

COMPANY



盈高科技  
**公司介绍**

杭州盈高科技有限公司 | 构建安全 健康 和谐的网络世界

[www.infogo.com.cn](http://www.infogo.com.cn)

4008-073-883



# 前言

“不谋全局者，不足谋一域”。

我们以网络准入微观切入，最终聚焦于整个信息世界的秩序。

运行有序，信息管理方以微力可以敌万军之侵。

秩是有条理，不混乱。序是有主次，不颠倒。

通过秩序建立稳定的具有延续性的运行态势。

我们做的是在信息世界的源头——终端建立一种良好的秩序，

以实现信息的安全顺畅流通。

万物有序方和，和则通，通则达。

# 目录

## CONTENTS

01 | COMPANY PROFILE  
公司介绍 01—10

02 | PRODUCTS  
产品介绍 11—24

03

CASES

典型案例

25—64

04

THANK-YOU LETTER

感谢信

65—68



# 公司介绍

COMPANY PROFILE



扫码查看详细公司介绍

# BUSINESS SERVICE SYSTEM

## 业务服务体系

### 盈高科技

成立于2006年

总部设在杭州

杭州、长沙两大研发中心

业务涉及接入边界安全、终端环境安全、数据安全、应用系统安全等领域, 包含网络准入、零信任、终端安全管理、杀毒、数据摆渡等安全产品。

营销服务体系已覆盖**31**个省级行政区。



# DEVELOPMENT HISTORY

## 盈高科技发展历程





# MAIN HONORS

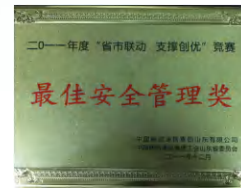
## 主要荣誉

国家级  
专精特新“小巨人”

准入控制行业  
标准制定者

连续13年  
网络准入控制  
市场占有率第一

- ▶ 国家高新技术企业
- ▶ 国家科技型中小企业
- ▶ 国家级专精特新“小巨人”企业
- ▶ 浙江省杭州市重点拟上市企业
- ▶ 浙江省软件核心竞争力企业
- ▶ 浙江省高新技术企业研究开发中心
- ▶ 浙江省信息安全标准化技术委员会单位委员
- ▶ 中国网络安全行业百强企业
- ▶ 中国保密协会会员单位
- ▶ 中国网络安全产业联盟成员单位
- ▶ 参与公安部准入控制行业标准制定
- ▶ 参与国家信息中心计算机终端核心配置国家标准制定
- ▶ 入选杭州市国际级软件名城创建项目



- ▶ 入选“瞪羚企业”
- ▶ 2017年厦门金砖峰会网络安全保障支撑单位
- ▶ 2018年青岛上合峰会网络安全保障支撑单位
- ▶ 完成国家发改委产业化示范工程
- ▶ 完成国家科技支撑计划
- ▶ 中国电子政务安全领域优秀服务商
- ▶ 电力企业信息化最佳合作伙伴
- ▶ 网络准入控制产品用户综合评价第一(数据来源于安在)
- ▶ 中国政企数字化网络安全企业50强
- ▶ 信创产业独角兽100强
- ▶ 荣获云安全联盟“2023安全金盾奖”
- ▶ 湖湘杯网络安全技能大赛技术支撑单位
- ▶ 湖南省网络安全优秀服务商



# PATENTS FOR INVENTIONS

## 发明专利

- ▶ 一种信息系统内网安全统一管理平台及管理方法
- ▶ 一种网络设备准入方法
- ▶ 一种ARP准入控制方法
- ▶ 一种SDN环境下的虚拟机风险快速隔离方法
- ▶ 一种快速的HTTP重定向方法
- ▶ 一种网络安全检测方法及装置
- ▶ 一种快速识别介入摄像头的系统及方法
- ▶ 一种违规外联检测方法及装置
- ▶ 一种实现用户和/或终端与SSID绑定的认证系统及方法
- ▶ 涉密文件检查方法及装置
- ▶ 终端设备的网页认证方法、装置、存储介质及处理器

- ▶ 数据处理方法及装置
- ▶ 网页标识信息的共享方法、装置、存储介质及处理器
- ▶ 一种数据流量监测分析方法
- ▶ 访问请求的重定向方法、系统、装置以及存储介质
- ▶ 涉密计算机显示图像光学控制装置
- ▶ 一种负载均衡设备
- ▶ 一种指纹识别装置
- ▶ 用于涉密审计的存储装置与涉密打印审计系统
- ▶ 实现相同子网不同VLAN的终端设备之间通讯的系统
- ▶ 思科环境下的网络准入控制系统
- ▶ 移动设备上的APP管理方法及装置



# 产品介绍

PRODUCTS



扫码查看详细产品介绍

# ACTIVE DEFENSE

## 以“强身健体”为本的主动防御

对于网络安全建设来说,与其先紧盯外部威胁,不如先强健自身安全。多年来,盈高科技一直在做的就是以“终端”为基础细胞单位,通过不断创新与扩充的终端安全产品体系,为客户打好网络安全健康根基,拥有主动防御内外威胁的能力,以更小的安全投入,收获更大的安全价值。这与美国系统网络安全协会提出的网络安全滑动标尺模型的理念不谋而合。

【SANS Institute:网络安全滑动标尺】



# PROTECTIVE SYSTEM

## “一体四驱”终端安全防护体系

在现代化网络安全建设中，“强身健体”是一个系统性的工程，包含多种层层递进的防护机制。盈高科技的“一体四驱”终端安全防护体系以此为理论基础，用一体化客户端和一体化平台管理，承载四层安全防护能力，为客户构建一个囊括“边界安全接入、终端安全管理、业务安全访问、数据安全流转”等价值于一体的“强身健体”方案，保障终端入网-在网-业务访问-数据流转等过程中的全方位安全。

### 统一终端安全运营平台

#### 终端入网-接入边界安全

<b>ASM 入网规范管理</b>
网络准入控制
人员身份认证
终端安全检查
资产智能识别
<b>IPAM IP地址管理</b>
流程化IP管理
自动化IP配置
可视化IP展示

#### 终端在网-终端环境安全

<b>MSEP 终端安全管理</b>
终端安全基线
软件标准化管理
终端外设管控
终端故障自愈
<b>TAM 终端防病毒系统</b>
终端威胁检测
终端威胁响应

#### 业务访问-应用系统安全

<b>i-ZTP零信任访问控制</b>	
业务安全收编	业务代理隐身
动态访问控制	安全工作空间
接入运维一体化	全链行为审计
<b>ISA盈高视频网空间资产测绘系统</b>	
资产智能感知	视频网脆弱性检测
视频图像故障感知	数据可视化看板

#### 数据流转-终端数据安全

<b>M-DLP 终端数据防泄漏</b>
敏感数据检查
文件外发管控
数据水印管理
<b>DFS 跨网数据安全交换</b>
敏感文件检查
跨网数据安全交换

数据融合  
能力协同

### 一体化客户端融合

# 盈高入网规范管理系统 (ASM)

违规不入网, 入网必合规

水至清则无鱼, 网至“清”则无毒



## 连续13年

保持网络准入控制行业市场占有率第一

## Gartner最先进的

第三代准入控制Appliance-Based NAC

## 标准制定者

参与公安部准入控制行业标准制定

## 用户口碑第一

准入控制产品用户综合评价第一

## 国内第一套

无客户端网络准入控制系统

## 国内第一套

单项目管理超100万终端的网络准入控制系统

# 盈二零信任访问控制系统 (ZTP)

全网统一信任接入, 让混合办公更简单更安全

基于软件定义边界 (SDP) 和终端安全技术构建的**统一安全接入一体化平台**, 摒弃传统的边界观念, 遵循“**永不信任**”的理念, 对每个访问请求都进行严格验证, 在不可信的网络环境中实现访问企业资源和数据时的安全、可信、高效。

## 全面安全

统一内外网接入安全, 覆盖接入、身份、终端、运维、数据和审计六大环节。

## 极致体验

统一的客户端、统一的管理平台, 提供优异的接入体验、操作体验、连接体验和管理体验。

## 高效落地

混合办公场景无忧部署, 产品快速交付落地, 且支持盈高ASM自动升级为全网统一接入。

## 广泛应用于以下场景

### 混合接入办公

许多企业已经逐渐形成在场办公与在线办公相结合的混合办公模式, 而这可能带来在外接入网络安全风险高、远程接入办公不稳定、运维管理不便利等一系列问题。

### 远程运维

运维人员通过远程软件进行运维时, 缺乏身份认证、访问控制、操作审计等措施, 通过VPN搭配堡垒机运维则成本高, 难以做到最小化权限控制。

### 使用专业VPN设备进行远程办公

使用专业VPN远程接入访问业务系统时, 可能因为直接暴露网关而招致攻击, 并且用户风险行为不可控, 远程终端难统一管理。

### 使用非专业VPN设备进行远程办公

用户使用非专业VPN设备远程接入时, 不仅容易为业务系统招致风险, 而且性能受限, 体验不好, 满足不了许多业务需求。

### 移动办公

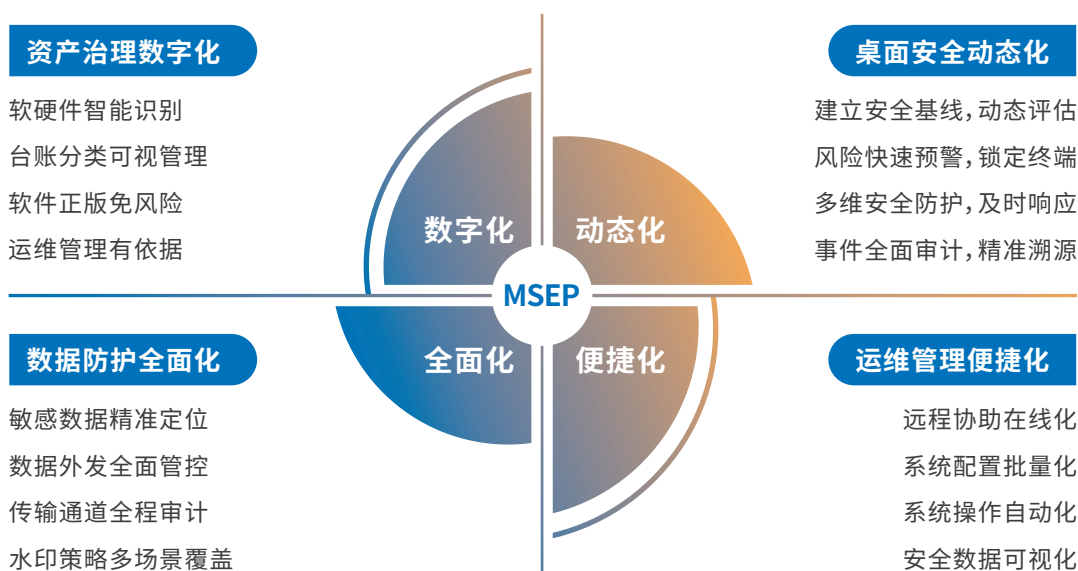
员工通过手机、Pad等进行移动办公时, 容易让端口暴露互联网, 并且难以管理用户权限, 也无法保证数据传输中的安全。

### 数据安全保护

员工从业务系统上下载数据落地后, 可能由于终端的不安全或者个人的安全意识薄弱, 导致数据的泄露, 并且远程接入中的数据的安全不受管控。

# 盈高多维终端安全管理平台 (MSEP)

更智能的资产治理及终端运维工具



## 杜绝版权法律风险

基于软件指纹识别、软件残留信息清理技术, 彻底解除企业软件版权风险。

## 净化终端办公环境

基于软件安装行为识别、软件无感知管理技术, 帮助企业打造简洁、高效的终端办公环境。

## 安全与方便, 两全其美

自动化风险识别, 轻量化数据防护方案, 不改变用户习惯, 不影响用户办公, 最小成本保障数据安全。

## 客户端流程化部署

自带网络准入技术, 引导式客户端部署, 比传统桌管软件减少90%的时间成本。

## 一平台, 全管控

MSEP、ASM、AV产品融合方案一个客户端保障网络、终端、杀毒全管控。

## 轻量级客户端

模块按需动态加载技术, 与传统桌管软件相比, 少占用50%的性能资源。

# 盈高主机监控与审计系统

打造信创终端一体化安全管控平台



面向国产化终端的安全防护，  
满足国家分级保护的管理要求



适配各类国产软、硬件平台，  
以及各类新老版本国产化操作系统



对终端用户行为、终端系统状态、  
终端网络行为等进行全面监控审计



提供全方位、多层次、立体化的  
安全保障

# 盈高白羽·一站式终端健康监护平台

无感知安全·自愈式运维

新一代终端安全管理系统

通过故障自愈技术和终端安全定格技术，实现“自愈式运维”和“无感知安全”



行业场景定制  
精准满足需求

自愈式运维  
减少70%初级故障

无感知安全  
终端管理轻松落地

# 盈高终端防病毒系统(TAM)

轻量级防护·智能式安全

集系统防护、多通道入口防护、文件实时防护等功能于一身，

拥有**业界独有**的未知威胁监测能力，**专业适配办公网场景**，

自主研发的启发式检测引擎及智能检测引擎，具备**业界领先的勒索挖矿专防专杀能力**，

同时还有补丁漏洞修复、外设管控、多行为审计、违规外联检测与阻断等主机安全能力。

## 四大核心亮点，全生命周期终端防护



## 广泛应用于以下场景

### 办公网终端防病毒场景

在程序执行、文件创建与修改、浏览器/邮件下载保护、文档浏览时提供全面的保护。

### 勒索、挖矿病毒防御场景

帮助用户及时发现并清除恶意程序与文件，为用户建立勒索挖矿“预防—监测—阻断”于一体的纵深防御方案。

# 盈高大禹·数据摆渡系统(DFS)

存转一体, 流转自治, 让文件安全管理更简单

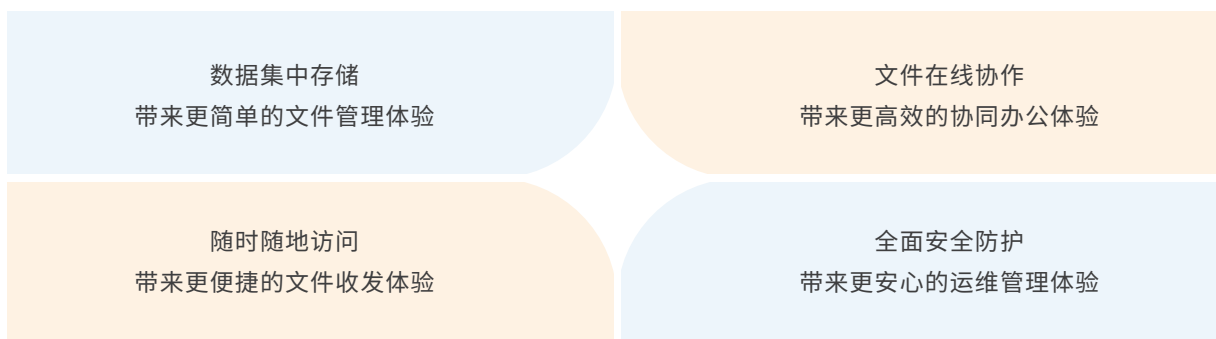
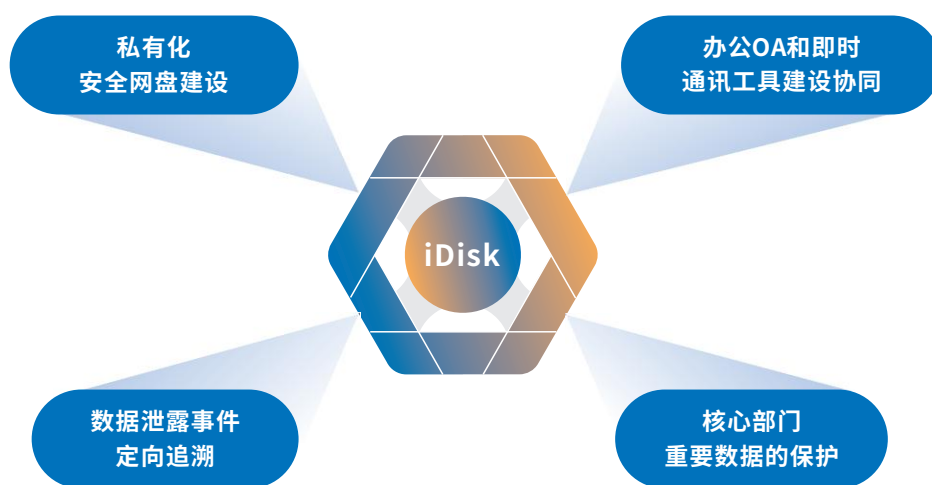
专为多网隔离、重要文件分散存储、跨网文件交换频繁的用户打造  
文件安全摆渡通道和文档协同共享平台集于一身



盈高大禹·数据摆渡系统采用软件定义边界技术理念, 运用存储分片加密、虚拟安全磁盘、可视化流程审批、在线文档协同等技术, 为文件的存储、使用、跨网摆渡、外发、传输进行全流程安全管理, 解决跨网文件交换难审计、终端文件分散难管控、文件管理安全与便捷难两全等问题。

# 盈高企业安全网盘 (iDisk)

数据安全集中管理与文档协同共享平台



# 盈高IP地址管理系统 (IPAM)

重新定义IP资源管理



盈高IP地址管理系统, 是针对IP管理实际工作中遇到的问题, 专门研发的一款IP地址管理工具。从IP地址的规划、分配、使用、回收等四个维度切入, 通过电子化、自动化、信息多元化的IP地址管理模式, 提高IP地址的管理工作效率, 节省时间及人力成本, 提高数据资产安全性, 实现IP地址的全生命周期数字化管理。

# 盈高视频网空间资产测绘系统 (ISA)

## 视频网资产安全可视化管理

盈高视频网空间资产测绘系统 (ISA), 专为各行各业视频网管理打造, 集安全感知、安全检测、安全响应、安全处置于一体, 形成视频网资产管理和威胁管理的双重闭环, 一方面实时监控视频网终端资产使用情况, 保障业务可持续性; 一方面持续监测分析视频网安全威胁并进行智能化处置, 快速识别并化解安全风险, 实现“可感知、可防控、可研判”的视频网终端安全可视化管理。

### 快速感知全网视频资产

- ▶ 检测各种视频前端设备、NVR设备和物联网设备
- ▶ 检测各种品牌、型号的摄像头设备
- ▶ 快速建立有效的摄像头资产台账
- ▶ 对摄像头被非法替换/仿冒/下线等风险进行检测、识别和阻断;

### 视频网脆弱性检测

- ▶ 对摄像头存在的弱口令、高危端口进行检测
- ▶ 对摄像头、NVR等产生的异常流量进行检测防止访问入侵
- ▶ 视频服务器业务瓶颈, 业务宕机, 业务运行状态第一时间感知

### 视频图像故障感知

- ▶ 超过10种图像特征识别算法
- ▶ 支持轮询式探测遮挡、黑白、模糊等视频图像问题
- ▶ 支持实时发现关键区域的物理攻击 (恶意遮挡、恶意移动)

### 数据可视化看板

- ▶ 安全威胁趋势
- ▶ 视频业务系统运行态势
- ▶ 全网告警分布
- ▶ GIS大图风险感知及指挥
- ▶ 实时风险滚动

#### 一快

**发现快:** 摄像头发现速率达20000路/小时, 多分支采取探针级联管控, 极限提速

#### 二准

**识别准:** 准确识别摄像头、红绿灯、抓拍机等90多类终端, 精确识别IPC终端, 识别准确率100%

**定位准:** 一键定位终端所在交换机端口, 通过GIS地图精确定位终端的地理位置

#### 三多

**可识别品牌多:** 支持海康、大华、宇视、天地伟业等主流品牌设备识别

**可识别种类多:** 可识别NVR、DVR、电子卡口、人脸识别、电子警察、设备箱等30余种IoT终端类型

**检测项多:** 除20余种基础检测项外, 还能够实现10余种视频摄像头的专属检测

#### 四强

**技术强:** 采用大数据分析, 自研视频质量检测算法

**兼容强:** 不改变拓扑结构, 探针扩展, 无限级联

**性能强:** 单机支持40G流量, 单个项目服务20万终端

**服务强:** 30个省市售后服务中心, 7×24小时响应



国家电网公司  
STATE GRID



中国国电

deli  
得力集团



中国兵器工业集团公司

华州



# CASES



中国一重

## 典型案例



沙钢集团  
SHAGANG GROUP

航空工业集团公司



ANSTEEL  
鞍钢集团



三门核电  
MNP/C



国家电网公司  
STATE GRID

## 政府行业案例

- 法院案例
- 税务案例
- 数据局案例

## 企业行业案例

## 医疗行业案例

## 电力行业案例

## 能源行业案例



扫码查看详细案例介绍

# GOVERNMENT 政府行业

## 5000+政府客户的信赖首选

- 国家统计局
- 国家发展和改革委员会
- 国家外汇管理局
- 国家中医药管理局
- 国家药品监督管理局
- 国家旅游局
- 国务院国有资产监督管理委员会
- 国家自然科学基金委员会
- 中国银行业监督管理委员会
- 中国交通通信信息中心
- 中国地震台网中心
- 中国福利彩票发行管理中心
- 北京市委办公厅
- 广东省委办公厅
- 浙江省委办公厅
- 江苏省委办公厅
- 湖南省委办公厅
- 福建省委办公厅

▲ 以上为部分客户名单,排名不分先后

- 
- 河北省委办公厅
  - 山东省委办公厅
  - 山西省委办公厅
  - 陕西省委办公厅
  - 黑龙江省人民政府
  - 内蒙古自治区人民政府
  - 江苏省人民检察院
  - 陕西省人民检察院
  - 山东省人民检察院
  - 湖南省人民检察院
  - 浙江省监狱管理局
  - 广东省公安厅
  - 广东省审计厅
  - 湖南省财政厅
  - 福建省交通厅
  - 安徽省自然资源厅
  - 河北省自然资源厅
  - 浙江省自然资源厅

# GOVERNMENT

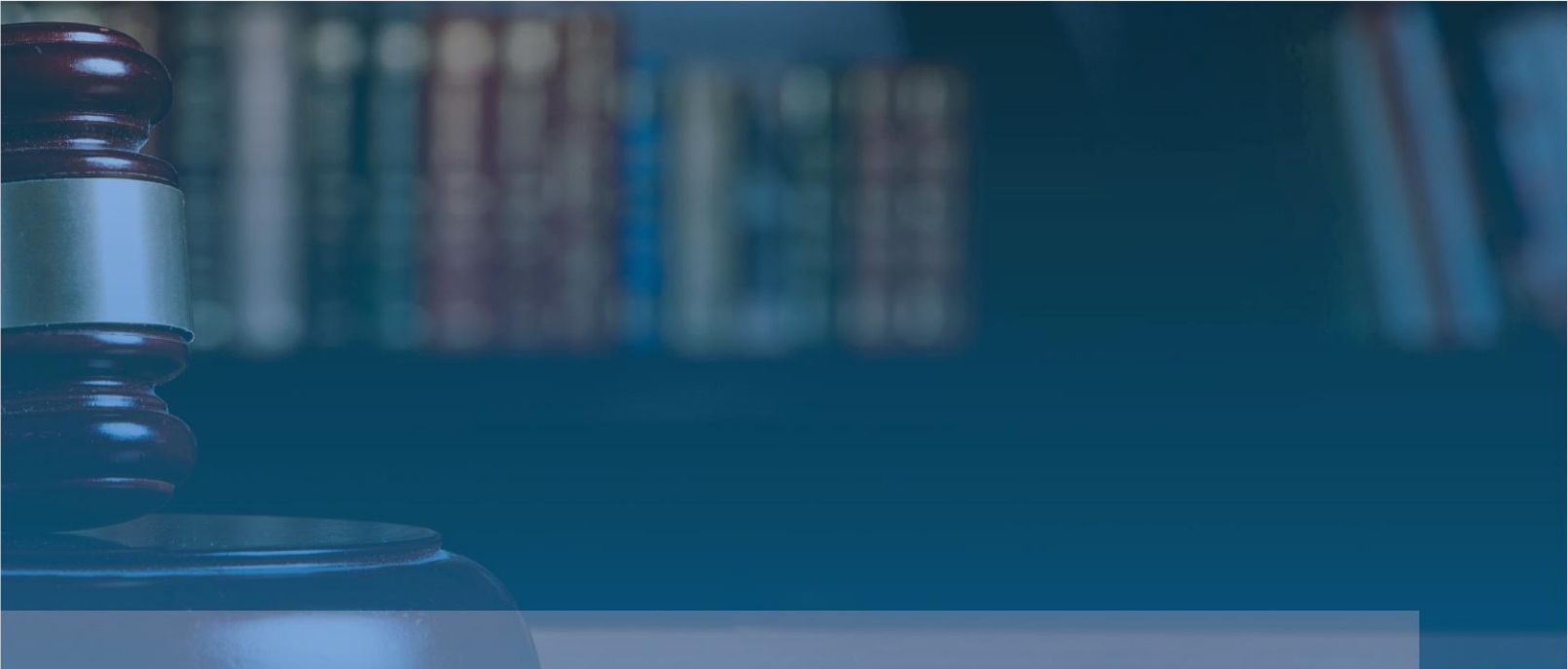
## 政府行业 → 【法院案例】

### 法院客户已遍及21个省级行政区域

#### 北京、上海、湖南、吉林4省/直辖市法院全覆盖

- 北京市高级人民法院(全市)
- 上海市高级人民法院(全市)
- 湖南省高级人民法院(全省)
- 吉林省高级人民法院(全省)
- 江苏省高级人民法院
- 湖北省高级人民法院
- 陕西省高级人民法院
- 北京市第一中级人民法院
- 北京市第二中级人民法院
- 北京市第三中级人民法院
- 北京市第四中级人民法院
- 上海市第一中级人民法院
- 上海市第二中级人民法院
- 上海市第三中级人民法院
- 广州市中级人民法院
- 苏州市中级人民法院
- 太原市中级人民法院
- 长沙市中级人民法院
- 长春市中级人民法院
- 宁波市中级人民法院
- 南通市中级人民法院
- 台州市中级人民法院

▲ 以上为部分客户名单,排名不分先后



- 张家界市中级人民法院
- 常州市中级人民法院
- 包头市中级人民法院
- 常州市中级人民法院
- 淮安市中级人民法院
- 抚顺市中级人民法院
- 汉中市中级人民法院
- 焦作市中级人民法院
- 舟山市中级人民法院
- 株洲市中级人民法院
- 湘潭市中级人民法院

- 衡阳市中级人民法院
- 常德市中级人民法院
- 怀化市中级人民法院
- 娄底市中级人民法院
- 永州市中级人民法院
- 岳阳市中级人民法院
- 邵阳市中级人民法院
- 郴州市中级人民法院
- 湘西州中级人民法院
- 揭阳市中级人民法院
- 西宁市中级人民法院

# GOVERNMENT 政府行业 → 【税务案例】

## 保障300+家税务客户内网安全

### 浙江、湖南税务实现全地市覆盖；江苏、河南税务实现超70%地市覆盖

- 国家税务总局浙江省税务局
- 国家税务总局湖南省税务局
- 国家税务总局湖北省税务局
- 国家税务总局辽宁省税务局
- 国家税务总局杭州市税务局
- 国家税务总局厦门市税务局
- 国家税务总局保定市税务局
- 国家税务总局武汉市税务局
- 国家税务总局长沙市税务局
- 国家税务总局西安市税务局
- 国家税务总局沈阳市税务局
- 国家税务总局哈尔滨市税务局
- 国家税务总局南京市税务局
- 国家税务总局开封市税务局
- 国家税务总局株洲市税务局
- 国家税务总局泉州市税务局
- 国家税务总局汕头市税务局
- 国家税务总局潜江市税务局

▲ 以上为部分客户名单, 排名不分先后



- 国家税务总局常州市税务局
- 国家税务总局南通市税务局
- 国家税务总局无锡市税务局
- 国家税务总局徐州市税务局
- 国家税务总局扬州市税务局
- 国家税务总局镇江市税务局
- 国家税务总局绍兴市税务局
- 国家税务总局台州市税务局
- 国家税务总局温州市税务局
- 国家税务总局湖州市税务局
- 国家税务总局金华市税务局
- 国家税务总局宁波市税务局
- 国家税务总局平湖市税务局
- 国家税务总局义乌市税务局
- 国家税务总局南阳市税务局
- 国家税务总局黄石市税务局
- 国家税务总局眉山市税务局
- 国家税务总局湘潭市税务局

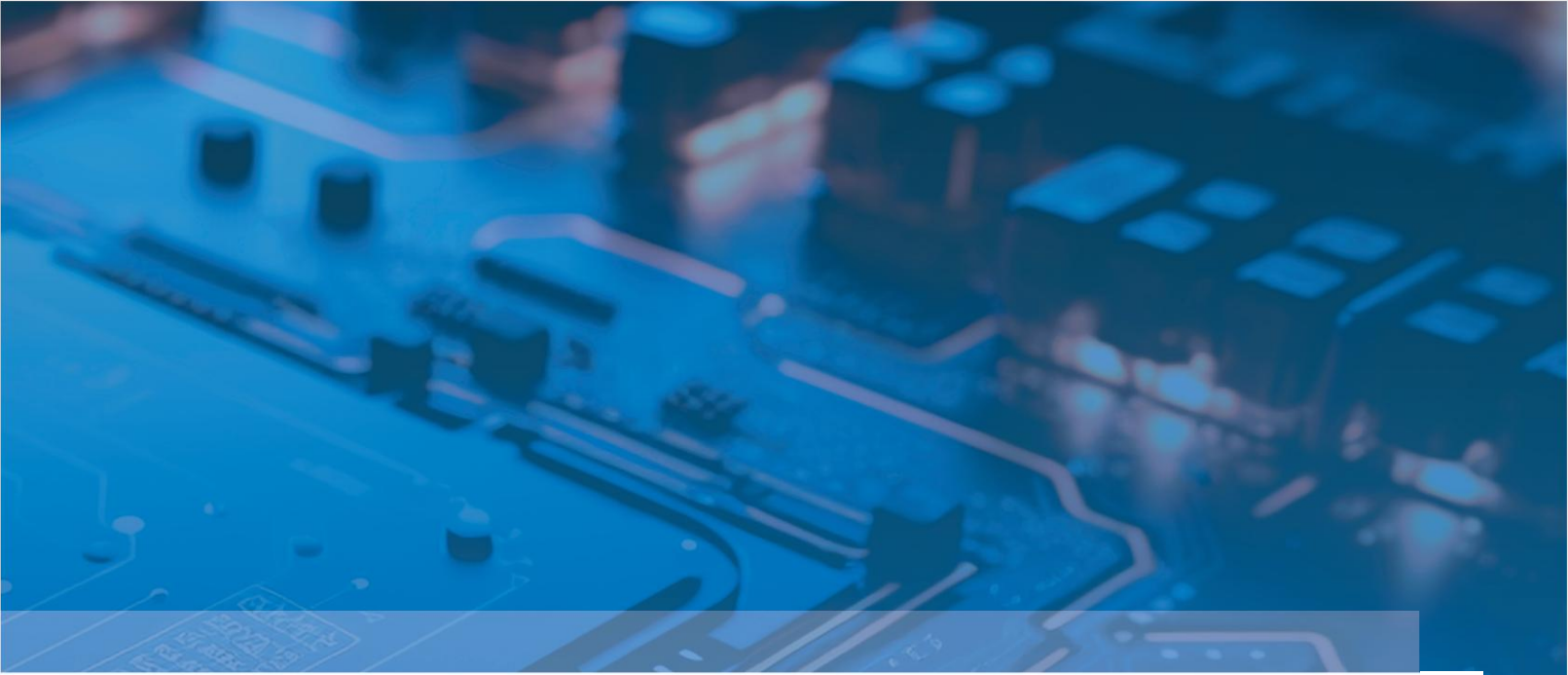
GOVERNMENT

# 政府行业 → 【数据局案例】

## 数据局客户已涉及12+个省份

- 南通市数据局
- 丽水市数据局
- 杭州市拱墅区数据资源管理局
- 石家庄市数据资源管理局
- 湖州市安吉县大数据发展管理局
- 余姚市大数据发展管理局
- 海安市数据局
- 启东市数据局
- 衢州市衢江区大数据中心
- 江门市政务服务和数据管理局
- 江山市大数据中心
- 深圳市盐田区政务服务和数据管理局
- 惠州市博罗县政务服务和数据管理局
- 武汉市武昌区电子政务信息中心
- 佛山市三水区政务服务数据管理局
- 鹤岗市萝北县政府信息化中心
- 长春市宽城区政务服务和数字化建设管理局
- 威海市大数据局

▲ 以上为部分客户名单,排名不分先后

- 
- 潍坊市大数据局
  - 高密市大数据中心
  - 潍坊市昌乐县大数据中心
  - 潍坊市奎文区大数据局
  - 潍坊市综合保税区大数据中心
  - 潍坊滨海经济技术开发区统计和大数据局
  - 南阳市卧龙区政务中心
  - 温州市永嘉县大数据管理中心
  - 武冈市人民政府信息中心
  - 长沙市数据局
  - 长沙市芙蓉区数据资源中心
  - 宁乡市数据资源中心
  - 张家界市人民政府发展研究中心
  - 衡阳市数据局
  - 石城县政务服务和大数据发展中心
  - 汉川市政务服务和大数据管理局
  - 武汉市洪山区大数据中心
  - 扬州市邗江区大数据管理局

# 北京市高级人民法院

## 客户简介

北京市高级人民法院是北京市行政区域内的最高审判机关,依据宪法等法律规定行使国家审判权。北京市最高人民法院十分重视网络信息化的建设。随着信息安全面临新形势新要求,北京高法在网络管理和终端安全方面,亦面临新挑战。

## 客户需求

如何做到全无盲点的网络准入控制,对终端和人员进行身份认证。

如何与现有的认证系统进行统一联动,实现对入网人员身份的确认。

如何保证终端安全性,做到杀毒软件的100%安装。

## 解决方案

本方案采用盈高的一体化终端安全管理平台,通过在法院内网部署ASM入网规范管理系统,基于虚拟网关(MVG)准入控制技术打通清晰的入网流程,应用于北京市高级人民法院下辖各中级人民法院和各区、县人民法院近20家,法院核心网络涉及终端数千台,确保全网终端、人员身份明确,保障使用安全。

## 方案价值



通过设备注册，可以查看到所有终端的使用者、部门、物理位置等，方便了维护人员的终端管理工作。



通过与现有的认证服务器联动，进行终端使用人员身份认证，保障了终端使用人员的合法化。



入网终端统一进行杀毒软件的安装，对未安装杀毒软件的终端将会进行统一安装，终端安检合规后方可访问网络，提高了整网安全性。

# 国家税务总局湖南省税务局

## 客户简介

国税、地税机构合并后，湖南省税务局终端数量暴增，管理难度加大，原有管理体系中的终端接入安全、基线安全等问题急需解决，如哑终端仿冒替代、终端非法接入、安全基线不统一等。

## 客户需求

确保接入内网的终端和人员是经过授权的、安全可信的。

需要保证必装软件的安装率，并对不符合条件终端进行实时智能修复。

需要对全网实现透明可视化管理，包括网络中的设备类型、设备数量、设备接入位置、终端安全状态、哑终端等全类型资产。

## 解决方案

通过在省、市、区县进行ACMS统一管理平台、ASM入网规范管理系统、ASC准入控制器三级级联部署，既可实现终端准入集中管控，数据统一，也可实现分级管理，灵活把控。

## 方案价值

建设全省的统一接入认证平台,实现对省市县三级税务网络终端接入的统一平台化管理



不管是PC终端、哑终端还是国产化终端,都必须通过准入系统的审核方可安全入网。



在全省税务终端范围内,提高了桌管软件及杀毒软件的安装率,保障终端安全性合规性。



对工作人员和访客人员的入网权限及资源访问权限进行精细化控制,禁止越权跨域访问。



远程维护功能、IP地址池管理、IP/MAC自动绑定等功能,大大提高了运维工作效率。



边界管理更清晰,防止了NAT、HUB等私接设备接入。



自动发现终端、采集信息并分类管理,实现更全面可视化的资产管理。

# 石家庄市数据资源管理局

## 客户简介

石家庄市作为河北省的省会，数字化发展进程推进得十分迅速，建设了大量信息化系统，并以“整体协同、集约高效、按需服务”为原则打造了全市一体化智能化云平台，让百姓们享受到更高效便捷的政府服务，真正响应了习总书记说的“推动信息化，更好造福社会、造福人民”。石家庄市数据资源管理局为保障政务外网安全平稳运行，需通过一定手段，使市、县两级政务外网中的所有终端接入可控、安全入网、合规运行、台账可视、风险可阻。

## 客户需求

- ▶ 政务外网使用人员众多，需要能够通过一定手段，控制人员接入风险；
- ▶ 接入终端数以万计，需要保证入网终端的安全性，一旦有非法终端企图入网，要能立即发现并阻止；
- ▶ 接入政务外网的终端资产数量多、种类杂且变动频繁，需要通过智能化管理代替人工管理，以保证资产信息的准确性与全面性；
- ▶ 政务外网实行分级管理，所以在准入项目建设中，既要保证市县两级的自主管理，又要满足市级中心对整体入网安全的统筹掌控。

## 解决方案

一方面，在市、县两级横向网分别部署盈高ASM入网规范管理系统，两级政务外网管理部门可根据需求，自行负责终端用户的管理、安全策略下发、用户账号自动与终端绑定，以及所有网络设备接入点和接入终端的管理。

另一方面，在市级政务外网核心部署“ACMS统一管理平台”，将市、县两级准入控制系统集中管控，市级平台既能统一下发策略，也可集中统计、展示辖区内终端安全风险数据，以便进行形势研判，做出应对与决策。

## 方案价值



### 人员管理升级

通过落实实名制,任何人员都必须实名使用网络,且生成入网记录,防止人员随意使用网络资源、访问网络应用;对所有接入终端的用户、IP、MAC等三要素进行自动化绑定,杜绝非法人员在非法地点用非法终端接入政务外网。



### 终端安全升级

终端必须通过杀毒软件安装、运行、更新等状态的全方位检查后,方可入网;当终端不合规时,ASM将阻断其网络连接,引导进入修复区,直至修复合格再接入网络,避免风险扩散;并且可以做到对信创终端完善的安检和修复,促使国产化替代进程更安全地推进。



### 资产管理升级

石家庄市数据资源管理局可以通过ASM主动采集政务外网中的各类办公终端、哑终端、终端软硬件等资产信息,并进行实时更新,形成完整的终端软硬件资产台账,可视化呈现让管理者对全网资产情况一目了然,便于综合管理及风险评估。



### 联动管理升级

通过ASM自定义的精细化分权管理体系,各级管理员可以完成所在辖区的基本终端审批、绑定等管理;市、县所有终端入网安全数据可汇总展示,使市级中心得以实现联合分析与研判。

# CORPORATE 企业行业

## 80+世界500强、130+中国500强企业的安心之选

- 沙钢集团
- 鞍山钢铁集团
- 厦门国贸控股集团有限公司
- 上海国际港务集团
- 杭州海康威视数字技术股份有限公司
- 中国铁路通信信号股份有限公司
- 桐昆集团股份有限公司
- 卧龙控股集团有限公司
- 荣盛房地产发展股份有限公司
- 华映科技(集团)股份有限公司
- OPPO广东欧珀移动通信有限公司
- 安克创新科技股份有限公司
- 上海晨光文具股份有限公司
- 广东小天才科技有限公司
- 得力集团有限公司
- TCL空调器(中山)有限公司
- 安踏体育用品有限公司
- 安徽江淮汽车集团股份有限公司
- 特步(中国)有限公司
- 东风本田发动机有限公司
- 九州通医药集团股份有限公司
- 北京汽车集团有限公司

▲ 以上为部分客户名单,排名不分先后

- 
- 郑州宇通客车股份有限公司
  - 扬子江药业集团
  - 广州汽车集团乘用车有限公司
  - 通用环球医疗集团有限公司
  - 奥克斯集团有限公司
  - 正大天晴药业集团有限公司
  - 上海复星医药(集团)股份有限公司
  - 北京同仁堂健康药业股份有限公司
  - 厦门建发集团有限公司
  - 天能集团
  - 山西杏花村汾酒厂股份有限公司
  - 华帝股份有限公司
  - 九牧厨卫股份有限公司
  - 中国铁建重工集团股份有限公司
  - 索菲亚家居股份有限公司
  - 浪潮软件集团有限公司
  - 杭州士兰微电子股份有限公司
  - 传化集团有限公司
  - 阳光电源股份有限公司
  - 浙江华友钴业股份有限公司
  - 华勤技术股份有限公司
  - 保利置业集团有限公司

# 中国联通北京市分公司

## 客户简介

中国联合网络通信有限公司北京市分公司，隶属于中国联合网络通信有限公司，是中国数据网的核心、互联网国际出口局、国际互联网的枢纽节点之一，资产规模近500亿元人民币，收入规模、利润贡献多年保持联通集团前列。

## 客户需求

北京联通为构建公司IT终端全生命周期管控体系，落实对投资成本、安全、运营等方面的各项管理要求，需要对公司所有单位的营业厅终端、办公终端、运维终端、客服坐席终端等进行统一规范管理，并贯穿终端购置需求提出、安装、使用、运维、终端报废全过程，总体有如下需求：

摸清家底	成本节流	管理增效	降低风险
摸清公司IT终端情况，形成终端管理全视角，实时精准掌握资产信息。	统筹管理、匹配终端配发和运维费用，盘活终端资产，实现成本节流。	实时掌握终端使用情况，提高终端利用率；拓展线上维护服务，提升运维效率。	掌控终端入网情况、接入情况、安全合规情况、软件下载安装情况等等，降低安全风险。

## 解决方案

通过盈高MSEP多维终端安全管理平台，基于最先进的第三代网络准入技术，打造了北京联通统一终端管理平台(IEMP)，具备标准化安装、准入管控及安全事件处置等能力，确保终端从入网、使用到离网的安全要素全过程覆盖。通过平台快速构建北京联通内网安全防控体系，驱动终端安全管理水平与防护能力双提升。

## 方案价值



通过终端及人员实名入网,实现“违规不入网,入网必合规”的终端安全管理目标。



实现办公终端、营业厅终端、客服坐席终端的全量统一纳管,覆盖范围包括北京公司所有二级单位。



实现新购置终端从下单到合规安装使用的闭环交付管理。



实现终端、打印机维护服务从线下向线上服务的转型。其中市区异地服务平均时长缩短30分钟-1小时以上,郊县异地服务平均时间缩短3-5小时,终端维修效率大幅提升。



实现 PC 终端、打印机维修过程的电子化透明支撑。属于公司 IT 资产的终端和打印机均可实现在线报修,服务进度实时查询,服务质量在线评价。经统计,平台上线以来用户终端维修满意度提升近30%。



实现办公软件的在线统一下载,在确保软件安全和正版的基础上,极大地提升了软件安装的便捷性。



实现终端资产多维分析,利于盘活资产,提升资产使用效率。

# 天能集团

## 客户简介

天能集团是全球知名的绿色能源系统方案解决商，中国企业500强之一，中国民营企业制造业500强第22位（2023年）。近年来，天能正加速构建绿色智造产业链和循环经济生态圈，为全球的消费者、工商业及公共机构提供一揽子的绿色能源解决方案。在此过程中，天能集团希望能搭建一套终端安全管理体系，实现客户端的注册管理，建立资产上报和策略下发体系，进一步提高终端的安全性与可靠性，为业务加速开展保驾护航。

## 客户需求

- ▶ 需要对终端网络准入进行控制，保障网络边界的完整性及可靠性，使恶意攻击人员无法接入到公司内网造成破坏；
- ▶ 需要对终端资产进行统一管理，并规范终端用户管理，降低计算机病毒和木马发生几率；
- ▶ 需要提升终端抵御安全威胁的能力，对不合规终端进行自动的安全加固或自动隔离；
- ▶ 需要通过集中的网络管理平台，实现基于终端资源、终端用户和终端安全的一体化管理，实现对整个终端的智能监控和联动管理。

## 解决方案

通过盈高ASM准入与MSEP桌管的联动配合，天能集团实现对内网所有终端可视、可控的客户端入网认证及安全规范管理，防止不符合安全要求的未知客户端随意接入内网；同时对接入网内的终端进行安全管理，维护内网终端及信息系统安全，提升内网抵御威胁的能力和网络安全管理效率；另外，通过盈高MSEP多维终端安全管理平台，天能集团实现了对全网终端软件的正版化和标准化统一管理。

## 方案价值



实现了无需改变网络结构的终端准入控制管理，终端经注册认证后方可入网，杜绝非法终端随意入网。



实现了对移动存储介质的合规使用管理，U盘等移动存储介质需进行注册，并在管理规范内使用。



实现了对全网终端、交换机、服务器、路由器、哑终端等设备的实时发现与智能分类管理，帮助管理员更清晰地掌控网络边界与全网设备情况。



统一了软件安装标准、软件使用标准、版权管理标准，管理员可以看到终端上的软件变动，也可以对违规软件进行强制卸载和删除，让软件管理更可控。



实现了更高效的终端运维管理，无论是补丁分发、远程桌面、文件下发还是统一屏保壁纸，都帮助运维管理提质增效。



实现对终端行为的审计，包括打印审计、邮件审计、软件变动审计等网络层面和系统层面的各类审计。



# MEDICAL 医疗行业

## 为30+全国百强医院、600+三甲医院的终端安全护航

- 浙江大学医学院附属第一医院
- 浙江大学医学院附属第二医院
- 浙江大学医学院附属邵逸夫医院
- 浙江大学医学院附属儿童医院
- 浙江大学医学院附属妇产科医院
- 浙江省肿瘤医院
- 中南大学湘雅二医院
- 中南大学湘雅三医院
- 南方医科大学南方医院
- 东南大学附属中大医院
- 上海交通大学医学院附属第九人民医院
- 上海交通大学医学院附属新华医院
- 上海交通大学医学院附属瑞金医院
- 上海交通大学医学院附属上海儿童医学中心
- 上海市第六人民医院
- 上海市肺科医院
- 北京积水潭医院
- 北京大学肿瘤医院
- 北京大学第六医院
- 北京大学深圳医院

▲ 以上为部分客户名单, 排名不分先后

- 
- 复旦大学附属肿瘤医院
  - 复旦大学附属眼耳鼻喉科医院
  - 复旦大学附属儿科医院
  - 复旦大学附属中山医院
  - 复旦大学附属妇产科医院
  - 首都医科大学附属北京儿童医院
  - 首都医科大学附属北京妇产医院
  - 福建医科大学附属第一医院
  - 海军军医大学第二附属医院
  - 陆军军医大学第二附属医院
  - 湖南省人民医院
  - 广州中医药大学第一附属医院
  - 广东省第二人民医院
  - 广东省中医院
  - 重庆医科大学附属儿童医院
  - 山东省立医院
  - 香港大学深圳医院
  - 中山大学附属第六医院
  - 安徽省立医院
  - 安徽省肿瘤医院

# 中国医科大学附属盛京医院

## 客户简介

全国百强医院——中国医科大学附属盛京医院是一所大型综合性现代化数字化大学附属医院，有南湖、滑翔和沈北三大医疗院区，均位于辽宁省沈阳市，科技创新中心位于辽宁省本溪市高新区“中国药都”，医院三大医疗院区、一个科创中心实行一体化管理，保障医院的协调运行和高速发展。

## 客户需求

- ▶ 全院网络设备及终端分散在各院区、各科室，需要收集设备信息，建立台账，实现对全网终端的安全管控；
- ▶ 对接入网络的终端做合规性检查，检查终端运行的应用程序，禁用非业务相关应用程序运行，保障设备性能；
- ▶ 需要能快速有效地发现和阻止内部主机的非法外联行为；
- ▶ 需要能对全网IP进行可视化管理的手段，避免IP冲突，防止IP被用于非法行为；
- ▶ 需要能管控终端设备的开关机，减少能耗和成本浪费；
- ▶ 需要能够对全网终端硬件资产进行细致的管理，防止硬件设备变动或遗失、资源闲置等情况的发生。

## 解决方案

全院旁路部署了1台ASM网络准入控制系统和多台ASC准入控制器，通过MVG准入技术，对全院3个院区近10000台终端实现端口级网络准入；为构建统一的终端安全防护体系，满足对终端的全面管理需求，在ASM的基础上，新增盈高白羽终端健康监护平台，实时发现并处置终端威胁，阻断各类违规行为并及时报警，满足国家安全管理的要求，构建全方位、立体式终端安全防御体系。

## 方案价值



所有设备入网先注册, 每台设备信息详实, 自动分类管理, 形成终端资产台账, 物理位置轻松定位, 管理更清晰, 便捷又高效。



对所有终端进行安全基线检查, 当终端安全不符合规范时, 限制其资源访问权限, 并自动提醒及引导修复。



发现违规外联的计算机后, 可自动阻断其非法联网行为, 同时向管理中心上报违规记录。



智能节能控制, 解决“长时间不关机”困扰, 帮助医院节约能耗成本, 延长设备使用寿命。



自动形成IP地址矩阵图, IP使用状态一眼看清, 且每台设备绑定唯一IP, 杜绝IP冲突事件发生; 非法行为会触发告警, 通过IP追溯定位到人。



当终端硬件资产发生变动时, 能及时告警, 让管理员及时知晓与应对, 智能辅助硬件资产保护与管理。

# 南方医科大学南方医院

## 客户简介

全国百强医院——南方医科大学南方医院是一所集医疗、教学、科研和预防保健为一体的大型综合性三级甲等医院。作为全国首批百强医院，南方医院信息化建设也走在行业前列，已经通过电子病历、区域医疗协同、移动临床、一卡通等数字化建设，实现了更加便捷高效的医疗服务。

## 客户需求

- ▶ 建立起对终端及人员的认证审核机制，保证入网终端及人员安全合规；
- ▶ 对于不安全终端，要能够及时发现并且主动隔离风险，避免造成更大范围的安全事件；
- ▶ 防止非法人员通过IP/MAC仿冒终端入网，对医院网络及数据安全带来威胁；
- ▶ 对网络边界设备（如HUB/NAT设备）等进行精确的管理；
- ▶ 防止终端移动存储设备的随意使用，带来网络安全风险或发生数据泄露事件；
- ▶ 要能快速定位问题终端，并提供终端远程维护功能，提升终端运维效率；
- ▶ 要能实现用户权限的细粒度分派及管理。

## 解决方案

方案采用ASM入网规范管理系统，基于“不改变网络、灵活客户端”的部署理念，将南方医科大学南方医院内网已有的防病毒系统、身份认证系统等多个安管平台统一纳入到互通、联动、智能的综合管理体系之中。

<b>实时发现终端</b>	使终端接入安全“无死角”，自动识别设备类型并进行归类统计；
<b>双实名强认证</b>	保证用户和终端时刻保持一一对应的可控状态；

<b>主动隔离安全风险</b>	入网前修复风险, 入网后隔离修复风险, 防止勒索病毒的传播和扩散;
<b>设备指纹识别</b>	能预先对网内所有IP设备进行扫描和指纹特征采集锚定, 并进行唯一关联绑定, 防止IP/MAC仿冒;
<b>角色网络权限控制</b>	通过灵活的终端分级、分组、分域管理, 根据不同组别资产或用户角色, 采取相应的安全检查规范;
<b>网络设备私接滥用管理</b>	NAT识别和检测机制能够对HUB共享接入行为做实时检测和阻断管理;
<b>远程管理</b>	包括远程操作远端终端的进程、服务、文件, 也可直接对远端终端PC桌面进行控制;
<b>移动存储介质管理</b>	通过对存储介质统一注册、授权, 加强存储介质的使用范围和权限管理, 能够对存储介质进行只读、禁用、放行、脱机生效以及时间范围等精细控制。

## 方案价值



### 全面安全保障

建立起医院内网信息安全防线, 覆盖网络安全、系统安全、应用安全、管理安全的多个层面。



### 简化安全管理

安全规范得到有效的部署和执行, 构建起单位统一的安全防御体系, 简化安全管理工作量。



### 降低管理成本

集中的策略制定使得用户轻松完善终端安全, 更加专注于自己的核心业务。



### 适应未来需求

盈高准入的主动策略管理方式, 可在未来安全事件爆发前有效地解决可能出现的安全问题。

# ELECTRICITY 电力行业

覆盖20+省份国网电力客户

超10家省级国网电力单位的共同选择

- 国家电网信通公司
- 国网福建省电力有限公司
- 国网陕西省电力有限公司
- 国网浙江省电力有限公司
- 国网上海市电力有限公司
- 国网重庆市电力有限公司
- 国网内蒙古东部电力有限公司
- 国网新疆电力有限公司
- 国网辽宁省电力有限公司
- 国网吉林电力有限公司
- 国网甘肃省电力有限公司
- 国网宁夏电力有限公司
- 国网河南省电力有限公司
- 国网重庆市电力公司
- 国家电网重庆检修分公司
- 国家电网重庆自动化分公司
- 国电新源电力检修分公司
- 国网甘肃省电力公司检修公司

▲ 以上为部分客户名单,排名不分先后



- 国网电力山东检修公司
- 国网厦门市电力有限公司
- 国网泉州市供电公司
- 国网西安市供电公司
- 国网常州市供电公司
- 国网徐州市供电公司
- 国网滨州市供电公司
- 国网沈阳市供电局
- 国网辽阳市供电局
- 国网朝阳市供电局
- 国网大连市供电局
- 国网鞍山市供电局
- 国网潍坊市供电局
- 国网威海市供电局
- 国网泰安市供电局
- 国网临沂市供电局
- 国网聊城市供电局
- 冀北电力检修公司

# 国网福建省电力有限公司

## 客户简介

国家电网福建电力有限公司一直高度重视网络安全工作,先后获得国网公司信息化工作先进单位、省公安厅网络安全先进单位等荣誉。在终端管理方面,福建电力内网设备数目庞大,且地理位置分散,如果日常的终端入网授权及设备信息维护都集中管理,将会带来极大的压力。

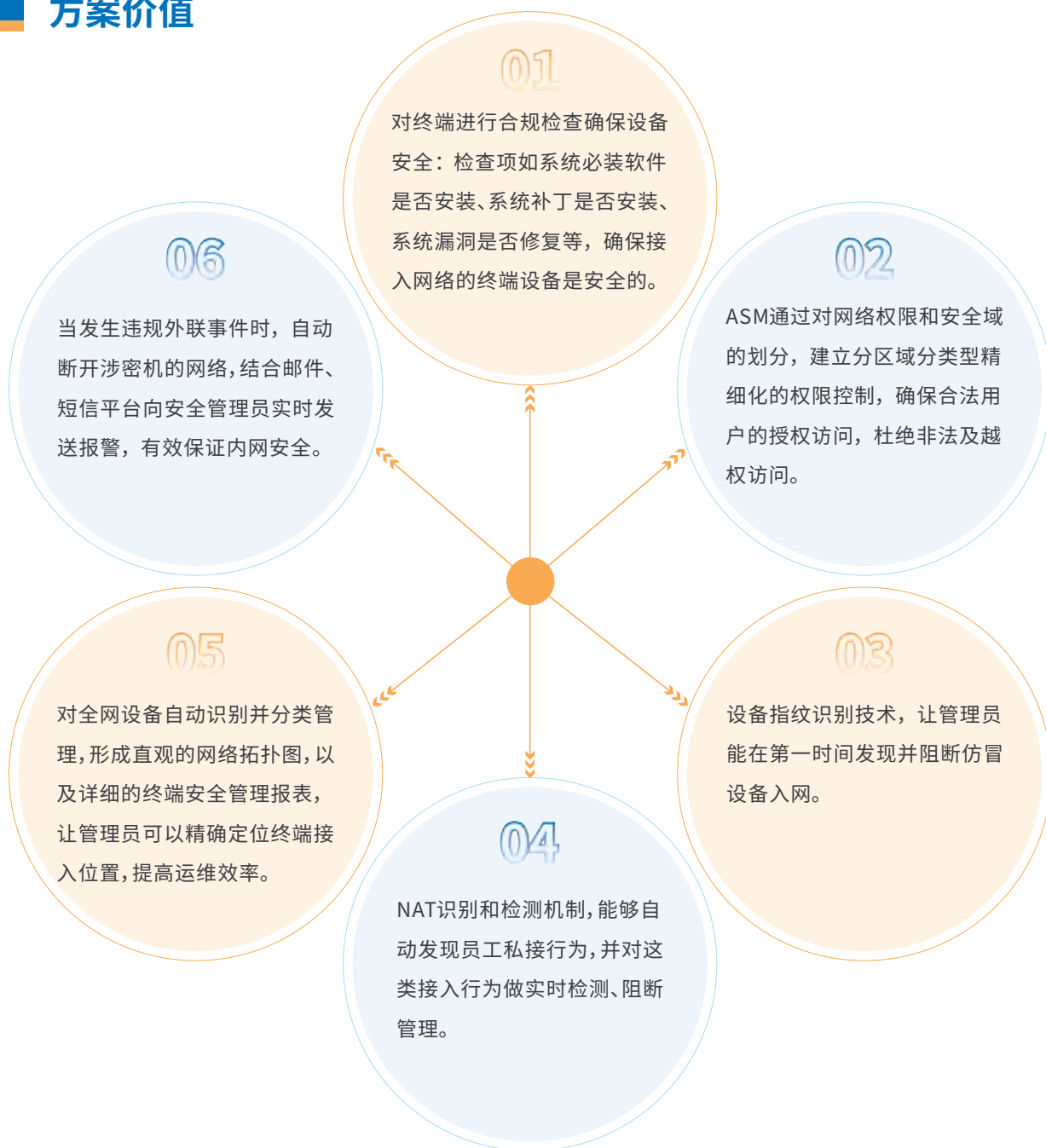
## 客户需求

- ▶ 对于公司必装软件,有员工私自卸载或不装,需要通过相应手段保证必装软件安装率;
- ▶ 需要防范非法人员通过办公区域的网络打印机、网络摄像设备等非智能IP设备,进行IP/MAC伪造从而非法入网;
- ▶ 需要能及时发现办公人员私接的HUB或小路由等设备并进行管理;
- ▶ 全网终端太多太杂,需要形成完整清晰的终端资产台账,以便管理。

## 解决方案

采用准入统一管理平台(ACMS)、准入控制系统(ASM)、准入控制器(ASC)三个层次的分布式部署方式,统一管理平台可将ASM、ASC等上报的信息进行收集和可视化展示,并进行深度分析。帮助客户实现全省超10万端点的安全管控,包括准入控制、安全基线检查、泛终端的发现识别与分类、终端精确定位等,大大提升福建电力泛终端管控力度,提高运维效率,强化终端安全。

## 方案价值



# 河南平高电气股份有限公司

## 客户简介

河南平高电气股份有限公司(以下简称“平高集团”)是国家电网公司全资子公司,是我国高压、超高压、特高压开关及电站成套设备的研发和制造基地。平高集团的信息化工作,以推进IT系统融合,提升综合业务支撑能力为工作重点,有力保障了各类信息化业务的开展。

## 客户需求

- ▶ 需要对入网终端进行访问权限控制,并保证进入内网的人员身份可查;
- ▶ 需要保证接入设备的合规性,如已安装杀毒软件、不能存在弱口令等,防止不安全终端接入网络危害整体安全;
- ▶ 需要对终端的非法外联行为进行及时到位的管控;
- ▶ 需要管控移动存储介质的使用,防止机密信息通过U盘等移动介质泄漏。

## 解决方案

平高集团通过策略路由模式部署了盈高ASM入网规范管理系统后,实现了对全网终端的安全准入管控,以及全网人员的认证入网,建立了统一的安全基线,不符合基线的终端无法入网;在此基础上,平高集团又部署了MSEP盈高多维终端安全管理平台,实现与ASM的3.0联动管控,进一步加强了企业内网安全,补足了运维管理短板,完整了内网信息安全防护管控体系,以保障内网网络及信息化系统的稳定运行,确保信息资产的安全合规。

## 方案价值



终端采用工号认证入网,人员与终端进行关联绑定,保障了进入内网的人员与终端的合法性。



实现了对入网终端的安全管理,保证了杀毒软件安装率,杜绝终端弱口令情况,有效降低终端安全风险。



实现对违规外联的秒级检测,能在终端发生外联之前实施阻断,并通过邮件、短信等方式向管理员及时告警。



通过对存储介质统一注册、授权,加强存储介质的使用范围和权限管理,并且通过U盘文件审计、U盘插拔记录、外设管控等手段,预防重要资料的外泄。



实现全面的软硬件资产管理,主动采集各类办公终端、哑终端、终端软硬件等资产信息,并进行实时更新,形成完整的终端软硬件资产台账,让管理者对全网资产可看易管。



# ENERGY 能源行业

## 单个准入项目管控终端超100万点

- 中国石油天然气股份有限公司
- 中国石化集团管道储运公司
- 国家能源集团
- 国家石油天然气管网集团
- 国家能源集团陕西电力有限公司
- 国家电投集团内蒙古能源有限公司
- 国家电投上海电力股份有限公司
- 中国华能集团有限公司湖南分公司
- 中国华能集团有限公司江西分公司
- 中国华电集团有限公司湖南分公司
- 中国大唐集团海外投资有限公司印度尼西亚米拉务
- 浙江浙能镇海燃气热电有限公司
- 浙江浙能天然气运行有限公司
- 浙江省电力建设有限公司
- 浙江国华浙能发电有限公司
- 安徽省能源集团有限公司
- 安徽省天然气开发股份有限公司
- 中化石油安徽有限公司
- 北京燃气集团有限公司
- 大连发电有限责任公司
- 大唐华银电力股份有限公司
- 华润新能源投资有限公司四川分公司

▲ 以上为部分客户名单, 排名不分先后



- 华润电力投资有限公司华北分公司
- 华润电力投资有限公司西南分公司
- 华能集团
- 华能北京热电有限责任公司
- 华能安徽分公司
- 华能集团有限公司南方分公司
- 华能武汉发电有限责任公司
- 华能新能源上海发电有限公司
- 华能青海发电有限公司
- 华能江西清洁能源有限责任公司
- 华电江苏能源有限公司
- 新华水力发电有限公司
- 三门核电有限公司
- 内蒙古京隆发电有限责任公司
- 佛燃能源集团股份有限公司
- 中海油珠海天然气有限责任公司
- 福建福清核电有限公司
- 上海大众燃气有限公司
- 南京华润燃气有限公司
- 广东国华粤电台山发电有限公司
- 广东珠海金湾发电有限公司
- 中天合创能源有限责任公司

# 中国石油化工集团有限公司

## 客户简介

该大型国有能源央企是国务院国资委直属的副部级中央企业，是中国最大的成品油和石化产品供应商、世界第一大炼油公司。由于网络规模庞大，终端地理位置分散，信息化程度较高，导致计算机终端在使用过程中存在着应用、管理、安全等多方面的挑战。

## 客户需求

公司有大量合作伙伴，经常需要接入到单位网络，需防止其伪造成内网设备接入网络。	确保终端设备系统补丁和杀毒软件及时更新，并符合密码安全策略。	实现对终端IP地址、物理位置及安全状况等信息的全面统计。
保障内网设备时刻处于安全健康的状态，对非健康状态的设备进行智能安全修复。	杜绝内网终端非法外联。	

## 解决方案

本方案采用盈高科技一体化终端准入安全管理平台，通过2000余台准入相关设备，管理总部网络及分公司网络中各类终端电脑、笔记本及其它设备超过100万点。整个方案基于PBR和MVG准入强制技术，实现级联管理，合法设备经过客户端安全检查合格后方可入网进行正常访问，来宾和访客只有经过审核后才能接入网络。

## 方案价值



实现了终端安全准入管理。从北京总部到各省分公司，所有的内网终端必须达到公司安全规范才能接入网络。



确保了公司内网安全制度的落实。通过准入系统的安全检查和修复，使得每个终端入网时均安装了公司要求的杀毒软件、系统补丁及防泄密安全客户端。



确保了审计和外联安全。通过技术手段统计了入网的设备、人员、时间等信息，有效控制和管理了外来人员入网的权限和记录。



增强了网络安全性。通过准入控制，在内网边界树立起了一道安全墙，杜绝了非法接入，非法外联等行为，优化了原有网络接入方式，保证了网络的安全性和可靠性。

# 华能集团

## 客户简介

华能集团是世界500强能源企业,持续引领行业进步。华能集团基础信息化建设已经比较健全,但存在终端数量庞大,管理职能分散的特点,无法对整个网络中的终端接入进行有效的安全防护,很多安全规范制度也无法彻底贯彻落实。

## 客户需求

<p>针对网内大量终端,不知入网用户是谁、不知入网终端情况、不知终端安全与否。</p>	<p>无法对新员工、临时运维人员、访客等临时接入的终端进行便捷的授权和管控。</p>	<p>既需要保证合法服务器的正常使用,又需要杜绝非法设备对于服务器的访问。</p>
---	--	---

## 解决方案

本方案通过ASM准入系统和ASC准入探针的配合,采用镜像准入技术和MVG准入技术,实现对全部终端的资产识别、准入控制、安检修复等,只允许受信终端设备接入网络,并开展正常的业务通信,禁止非授权设备访问,规范入网流程、防范接入风险、追溯威胁源头,确保终端安全可控从而提升华能集团内网整体安全防护水平。

## 方案价值



### 自动化的终端安全管理

对终端和人员的“入网—在网—退网”进行流程化管理，自动进行风险隔离、终端安全风险修复、终端违规操作阻断，保护重要资料安全。



### 提升运维管理工作效率

直观展示风险点数量及所在位置，信息中心管理员可以在管理平台直观查看内网安全情况，只需要设定安全策略即可实现全网运维管理，大大简化运维工作，提升运维效率。



### 边界安全态势统计

统计网络边界接入设备情况，并对网络边界风险点进行详细统计，信息中心管理员可以实时掌握网络边界使用情况及安全状态，通过对使用情况和安全状态的分析得出边界安全态势图，为针对性优化网络结构和解决内网边界安全风险提供依据。



# THANK-YOU LETTER

## 感谢信

(部分节选)



中共浙江省委办公厅网络信息处理中心

盈高入网规范管理系统用户使用报告

我单位为加强网络安全防护与管理措施，于2012年初部署应用了杭州盈高科技...

在使用过程中，该系统性能良好、运行稳定、操作便捷。通过该系统，实现了对我厅网络业务终端和相关信息系统安全的动态管理...



浙江省委办公厅

盈高入网规范管理系统用户使用报告

山东省委办公厅信息中心于2013年初应用了杭州盈高科技有限公司的盈高入网规范管理系统...

在使用过程中，该系统性能稳定、运行良好、操作便捷。原厂研发投入强大，技术支持响应及时...



山东省委办公厅

湖南省人民政府办公厅

感谢信

杭州盈高科技有限公司：

我单位通过部署贵公司的入网规范管理系统，经过一段时间的使用，使得我们的网络安全性有所提高...

贵公司派出的技术工程师...在实施和维护过程中，表现出了专业、耐心、高效、负责的工作态度...

祝愿贵公司一如既往地发挥行业表率作用，让更多的单位获得优质的网络安全服务...



湖南省人民政府

感谢信

杭州盈高科技有限公司：

为加强网络安全防护与管理措施，提高对各预算单位接入终端的管理力度，提升金财专网的安全性...

通过贵公司的ASM产品，我单位设立了终端接入两门框，确保了各预算单位接入终端的安全等级...

特此对贵公司所提供的安全产品和服务表示感谢！



湖南省财政厅

湖南省高级人民法院

表扬信

杭州盈高科技有限公司：

针对2017年5月12日互联网上出现Wannacry勒索软件事件，贵公司响应快速，及时帮助我院进行了内网终端安全检查和漏洞升级...

在此，对贵单位表现出的及时、专业、尽责，表示感谢，并期待今后能为全省法院提供更为优质、快捷的服务！



湖南省高级人民法院

感谢信

致盈高科技有限公司：

我单位在今年部署了贵公司的ASM入网规范管理系统，经过一段时间的使用，目前实现了一套更加规范的网络管理架构...

另外，贵公司派出的工作人员在实施过程中非常耐心，我们对其表现出的敬业精神表示衷心的感谢...

祝愿贵公司一如既往地发挥行业表率作用，进一步加强支持和服务力度，让更多的单位得到优质的网络安全服务...



湖南省交通厅

用户使用报告	
用户单位名称	浙江省文化厅
产品名称	漏洞扫描系统
工程时间	2012年4月2日
型号及规格	ASM4000-L/2000点
使用情况	<p>我厅于2012年应用了杭州蓝高科技的漏洞扫描系统,很好地解决了我厅外来计算机设备随意接入的问题,同时加强了内部计算机设备的安全使用规范,提高了电子政务内网的整体安全性,响应了文化部对终端计算机安全加固的指示,满足国家等级保护和分级保护的要求。</p>
用户评价	 <p>用户签字: _____ (公章) 2012年5月11日</p>

浙江省文化厅

### 感谢信

致杭州蓝高科技有限公司:

2022年8月,贵公司在“粤盾-2022”广东省数字政府网络安全实战攻防演练行动中为我单位提供网络安全支撑服务以及安全设备。演练期间,我单位通过贵司漏洞扫描系统,提前针对内网终端进行准入控制,杜绝违规终端接入内部网络,同时对接入终端进行系统漏洞检查并提供自动修复方式。提供杀毒软件检查方式,保证内网杀毒软件安装率达到100%。梳理全网终端资产,为网络管理员对违规终端溯源提供有效的数据支撑。感谢贵司的专业技术设备发挥的重要作用,贵司参与人员\_\_\_\_\_、\_\_\_\_\_二位同志尽职尽责、积极配合、快速响应,以饱满的热情、过硬的技术和优良的服务有效保障了省局信息系统及平台的安全稳定运行。

在此,特向贵公司及相关同志致以诚挚的谢意,希望在今后加强合作,继续得到贵公司的支持!

此致,

广东省监狱管理局信息技术处  
2022年8月25日

广东省监狱管理局

### 感谢信

杭州蓝高科技有限公司:

我单位自部署贵公司ASM漏洞扫描系统,经过一段时间的使用,目前实现了一套更加规范的网络安全架构,建成了一体化的计算机接入控制安全平台。漏洞扫描实现了全网终端实名制接入,并且还开发推送违规终端,杜绝终端非法外联情况,提升了网络安全防护能力。

在建设过程中,蓝高科技提供了细致的需求调研与分析,编制了全面的安全解决方案和切实有效的实施方案,工程师\_\_\_\_\_在系统部署实施过程中体现了高超的技术水平和认真负责的工作态度,网络准入控制系统的实施部署如期完成。

深刻体会到了贵公司一切以客户为中心,力争为客户提供最完美服务的宗旨,也对贵公司对我单位信息安全建设的大力支持表示感谢!

对于蓝高科技在产品方面及服务过程中的优异表现,我可深表感谢!

祝愿贵公司一如既往,发挥行业表率作用,进一步加强支持和服务力度,让更多的单位得到优质的网络安全服务,为国家网络安全事业做出更大贡献!

最后祝愿贵公司的业务蒸蒸日上!

国家税务总局南通市税务局  
信息中心  
2022年8月11日

南通市税务局

### 感谢信

蓝高科技有限公司:

感谢贵公司对我们信息安全建设项目的鼎力支持!在我双方人员的共同努力下,不懈努力下,我们顺利完成这次的网络安全项目,搭建了更加稳定通畅的网络架构,建成了一体化终端安全管理平台,实现了全网的透明化管理。

感谢你们为我们提供优质的产品,使我们在短时间内高质量的完成了这个项目,应用了你们系统后,我们的多个网络安全问题得到了彻底的根治,在管理方面的问题也得到明显改善,贵公司派出的工作人员更是本着高度负责的精神全程协助我们的工作,非常耐心地为我们解决每一个小问题,特此对贵公司为我单位信息化建设付出的智慧与辛劳表示感谢!

祝愿贵公司一如既往,发挥行业表率作用,进一步加强支持和服务力度,让更多的单位得到优质的网络安全服务,为国家网络安全事业做出更大贡献!

深圳航空有限责任公司  
2017年11月8日

深圳航空有限责任公司

### 感谢信

杭州蓝高科技有限公司:

2017年举世瞩目的金砖会晤在厦门圆满落幕,感谢贵公司对此次会议网络安全保障工作的鼎力支持,协助我单位圆满完成网络安全任务。

贵公司从维护会议网络安全的大局出发,充分发挥技术优势,为会晤官网网络提供了完善的准入控制解决方案,确保了入网人员及设备的安全合规,主动规避了安全风险,实现了高效的安全管理,保障了两会业务系统稳定运行,和媒体工作人员安全流畅入网,让会议信息得到了及时传播。

在此,对贵单位卓有成效的工作表示衷心感谢,希望在今后的工作中,我们能够进一步深化双方合作,共同为网络安全事业贡献力量。

厦门市美亚科信科技股份有限公司  
2017年9月8日

护卫金砖峰会网络安全

### 感谢信

杭州蓝高科技有限公司:

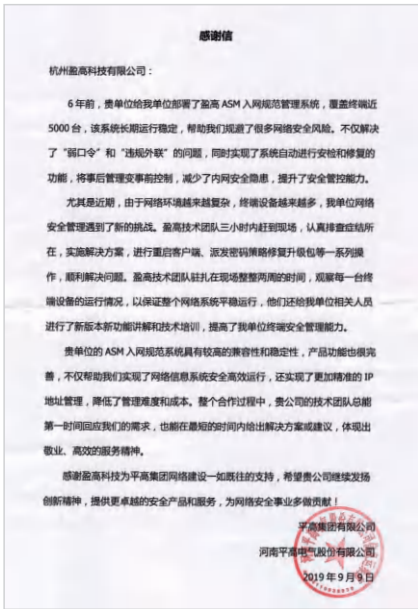
感谢贵公司对我们OPPO网络准入管理系统项目的人力支持!在我双方人员的共同努力下,不懈努力下,我们顺利完成这次OPPO网络准入管理系统项目,搭建了更加稳定通畅的网络安全架构,建成了一体化终端准入控制平台,实现了全网的透明化管理。

感谢你们为我们提供优质的产品,使我们在短时间内高质量的完成了这个项目,应用了你们系统后,我们的多个网络安全问题得到了彻底的根治,在管理方面的问题也得到明显改善,贵公司派出的工作人员更是本着高度负责的精神全程协助我们的工作,非常耐心地为我们解决每一个小问题,特此对贵公司为我单位信息化建设付出的智慧与辛劳表示感谢!

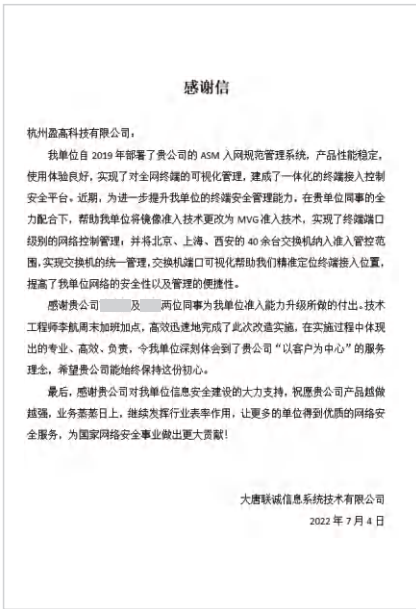
祝愿贵公司一如既往,发挥行业表率作用,进一步加强支持和服务力度,让更多的单位得到优质的网络安全服务,为国家网络安全事业做出更大贡献!

广东欧珀移动通信有限公司  
2017年3月21日

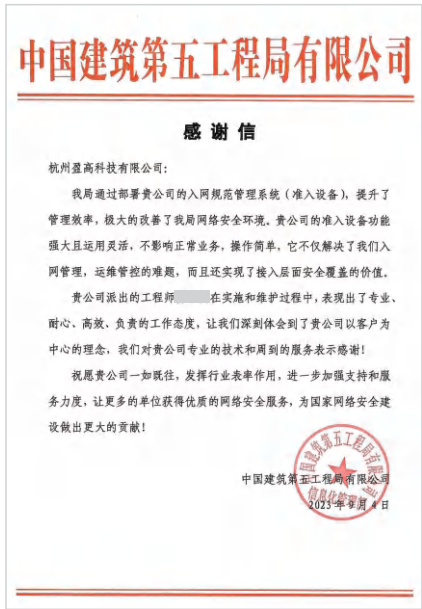
广州欧珀集团移动通信公司



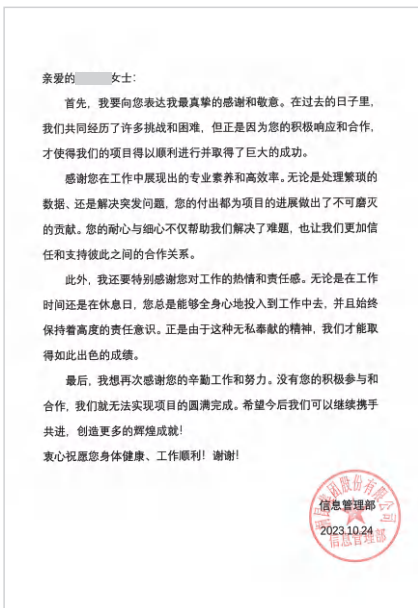
平高集团有限公司



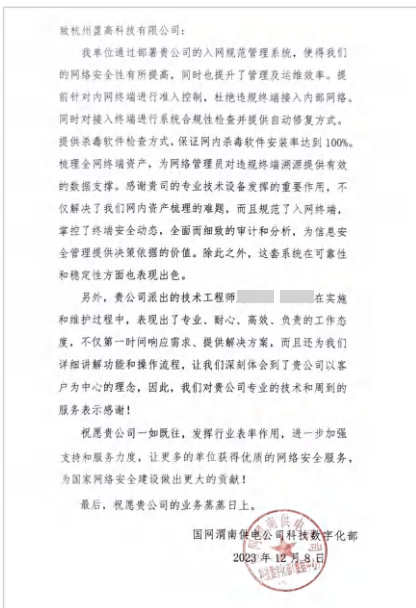
大唐联诚信息系统技术有限公司



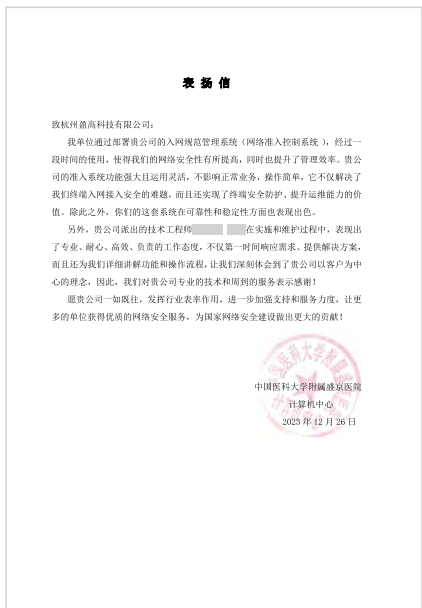
中国建筑第五工程局有限公司



桐昆集团股份有限公司



国网渭南供电公司



中国医科大学附属盛京医院



杭州盈高科技有限公司 | 构建安全 健康 和谐的网络世界

### 华东大区(杭州)

地 址: 杭州市西湖区西斗门路3号天堂软件园D幢13楼CD座  
联系人: 王先生  
电 话: 0571-88271902/88271903/13575492649

### 华中大区(长沙)

地 址: 湖南省长沙市芙蓉中路三段420号华升大厦13楼  
联系人: 谢女士  
电 话: 0731-88851322/88864316/18711098400

### 西南大区(成都)

地 址: 成都市高新区美年广场美岸7栋2单元2502室  
联系人: 游先生  
电 话: 18683719588

### 东北大区(沈阳)

地 址: 辽宁省沈阳市和平区八经街3号天惠大厦2404  
联系人: 李先生  
电 话: 15942339192 / 18698864400

### 华北大区(北京)

地 址: 北京市海淀区上地南路硅谷亮城2A-506  
联系人: 秦先生  
电 话: 010-82770220/13810787673

### 华南大区(广州)

地 址: 广州市天河区天河北路626号保利中宇广场A座405房  
联系人: 黄先生  
电 话: 020-38921462/13570917161



扫一扫  
获取各办事处联系方式



扫一扫  
一起趣看安全界