击检测报警的目的 IP 地址

管理能力	管理接口配置	系统预置管理口（IPv4 及 IPv6），并可配置 IP、子网掩码及网关、 DNS
	监听接口配置	可启停监听接口，并指定监听白名单
	接口工作模式	可定义以上接口的工作模式，自动协商或手动配置
	时间配置	可指定时间和时区，提供 NTP 方式，预置 NTP 并可配置
	SNMP	支持 SNMP 管理，可以提供主机名、CPU、内存、存储信息
	syslog	网络报警信息可以通过 syslog 方式发送到第三方主机
	证书管理	提供独立的 license 管理机制，以证书导入时间为基准，证书到期后 签名库不再升级
	设备升级	提供设备自身的软件升级机制
	签名升级	提供在线的自动、手动升级机制，同时提供手动升级包方式
	用户管理	提供管理员帐号，可以修改密码
	用户安全	提供验证码登录机制、提供超时机制
	串口管理	提供串口命令行，可以修改管理口配置及审计管理员密码，提供基本的网络层 debug 命令
设备监控	系统配置	软件版本、规则库版本、license 信息、设备序列号
	系统状态	CPU、内存、磁盘、关键组件状态、uptime
	网络流量	24 小时、一周趋势：不同监听接口的网络流量总和及分网口的流量
	协议流量统计	24 小时、一周趋势：不同网络协议的流量大小
	文件数量统计	24 小时，一周趋势：不同文件类型的趋势图

	日志外发统计	24 小时，一周趋势：不同文件类型的趋势图
	网卡状态	不同的网卡当前工作状态，包括底层统计数据
安全性及其他	外发流量认证/加密	接口外发流量采用认证及加密
	磁盘文件加密	提供加密磁盘保护机制
	系统固化	设备接口进行系统漏洞扫描，不应发现内置服务版本及发现漏洞
	登录次数限制	鉴别失败超过设定值，锁定源 IP 5-10 分钟
	审计日志	审计用户登录、策略配置更改、管理员增删改、对审计日志的操作 等! 只允许用户管理员查看，提供查询和导出功能。
	设备日志	设备运行状态及 debug 需要的日志信息提供导出功能
	旁路阻断	支持旁路阻断

4.2.1. 网络全流量采集处理

网络全流量采集部署在系统中的核心网络节点上，采用侦听网络数据包的方法将网络流量捕获同时对网络流量进行协议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及流量中重要的负载信息。

支持常见数据包解码包括IPv4, IPv6, TCP, UDP, SCTP, ICMPv4, ICMPv6, GRE, Ethernet, PPP, PPPoE, Raw, SLL, VLAN, QINQ,

MPLS, ERSPAN, VXLAN；支持常见应用层协议解码包括 HTTP, SSL, TLS, SMB, DCERPC, SMTP, FTP, SSH, DNS, Modbus, ENIP/CIP, DNP3, NFS, NTP, DHCP, TFTP, KRB5, IKEv2, SIP, SNMP, RDP 等几十种协议解析还原能力。

支持 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为、IM 通信等行为描述；

网络流量采集模块可以支持 IPv4/IPV6，同时提供 IPv4 网络和 IPv6网网络的监听能力；支持 Overlay 网络流量支持，如 GRE, VLAN, QINQ，VxLAN，IPv4 in IPv4，IPv6 in Ipv6，Teredo，MPLS 等，

协议解析之后的元数据支持通过加密通道传送到上游 XDR 平台或其他 SIEM 平台进行处理，

4.2.2. 网络全流量采集过滤

支持通过流量黑、白名单及协议类型的流量过滤方式，过滤掉不需关注的流量或仅接收需要关注的流量；

4.2.3. 文件还原

支持从 HTTP、SMTP 、FTP、NFS、SMB、HTTP2 等协议还原文件，支持还原压缩文件包括 rar/zip/gz/bz2/tar/tgz 等；支持文档类型包括 doc/docx/xls/xlsx/ppt/pptx/wps/pdf 等；支持脚本文件还原

包括 sh/bat/php/jsp/asp/aspx;支持程序还原包括 exe/jar/war/class/swf 等。

4.2.4. Pcap 抓包

支持对流量抓包导出 PCAP,可通过界面配置 IP、端口或协议进行指定时长内的流量抓包并导出为 PCAP，可通过下载 PCAP 包进行深入分析和攻击溯源分析。

4.2.5. 网络全流量攻击检测

网络全流量攻击检测通过全流量的采集、检测及分析来检测来产生网络的攻击，根据数据包特征对流量进行深度解析，通过对数据流中威胁行为识别，达到恶意攻击流量检测的目的。

支持全流量采集，对网络全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、重要负载信息，传送到检测和分析模块进行统一处理；通用协议命令解码、WEB 应用漏洞利用及程序攻击、恶意文件及病毒攻击、异常威胁、异常用户名登录请求、可疑执行代码等非正常和非 RFC 遵从的请求行为进行攻击检测和发现以风险级别实时呈现给上游的 XDR 系统。

可实时检测多种网络协议中的攻击行为，提供 ids、webids、webshell 等维度的威胁检测能力；

支持检测如多种网络应用、木马、广告、exploit 等多种网络攻击行为；同时支持 IDS 检测规则；

支持检测如 sql 注入、跨站、webshell、命令执行、文件包含等多种 web 攻击行为，可精准检测 php 后门并记录相关信息，拥有实时匹配能力，能精准发现恶意软件、APT 事件等网络攻击事件；

支持对 web 漏洞发现和基于 web 漏洞攻击的进行深度分析能力，可针对如 web 请求的 URL、GET/POST 数据包、HTTP 请求头及响应报文等数据维度分别制定针具有针对性的攻击检测规则；

通过对网络攻击告警定义威胁类型、威胁等级、kill chain 阶段、及 ATT&CK 等标签，可直接体现攻击结果是企图、成功、失陷等，将攻击过程根据 kill chain 及 ATT&CK 的各阶段进行标签化；可展示一次网络攻击的完整过程；

4.2.6. 流量及状态统计

支持监控系统运行状态包括 CPU、内存、磁盘、关键组件等状态信息；

提供不同时间纬度的网络流量趋势如 24 小时、一周的网络流量趋势；同时可支持监听不同接口的网络流量总和及分网口的流量趋势。

支持对流量中不同协议类型的流量统计包括 24 小时、一周的趋势及不同网络协议的流量大小。

支持对经过流量还原的文件数量统计包括 24 小时、一周的趋势及不同文件类型的趋势统计。

支持统计通过外发的日志数量统计包括 24 小时、一周的趋势及不同文件类型的趋势统计。

同时支持监控网卡的状态包括不同的网卡当前工作状态及底层不同纬度的数据统计。

4.3. 系统组成与架构

未来智安 NDR 模块包括流量传感器、管理控制台组成。其中流量传感器有流量采集、协议解析、文件还原、检测引擎、威胁情报、数据外发等子模块组成。管理控制台负责 NDR 的运维管理和系统监控，包括管理接口配置、监听接口配置、接口工作模式、时间配置、SNMP、syslog、证书管理、设备升级、签名升级、用户管理、用户安全、串口管理、网络流量、协议流量统计、文件数量统计、日志外发统计、网卡状态等自模块组成。

5. 产品典型部署场景

通过部署未来智安的 NDR 平台可以帮组客户进行未知威胁的检测、分析、溯源，提升安全运维人员对攻击事件的响应和处置效率，最大限度的减少网络攻击带来的损失和影响。可以在每个不同区域分

别部署未来智安 NDR 流量传感器，对不同区域中的流量进行全量采集和检测，可以将部署在不同区域未来智安 NDR 流量传感器还原的流量日志、告警信息、还原的文件等发送给一个或多个未来智安 XDR 集群进行存储和深度分析。

相关配置：

分析平台配置：

1.设备规格：2U，标准机架式。

2.电源：800W*2

3.CPU：2×16 核

4.内存：128GB，

5.硬盘：系统盘 960G SSD+存储盘 32TB 企业级硬盘

6.管理口：千兆电口*2

7.分析平台性能 10000 eps，日志处理速度 90 万条每分钟；单台分析平台实际可处理流量 4Gbps。

探针配置：

1.设备规格：2U，标准机架式。

2.电源：800W*2

3.CPU：2×16 核

4.内存：128GB，

5.硬盘：系统盘 960G SSD+存储盘 6TB 企业级硬盘

6.管理口：千兆电口*2

7.镜像口：千兆电口*2、万兆光口*2