SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

深信服终端检测响应平台 EDR案例集

下一代终端安全解决方案

深信服
终端检测响应平台EDR

专注于企业级终端安全领域
轻量易用、实时保护、东西向可视可控

WannaCry，一种大小仅为3.3MB的勒索病毒软件，共造成100多个国家和地区超过10万台电脑遭到了勒索病毒攻击，共计造成损失超过80亿美元，值得关注的是企事业单位是本次攻击主要的受害者。

而勒索病毒仅是企业级终端威胁的一个典型代表，随着各类终端威胁的持续泛滥、增强、创新，战胜当前安全威胁的有效方法就是基于攻击链构建实时保护。

深信服专注于企业级安全、云计算领域20年，凭借深厚的积累发布了适合中国企业级用户的下一代终端安全产品EDR，以「轻量易用、实时保护、东西向可视可控」为价值主张。通过集成防病毒、EPP、EDR三位一体的终端安全软件帮助用户以较低的运维成本，带来显著的终端安全价值提升。

识别二维码

可查看EDR品牌白皮书、快速使用指南等产品资料

目录 CONTENTS

一 产品概述

PRODUCT OVERVIEW

产品简介

深信服EDR是一款轻量易用、实时保护、东西向可视可控的下一代终端安全产品

预防	漏洞补丁管理	系统安全基线核查	微隔离流量可视	微隔离流量可控	USB管控	一键端口封堵
防护	勒索诱饵防护	无文件攻击专防	进程黑白名单	全球热点威胁同步	远程登录防护	轻补丁漏洞免疫
检测	文件实时监控	WebShell检测	暴力破解检测	违规外联监控	流行病毒快速检测框架	SAVE引擎
响应	宏病毒修复	僵尸网络举证	进程溯源	终端隔离	清除&移除	终端围剿式查杀
运营	资产信息清点	可视化首页&报表	警报	API接口支持	网端联动	批量部署

客户端轻量化，业务无感知，无需复杂配置，半自动化安全运维

【轻量易用】

- 基于威胁攻击链多达30个功能构建多层次防御
- 恶性病毒（感染型病毒、宏病毒、CAD病毒、勒索病毒等影响业务连续性的病毒）清除修复能力强
- 网端联动达到Gartner定义的最高层级

【实时保护】

创新微隔离技术基于业务维度让终端间流量可视可控，同时做到业务简单落地，高效运维

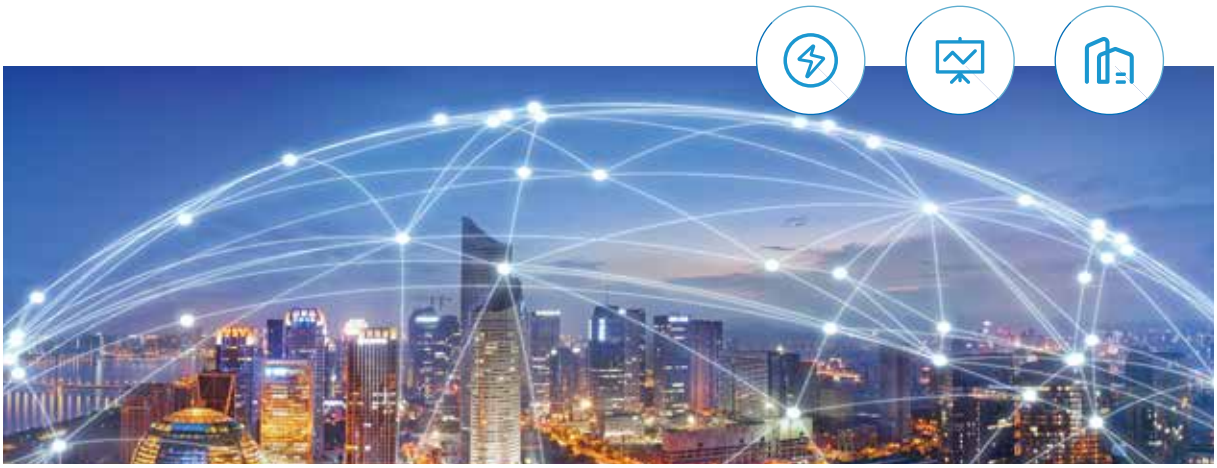
【东西向可视可控】

深信服终端检测响应平台EDR
SANGFOR Endpoint Detection Response

基于AI

深信服人工智能检测引擎SAVE
SANGFOR AI-based Vanguard Engine

一个管理台+轻代理客户端
平台统一管理，适配复杂类型终端



市场成果

实际部署安装超过400W终端

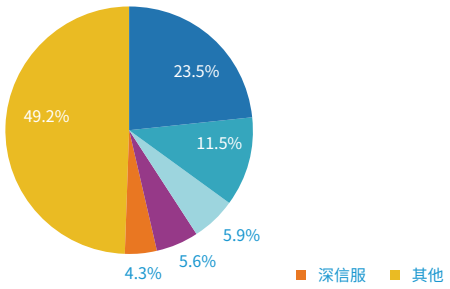
客户数量6000+，交付经验丰富

日均阻止超过520W次攻击威胁

超过200名安全人员支持，时刻应对攻防对抗

IDC
ANALYZE THE FUTURE

2019年终端安全软件市场份额



来源：IDC 中国，2020
备注：所有数据均为四舍五入后取值

在2019年终端安全软件市场份额中，深信服EDR排名第5，国内厂商排名第3。
如此快速的增长得益于EDR本身优异的安全效果，前身作为深信服网络安全应急响应的自动化处置工具，在近10年的技术积累之后，在2018年年底正式作为产品上市，只用了一年的时间就获得了众多用户的青睐，深信服也因此迅速加入一线终端安全软件厂商行列。

荣誉奖项

微软官方Windows推荐防病毒软件

微软通过严苛的各类测试，进入官方推荐防病毒软件名录

微软WHQL徽标认证（Microsoft Windows Hardware Quality Lab）

表彰深信服EDR在Windows系统中优异的兼容稳定特性

人工智能检测引擎SAVE入围VirusTotal平台

引擎入围国际最大在线查毒网站，象征引擎检测能力获得国际认可

赛可达优秀产品奖SKD AWARDS

获得国际第三方终端安全实验室2018年度优秀产品奖，以表彰EDR人工智能检测引擎SAVE优异的检测能力

赛可达实验室东方之星

获得国际第三方终端安全实验室东方之星证书以表彰EDR一流的安全防护效果

中国信息产业创新发展明星奖

获得中国信息产业商会颁发的创新发展明星奖，用以表彰EDR在客户侧实际使用中的优秀效果

CDM杂志“Next Gen”大奖

国际知名信息安全杂志CDM杂志颁发的“Next Gen”大奖，用以表彰优秀的下一代安全防护能力

用户案例

CUSTOMER CASE

政府行业用户案例

国家互联网应急中心 CNCERT	中国气象局	公安部一所
国家药品监督管理局	公安部治安管理局	河北省公安厅
山西省水利厅	四川省财政厅	新疆自治区公安厅
湖南省监狱管理局	新疆自治区司法厅	浙江省环保厅
南宁市公安局交通警察支队	济南市公安局交警支队	广州开发区信息化办公室
濮阳中级人民法院	中共嘉峪关市委政法委员会	重庆市国有资产监督委员会
人民政协报	人民邮电报	天津市环保局
人民日报媒体技术股份有限公司	新疆石河子融媒体中心	农民日报
南京溧水区政府	阿克苏信息中心	河源市源城区法院
秀山县政府	重庆市高新区管委会	潍坊市自然资源局

*以上案例排名不分先后

湖南省监狱管理局

项目背景

湖南省监狱管理局是主管全省监狱工作的职能机构，下辖省直20所监狱和1个未成年人管教所、1个医院、1个后勤事务管理所，分布在长沙等11个地方，本次项目为智慧监狱，打破传统IT建设，建设“数字法治、智慧司法”信息化建设目标，提高监狱管理工作水平和管理效率，促进执法规范化建设的内在要求、实现监狱持续安全稳定，满足监狱在安全防范、公正执法、 改造质量、管理水平等方面的需要，更好地发挥监狱的本质职能。

用户痛点

使用卡慢

C端杀毒软件导致老旧电脑系统使用卡慢，广告弹窗，文件未经允许上传云端等影响业务效率，业务人员希望更加使用轻量化的终端安全软件。

网端割裂防护

网络侧与终端侧无法协同配合应对安全威胁，安全效率低下。

终端病毒泛滥

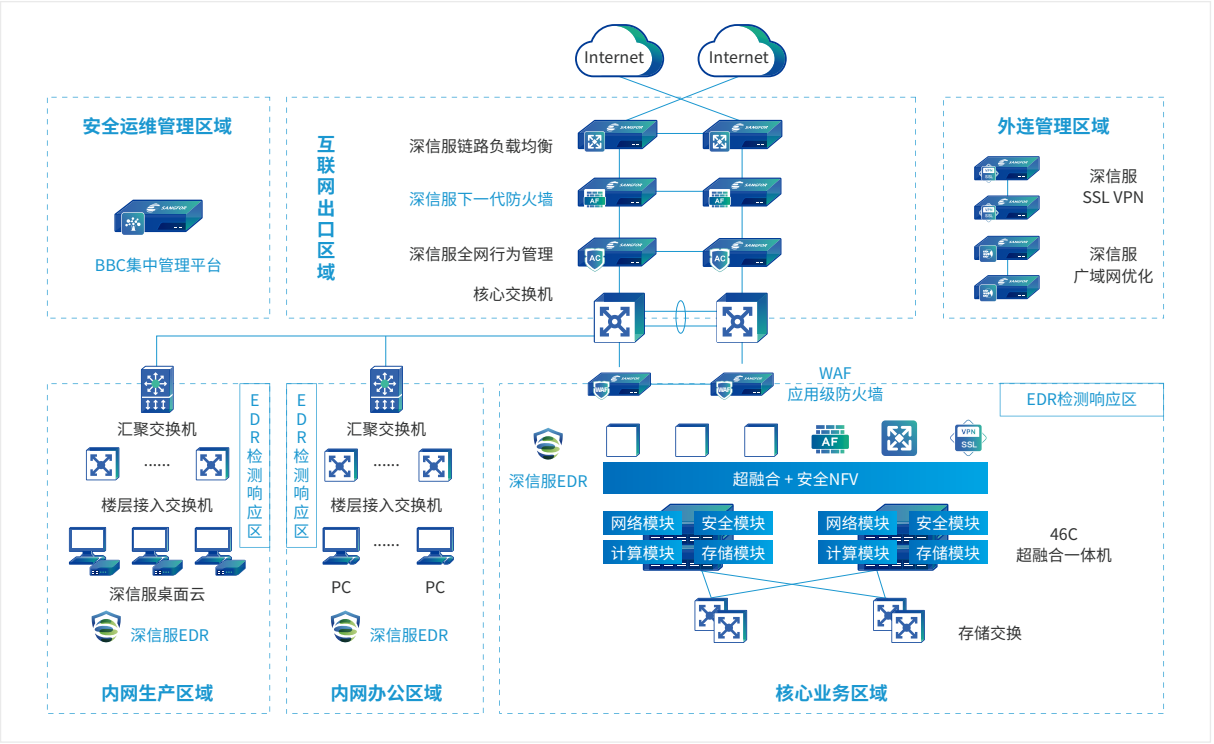
由于传统防病毒设备防护效果弱，文件落地到磁盘后才可以进行检测，无法主动防御，病毒很容易进入内网进行传播。

业务流量盲区

终端与终端间的访问关系不可视，内部业务流量陷入盲区。

深信服EDR解决之道

深信服结合湖南省监狱管理局的需求，通过在全省近8000个PC与服务器终端部署EDR，在总部的管理平台进行统一管理，以保障该机构的安全管理效率。



产品价值

跨地域终端统一管理

通过EDR统一管理平台，对批量终端进行统一安全管理，并梳理全部终端资产信息。同时通过终端发现技术，对内网中未装EDR的终端进行扫描确认，驱动业务人员安装。

轻巧简单

客户端基于轻代理模式，客户端轻量化业务无感知，无需复杂配置，半自动化安全运维，安装即防御。

一键联动处置

网络侧设备发现某一终端存在威胁，原控制台即可直接下发EDR处置命令，安全处置闭环。

业务流量可视可控

创新微隔离技术基于业务维度让终端间流量可视可控，同时做到简单落地，高效运维。

中国气象局

项目背景

中国气象局是国务院直属事业单位。国家气象信息中心主要负责拟定气象信息网络系统发展规划，制定气象信息网络业务技术标准、规范，并牵头全国气象计算网格（CMAGrid）系统建设和运行。国家气象信息中心部署了新一代天气雷达信息共享平台，平台内部有数千节点的计算节点，平台用户涉及到分布在全国31个省、自治区、直辖市的众多分支机构，信息中心领导非常重视平台的网络安全和虚拟化安全。本次项目通过对国家气象信息中心新一代天气雷达信息共享平台安全建设的有效补充、更新、完善，更换业务网络中老旧、故障频发的设备，补充必要的专用安全防护设施，完善国家级网络系统安全区域建设，满足信息系统等级保护的要求。

用户痛点

资源占用高

一般的杀毒软件比较重载，资源占用高，导致老旧电脑系统使用卡慢，业务人员希望使用更加轻量化的终端安全软件。

病毒防护效果差

传统防病毒方式防护效果弱，没有主动防御，且对于恶性病毒处置效果差，严重影响到业务的连续性。

资产全貌盲区

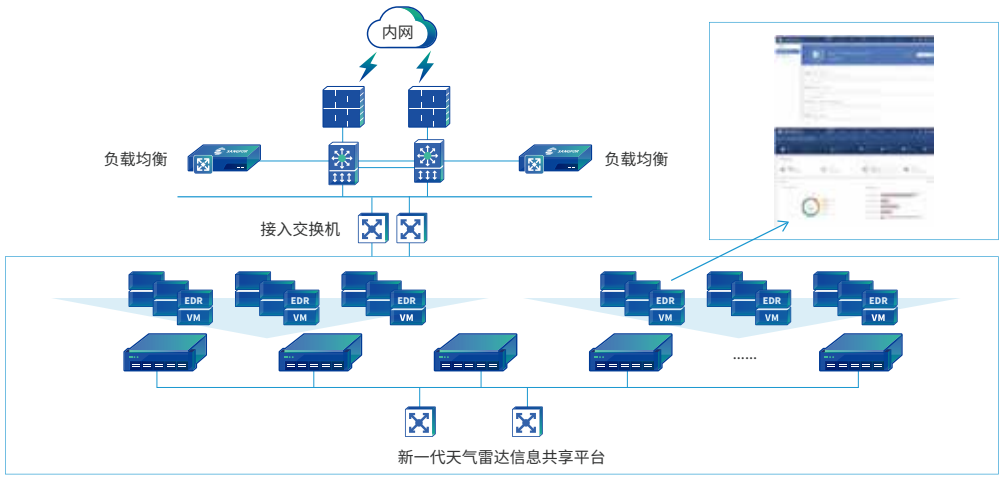
无法看清资产全面，难以总览安全风险。

业务访问不可控

东西向攻击难以管控，入侵防护能力不全面。

深信服EDR解决之道

通过在云平台2000个终端点部署EDR，实现国家气象信息中心新一代天气雷达信息共享平台的全面安全升级。



产品价值

轻巧简单

客户端基于轻代理模式，客户端轻量化业务无感知，无需复杂配置，半自动化安全运维，安装即防御。

基于应用角色的可视化访问控制

微隔离方案提供全面基于主机应用角色之间的访问控制，简单高效做到可视化的安全访问策略配置，并且通过基于安装轻量级主机Agent软件的方式，完美实现与虚拟化底层平台解耦合。

国家药品监督管理局

项目背景

国家药品监督管理局是国家市场监督管理总局管理的国家局，为副部级。负责药品、医疗器械和化妆品安全监督管理、标准管理、注册管理、质量管理、上市后风险管理，以及执业药师资格准入管理，组织指导药品、医疗器械和化妆品监督检查等职能。

总局现有应用系统涵盖了办公系统、专网（电子政务外网）系统、应急指挥系统、食品药品监管统计信息系统、药品生产和监管信息直报系统等。总局“云计算”平台，逐步实现上述业务应用系统向云平台迁移，实现以技术手段建设促进食品药品安全监管的有序发展的目标。项目建成后，各部门只需通过在虚拟的平台上部署自己的应用，而后端的平台交给云计算中心处理，可以简化用户部署的繁琐性和维护的复杂性，也提高资源的利用率，各部门无需独立购买硬件和基础软件来部署独立的应用。

用户需求

查杀效果

对比专业杀毒软件要有更强的查杀效果，尤其是未知威胁、0day漏洞相关的查杀与防护，并明确漏报率、误报率都要低于业界平均水平。

云内的安全态势可见

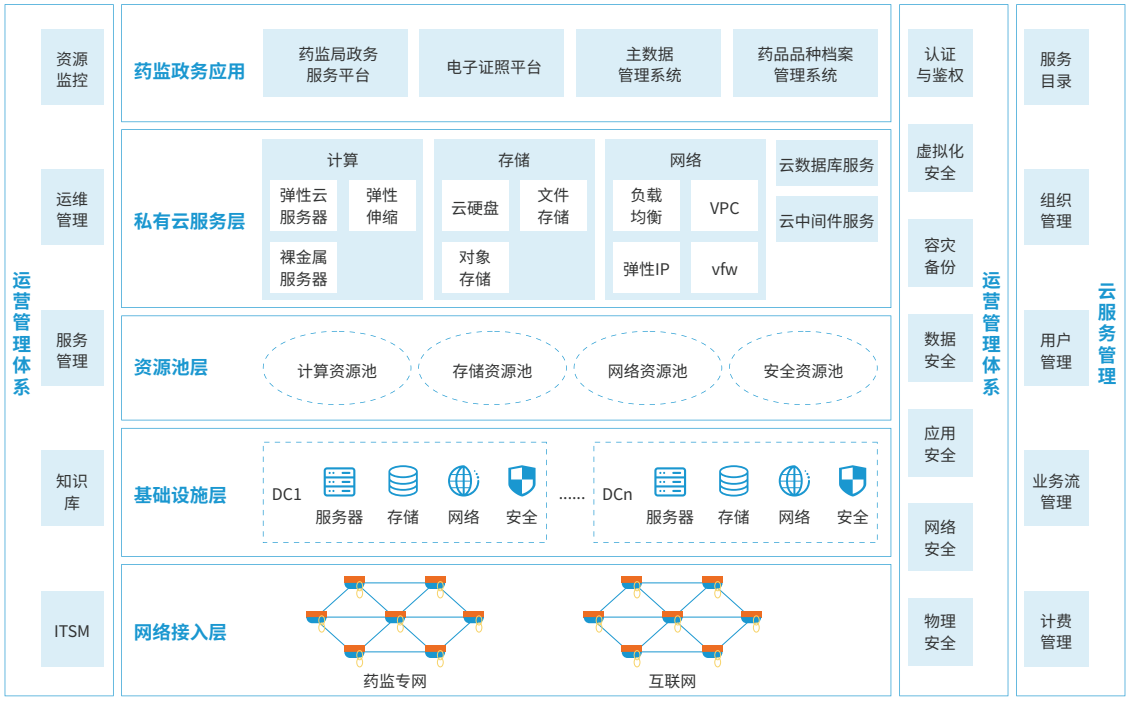
由于网络实现虚拟化，云内业务系统边界不可见、云内系统业务流量不可见，则云内的安全态势不可见，客户的建设的行业云亟需云端安全防护并掌握云内安全态势。

提升云内安全管控效率

业务转型迅速，调整频繁，安全防护策略的修改也变得频繁。当前云内缺乏统一、可视的云安全管理手段，云内安全管控的效率很低，亟需提升。

深信服EDR解决之道

在云平台部署深信服终端检测响应软件EDR以及linux客户端20个终端，实现云平台东西向流量安全防护和流量可视。



产品价值

多引擎技术打造终端多维防御

EDR具备基于无特征检测技术的人工智能引擎，辅以家族基因分析的特征检测引擎、行为引擎、基于大数据分析平台的云查引擎，多维度漏斗式检测能够有效应对恶意代码及其变种，保障低误报率的同时保持高检出率。

东西向流量可视守护云内安全

EDR应用微隔离技术，通过系统Agent获取云上虚拟机的流量，实现云上业务东西向流量的可视化和云中风险可视化，同时，在不受底层虚拟化平台和物理机器影响下，EDR配置的可视化访问隔离控制策略，能够帮助用户更好地预防云环境下的安全威胁。

架构简单熔炼产品集成度

EDR推出“智防、智控、智响应”三大模块，功能明确、脉络清晰，三智合一的连锁闭环实现“预防-防御-检测-响应”安全防御，简单易用降低安全运维成本。

企业行业用户案例

国网信息通信产业集团有限公司	膳魔师（中国）家庭制品有限公司	可口可乐装瓶商管理服务（上海）有限公司
徐工集团有限公司	中国建筑西南设计研究院	贵州茅台酒股份有限公司
完美日记科技（广州）有限公司	天津高速公路集团	中国铁路通信信号集团有限公司
山东金城医药集团股份有限公司	三清山旅游产业发展集团有限公司	贵州省烟草公司毕节市公司
深圳市广和通无线股份有限公司	华中药业股份有限公司	江苏港龙地产集团有限公司
西宁市电视台	西可通信技术设备（河源）有限公司	云南云天化股份有限公司
云南云天化信息科技有限公司	双胞胎集团	吉安市木林森半导体材料有限公司
云南云路工程检测有限公司	东风柳州汽车有限公司	宁波中哲慕尚控股有限公司
社会科学文献出版社	成都新潮传媒集团有限公司	重庆市城市建设投资（集团）有限公司
北京易华录信息技术股份有限公司	成都启迪数字医疗科技发展有限公司	天音通信发展有限公司

*以上案例排名不分先后

徐工集团有限公司

项目背景

徐州工程机械集团有限公司成立于1989年，经营范围覆盖各类工程机械、电子产品、通用基础零部件等的生产制造、加工、销售，提供技术服务和互联网信息服务，成立30年来始终保持中国工程机械行业排头兵的地位，目前位居中国工程机械行业第1位，世界工程机械行业第5位，是中国工程机械行业规模最大、产品品种与系列最齐全、最具竞争力和影响力的大型企业集团。

用户痛点

虽然在此前已经购买了卡巴斯基的终端杀毒和飞塔的防火墙，但是依然难以抵御最新的安全威胁，依靠边界防火墙的传统防护手段已经不足以支撑业务应用的快速发展，徐工集团亟需更为严密牢固的安全护城河。

众多终端缺乏有效管理手段

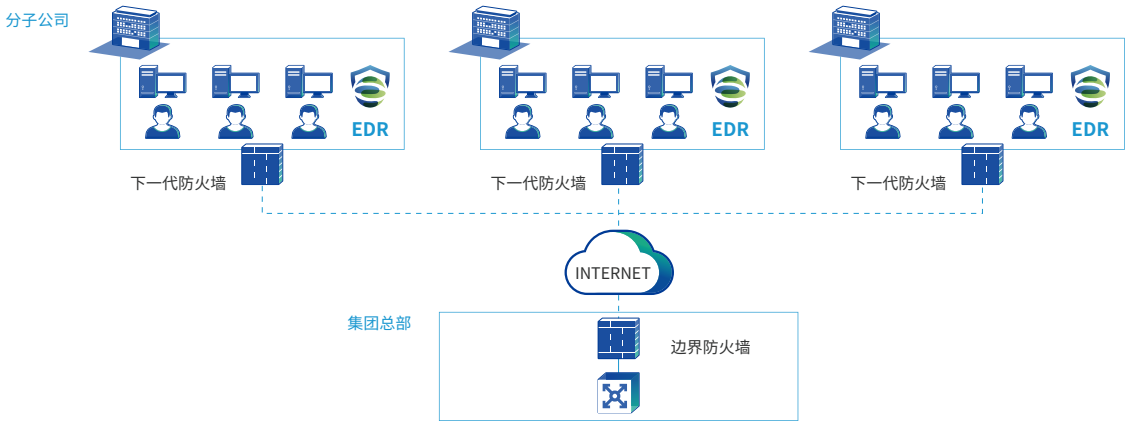
用户共有PC终端点数2W+，许多的业务终端承载着重要的生产资料，各分子公司没有专业的安全管理人员，缺乏终端管控能力。一旦某台终端感染病毒，将有可能横向影响多台终端，导致公司业务系统引线式崩溃，损失巨大。

新型威胁缺乏针对性应对措施

面对最新型的勒索病毒，传统的防病毒方式没有有效的处置手段去解决问题，影响业务的正常运行。此外，仅靠网络侧防火墙进行防御导致信息安全防护能力薄弱，用户希望通过网端联动，建立闭环的安全体系，提高信息安全等级。

深信服EDR解决之道

为了保证徐工集团业务网络环境的稳定进行，根据集团的终端分布情况和网络安全需求，为用户规划【EDR+AF+SIP】的解决方案，通过EDR在终端部署2000PC终端，实现网端联动的安全闭环。



产品价值

集中管控安全管理

用户侧终端EDR通过EDR控制中心平台进行统一管控，用安全策略模板方式对指定终端组快速部署安全策略，可一键下发隔离处置策略、文件扫描配置策略，设置威胁处置方式和信任目录，同时规范用户行为，管控Agent端软件的启用禁用，做到规范处置、安全管理。

勒索病毒安全防护

深信服EDR人工智能SAVE引擎，具备超强泛化能力，能够适应离线检测环境，同时配合文件信誉库、行为分析引擎、基因检测引擎、安全云脑等多个引擎，对病毒特征进行逐一判断、多维鉴别，有效提高勒索病毒及未知病毒的查杀精准度。

网端联动安全闭环

深信服EDR与防火墙AF进行协同联动响应，内外部威胁情报可实时共享，为勒索病毒及其变种的威胁检测提供有力支持。EDR通过与AF、SIP进行关联检测、取证、响应、溯源，能快速定位攻击主机，进行隔离处置，形成安全闭环处置。

膳魔师（中国）家庭制品有限公司

项目背景

膳魔师（中国）家庭制品有限公司，系享誉国际已百年之全球最大知名高真空系列产品品牌THERMOS（膳魔师）家族的一员。现今，因为膳魔师优越的保温性能，已成为保温瓶全球通用的称呼，实际意义即为THERMOS便是保温容器的始祖。
多年来，膳魔师业务一直持续快速增长，原有的传统杀毒软件已经无法满足用户对于服务器以及PC的安全需求，包括无法针对业务视角的隔离防护以及跟网络安全网关产品的联动的缺失，传统杀毒软件已经无法适应目前的网络安全趋势。

用户需求

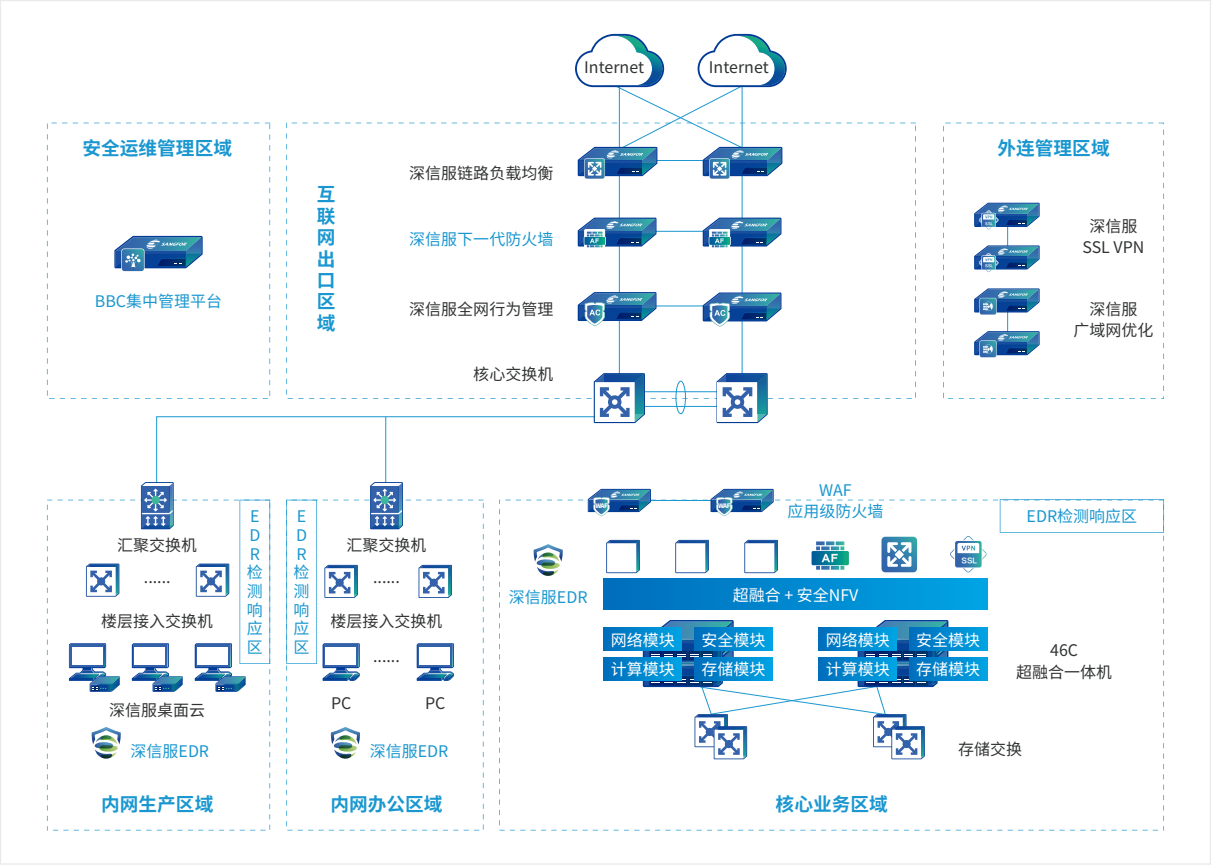
业务流量及应用可视化
云桌面虚拟机的东西向不可视不可控，需要总览业务流量，把控安全风险。

病毒防护能力强
勒索病毒变种丰富，传统的反病毒防护检测失效，需要基于AI来预防勒索病毒及其变种。

虚机之间威胁检测与隔离
东西向攻击难以管控，入侵防护能力不全面，需要对终端全面管控，阻止威胁的横向移动与传播，减少业务风险。

深信服EDR解决之道

结合膳魔师安全建设现状，以及对安全威胁和实际需求的分析，通过EDR部署1130个终端，以及统一的EDR管理平台，实现对膳魔师业务的全面安全防护。



产品价值

虚拟流量可视化

通过云平台将虚拟机内部流量镜像、虚拟安全设备等方式获取云环境中的流量，对云环境内核心且关键流量中存在的异常进行检测，以此形成虚拟流量的逻辑拓扑图。

终端病毒防护

使用多维度轻量级的无特征检测技术，包含AI技术的SAVE引擎、行为引擎、云查引擎、全网信誉库等，具备已知病毒99%检出率、未知病毒/变种97.85%检出率的检测能力，并呈现威胁检测更智能、更精准，响应更快速，资源占用更低等特点。

微隔离

通过部署EDR管理平台以及兼容了不同操作系统的客户端，实现东西向流量的访问控制，全面解决信息系统内部网络互访不可控问题，规范化主机、业务等网内不同对象的网络访问行为。

可口可乐装瓶商管理服务（上海）有限公司

项目背景

可口可乐装瓶商管理服务（上海）有限公司，统筹管理可口可乐系统在中国大陆市场的不含汽饮料的生产，包括“美汁源”、“酷儿”果汁饮料、“水动乐”果味营养素饮料、“果粒奶优”含乳饮料等9个品牌的产品。在数字化时代下，可口可乐装瓶商管理服务（上海）有限公司蓬勃聚势，全力发展并实施适应“精实增长”的数字化战略和工业4.0，通过智能技术与自动化设计，打造智能制造。工业制造4.0不断提速，工厂里越来越多的生产设备和数据需要接入网络，各种未知的网络威胁也在逐年激增。

用户痛点

未知威胁查杀能力弱

变种病毒大规模爆发，传统基于特征库防御的方式很容易被绕过，且感染率高难以根治，需要实时对未知威胁进行查杀和防护。

威胁定位处置时间长

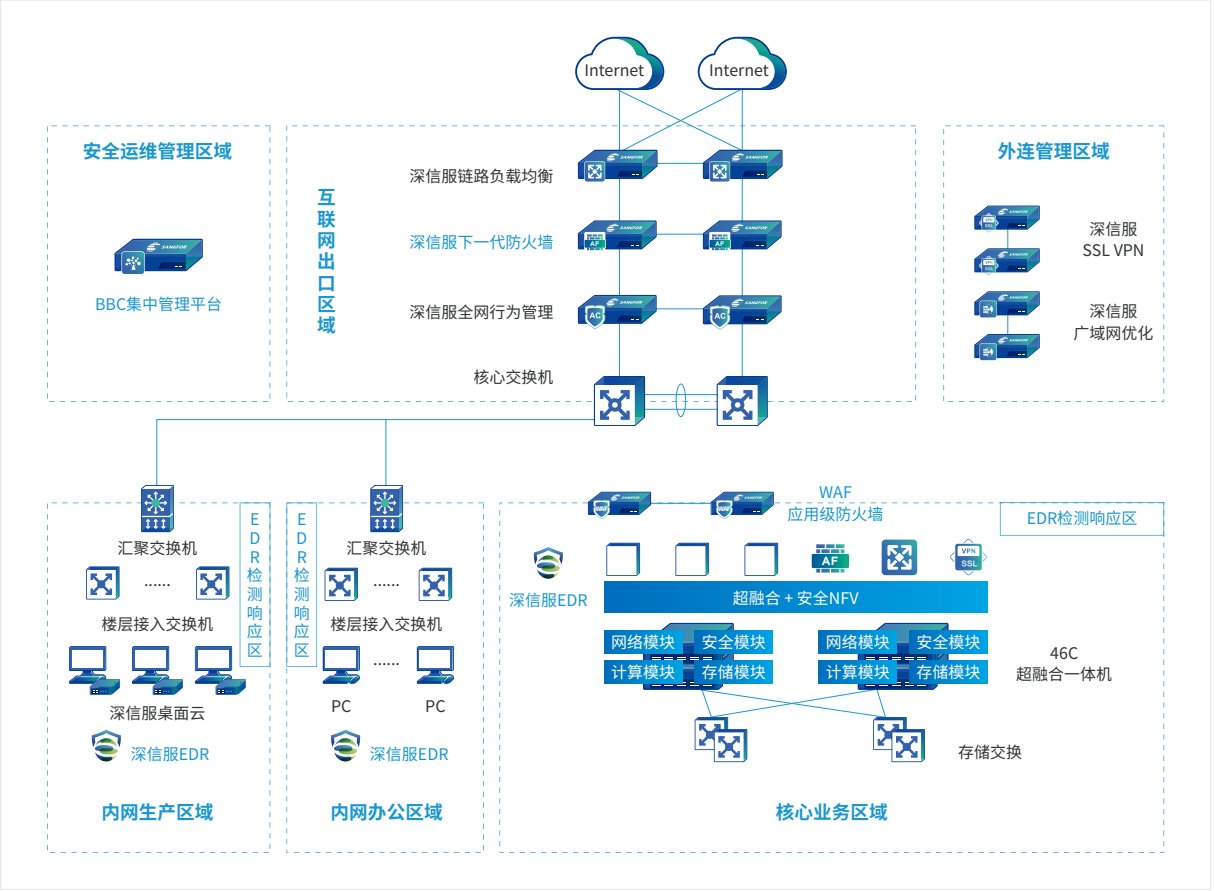
网络侧设备在发现某一终端外联恶意链接，定位后人工使用终端软件再去分析处置，信息不同步，处置操作割裂，需要能快速定位并响应处置，减少威胁对业务的影响。

资产全貌看不清管不住

公司对于自身的资产情况、脆弱情况以及内外的威胁情况，完全看不清也控不住，需要增强安全统一管理的流程建设。

深信服EDR解决之道

深信服结合企业的自身安全状况，通过EDR部署200点服务器终端，帮助公司构建应对未知威胁的安全防御体系。



产品价值

人工智能引擎检测

深信服EDR的SAVE检测引擎通过与AI技术相结合，在已知病毒样本库的基础上利用AI的泛化学习能力，总结出数千高维特征对恶意文件进行鉴定，有效应对未知威胁。在一台主机发现威胁后，立即将此病毒文件的特征值进行全网通报，彻底解决病毒反复感染问题。

威胁深度溯源分析

在网络侧发现威胁马脚后，EDR终端侧进一步定位，协同分析深度溯源，并一键下发处置命令，快速响应。

资产统一可视、可管理

部署深信服安全感知平台SIP，在安全事件发生的第一时间确认问题源头，实现一平台清晰掌控多地内网安全状况，安全真正实现“运筹帷幄于千里之外”。

教育行业用户案例

佛山市南海区教育局	昌黎县教育和体育局	北京航空航天大学
南昌大学	南方科技大学	武汉轻工大学
遵义红花岗区教育局	云南农业大学	东华理工大学
武汉体育学院	云南师范大学	昆明理工大学
新余市教育局	广西外国语学院	中北大学
黔南民族师范学院	华南师范大学附属东莞学校校区	景德镇陶瓷大学
江西师范大学	江西中医药大学	江西农业大学
南昌理工学院	贵州建设职业技术学院	山东信息职业技术学院
潍坊职业学院	洛阳职业技术学院	杨浦教育信息中心
宁夏理工学院	北海职业学院	江西泰豪动漫软件学院

*以上案例排名不分先后

佛山市南海区教育局

项目背景

佛山市南海区教育局是广东省首个“互联网+教学范式研究”试验区，多年来，佛山市南海区教育局把“教育信息化”作为一个品牌来打造，自1999年起教育信息化建设至今，取得了优秀的成绩。但是随着国家“教育信息化2.0”要求提出，南海区教育局在网络信息安全方面的管理瓶颈日渐凸显，南海区师生电脑终端规模已达十万余台，大规模的电脑终端投入使用，导致日常管理难度大幅攀升，且勒索、挖矿等病毒越来越猖獗；电教室出现大面积的僵尸网络；师生电脑终端大规模蓝屏、死机等问题，严重影响了信息化教学的开展与效率。如何对这些终端进行有效安全的治理和综合管理，满足国家当前对信息网络安全管理的要求，成为当前南海区教育信息化持续推进与深化的首要课题。

用户痛点

被动防御模式难以应付APT、0Day等新型攻击

虽然教育城域网出口已部署防火墙且设置访问控制策略，但面对新型的复杂的APT、0Day攻击，这种被动防御模式难以抵御，导致外部向内部的攻击威胁不断。

网络安全措施割裂，面对恶意攻击与病毒传播难以控制

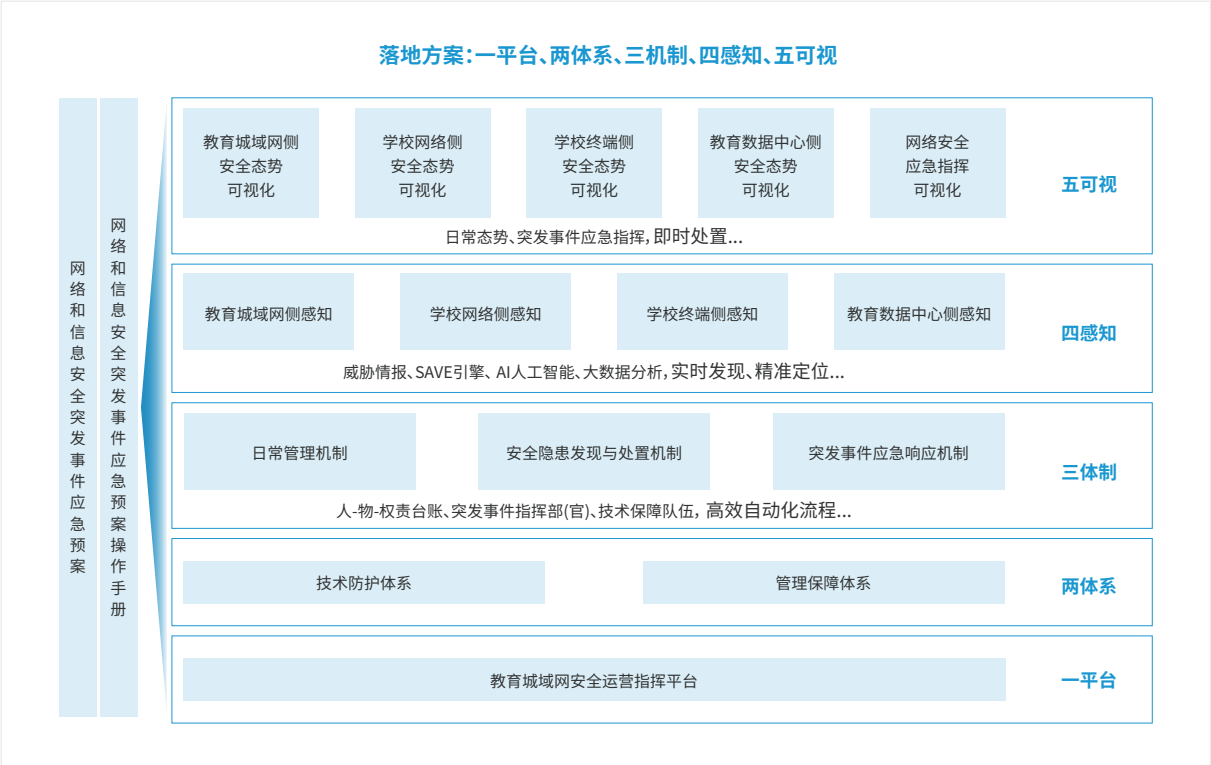
各学校运维能力参差不齐，安全防护建设不一，甚至存在“裸奔”情况，一台电脑终端受病毒感染后，向校园网内及其它学校肆意传播，难以遏制。

十万余台电脑终端资产，对安全性提出更高挑战

终端分散于各学校的教室、办公室、图书馆等地方，难以统计清终端数量、安全状况，导致难以实现统一的资产安全运营管理。

深信服EDR解决之道

针对南海区教育局面临的网络安全困局，深信服安全专家团队深入调研与洞察，以安全态势感知+终端检测响应为核心，通过EDR部署14万PC终端，构建南海区教育信息化安全管理体系，全面解决南海区教育局所面临的网络安全、终端安全、安全运营等系统性难题。



产品价值

多维度威胁防御体系

通过构建全新轻量级、智能化、响应快的终端安全系统，提供全网终端病毒、木马、入侵攻击等威胁防御能力。

全网多维度威胁监测体系

深信服安全感知平台提供非法外连、漏洞利用攻击检测、Web应用攻击检测、僵尸网络检测、业务弱点发现等多维度的威胁检测能力。

统一安全应急中心

将全网流量信息进行集中汇总，利用智能化的检测技术发现潜伏到网络内部的高级威胁，可以实时通知到各负责人及管理员，并通过安全设备联动快速对威胁进行响应处置。

南方科技大学

项目背景

南方科技大学（Southern University of Science and Technology），简称“南科大”，是国家高等教育综合改革试验校、广东省高水平大学重点建设高校，由广东省领导和管理的全日制公办普通高等学校，是深圳市创办的一所创新型大学，目标是迅速建成国际化高水平研究性大学，建成中国重大科学技术研究与拔尖创新人才培养的重要基地。南科大以理学、工学学科为主，兼具部分特色人文社会学科与经济、管理等学科。

用户痛点

终端访问控制缺失

由于虚拟机内部的流量不可视，东西向缺失管控，威胁横向入侵风险大，需要实现对虚拟流量可视化管控，减少威胁的影响面，保障业务的连续性。

病毒查杀能力失效

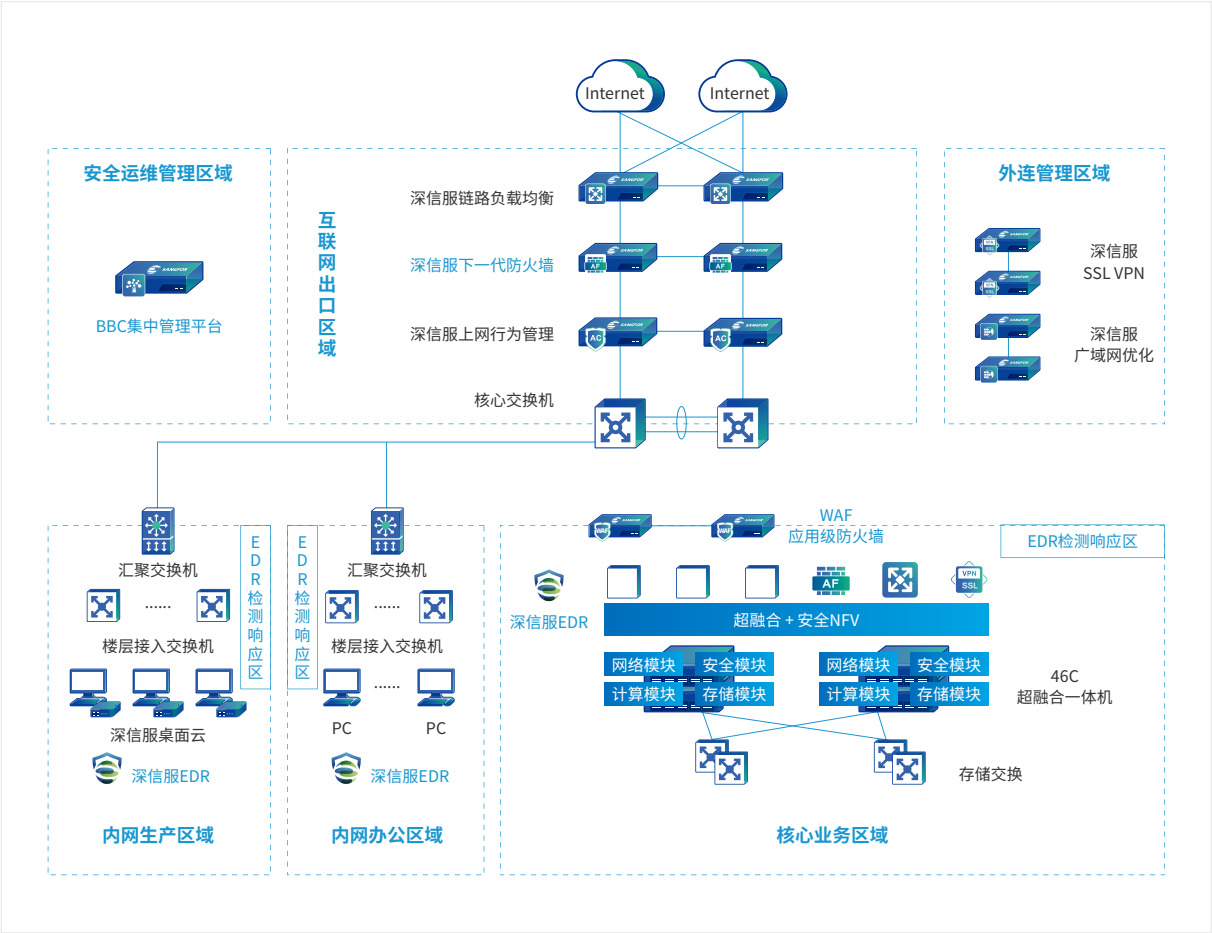
传统基于特征库的静态反病毒能力已对勒索病毒已失效，满足不了学科规模和教育水平一直持续发展的南方科技大学的安全需求，需要针对勒索病毒的专项检测能力，来保护终端安全。

东西向攻击难以管控

当有威胁入侵时，防护能力不全面难以管控，存在大面积数据安全的风险，需要有效的预防措施。

深信服EDR解决之道

针对南方科技大学面临的安全问题，并结合实际需求，在云主机部署EDR进行统一的安全管控。



产品价值

针对勒索病毒的全流程防护

通过事前的安全基线检查及修复、漏洞检测及补丁修复、防爆破检测和防御，事中的高效勒索诱捕、目录防护方案、基于文件实时监控的防御方案，事后的备份恢复机制，将勒索病毒拒之门外。

遵循Gartner自适应闭环架构

根据Gartner自适应闭环架构的四阶段模型，深信服EDR通过实现预防、组织、检测、响应各阶段共12个关键功能来有效保护终端安全。

微隔离与降低威胁影响面

通过全面部署应用深信服终端检测与响应系统，打造基于系统层面之上的细粒度隔离访问控制，实现不同终端、不同部门、不同角色之间的安全隔离和访问控制，规范内部网络不同对象的访问行为。

宁夏理工学院

项目背景

宁夏理工学院位于宁夏回族自治区石嘴山市，是教育部批准的民办普通本科高等学校，有专任教师600余人，全日制在校生11600余人。2019年9月20日，荣获全国绿化模范单位称号。根据教育厅关于开展教育信息化试点工作的通知，为了实现教育信息化、决策科学化和管理规范化的目标，需要把学院建成一个先进的数字化虚拟校园，为校内外用户和各种终端设备提供所需的各种资源和服务，方便全校师生员工的教学、科研等各种活动，达到提高办学水平的目的。

用户痛点

内网终端安全建设匮乏

内网安全是安全建设的短板，一旦一个终端感染如勒索病毒将直接横向影响到其他师生的网络安全，导致其他主机被加密，影响教师领导办公效率，进一步影响理工学院内网业务安全。

安全资产不可视

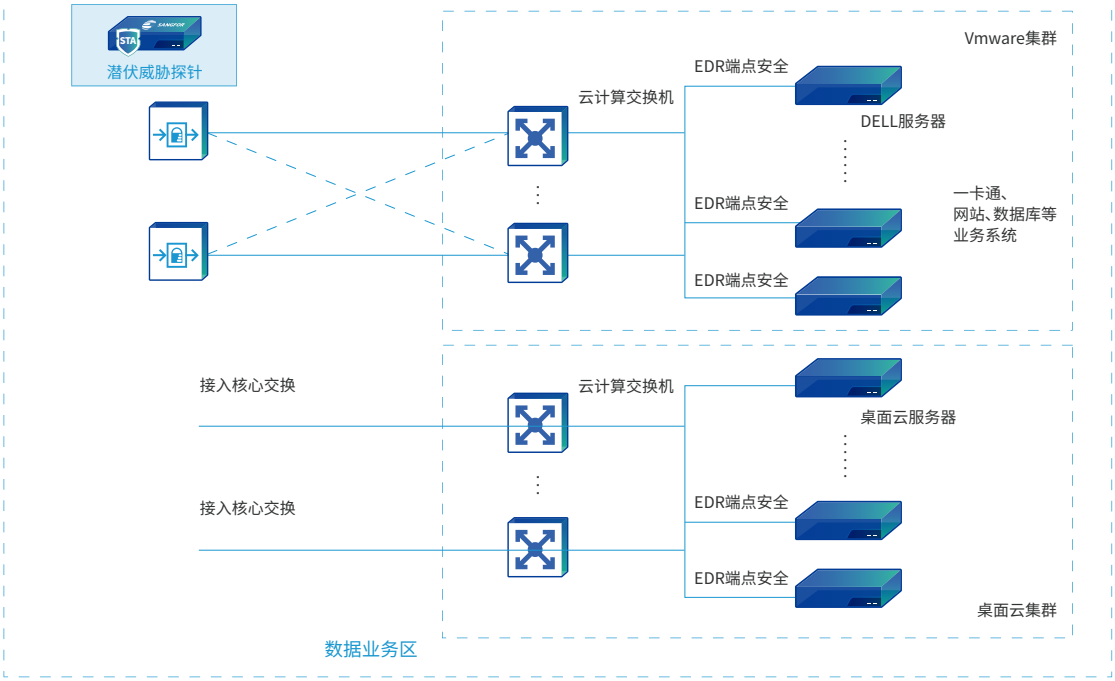
云环境的随需部署和动态迁移，使安全策略的部署变得复杂，需要一个灵活动态安全机制来适配虚拟化网络安全防护。

VDI场景下性能消耗要求严苛

由于虚拟桌面是通过后台的虚拟机提供计算能力，其性能不如物理桌面，对应用软件性能消耗要求严苛，高负载场景并不非常适用。

深信服EDR解决之道

面对云主机安全的挑战，深信服EDR提供了轻端重云的云平台安全解决方案，部署6000个PC终端，有效解决了用户对当下云计算环境的安全需求。



产品价值

威胁情报关联检测

深信服EDR将端点事件信息返回到安全云平台，通过云端反馈威胁情报进行智能分析精准判断，检测能力超越传统的黑白名单和静态特征库；同时可与防火墙进行自动化联动检测和防护，形成应对威胁的云网端立体化纵深防护闭环体系。

轻端重云架构减少性能消耗

深信服EDR采用完全无驱动、轻计算的设计，所有功能都跑在应用层进行安全的检测，即使agent意外退出也不会造成服务器的重启，可最大程度避免对agent对服务器的稳定性和性能造成影响，实现轻量化部署。

混合场景下的兼容适配

混合云跨平台统一部署管理，兼容Windows/Linux主机系统所有服务器版本。EDR与虚拟化基础设施解耦，无论是在物理机、私有云、公有云的环境下，均可以使用统一的方案解决安全问题，甚至服务器在多种IT设施之间进行迁移也可以透明地支持。

医疗行业用户案例

中华人民共和国国家卫生健康委员会	上海市杨浦区卫生健康委员会	南京医科大学第四附属医院
楚雄州医院	北海第一人民医院	吉林省吉林中西医结合医院
常熟北部医院	扬州东方医院	深圳市医学信息中心
宁德市卫计委	西宁市第三人民医院	天津市胸科医院
黄冈市中心医院	天津市儿童医院	天津市第一医院
天津市华兴医院	云浮市中医院	南京一民医院
港口医院	青海省第四人民医院	青海红十字医院
武穴市中医院	河池市人民医院	沈阳市儿童医院
滁州中西医结合医院	禅城区人民医院	新兴县中医院
成都西囡妇科医院	中信医疗健康产业集团有限公司	平果县妇幼保健院

*以上案例排名不分先后

中华人民共和国国家卫生健康委员会

项目背景

国家卫生健康委员会是主要牵头制定和落实《“健康中国2030”规划纲要》的部门。国家卫生健康委员会认为人口健康信息化和健康医疗大数据是国家信息化建设及战略资源的重要内容，是深化医药卫生体制改革、建设健康中国的重要支撑，因此在17年1月份制定了《“十三五”全国人口健康信息化发展规划》，要求各省、自治区、直辖市卫生计生委，新疆生产建设兵团卫生局、人口计生委，委机关各司局，委直属和联系单位贯彻执行。

用户需求

南北向，东西向流量的完整防护

客户平台参与建设厂商众多，需要通过一个完整生态性方案解决南北向及东西向流量防护。

合规保护云内安全风险

配合云等保2.0需进行完全的方案合规设计，保障了用户云平台业务上线后的云内安全风险。

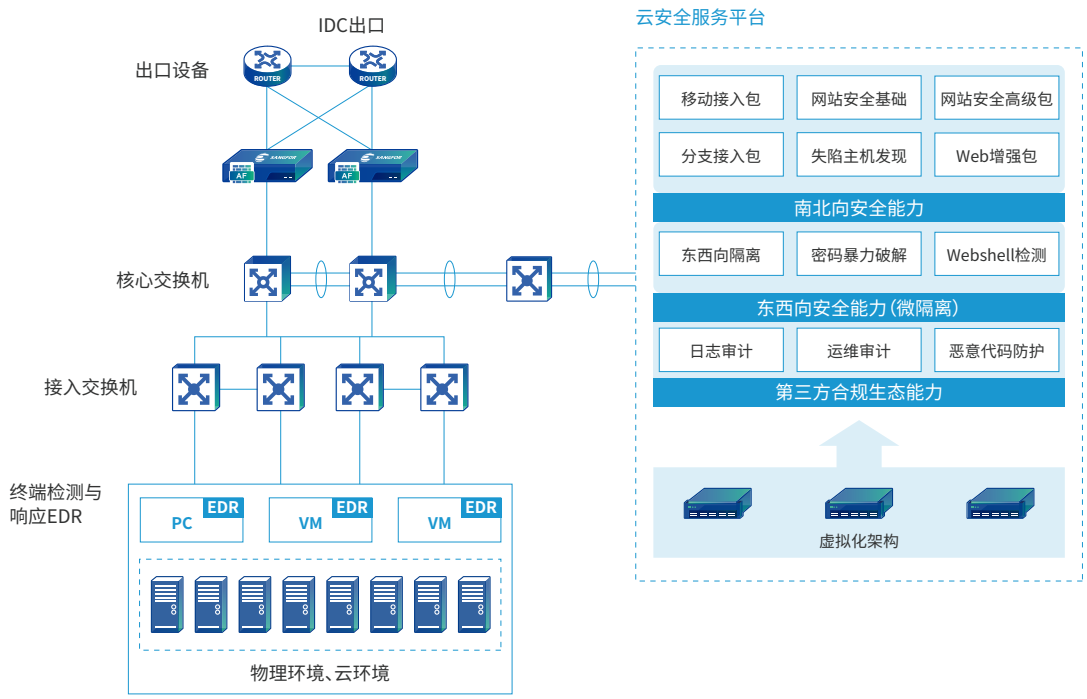
虚拟化平台解耦合

不依赖于虚拟化平台本身特性即可实现安全能力，与平台解耦合，通过系统层面即可实现流量隔离。

深信服EDR解决之道

通过EDR部署800个服务器终端，并与安全组件化团建+第三方生态产品相结合，实现整体安全加固及合规保障。

基于软件定义的安全资源池:软件安全产品组件化+EDR+第三方生态产品



产品价值

混合场景下的兼容适配

混合云跨平台统一部署管理，兼容Windows/Linux主机系统所有服务器版本。EDR与虚拟化基础设施解耦，无论是在物理机、私有云、公有云的环境下，均可以使用统一的方案解决安全问题，甚至服务器在多种IT设施之间进行迁移也可以透明地支持。

轻端重云架构减少性能消耗

深信服EDR采用完全无驱动、轻计算的设计，所有功能都跑在应用层进行安全的检测，即使Agent意外退出也不会造成服务器的重启，可最大程度避免对Agent对服务器的稳定性和性能造成影响，实现轻量化部署。

威胁情报关联检测

深信服EDR将端点事件信息返回到安全云平台，通过云端反馈威胁情报进行智能分析精准判断，检测能力超越传统的黑白名单和静态特征库；同时可与防火墙进行自动化联动检测和防护，形成应对威胁的云网端立体化纵深防护闭环体系。

常熟市第二人民医院

项目背景

江苏省常熟市第二人民医院（常熟市涉外医院）暨扬州大学第五临床医学院，是一所集医疗、教学、科研、预防、康复为一体的三级乙等综合医院。为提升医疗水平更好服务地方百姓，二院建立了完善医疗信息体系，来加固医院安全体系的建设。

用户需求

内部安全域可视可控

随着智慧医疗、大数据医疗等新技术的引进，医院多系统数据共享和调用带来的横向访问逻辑复杂化，内部安全域之间和内部的安全监管需求产生更高的要求。

终端设备统一管理

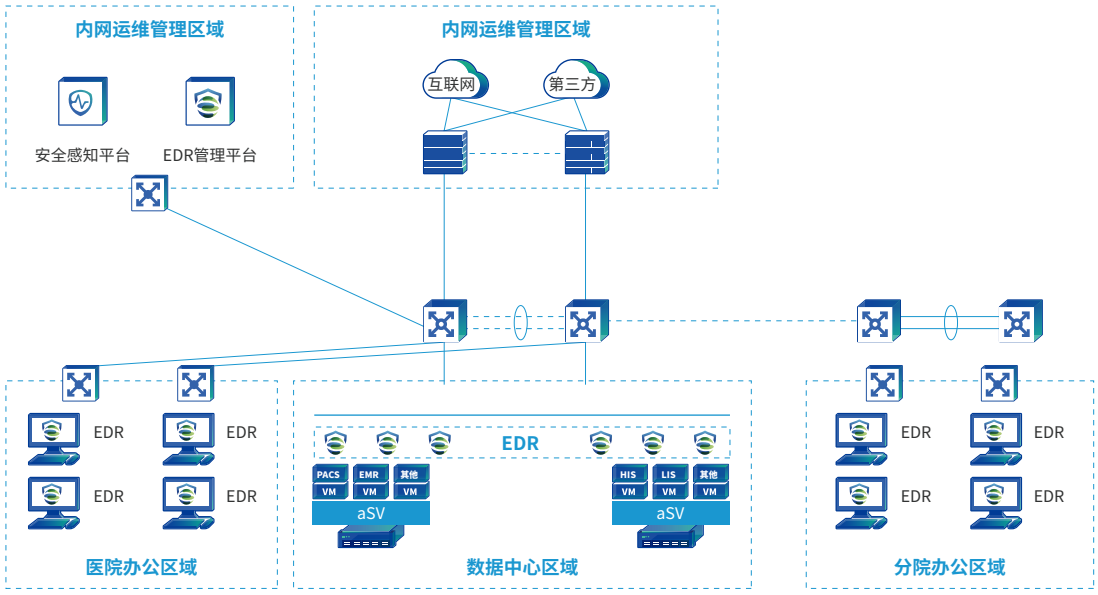
随着医院的业务发展，其终端设备众多，需要进行统一管理，做到资产安全的可视可控。

威胁快速响应与处置

在病毒爆发的场景下，需要人为再去处理，信息不同步，运维工作繁重，且响应处置的效率不高，需要更快的处置效率。

深信服EDR解决之道

结合二院的安全建设现状及实际需求，采用“边界-终端”纵深立体安全防御联动理念，通过EDR部署1550个PC终端，实现医院动态安全感知、风险快速溯源及处置。



产品价值

终端轻量级多引擎的检测技术

深信服EDR基于AI人工智能引擎，并结合基因特征、行为分析多引擎的配合、检测流水线的优化设计以及云查服务，具有强大的病毒检测能力。

多层级响应联动机制

当发生威胁时，通过SIP全面感知，EDR精准溯源分析，可将终端域风险迅速隔离，并在网络域自动生成联动封锁规则，全面封锁恶意威胁，做到安全风险一键处置。

基于应用角色的可视化访问控制

微隔离对不同安全域应用角色之间服务访问进行安全隔离和访问控制，减少了对物理、虚拟的服务器被攻击的机会，并且基于安装轻量级主机Agent软件的访问控制，不依赖于虚拟化平台本身特性即可实现安全能力，与底层虚拟化平台解耦合。

楚雄州医院

项目背景

楚雄彝族自治州中医医院成立于1979年，2003年组建为云南省彝医医院，是全国唯一的省级彝医医院。通过3次扩建，医院已发展成云南省集中医药、彝族医药医、教、研为一体的现代化综合性三级甲等中医医院、全国重点民族医医院、全国彝医药标准化研究推广基地。医院在继承中创新，在创新中发展，积极发挥中彝医药特色和优势，加大科研力度，共获国家级、省州级科技进步奖45项。医院在信息化建设方面也紧跟时代的发展，不断完善内部业务系统，加固整体安全，致力于建设成为一个现代化发展的中医院。

用户需求

等保合规需求

对医院进行安全建设，以及安全基线核查，以通过等保测评，满足等保合规的要求。

资产设备统一管理

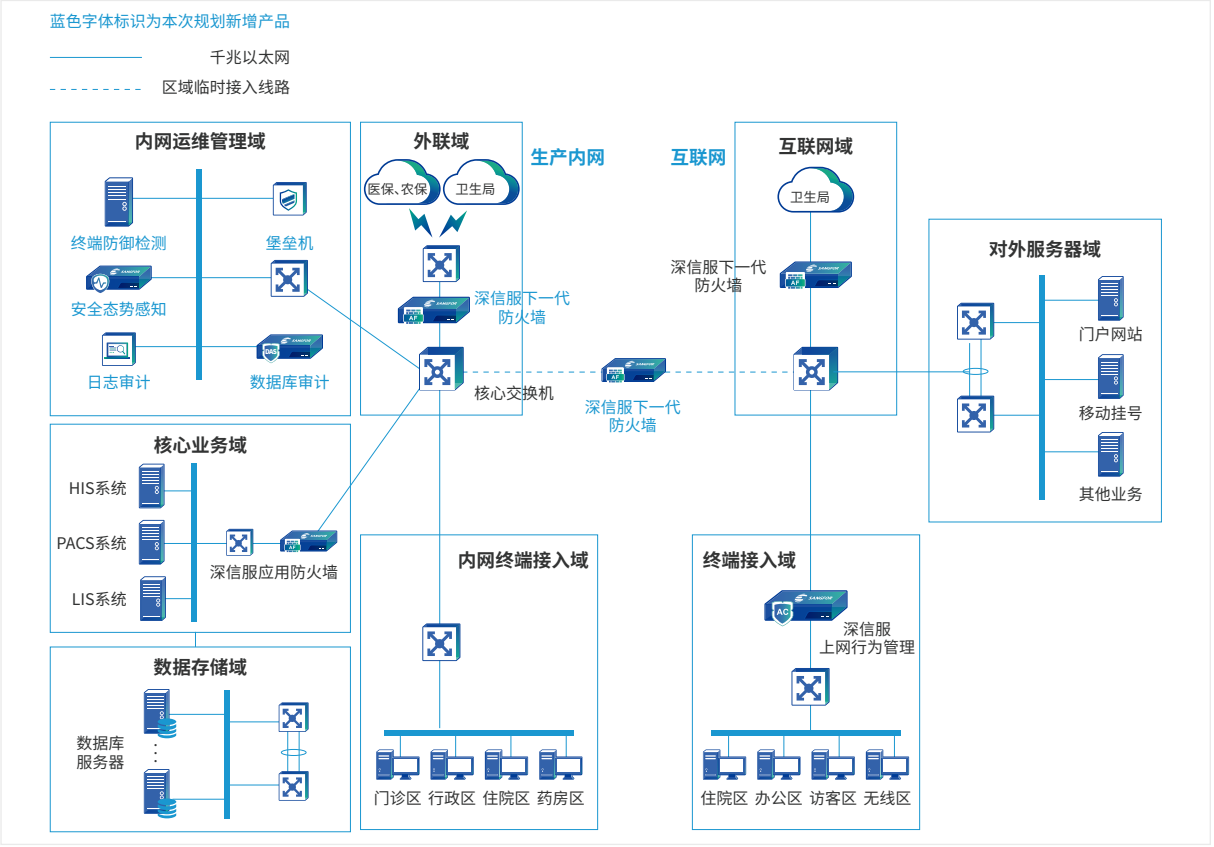
随着医院的信息化建设与发展，终端设备越来越多，需要实现针对设备的统一管理，减少安全运维成本。

快速的威胁响应与处置

当威胁发生时，能自动快速地发现风险、分析威胁、并快速响应，形成网端云的威胁定位、分析、处置的安全闭环。

深信服EDR解决之道

根据楚雄州中医医院目前的计算机信息网网络特点及安全需求，提出“云-网-端”三维一体的整体加固方案。通过EDR部署2000个PC、50个服务器，实现对医院的全方位一体化安全防护。



产品价值

等级保护，完整合规

通过对主机进行安全基线核查，可判断在身份策略、访问控制策略、安全审计策略、剩余信息保护策略、入侵防范、恶意代码防范六个方面的基线策略是否合乎要求，贴合国家政策法规，有效满足三级等保中所规定的终端安全相关控制点要求，做到“可管可控、精准防护、可视可信、智能防御”。

轻量级人工智能SAVE引擎

深信服EDR人工智能引擎SAVE是一款轻量级的本地引擎，引擎模型更新量小，内存占用低。它采用无特征检测技术，利用深度学习技术对数亿维的原始特征进行分析和综合，具有超强泛化能力，不依赖云端病毒特征库也能查出最新勒索病毒，近乎于预测勒索病毒攻击。

云网端协同联动

通过态势感知平台助力客户做到全网安全设备日志的统一处理，做到全网安全可视，风险发现和事件处置，通过云图将边界安全设备运行状态统一汇总、分析、展示，终端EDR上报与接收威胁，收到威胁情报进行自升级并自动处置。

金融行业用户案例

德州银行	东方财富信息股份有限公司	亚太财产保险有限公司
山东省国际信托有限公司	山东重工集团财务有限公司	中国人民银行南昌分行
银联国际	交银康联人寿保险有限公司	财务集团财务有限公司
上海人寿保险有限公司	新时代信托股份有限公司	华夏银行内蒙古分行
青海农牧担保公司	中国能源建设集团财务有限公司	新湖财富投资管理有限公司
中国投融资担保有限公司	天津海河金岸投资建设开发有限公司	石家庄汇融农村合作银行
天津长城滨银汽车金融有限公司	赫章县农村信用合作联社	青海省股权交易中心
华贵人寿保险公司	淮北农村商业银行股份有限公司	安徽太湖农村商业银行股份有限公司
安徽望江农村商业银行股份有限公司	中再资产管理股份有限公司	深圳市鲲鹏股权投资管理有限公司
杭州聚源金融信息服务有限公司	吉林丰满惠民村镇银行股份有限公司	湖南省信托有限责任公司

*以上案例排名不分先后

银联国际

项目背景

银联国际是中国银联负责运营国际业务的子公司，以会员制吸引全球合作伙伴，拓展银联卡境外受理网络，扩大银联卡发行和使用，开展创新支付的跨境应用，提升银联品牌的国际影响力。通过与全球2000多家机构合作，目前银联卡全球受理网络已延伸到174个国家和地区，境外50个国家和地区发行了银联卡。在业内具有强大的影响力。

银联国际生产网在去年勒索病毒肆虐的大环境下，客户意识到内网安全建设存在薄弱点，尤其是生产网上跑核心业务的虚拟机安全建设不足，存在勒索病毒等高级威胁入侵的风险，由此开始提出虚拟化安全建设的相关要求。

用户需求

对于新型勒索病毒等高级威胁的防护

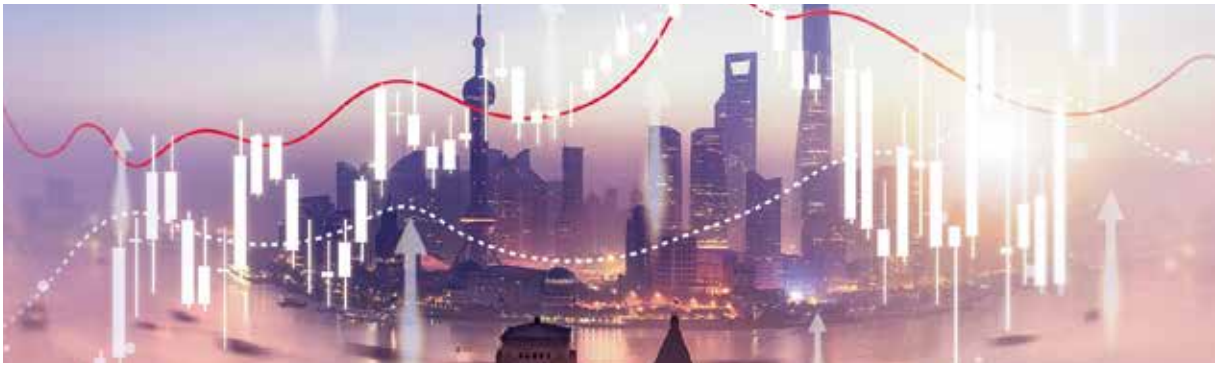
目前云上无安全设备，对于病毒的防护，特别是高级的勒索病毒或未知威胁，防护能力弱，需加强病毒检测能力的安全建设。

防范威胁横向传播风险

虚拟机之间，网络边界模糊，访问关系不可视不可控，一旦发生威胁并横向传播，给业务的安全性与稳定性带来非常大的风险。

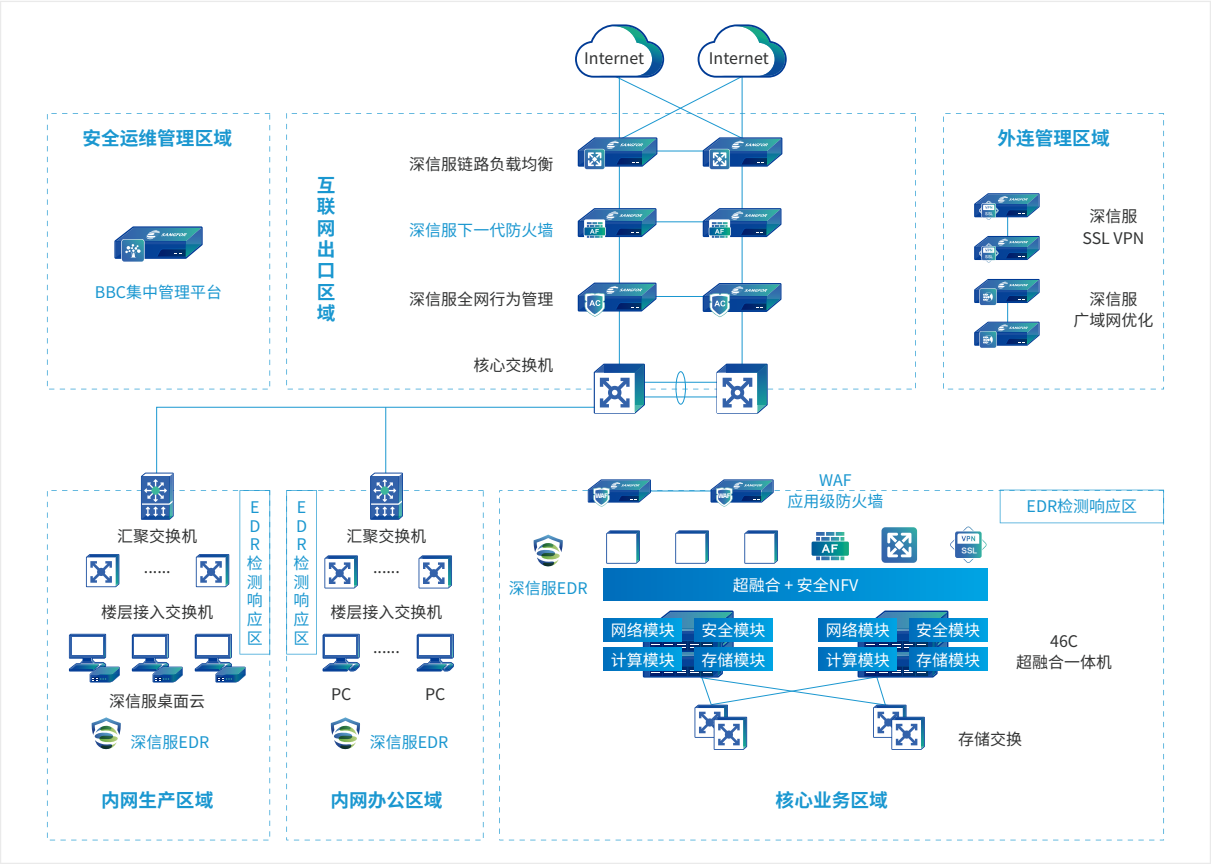
本地化部署设备满足合规性要求

通过安全云脑本地化，赋予EDR强大的信息和样本检测能力。



深信服EDR解决之道

深信服结合银联国际的安全需求，通过EDR部署50个Windows客户端和250个linux客户端，以保障核心业务的安全。



产品价值

EDR离线查杀能力

金融客户基于安全和合规的考虑，提出了终端安全检测的产品不能联网的要求，通过深信服安全云脑本地化，轻量级SAVE引擎定期更新，使之拥有强大的离线检测能力。

EDR东西向安全可视及微隔离能力

EDR通过获取云上虚拟机中的流量，对环境内核心且关键流量中存在的异常内容进行检测，形成流量逻辑拓扑图，同时结合微隔离，做到可视化的安全访问策略配置，使得本来不清晰的云上访问关系和流量路径变得可视可控。

虚机端口统一管控能力

EDR管控平台支持多级虚机管理，用户可基于业务、部门等对所有虚拟机、PC终端端口进行多维度灵活管控，实现对勒索病毒等蠕虫病毒的传播途径阻断。

山东省国际信托有限公司

项目背景

山东省国际信托有限公司是于1987年3月经中国人民银行和山东省人民政府批准设立的非银行金融机构。现已发展成为以管理省基建基金、资金信托、财产信托、投资银行、融资租赁、资产管理、证券投资基金为主要业务的金融公司。公司成立以来，受省政府和省发展改革委员会委托，精心管理省基建基金，有力地支持了全省重点项目建设。

用户需求

勒索病毒高威胁场景防护

当内部出现勒索病毒等攻击事件时，传统的病毒防护能力失效，无法保障业务安全性，需要加强高级威胁的病毒查杀能力。

业务流量可视可控

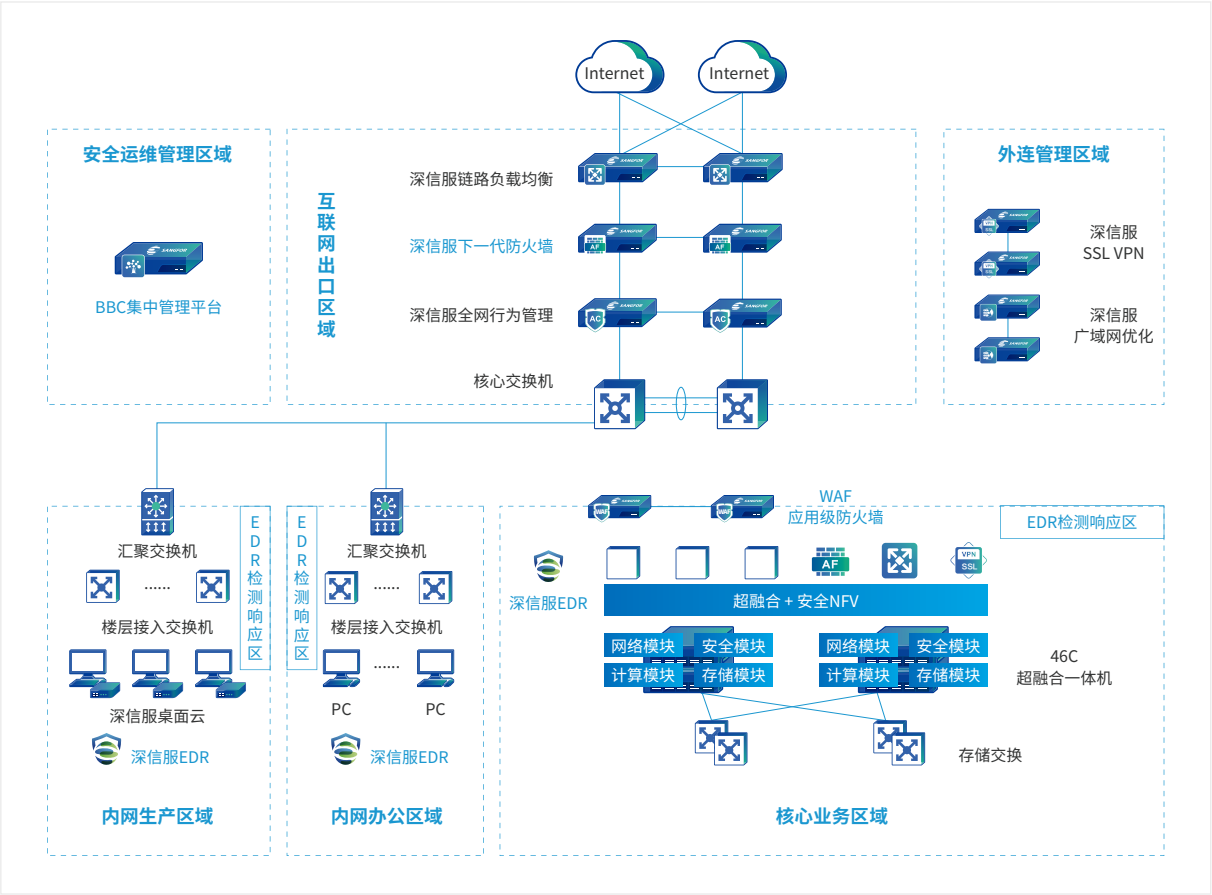
看不清内网各业务之间的流量访问情况，以及潜在的威胁情况，资产安全存在很大的盲区，需要可视化管理。

威胁溯源分析、联动响应处置

在网络侧发现问题后，无法溯源问题，及时对威胁进行分析、响应和处置，需要网端联动，快速联动的处理安全事件。

深信服EDR解决之道

深信服结合山东省国际信托有限公司的安全建设现状及实际需求，提出【EDR】+【下一代防火墙】，协同联动的完整安全体系解决方案。通过EDR部署，帮助金信实现“防御-检测-响应”的闭环安全体系。



产品价值

人工智能引擎精准查杀能力

人工智能SAVE引擎通过机器学习建立查杀基线，基于模型的无特征检测分析更全面，强大的泛化能力能有效预防勒索病毒，挖矿病毒甚至未知病毒。

微隔离与安全威胁可视化

通过微隔离实现业务流量及应用可视化，及时阻断勒索病毒等蠕虫病毒的传播途径，对恶意主机一键隔离，对感染型病毒进行剥离并修复感染文件，防止内网病毒大面积扩散。

威胁处置闭环与设备联动

借助可视化预警监测平台，可视化形式呈现针对内网关键业务资产的安全威胁，并通过该平台对内网所有安全系统进行统一管理和策略下发，打造“防御-检测-响应-联动”整体安全闭环体系。

德州银行

项目背景

德州银行，成立于2004年12月7日。在市委、市政府的正确领导下，在人民银行、银行业监督管理机构的政策指导和行业监管下，在广大股东单位和企业的密切配合下，在广大市民群众的广泛信赖和大力支持下，德州市商业银行 紧紧立足“地方金融 市民银行”市场定位，以建设“经营业绩好、资产质量好、内控管理好、遵纪守法好、社会服务好”的良好银行为目标，集优资源，集约经营，实现了速度与结构、规模与效益的有机统一。

用户需求

病毒查杀能力

当内部出现勒索病毒等攻击事件时，传统的病毒防护能力失效，无法保障业务安全性，需要加强针对高级威胁的病毒查杀能力。

轻量，资源消耗少

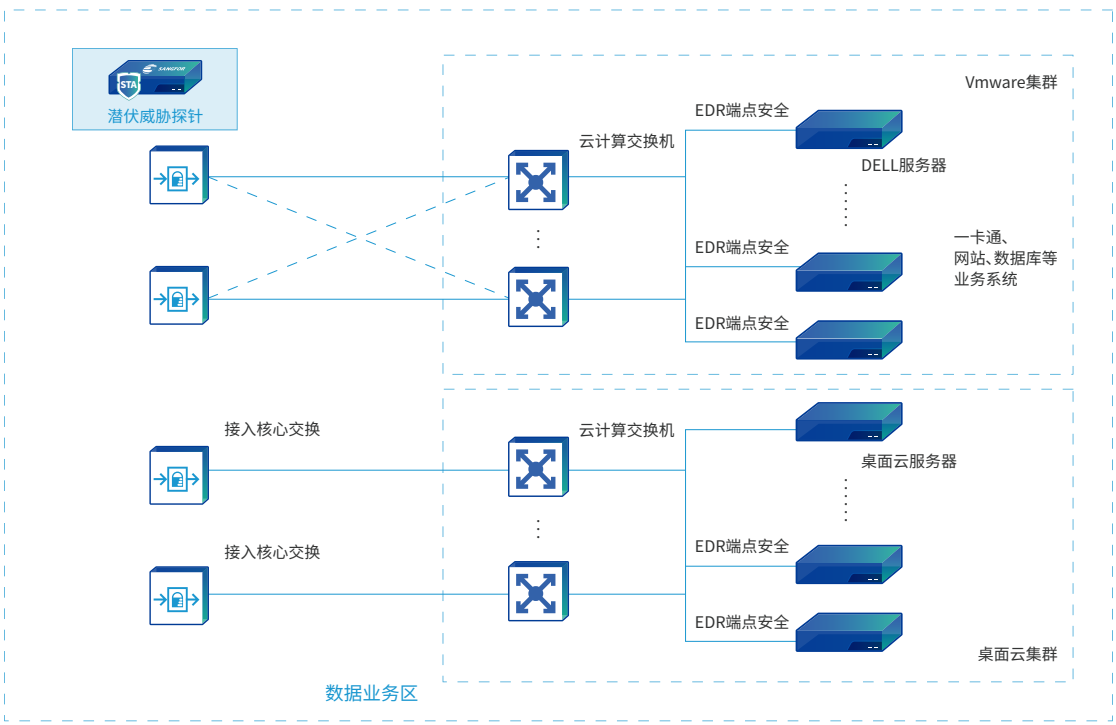
传统的杀毒软件十分重载，安装在终端性能消耗大，影响业务的连续性与稳定性。

资产安全统一运维管理

随着德州银行的业务发展，需要对终端资产进行统一管理，实现可视可控可管理，以减少安全运维成本。

深信服EDR解决之道

深信服结合德州银行的安全建设现状及实际需求，通过EDR部署个120个客户端，帮助客户实现轻量、实时、可靠的病毒查杀能力，给银行业务保驾护航。



产品价值

离线病毒查杀

人工智能SAVE引擎通过机器学习建立查杀基线，基于模型的无特征检测分析更全面，强大的泛化能力能有效预防勒索病毒，挖矿病毒甚至未知病毒。

轻巧、简单、资源消耗少

轻代理模式老旧电脑不卡慢，业务人员无感知，安装即防御，不需要过多关注就可以有效安全防护。

全面适配，统一资产管理

通过EDR平台，对终端进行策略下发，用户可基于业务、部门等对所有虚拟机、云桌面进行多维度灵活管控，实现资产业务统一管理。

SANGFOR
深信服科技

深信服让IT更简单，更安全，更有价值!

深圳市南山区学苑大道1001号南山智园A1栋
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

深信服官方微信

深信服移动官网