数字冰雹
DIGITAL HAIL

网络安全大屏可视化决策系统

产品白皮书

北京数字冰雹信息技术有限公司

目 录

1. 产品概述

数字冰雹“网络安全态势感知大屏可视化决策系统”，面向网络指挥监控中心大屏环境，具备大数据显示性能以及多机协同管理机制，可良好支持大屏、多屏、超大分辨率等显示情景。

系统支持整合各信息系统数据资源，凭借先进的人机交互方式，实现对网络威胁攻击、网络舆情、网络设备运维数据等信息的可视化监测分析，辅助用户快速识别网络异常情况，全方位感知网络安全态势。

2. 产品功能

2.1. 威胁情报态势显示

2.1.1. 网络威胁态势可视化

支持基于地理信息系统，对全网主机及关键节点的综合安全信息进行可视化监测，可根据网络威胁事件的来源信息和目标信息，对攻击来源、攻击目的、攻击路径进行溯源分析，帮助用户快速发现网络安全隐患，深度分析挖掘网络威胁攻击特征，提升对潜在威胁、未知威胁的预判和主动防御能力。

2.1.2. 网络威胁事件加测

支持集成各类网络检测系统数据，对恶意域名、漏洞攻击、流量异常、僵木蠕毒、DDos 攻击、工控网络、APT 攻击等各类网络威胁事件进行实时可视化监测，对各类网络异常事件进行分级告警，帮助用户快速发现网络安全隐患，更好地防范和抵御网络威胁事件。

2.1.3. 网络舆情可视化

支持与主流舆情信息采集系统集成，对来自境内外各个宣传渠道的敏感信息进行实时监测告警

和可视化分析，支持舆情发展态势可视分析、舆情事件可视化溯源分析、传播路径可视分析等，帮助管理部门第一时间掌握最新舆情态势，以提升管理者对网络舆情的监测力度和响应效率。

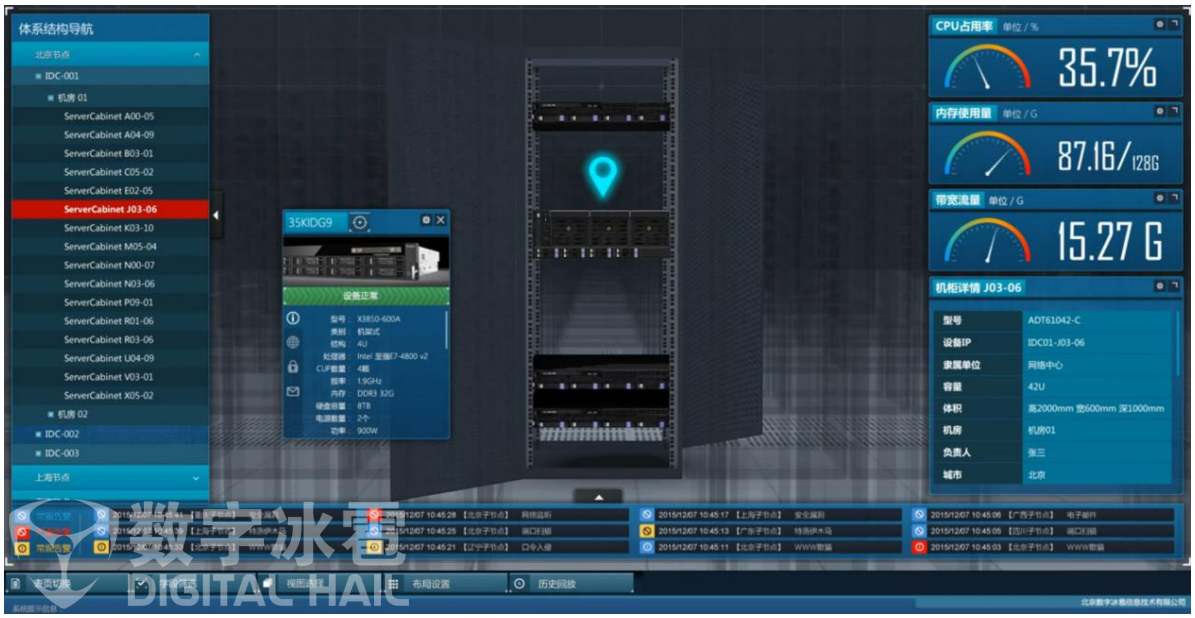
2.2. 网络运维可视化

2.2.1. 建筑环境可视化

支持通过三维建模，对网络中心的外部环境、楼宇外观、机房内部结构、管线进行立体仿真展示，真实完整地展现整个网络中心全景，并可进行点选查询、视点调整及场景切换。

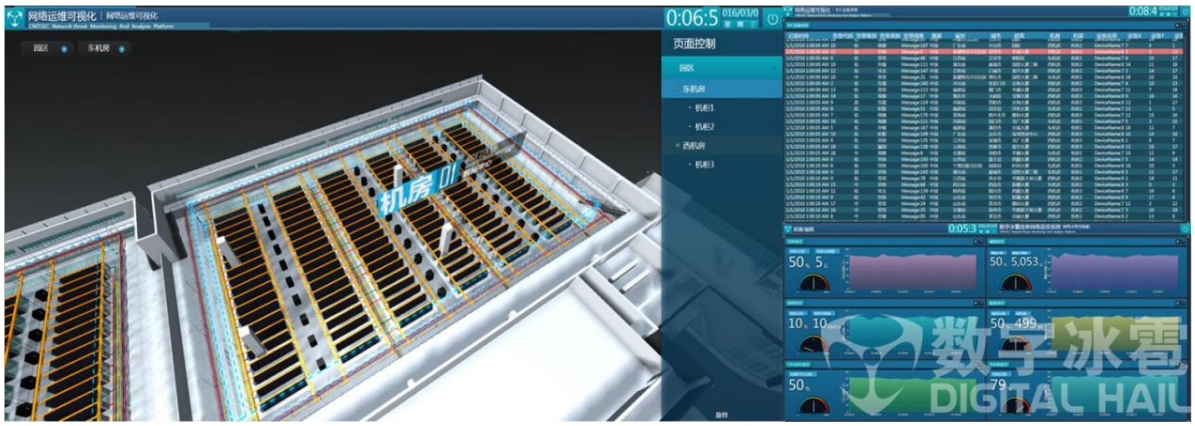
2.2.2. 网络设备可视化

支持对机房内部结构进行三维仿真展示，真实反映现有设备的数量、类型及分布情况。并支持与网络监控、主机监控、存储监控等系统集成，对网络设备运行状态进行实时可视化监测，并可提供点选查询、视点调整等多种交互支持，可下钻查看具体服务器的属性信息，帮助用户更加直观地掌握设备运行状态。



2.2.3. 运维数据可视化

支持与楼控、安防、消防、视频等监控系统集成，为机房运维提供统一的可视化监测平台，对网络中心机房温湿度、电力系统运行状态、机房能耗等运维数据进行实时监测分析，帮助管理者清晰直观地掌握网络中心运营状态，提高运维效率。

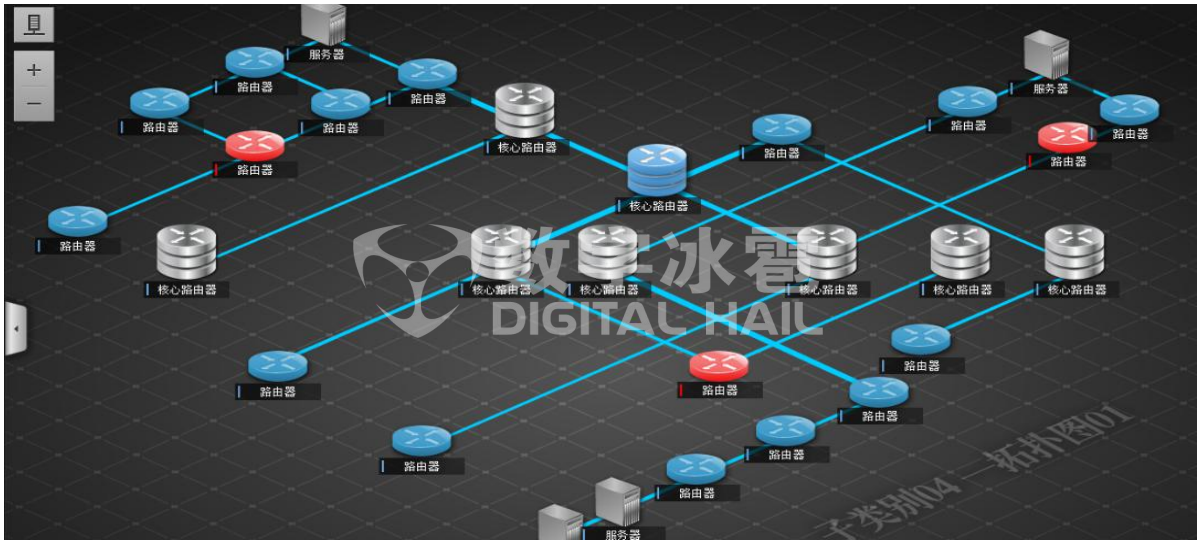


2.2.4. 信息资产可视化

支持与各类 IT 资产配置管理数据库集成，对用户网络运行范围内的信息资产安全状态进行实时可视化监测，并结合 IDS、VDS、防火墙、主机监控等系统运行数据，帮助用户快速发现信息资产安全隐患，加强管理者对信息资产安全态势的监测与感知。

2.2.5. 拓扑层级结构可视化

支持从地理空间分布维度和逻辑层级结构维度，通过多种可视化网络拓扑分析方式，对各网络节点的地域分布、网络状态、业务流量状态等信息进行可视化分析，并对网络异常情况进行可视化告警，帮助用户综合掌控跨地域、大范围网络态势，快速识别网络异常情况。



2.3. 应急指挥调度

2.3.1. 情报监测告警

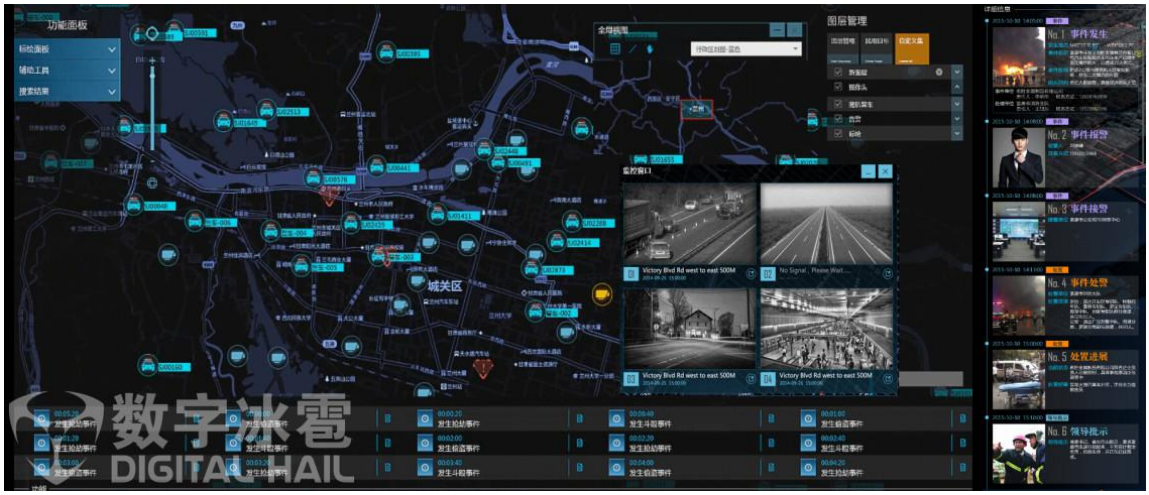
支持整合情报数据资源，基于时间、空间、数据等多个维度为各类网络安全事件建立阈值告警触发规则，自动监控各类网络安全事件的发展状态，进行可视化自动告警。

2.3.2. 突发事件监测

支持接入网络安全监控系统数据 ,对突发网络安全事件进行可视化监测分析 ,并进行态势显示、快速定位，标示事件内容；同时可智能化筛选查看相关网络安全事件，方便指挥人员对突发事件行判定和分析，为事件处置提供决策支持，最大限度降低突发事件的影响，提高用户对突发网络安全事件处理效率。

2.3.3. 可视化通讯指挥

系统支持集成视频会议、远程监控、图像传输等应用系统或功能接口，可实现一键直呼、协同调度多方警力资源，强化管理部门扁平化指挥调度的能力，提升处置突发事件的效率。



2.4. 数据分析研判

2.4.1. 数据分析决策驾驶舱

支持对接网络监管各部门既有海量业务数据，提供统计图表、分布图、关系图、空间统计图、空间分布图、空间关系图等多大类近百种数据可视分析图表，进行多维度分析研判，并支持组合为数据分析驾驶舱进行综合显示，实现多指标数据的并行监测分析，为用户决策研判提供全面的数据支持。

2.4.2. 全时空数据查询分析

支持将多源、异构、海量数据进行时空校准，并按照时间/空间/层级结构等维度进行可视化分析，支持数据实时显示、态势历史回溯，辅助用户全面掌控数据变化态势、深度挖掘运行数据的时空特征及变化规律。

2.4.3. 统计分析决策支持

提供统计图、统计表、单柱图、簇状柱图、堆积柱图、气泡图等多种统计分析视图，支持将海量业务数据的特定指标，按业务需求进行多维度并行分析，并提供上卷、下钻、切片等数据分析支持，可点选查看同一数据指标在不同维度下的分布特征，帮助公安各部门洞悉复杂数据背后的关联关系。

2.4.4. 可视分析决策支持

支持对网络监管各部门既有海量情报数据，基于栅格、聚簇、热图、活动规律等多种可视化分析手段进行可视化分析研判；可与网络安全监管细分领域的专业分析算法和数据模型相结合，助力用户挖掘数据价值，提高决策的能力和效率。

2.4.5. 行业模型算法集成

支持与网络监管管理细分领域的专业分析算法和数据模型相结合，支持计算结果与其他来源数据的融合可视化分析，将现有信息资源与人工智能计算结果进行串并分析，充分利用已有信息化建设成果，为用户提高分析研判、指挥决策效率等方面提供智能化决策支持。

2.5. 多维数据感知

2.5.1. 多类型地图数据融合

支持全球范围多种通用地图数据（如政区图/地形图/卫星图等）接入，支持警用地理信息系统PGIS、天地图等专用地图数据接入；支持加载全球范围高精度高程数据、各类矢量地理要素数据、倾斜摄影数据、无人机航拍数据、大规模城市建筑轮廓数据、精细建筑结构数据等，良好满足用户的应用需求。

2.5.2. 视频监控数据深度集成

支持 GB/T28181 标准，支持深度集成海康、大华、宇视等主流视频平台，并支持综合集成各类视频资源形成统一的视频访问平台，可在二/三维态势地图上标注摄像头对象，并关联其视频信号源，可以通过在地图上点击、圈选等多种交互方式，调取相应监控视频。

2.5.3. 强大的多源数据融合

兼容现行的各类数据源，如 SQL Server、Oracle、MySQL、PostgreSQL、Hadoop 以及仿真引擎等；支持地理信息数据、业务系统数据、视频监控数据接入，实现跨业务系统信息的融合显示，为用户决策研判提供全面、客观的数据支持和依据。

2.5.4. 各类传感器数据融合

支持城市设施中交通无线传感器、温度传感器、压力传感器等物联网传感器数据接入，如道路交通、环境保护、公共安全、楼宇消防、路灯照明管控等众多领域，结合云计算、移动互联网、RFID 等技术手段，实现城市各领域基础设施的状态查看、预测分析和预防性维护，辅助决策人员统筹协调城市资源。

2.5.5. 多业务系统数据融合

支持对接公安、交通、消防、人力社保、财政、城管、规划等多部门现有业务系统，将不同平台系统数据综合汇集于系统之上以进行可视化并行分析，支持高性能实时数据接入、转换、萃取、同步分析显示，为用户决策研判提供全面、客观的数据支持和依据。

2.6. 成果展示汇报

2.6.1. 工作规划展示

支持对网络监管部门预防、制止和打击网络犯罪活动 ,维护网络秩序等工作规划进行详尽展示，运用多种可视化手段对规划方案进行呈现，并对主要规划指标进行分析，多角度展示网络监管各部门工作规划内容。

2.6.2. 工作成果展示

支持聚焦网络安全维稳工作领域，运用影视级的可视化渲染技术，对网络安全监管重要指标及成果进行全面、清晰、高效地展现，宏观体现网络安全监管工作成果。

2.6.3. 重点项目展示

支持网络安全监管、打击等重点工作进行展示，对项目信息、计划、预案部署、成效等内容进行可视化呈现，突出网络监管重点项目建设成果和关键指标。

2.6.4. 重要事件复现

支持重点事件的态势回溯，对事件起因、发展过程、处置结果等信息进行直观展示，辅助用户对重要事件进行分析、展示、比较、推理、判断。

2.7. 大屏环境支持

2.7.1. 超高清小间距显示大屏

为指挥中心量身打造超高清小间距 LED 大屏显示解决方案，支持无缝、无边框、无限拼接，可自定义整屏尺寸，任意分辨率下，画面显示效果精准完整；具备低亮高灰技术内核，画质细腻流畅，观看舒适；亮度智能调节，满足多种室内环境应用场合；超宽视角（水平/垂直均 160 度），任意角度良好显示；超高刷新率，纳米级响应速度；安全低噪、稳定耐用，为用户提供超凡的大屏使用体验。

2.7.2. 专业操控席位定制

可针对指挥中心复杂场景设计定制，打造结构合理、科学布局、符合人体工程学设计的专业操控席位。支持指挥决策、信号调用、会议室系统切换、音视频播放、灯光环境管控、远程互动等工作的远端集中控制，大幅度提升系统的易用性，为用户提供定制、便捷地交互体验。

2.7.3. 大屏超高分辨率输出

支持超高清、无形变、无限分辨率的大屏图像输出，系统输出分辨率与大屏物理分辨率一致，

实现超高分辨率点对点(无形变)图像输出;结合产品自有的集群并行渲染机制,支持无限分辨率显示输出和动态扩展。真正发挥大屏硬件显示潜能，构建超高清的大屏综合态势监测系统。

2.7.4. 大屏矩阵控制集成

深度集成主流大屏控制技术，支持大屏整体显示布局切换、超高分辨率画面无缝切换、多屏联动数据分析、多屏显示内容联动交互控制、单屏显示内容操作控制等，充分满足用户的使用需求。

2.7.5. 一体化交互控制台

原生支持大屏多屏交互联动控制，支持席位、电子沙盘、手持/固定触控终端等多种控制设备，具备单点主控、集群联动的一体化操作模式，通过统一的控制终端，轻松对多屏显示内容集中控制，如主题切换、分析态切换、可视化对象浏览、点选、筛选、圈选、地图平移放缩等功能。

多种交互设备支持

3. 配套服务

3.1. 完善的实施团队，全流程跟踪服务

全方位自有技术团队，能力全面，深谙数据可视化技术特性，具备行之有效的方法体系，确保项目实施高效、品质可靠；公司拥有十余年项目实施经验，既横跨众多行业，又高度专注于数据可视化分析决策领域，为用户提供大量可借鉴经验，助力用户在更高起点对自身系统进行规划建设；设计师、工程师黄金配比，提供从规划设计、制作实施、定制开发到联调测试一站式全流程服务；拥有先进的产品体系和交付能力，良好的业界口碑，帮助用户驾驭数据、彰显价值！

3.2. 全配置式架构，个性化定义主题

全自主可控技术体系，可根据用户的实际业务决策需求，进行可视决策主题、可视化页面风格标识、可视化对象、组件、人机交互等深度定制。具备模块化、全配置式软硬件架构，可视决策主题、可视化页面、可视化对象均可复用可调整可扩展，可充分应对未来业务需求变化，为系统未来扩展维护提供坚实保障。

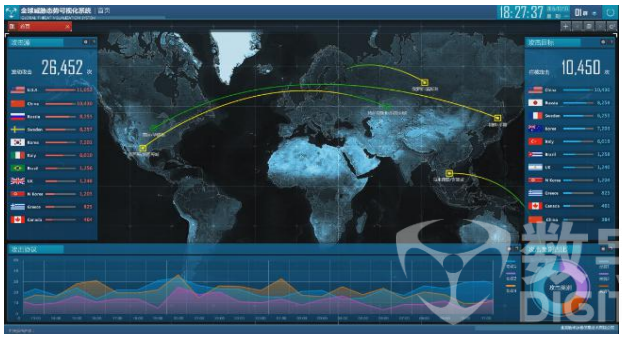
3.3. 可交付编辑工具，未来扩展灵活

可提供一系列可视化编辑工具，地图风格、模型对象、空间对象、场景对象、可视化组件、可视化应用均可实现自定义配置；图形化交互界面，操作简单直观，易于掌握；具备完备的地图效果配置、强大的数据驱动定义能力、广泛的空间对象支持、强大的组件样式配置、丰富的可视化基础页面库，可根据未来业务变化进行灵活调整；可预置丰富的业务数据分析可视化组件，配置结果所见即所得，可快速构建出样式出众、灵活、功能强大的可视化应用。

4. 产品优势

4.1. 全方位网络态势感知

从全网整体安全态势，到数据中心 3D 呈现，再到信息资产以及安全数据的监测，系统支持从地理空间分布、逻辑拓扑层级结构 ,并行对全网主机和关键节点的综合安全信息进行网络态势监控。



4.2. 助推网络安全主动防御

通过采集全网流量数据，对网络安全事件情报进行智能分析和联动响应，帮助用户把握网络安全事件发展趋势，为安全决策、应急响应以及威胁事件的主动防御提供有力支持。

4.3. 扁平化指挥高效响应

通过指挥中心大屏即可全面监测网络态势、应急资源分布等，并提供强大的可视化通讯指挥支持，可一键调度多方应急资源，实现威胁事件“一站式”流转，提升处置突发事件的效率。

4.4. 系统整合协同防御

能够将用户网络安全防御体系中防火墙、UTM、IPS、防病毒等各个组件信息充分整合，充分发挥各安全设备的整体效能，大幅提升用户网络整体安全防御能力。

4.5. 全时空态势分析研判

支持将情报数据按照时间维度和空间维度进行可视分析，满足用户实时监控、历史回放、模拟推演等应用情景的需求，辅助情报监测人员全面掌控数据变化态势，进而网络安全事件分析研判的能力和效率。