数据及网络安全治理

扫码观看报告解读

B.26
网络安全态势感知与威胁防控平台的探索与建设

陕西省宝鸡市中级人民法院课题组*

摘　要： 随着人民法院信息化建设进入4.0时代，数据在内外网和各信息系统之间传输愈加频繁，为充分保障网络和数据安全，陕西省宝鸡市中级人民法院积极探索、主动创新，全力推动网络安全由被动防御到主动防护、由局部建设到整体融合的转变，建成了网络安全态势感知与威胁防控平台。该平台利用大数据技术，借助分布式计算和搜索引擎，分析获取实时网络流量和设备日志，快速精准定位已被病毒感染的终端和面临网络威胁的设备，可视化呈现网络安全风险，协助网络安全人员及时优化网络安全策略，实施积极主动的安全防护措施。宝鸡两级法院依托该平台的事前监管、事中监测、事后响应机制，全面构建了主动安全防控体系，实现了网络安全的全链条闭环管理。

* 课题组负责人：尤青，陕西省宝鸡市中级人民法院党组书记、院长。课题组成员：任笑生、李龙。执笔人：任笑生，陕西省宝鸡市中级人民法院司法行政装备管理处副处长；李龙，陕西省宝鸡市中级人民法院司法行政装备管理处四级主任科员。

关键词： 网络安全 态势感知 安全防护 数字法院

随着网络技术的不断更新，各种攻击工具越来越智能化、平民化，攻击能力更强，攻击方式更加复杂多变，且更易于被攻击者掌握。法院作为国家审判机关，专网内部存有大量的敏感数据，一旦网络被攻陷造成数据被窃取、丢失和篡改，将会造成非常严重的后果，因此，法院网络安全建设是人民法院信息化建设的基石。

近年来，陕西省宝鸡市中级人民法院（以下简称“宝鸡中院”）始终以总体国家安全观为引领，统筹发展和安全，严格落实网络安全保护责任，强化网络安全数据保障能力，建成了以网络安全态势感知与威胁防控平台为中心，边界安全防护、终端安全防护、服务器安全防护为一体的三重防护，涵盖资产管理、数据采集、扫描监测、高危预警、指挥调度、态势感知、威胁处置、分析回溯等功能的人民法院网络安全态势感知与威胁防控体系，实现了宝鸡两级法院网络安全的整体防护和统一监管。

通过网络安全态势感知与威胁防控体系建设，可全面监测宝鸡两级法院专网和互联网的实时网络状态，极大节约了网络安全建设成本，提升了网络安全运维质效，减少了网络安全资源投入，增强了法院网络的安全性、稳定性和可控性，全面提高了宝鸡两级法院网络安全保障能力和网络风险化解水平。

一 现实需求

随着法院信息化建设的不断推进，法院专网与互联网进行数据交互的业务需求不断增加，数据交互量逐年增长，面临的安全形势也越发严峻。目前，传统的法院网络安全防护体系面临威胁定位能力不足、持续监控能力缺失等多方面的问题。

1. 高级威胁智能检测需求

传统安全防御体系的设备和产品主要依靠攻击特征库的模式匹配完成对

攻击行为的检测，而现在的多数威胁攻击则是采用未知漏洞、Oday、未知恶意代码等未知行为进行网络攻击。因此，依靠已知特征、已知行为的传统安全防护设备和产品将无法有效检测网络攻击行为。

2. 网络攻击回溯分析需求

传统的安全事件分析思路是遍历各个安全设备的告警日志，尝试找出其中的关联关系。但这种方式通常无法对网络攻击的各个阶段进行有效检测，对告警日志的分析效率低下。若进行全网数据采集，存在两方面的弊端：一方面，存储空间占用率高，每天产生的数据会占用过多的存储空间，法院中心机房没有足够的资源来支撑长时间的存储；另一方面，采集内容包含许多非结构化数据，涵盖了视频、图片、文本等多种格式，不能直接进行格式化检索，难以从海量数据中找到有价值的信息。

3. 安全威胁快速识别需求

鉴于司法公开与司法在线服务的需要，多数法院开通了法院专网与互联网的数据交换通道，经常会面临来自互联网的攻击威胁，虽然法院安全运维人员已经在网络各个位置部署了大量的传统安全设备，但仍然会有隐藏于数据中的网络威胁绕过传统防护到达法院专网内部，产生重要数据资产泄露、损坏或篡改等风险。由于无法及时发现潜藏在数据中的安全威胁，难以从源头消除法院专网中存在的安全隐患。

4. 网络边界纵深防御需求

按照网络互联共享的特性，法院专网实现了上下级法院的互联互通，但在与互联网进行数据隔离交换的同时也为网络攻击、漏洞入侵、恶意程序的传播等提供了天然的通道。前端互联网接入区域业务结构复杂，虽然已在暴露的网络接入点部署了大量的传统防护设备，但没有不透风的墙，容易被不法人员利用侵入，这些可信程度相对较低的区域会对核心应用服务、骨干链路设备节点和安全管理控制系统造成巨大威胁。一旦非授权用户非法接入法院专网，就可以进行探测和攻击，直接影响法院专网内线业务的正常运行。目前法院传统的网络安全防护设备还不具备跨网探测防护处置的能力。

5. 终端安全处置管控需求

随着人民法院信息化建设的不断推进，法院信息系统已经高度自动化、智能化，能够高速、高效地为用户提供更好的服务。而法院干警通过终端在信息系统中生产大量数据，但这些终端的管理和安全防护技术手段却相对落后，在当前快速复杂多变的信息安全形势下，无论是外部黑客入侵，还是多数情况下内部用户无意识造成的问题，安全防护手段都正在变得越来越捉襟见肘，终端防护压力越来越大，统一安全运维处置能力和有效的合规管控能力是目前终端安全管理面临的最大问题。

6. 服务器安全精准防控需求

在目前的网络安全大环境下，病毒的攻击技术越发精准，攻击手段越发隐蔽，传统防控手段和防病毒安全系统已无法完全保障法院服务器的安全，难以避免病毒对数据、应用、网络等资产造成威胁，服务器操作系统的原有安全防控体系不完善，无法对网络攻击进行精准防控，这些都是服务器安全防控的痛点。

二　建设目标

宝鸡中院建设的网络安全态势感知与威胁防控平台以实现体系化网络安全防护和保障业务系统安全为核心，旨在满足人民法院服务司法管理、服务审判执行、服务人民群众的需要，是适应新技术新模式的安全发展趋势、保障和助力审判工作现代化的重要组成部分。通过高级威胁检测和深度分析，对高级威胁恶意行为的早期快速发现和威胁告警，对受害终端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精准研判与溯源，做到网络安全防患于未然。主要有以下四方面的目标。

1. 高级威胁的精准检测

与传统的安全检测能力相比，网络安全态势感知与威胁防控平台可以快速发现高级网络攻击，准确率高，误报率低，能够及时发现各种未知威胁攻击，对攻击类型、攻击方式进行精准分类。

2. 网络攻击的溯源分析

通过还原和存储网络流量的源数据，回溯已经发生的网络攻击行为，分析攻击路径、受感染面和信息泄露状况，对攻击行为进行可视化呈现，详细排查系统存在的安全漏洞，并为修复整改提供技术支撑。

3. 安全事件的快速响应

通过收集和分析分散在大量终端和服务器上的威胁情报和日志上下文，建立分级告警机制，限定响应时间，在第一时间发现风险威胁，及时分析、研判和处置终端和服务器的重大安全事件，降低安全损失。

4. 安全合规的有效实现

借助大数据平台技术，网络安全态势感知与威胁防控平台在增强安全防护能力的同时，设置网络安全设备的运行参数范围，限定设备在合理的阈值内运转，可以有效满足新的等级保护安全防护要求，为等保测评奠定安全技术基础。

三　平台架构与组成

网络安全态势感知与威胁防控平台是基于新一代的网络安全防控理念，以“一个中心、三重防护”为架构（见图 1），即以网络安全态势感知能力为中心，将传统的被动防御转变为主动防护，实现对终端、服务器、网络边界的三重防护。平台通过整合集成多个系统的功能模块，形成了集网络流量采集、威胁监测呈现、溯源路径分析、防护联动响应于一体的网络安全防护体系。

（一）“一个中心”建设

网络安全态势感知中心由全流量数据采集系统和威胁分析系统组成，构建了覆盖宝鸡两级法院的高级威胁检测网，提供了全方位的网络安全态势感知能力。

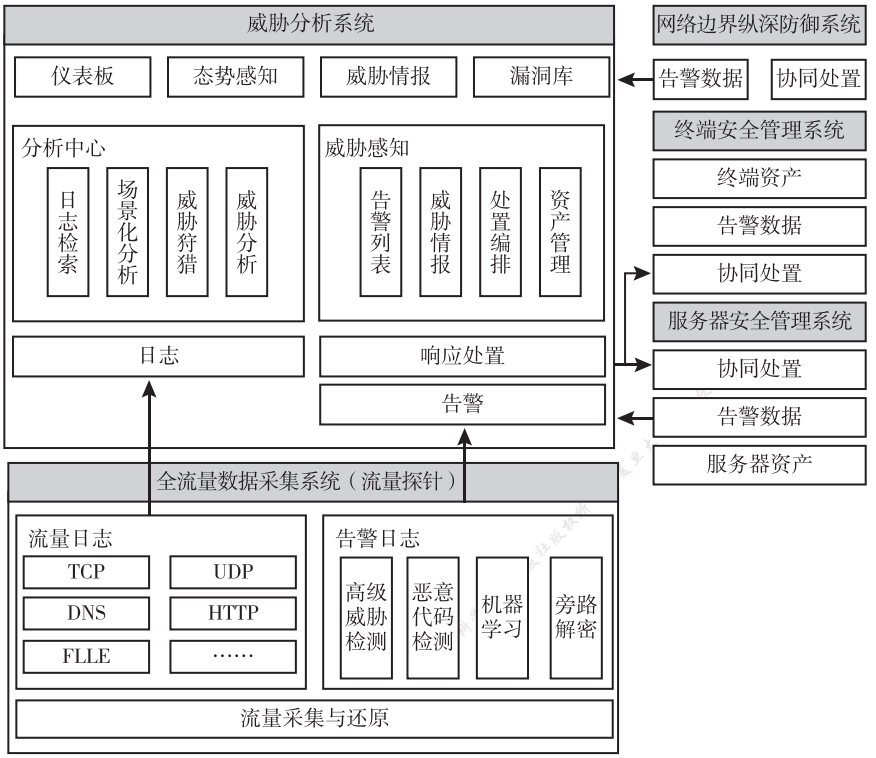

图 1　平台架构

1. 全流量数据采集系统

全流量数据采集系统是威胁分析系统的重要数据来源，可以发现隐藏较深的网络威胁行为，及时汇集分析法院专网和互联网的告警数据，通过分析研判提高法院专网和互联网的整体协调能力。系统主要有以下四部分功能。一是流量采集与还原。全流量数据采集系统可对网络流量进行采集，解码还原出真实的业务数据，再进一步分析数据内容，提取负载信息，通过加密通道传输至威胁分析系统，可以从多个维度综合评估网络威胁。二是高级威胁检测。全流量数据采集系统具备检测高级威胁和未知威胁的能力，借助威胁情报源、智能检测引擎、机器学习、沙箱等先进技术，检测和发现多种网络协议中的 APT 攻击、勒索软件、远控木马、僵尸网络、间谍软件、网络蠕

虫、钓鱼软件等高级网络攻击。三是恶意代码检测。全流量数据采集系统基于人工智能杀毒引擎，依靠机器学习模型对未知程序进行分析研判，获得软件的恶意概率，从而在可控的误报率下尽可能多地发现恶意程序。四是旁路解密。该功能可以对加密攻击流量进行解密、安全检测、审查、分析和拦截，缩小网络安全盲区，还可通过旁路非代理的方式将解密还原后的 HTTP 流量以可视化图表的形式呈现。

2. 威胁分析系统

威胁分析系统是网络安全态势感知与威胁防控平台的核心，可以将全流量数据采集系统提交的流量日志和告警日志进行存储并快速处理，能对所有数据进行日志关联分析，以图表的形式展示威胁态势分析结果，以攻击链的视角还原告警信息中的受害主机被攻击的全过程。系统主要具有五部分的功能。一是数据存储与检索。威胁分析系统基于大数据平台，可以提供大并发量的计算和查询，将采集的告警数据进行存储、预处理和检索，通过分布式计算和搜索引擎技术对所有数据进行处理，提供充足的存储空间和计算能力。二是多源威胁情报与威胁狩猎。威胁分析系统同步接收云端的威胁情报源数据，依靠失陷检测类情报、IP 信誉情报、文件信誉情报、漏洞情报等数据源，运用自动化的数据处理技术，对 APT 攻击、新型木马、特种免杀木马进行规则化描述，还原攻击者全貌，通过威胁狩猎维度将攻击行为进行重新划分，对告警进行深度关联分析，运用先进的可视化呈现技术，推演出威胁攻击的全过程。三是威胁场景化分析。威胁分析系统将获取的数据按照基础架构安全分析、纵深防御验证分析、积极防御策略分析等模式，以全自动或半自动方式针对特定场景进行建模分析，在无法确定具体威胁阈值的情况下发现高价值的网络安全事件，为多维度发现、判断网络安全问题提供帮助。四是自动化编排响应。威胁分析系统的自动化编排响应包括自动化安全编排功能和风险事件管理功能，可以通过标准的 API/openc2 接口与防火墙、终端安全管理系统、服务器安全管理系统等多种处置设备联动并下发响应指令，完成应急响应工作的联动与处置，实现安全设备间的协同防御。五是威胁态势呈现。威胁分析系统的态势呈现是基于权威度安全要素信息采集和数

据集中分析，利用大数据存储和实时运算能力，展示法院专网和互联网的风险态势、脆弱性态势、法院资产安全状态和可能遭受的攻击威胁类型分布等，满足网络安全日常巡检需求。

（二）“三重防护”能力

网络安全态势感知与威胁防控平台通过终端安全管理系统、服务器安全管理系统和网络边界纵深防御系统，构建了针对终端、服务器和网络边界的三重防护能力，为法院业务信息系统打造了一个可信、可靠、可控的网络环境，提升了系统及应用层面的安全水平。

1. 终端安全管理系统

终端安全管理系统作为终端合规管控的一体化解决方案，通过建设恶意代码防范体系、落实终端安全管理技术措施、部署统一终端运维和安全审计功能等方式，彻底解决了终端安全管理“最后一公里”的问题，使终端管理更加合规。系统大大加强了终端的安全运行支撑能力，可以实现防病毒、补丁管理、终端准入、软件统一分发卸载、终端安全策略管理、终端行为审计，确保终端看得见、管得住。系统主要有以下五部分功能。一是系统合规与加固。对计算机操作系统的基线配置、漏洞补丁、软件安装合规性等情况进行检查、修复和优化，加固系统自身，收缩暴露面，达到系统强化的效果。二是威胁防御与检测。强大的防御、检测和响应能力，能够通过多个病毒防护引擎，检测和防护可能感染终端的安全威胁，实现精准防护、高效检测和联动响应。三是终端管控与审计。基于运维管控、终端审计功能构建完善的主机管控与行为审计体系，有效管控法院信息化资产的外部设备、移动存储介质，严格审计系统行为、网络行为、应用进程行为加强终端管控与审计能力。四是终端数据防泄露。以深度内容分析为基础，覆盖法院内所有终端的网络、邮件、外设、应用等数据通道，洞察敏感数据的分布、传输与应用，对数据进行及时识别、监控和保护，通过安全水印技术进行数据泄露的溯源，提升数据安全管控能力。五是协同防御。依托网络和终端的检测与响应，实现深度威胁监测、协调防御实时阻断和一键处置联动功能。当网络流

量分析发现存在恶意访问的 URL 或者 IP 时，终端安全管理系统接收威胁分析系统下发的处置策略，自动阻止处置策略定义的操作，快速完成业务流量的处置和拦截。

2. 服务器安全管理系统

服务器安全管理系统为法院专网的服务器提供全方位的安全检测与加固，持续对服务器进行威胁监测，在第一时间精准发现恶意扫描、爆破登录、无文件攻击、文件篡改、文件泄露、病毒横向扩散等安全威胁和入侵事件，梳理服务器可能存在的暴露面，批量为服务器安装补丁，修复系统漏洞，防止各类恶意入侵及破坏性攻击，有效抵御黑客攻击和恶意代码，实现资产发现、漏洞检测、漏洞利用防护的闭环管理，打造服务器的安全防护能力。系统主要有以下三部分功能。一是资产行为管理。通过自动收集服务器上的资产信息，梳理服务进程及其子进程进行的命令执行、文件创建、网络外联等行为，快速定位法院业务信息系统的暴露面，实现端口访问控制和异常 IP 阻断。二是威胁风险检测。检测服务器可能存在的风险和威胁告警，统计并展示服务器的风险异常和可疑威胁趋势，利用风险管理功能进行统一查询、筛选、研判和处置。三是 Web 应用动态防护。Web 中间件防护插件可及时发现恶意代码和漏洞，检测并阻断通过 URL 针对服务器的攻击行为，防御各种传统签名方式无法有效防护的漏洞利用攻击。

3. 网络边界纵深防御系统

网络边界纵深防御系统是在网络安全域划分及边界整合的基础上，根据网络边界的接入场景实时调整网络节点安全策略，实现数据在多重网络间可控流转，达到设备安全隔离保护的效果，有效抵御跨网攻击行为，降低恶意代码扩散的风险。系统主要有以下两部分功能。一是精细化访问控制。系统以 IP、安全域、VLAN、时间、用户、地理区域、服务协议及应用等多种管理方式进行访问控制，配置应用控制、入侵防护、URL 过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，对服务协议进行精细粒度的控制，过滤不受信任的网络行为。二是一体化威胁防控。借助人工智能大模型设计的一体化新时代病毒防护引擎，可定位并拦截已知威胁和未知威胁，

免疫绝大多数加壳的变种病毒，查杀 HTTP、FTP、SMTP、POP3 和 IMAP 流量中的病毒，实现法院专网和互联网的全网络安全防护保障。

四　平台部署与实施

（一）平台的部署实施

法院的网络具有业务模式复杂、流量跨越多个网络区域、存储大量工作秘密和敏感数据、流量规模大等特点，因此，网络安全态势感知与威胁防控平台将宝鸡两级法院的信息化资产进行集中管控和统一安全管理接入，为确保资源的高效利用，平台采用一级部署模式（见图 2）。流量探针旁路连接宝鸡中院专网和互联网的核心交换设备，全面采集宝鸡两级法院的全流量数据。

平台内的组件联动。配置网络安全态势感知与威胁防控平台的通信资源，针对不同系统组件之间的数据信息通信，开放对应的端口，设置相应的传输协议及服务，确保平台的整体联动性。

平台与网络的连接。网络安全态势感知与威胁防控平台以旁路的方式分别获取互联网侧核心交换设备的网络流量和法院专网核心层的网络流量，可全面监测法院专网和互联网的全流量网络运行状态。平台的管理端口通过专网线路对法院内外网接口的 IP、DNS、NTP 和 SNMP 进行配置，管理各组件的规则包版本。

（二）网络安全体系建设

1. 网络安全处置值守机制

网络安全态势感知与威胁防控平台实施部署完成后，宝鸡中院安排信息安全工作人员开始对全市两级法院的网络安全进行全程值守。将网络安全态势和系统运行监控情况连接大屏，实时监测全市两级法院的联网终端资产概况、外部访问情况、横向访问情况、法院专网外联访问态势、网络脆弱性、

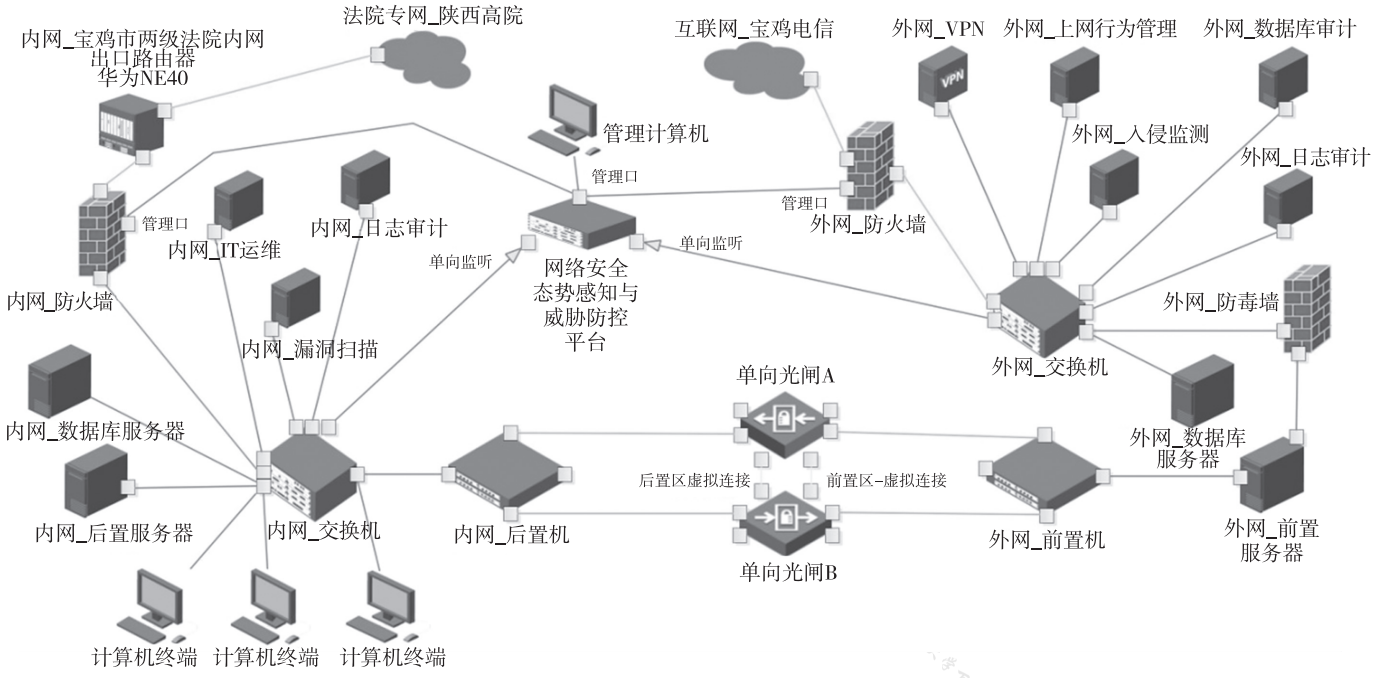
内网_宝鸡市两级法院内网
出口路由器
华为NE40
法院专网_陕西高院
互联网_宝鸡电信
外网_VPN
外网_上网行为管理
外网_数据库审计
管理计算机
管理口
外网_入侵监测
外网_日志审计
管理口
外网_防火墙
管理口
内网_防火墙
内网_IT运维
内网_日志审计
单向监听
单向监听
网络安全
态势感知与
威胁防控
平台
外网_防毒墙
外网_交换机
内网_漏洞扫描
单向光闸A
内网_数据库服务器
外网_数据库
服务器
后置区虚拟连接
前置区-虚拟连接
内网_后置服务器
内网_交换机
内网_后置机
外网_前置机
外网_前置
服务器
单向光闸B
计算机终端
计算机终端
计算机终端

图2　平台拓扑图

威胁感知态势等网络状态，依据态势感知所报威胁告警事件的处置预案进行网络安全处置，将处理过程和结果重新记录回网络安全态势感知与威胁防控平台，形成值守处置知识库。

2. 信息资产全生命周期安全管控机制

网络安全态势感知与威胁防控平台可对登记在资产探针上的法院内联网的信息化资产（终端、服务器、交换机、打印机等）进行管理，实现设备资产管理与态势感知监测的探针体系联动。新增的硬件设备上线并登记后，可对该设备的网络安全状态、系统漏洞、木马病毒、配置安全等多个维度进行全方位的监管。态势感知与威胁防控平台若发现未登记设备接入网络，会立即发出非法接入网络的告警预警。

3. 网络安全风险处置和追溯机制

根据网络安全态势感知与威胁防控平台中的集中管理和威胁运营模式，制定网络安全风险处置预案和威胁分析追溯方案，针对每一项可能发生的网络安全风险事件，利用溯源功能找到问题设备和使用人，明确事件处置的责任人，事后开展网络风险事件的复盘推演，给予对应的处置方案，及时修复存在的网络隐患，提升法院网络的安全性。

4. 非法操作行为处置机制

网络安全态势感知与威胁防控平台可借助探针发现感染木马病毒的终端、使用人的状况。宝鸡中院定期对全市两级法院的网络安全状况进行通报，将感染病毒木马的设备 IP 地址、使用人、归属法院、病毒类型等下发，责令定期整改，通过约谈问题设备的使用人，增强人员网络安全防护意识，完善网络安全体系建设。

五　建设成效

通过网络安全态势感知与威胁防控平台建设，宝鸡中院初步建成了两级法院网络安全防护体系，通过统一的数据采集、威胁监测、问题处置、回溯分析等方式，将原先分散、单一的网络安全防护手段进行整合，通过平台进

行集中管理，借助大数据、分布式计算等技术，对威胁告警日志进行存储和智能分析，完整回溯网络安全风险事件，对未知威胁的恶意行为快速发现、精准定位、持续监控，全面提升宝鸡两级法院业务关键信息基础设施的网络安全保障能力。

1. 提升系统整体安全防护水平

网络安全态势感知与威胁防控平台通过感知采集、关联分析、风险画像、威胁处置、行为回溯等多个环节为法院专网与互联网提供可靠的网络安全保障。

事前管理信息化资产，提前发现并处置可能存在的网络安全隐患。通过将所有的信息化资产录入网络安全态势感知与威胁防控平台，实现宝鸡两级法院信息化资产的集中统一管理，摸清资产画像家底；通过定期对法院内的关键信息基础设施进行资产脆弱性评估，分析可能的受感染面，缩小资产的暴露面；通过加强资产设备的安全病毒防范、补丁管理、移动存储介质管控等手段减小资产感染高危漏洞的隐患。

事中监测威胁分析，研判并及时处置网络安全风险事件。借助实时监测网络流量、扫描通道样本、分析告警日志等手段，及时发现网络攻击行为，迟滞对法院网络的攻击时间，缩小网络安全风险事件对法院网络的威胁面；通过处置联动功能，及时响应并快速处理威胁和网络安全事件，实现主动应对网络安全风险。

事后回溯网络风险，形成网络安全全链条闭环管理。借助威胁分析系统，全面调查网络攻击事件，还原网络攻击路径，防止潜在的被攻击风险；通过网络风险回溯分析，对法院网络安全防护等级进行系统性评估，识别确认的威胁和漏洞，分析可能的风险和后果；通过制定改进措施，完善网络安全事件应急响应预案，增强网络安全防护等级，全面提升网络安全防护能力。

2. 完善网络安全运维管理机制

借助网络安全态势感知与威胁防控平台，制定信息安全防护策略，对法院重要的网络资源设备进行全面管理，定期检查设备的整体工作状态，提升关键防护设备的健壮性；通过制定安全运维管理服务流程，实现了节点可监

测、过程可管理、结果可跟踪；借助平台的安全态势评估手段，完善网络安全策略，通过宏观态势预测全面评估系统整体安全性，为制定网络安全运维管理机制提供强有力的支持。

3. 强化威胁态势可视化呈现能力

网络安全态势感知与威胁防控平台可以对宝鸡两级法院的网络流量进行采集，按照不同的安全分析模型，结合自有的多维度海量大数据对网络全流量进行分析，通过信息安全全景关联，将结果以可视化的动态图表形式展现，提升法院网络态势感知可视化视觉效果，增强系统的易用性和信息的直观性；通过对异常行为、攻击源、脆弱性资产、外部 IP 访问次数、资产访问次数、源资产访问次数、目的资产访问次数等主要监测数据进行梳理汇总分析，提升网络安全管理人员对未知威胁的发现速度和处置效率，最大限度降低网络攻击威胁，提升法院网络内部安全基线。

六　存在问题与思考

1. 网络安全理念有待提升

人民法院网络安全是法院信息化建设的重要组成部分，法官干警现有的安全管理理念未能及时根据新时代网络安全的发展更新迭代，区块链、人工智能大模型、云原生、大数据等新兴技术层出不穷，传统的网络安全意识已无力应对复杂的网络威胁，因此需要规范化建立顺应时代发展的网络安全管理体制机制，从安全管理机构、安全管理策略、安全管理规章制度、安全管理规范、安全管理操作流程等方面，加强法官干警的网络安全理论学习，增加网络安全专项培训频次，转变法官干警陈旧的网络安全理念，以规范化的管理方式多维度提升法院网络安全管理理念。

2. 常态化网络安全绩效考核机制有待完善

现今的网络安全形势日益严峻，潜在的网络安全风险易发多发，网络安全工作重要性日趋凸显，现有的网络安全工作体系缺乏有效的绩效考核机制。为扎实开展网络安全工作，人民法院需要建立更合理的常态化网络安全

绩效考核机制，通过全面加强网络安全信息检查和评估，定期汇总网络安全情况，形成网络安全报告，准确把握安全风险的发生规律，及时有效发现网络安全风险薄弱点，将网络安全考核措施逐层落实，对好的经验做法加以表扬，对存在的问题督促整改，逐步升级完善网络安全绩效考核机制，实现对网络安全风险和威胁的积极主动应对，达到主动防御、安全可控的防护效果。

3. 网络安全经费占比仍需稳步提升

法院的网络安全建设是一项复杂而庞大的工程，需要投入大量的人力、物力和财力。网络安全建设涉及的技术不断更新迭代，随着黑客技术的不断演进和网络攻击手段的日益复杂化，网络安全设备必须与之同步更新，才能达到有效防护的效果。多年来，部分法院存在重建设、轻安全的情况，经费大多投入信息系统建设，网络安全建设经费投入较少，导致网络安全防护存在短板。网络安全建设经费不但要充足而且占比要稳步提升，才能维持网络安全设备的不断升级和更新，补足网络安全防护的短板。

4. 专业人才队伍建设仍需加强

目前法院从事信息化工作的人员普遍不足，网络安全专职工作人员更加稀缺，尤其是基层法院信息化工作人员身兼数职的现象十分普遍，不能全身心投入网络安全工作，出现网络安全风险后也多是事后处置，无法及时消除网络安全隐患，上述问题都极大制约了法院信息化的建设和发展。这就需要结合法院的工作特点，持续加强网络安全技术水平专项培训，提升法院现有信息化工作人员的专业技术水平和业务能力。同时，大力协调人事管理部门积极落实最高人民法院《关于人民法院信息化人才队伍建设的意见》，保障必要的岗位编制，增设合理的晋升渠道，为信息化工作人员创造良好的从业前景。