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

深信服EDR主打PPT

轻量易用，实时防护，东西向可视可控

产品运营部

密级：内部公开　定密部门：产品运营部

目录

市场成绩及客户成功案例

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

- 实际安装超过400W终端
- 5000+客户的最优选择
- 7*24小时持续威胁响应
- 全球威胁情报实时同步
- 老旧系统（Win7，XP等）持续支持

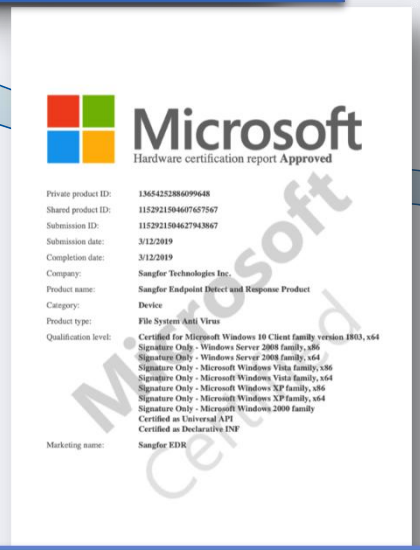
CNCERT/CC 国家互联网应急中心
UnionPay 银联 UnionPay International
福耀集团 Fuyao Group
中华人民共和国国家卫生健康委员会 National Health Commission of the People's Republic of China
国家药品监督管理局 National Medical Products Administration
贵州茅台集团 KWEICHOW MOUTAI GROUP
国家信息中心 国家电子政务外网管理中心
SARFT 国家广播电影电视总局
宝马（中国）
XCMG 徐州重工机械
中国联合航空 CHINA UNITED
KONKA 康佳
中国气象局 China Meteorological Administration
国家电网 STATE GRID
中国国电 CHINA GUODIAN

市场成绩及客户成功案例

赛可达实验室东方之星证书

微软官方Windows 10/8/8.1
推荐防病毒软件

赛可达优秀产品奖
SKD AWARDS



微软WHQL徽标认证

中国反网络病毒联盟成员单位

Save引擎入围
Virustotal检测平台

目录

下一代EDR产品-深信服终端检测响应平台EDR

下一代EDR
（三合一）

下一代AV杀毒

除静态特征和启发式检测外（上一代）
融合AI的文件检测技术（下一代）

EPP（终端防护平台）

事前提前预知风险并修复
事中构建多层次立体防护

EDR（终端侦测与响应平台）

事后对内部终端进行持续监测，找出绕过防御的恶意攻击

城门卫兵

驻守城门的卫兵，拿着画像去比对行人，判断行人是否为通缉犯

城墙士兵

找到城墙破损进行修复，如果发现外敌，通过护城河，城门，落石各种方式进行防御

反间谍

在城内各处打探消息，持续监测，主动发现绕过城墙进入市区的间谍

深信服终端检测响应平台EDR

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

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
- 轻补丁内存免疫

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
- AI 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

深信服下一代EDR

轻巧简单

客户端轻量化业务无感知

实时保护

AI赋能实时保护终端安全

流量可视管控

终端间流量可视可控

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

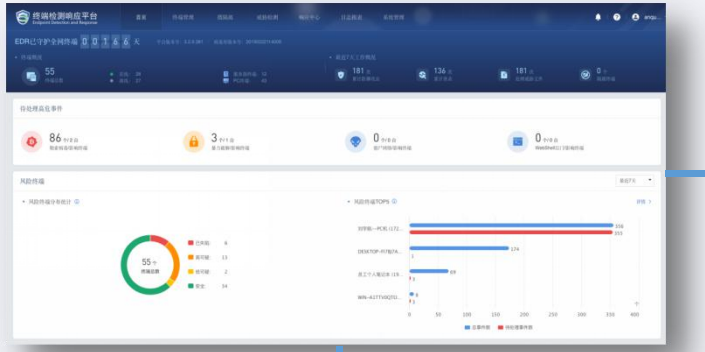
多达30项子功能，闭环防护对应阶段，防病毒只是核心功能之一

复杂类型终端，一个平台全部管理

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

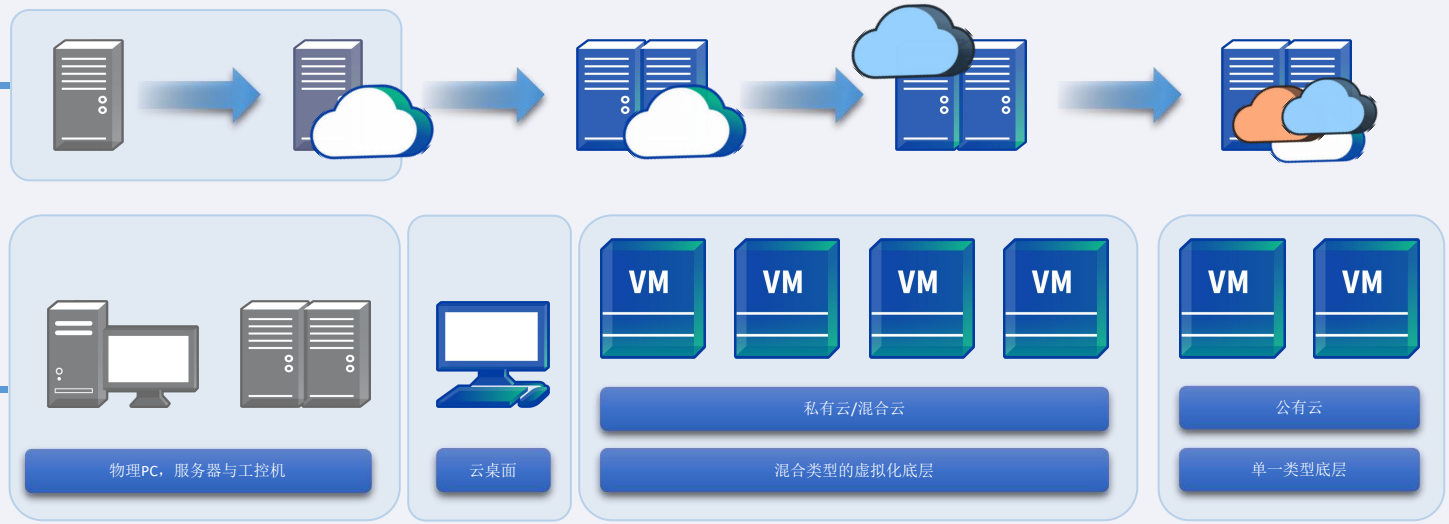
轻巧简单

本地或云WEB管理控制台



EDR客户端　　EDR客户端

全面适配混合架构，让安全与架构共同过渡



统一管理平台，保护办公网络及数据中心各类型资产

终端系统兼容（含国产化）

Windows　CentOS　Ubuntu　redhat　SuSE

Debian　红旗Linux　Red Flag Asianux　中标麒麟　Oracle linux

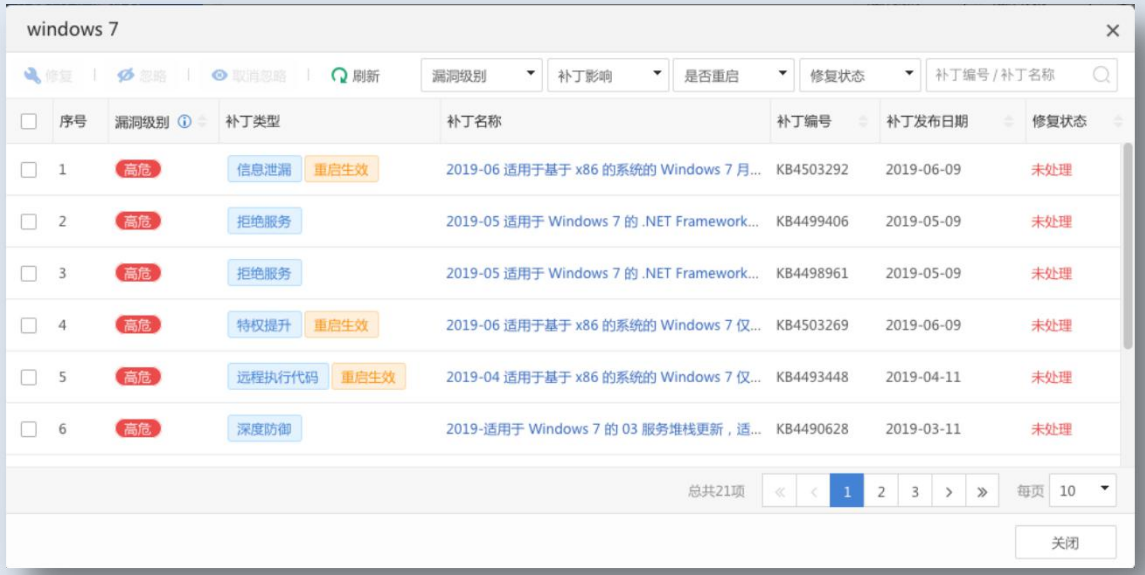
虚拟化底层兼容

VMWARE虚拟化　华为Cloud　华三H3Cloud　深信服虚拟化　Nutanix

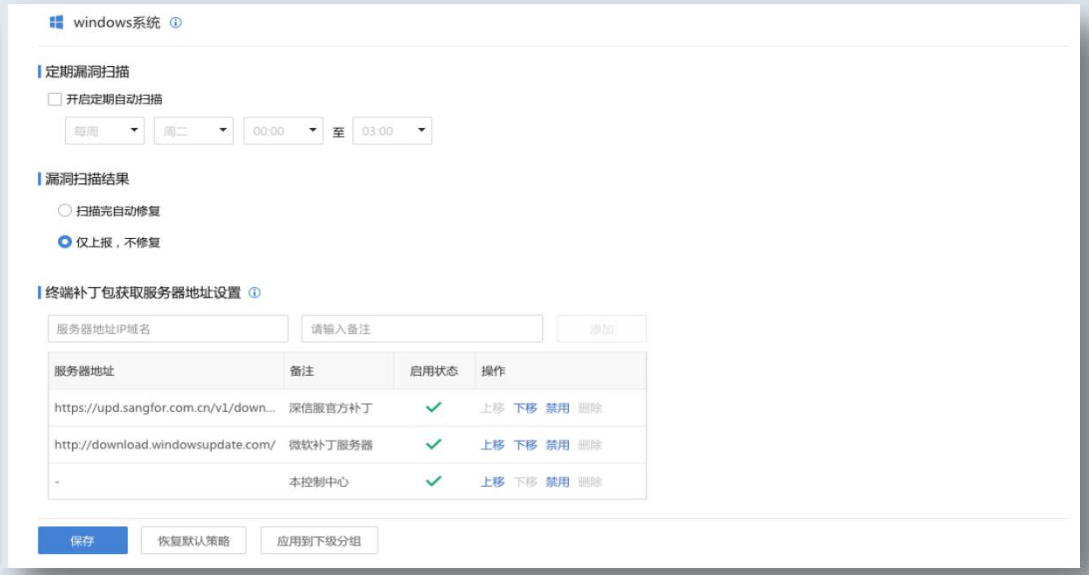
SmartX　Zstack　阿里云　腾讯云

摆脱复杂补丁选择，漏洞团队精心筛选

轻巧简单



标签化补丁说明，让漏洞修补不再盲目



深信服精选补丁库，兼容稳定有保障

安全基石
终端兼容性安全实验室

打造EDR终端安全兼容性实验室，遵循着【没有稳定兼容，一切安全都是空谈】

建设了基于2000+物理机、8000+虚拟机的兼容性环境。保障最优补丁筛选，适应复杂环境下发

终端资产的多维度信息采集，数据支撑安全运维

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

轻巧简单

终端分组，方便管理权限划分

操作系统/硬件信息/磁盘分区/资源占用

终端软件分布梳理

端口进程/启动项/计划任务/共享开放

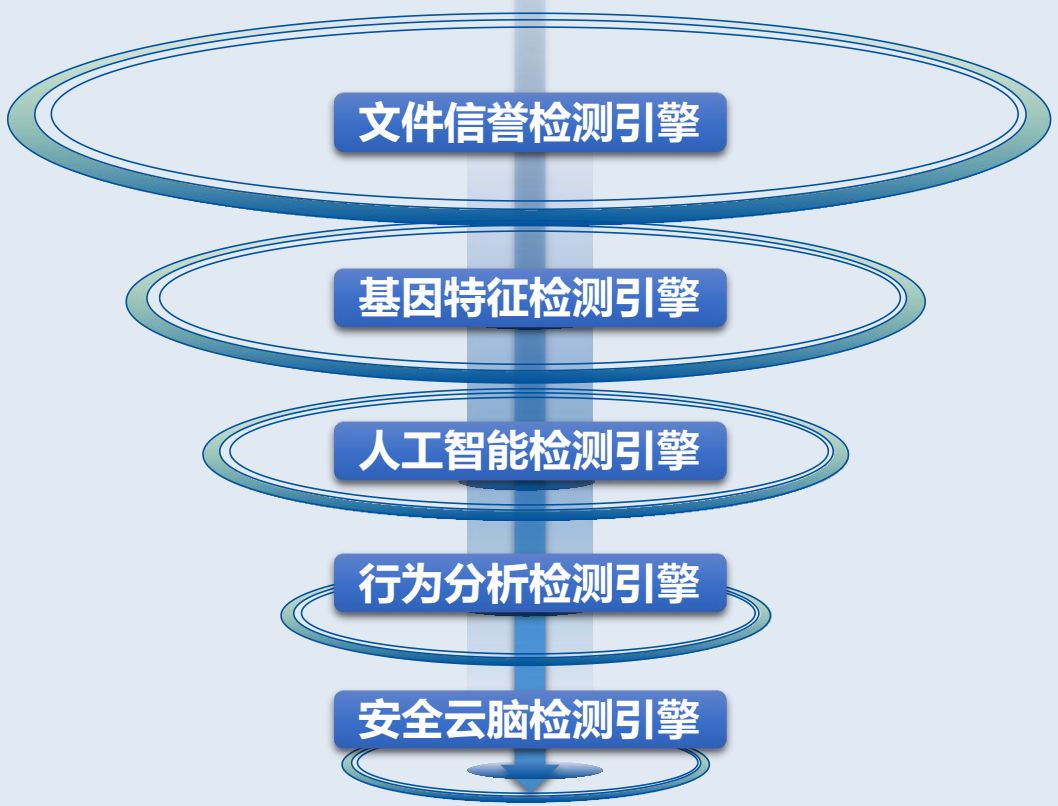
账户信息/账号脆弱性/异常权限账号

终端发现（未部署EDR的终端）

基于AI的漏斗型检测框架，高检出，低误报，资源消耗少

实时防护

多维度漏斗型检测框架　　层层过滤，快速识别



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

创新人工智能模型化检测技术
有效检测病毒变种及未知威胁

高检出

多层次过滤，不同类型威胁使用最优引擎检测

低误报

灰度文件进一步检测，防止误报警报疲劳

资源消耗少

90%文件被第一层引擎过滤，不需要所有引擎并发检测

恶性病毒检测清除修复效果最优

实时防护

感染型病毒

CAD病毒

宏病毒

0day病毒

勒索病毒

网“端”云协同联动，高效威胁处置

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

实时防护

2个5分钟

全球热点威胁爆发**5分钟内**同步至深信服云图

深信服云图深度分析后**5分钟内**赋能在线产品应对攻击

单一入口

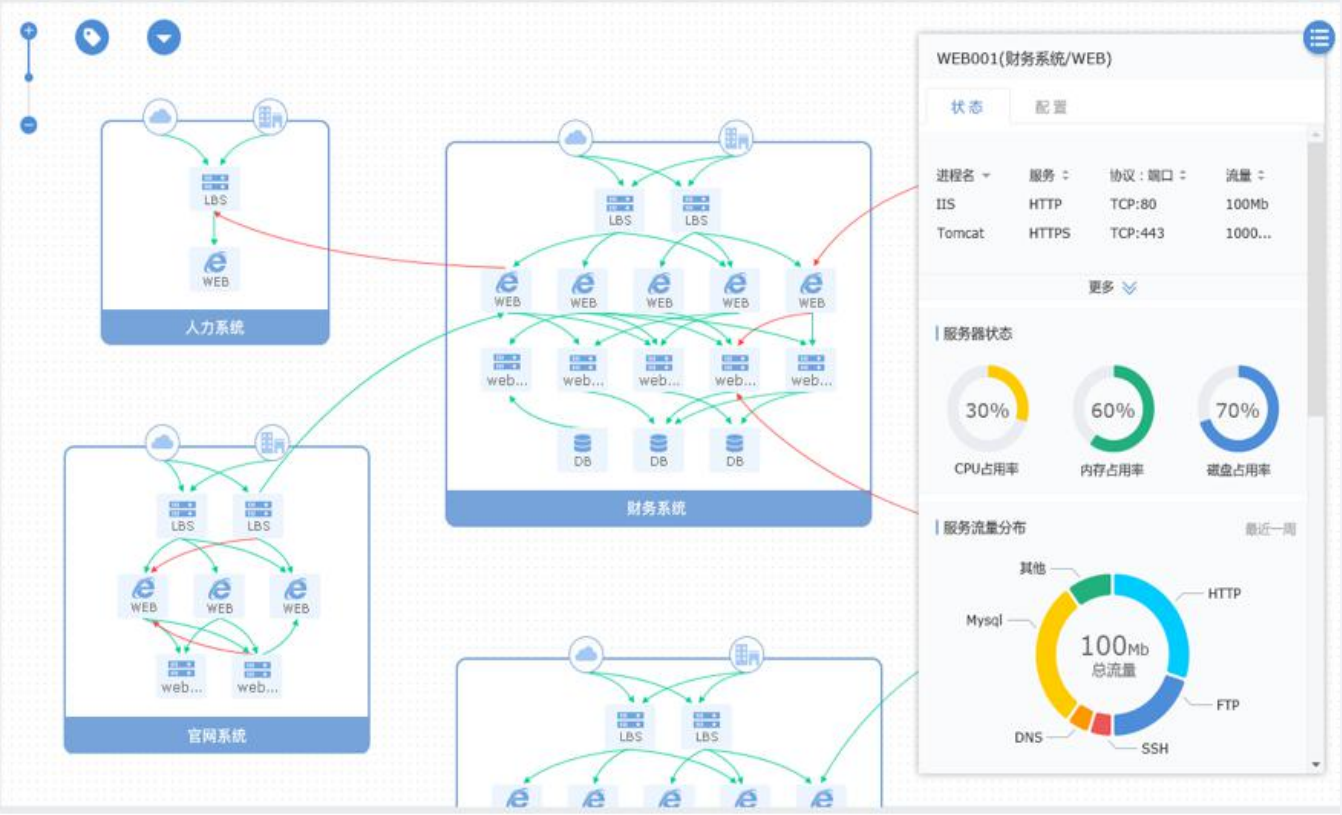
AF/SIP管理平台即可下发EDR查杀指令，快速处置威胁

深度协同

可以对僵尸网络进行溯源取证，让威胁定位更加精确

创新微隔离技术的全流向可视可控

流量可视管控



全网终端访问关系可视

对流量状态进行可视化展示，包括进程，服务，协议，流量等细粒度状态分布

全网终端访问关系可控

绿线放通，红线封堵
对IP，端口等维度进行策略限制

目录

产品管理平台部署形态

产品部署架构

本地或云WEB管理控制台

软件管理平台

终端范围	平台性能要求		
	CPU	内存	磁盘
1~50	2核	2G	500G
50~500	4核	4G	500G
500~2000	4核	8G	1TB

硬件管理平台

终端范围	管控终端数量
EDR-1000-A300	1000
EDR-1000-B600	2500
EDR-1000-C300	5000

云端SaaS管理平台

终端范围	管控终端数量
云EDR管理平台	2000

产品客户端授权模块

产品灵活选型

EDR报价一纸通		EDR终端检测响应平台	智防	智控	智响应	售卖模式
PC端	Windows	必选【只买一个】	必选 阶梯式价格 数量越多单价越低	可选 阶梯式价格 数量越多单价越低	可选 阶梯式价格 数量越多单价越低	每个端点价格 = 永久使用 + 一年规则库更新 -- 后续升级 每年25%
服务器端	Windows Server	必选【只买一个】	必选 三智合一，一个终端一个授权 一个授权=智防+智控+智响应+服务端防护			
	Linux Server					

产品客户端授权模块

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

产品灵活选型

控制中心	智防	智控	智响应	Server特供
安全策略	病毒查杀	微隔离可视	全网威胁定位	Webshell检测
终端资产管理	文件隔离	微隔离可控	SIP联动响应	服务器防护
全网风险可视	主机隔离	USB管控	AF联动响应	
	终端基线检查	违规外联管控	AC联动响应	
	僵尸网络检测	批量脚本下发执行	云SOC联动响应	
日志报表	暴力破解检测			
级联管控	文件实时检测			
安全策略	漏洞补丁			

安全云脑在线分析	服务
人工智能算法更新	
通用特征升级	

京东方科技集团股份有限公司（BOE）

背景

京东方科技集团股份有限公司（BOE）创立于1993年4月，是一家为信息交互和人类健康提供智慧端口产品和专业服务的物联网公司。根据市场咨询机构IHS数据，截至2018年第三季度，BOE（京东方）智能手机液晶显示屏、平板电脑显示屏、笔记本电脑显示屏、显示器显示屏、电视显示屏出货量均位列全球第一。

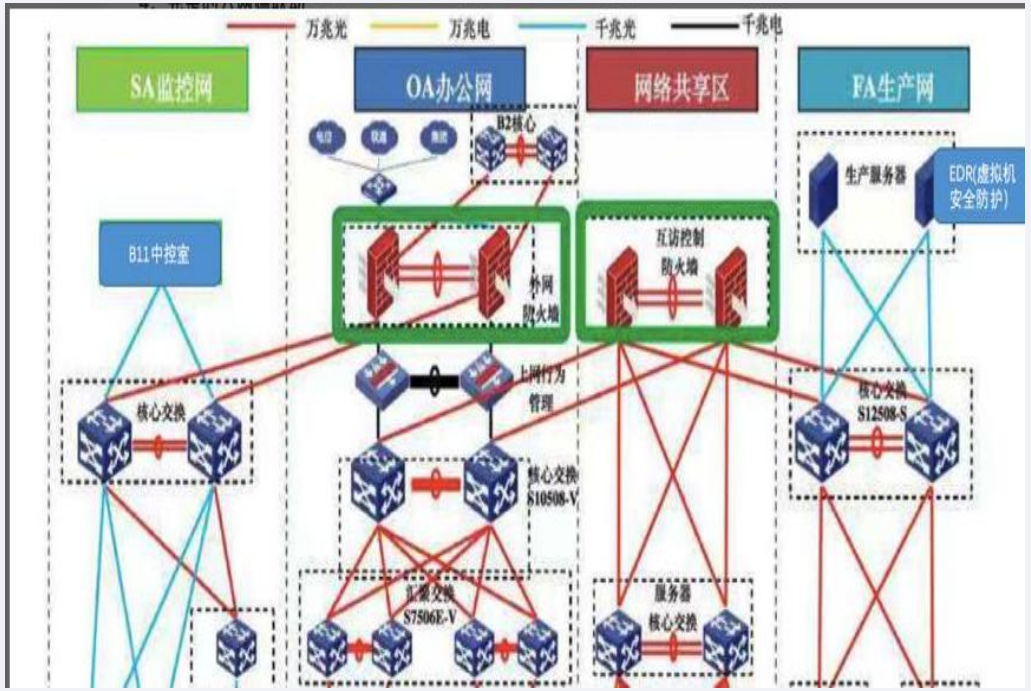
随着京东方整体业务的发展，京东方对于信息化的需求越来越大，专门成立信息安全小组，构建整体信息化运营机制；与此同时，安全成为了京东方考虑的核心重点，同时对于品牌有着极高的要求。

解决方案价值

可管可控、精准防护、可视可信、智能防御：满足了绵阳京东方制定的“可管可控、精准防护、可视可信、智能防御”防护策略，一、二期设备共同构建“预防-防御-检测-响应”的闭环安全体系，有效帮助用户及时发现和处置数据中心发现的威胁，降低安全运维成本。

EDR的离线检测能力：绵阳京东方产生业务系统处在绵阳京东方内网，EDR离线检测能力解决了无直接访问互联网权限的用户“需要联网才能提供有效检测防御”的业务需求。

AF/AC的安全能力与端点EDR强强联合：AC通过识别是否合法用户通过合法路径访问等进行精细化认证，联合EDR终端资产核查，落实责任到人，并且分不同等级基于不同客户的访问权限，安全访问方面更加精细化，解决用户所担心的L2-7层的安全隔离和防护问题。



整体拓扑

福建福耀玻璃工业集团股份有限公司

背景

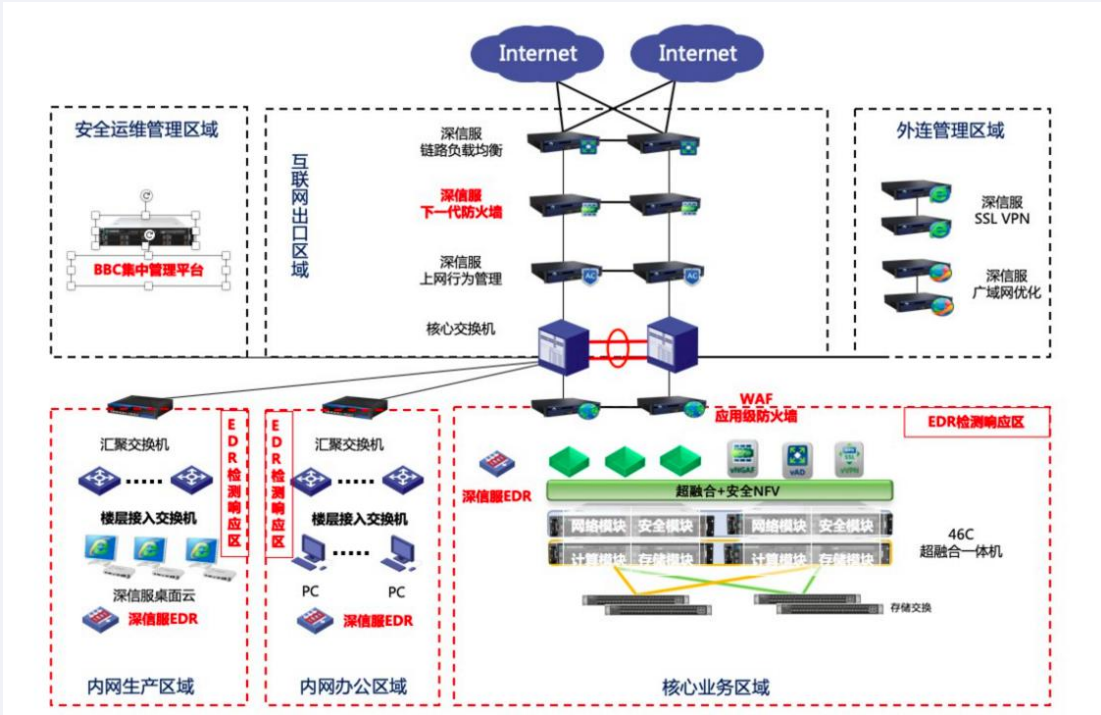
福耀集团（全称福耀玻璃工业集团股份有限公司）是专注于汽车安全玻璃和工业技术玻璃领域的大型跨国集团。在全球，福耀集团汽车玻璃市场份额约占23%，产品行销到了约70个国家和地区，为宾利、奔驰、宝马、奥迪、通用、丰田、大众、福特、克莱斯勒、日产、本田、路虎等世界知名品牌提供全球配套服务。同时，福耀集团不断推进“智能制造”，从“大制造”到“强制造”，力求成为一家改变世界汽车玻璃行业格局，推动中国汽车玻璃真正走向世界的伟大企业。

解决方案价值

集中管理、精准防护： 满足了福耀集团对公司整体安全加固的目标，各分公司安全状况能够及时汇总至总部安全感知平台，且可以与网络中下一代防火墙、上网行为管理、终端检测响应EDR做到联动封锁、集中管控，形成一套安全、有效、可落地的方案。

广泛的兼容能力：福耀集团国内部分事业部有大量的业务服务器，不同服务器使用系统涵盖大部分系统及版本，通过EDR广泛的兼容能力实现对全部服务器的集中管控。

云网端协同联动的安全加固方案：一期建设完毕后，深信服还会继续提供二期、三期加固建设，内容包括日志审计+基线核查+运维审计+桌面云+EDR加点+探针加点+安全服务，还会协助福耀集团制定相应的规章制度，建立完善的安全防护体系。



整体拓扑

深圳市左右家私有限公司

背景

深圳市左右家私有限公司是一家生产高档家私的内资民营企业，拥有一条集研发、设计、生产、销售于一体的完整产业链，占地面积近100万平方米。发展至今，在国内市场拥有1680多家品牌专卖店与经销点，拥有独立进出口权，产品行销海内外，实现了国内外市场的深度覆盖。

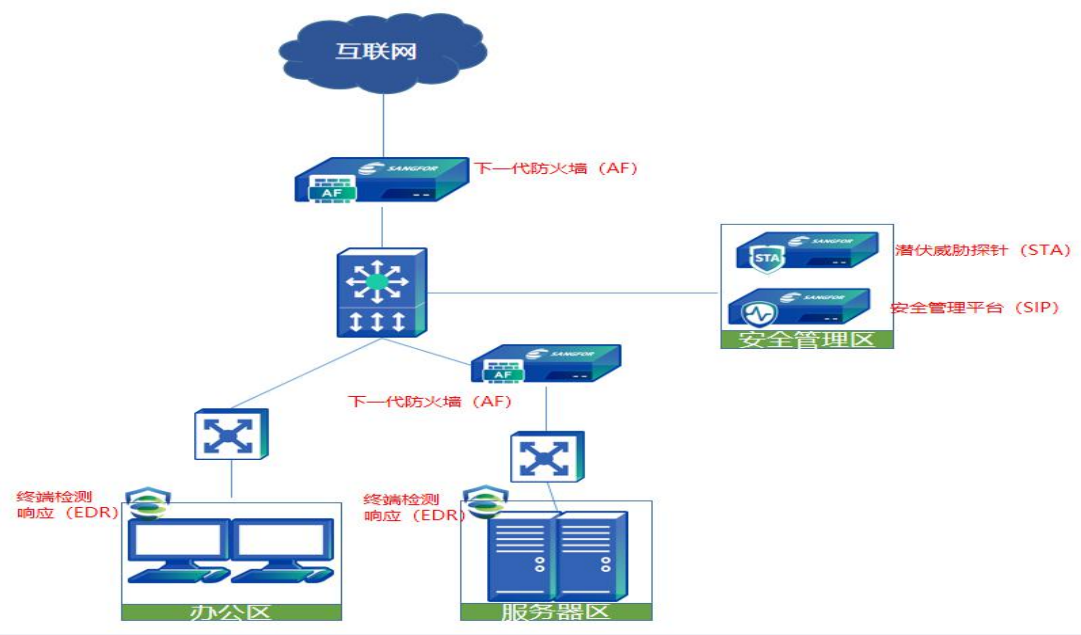
2019年4月，客户内网有10台电脑中了挖矿病毒，70台电脑无故卡慢、无故蓝屏，还出现了丢包的情况。此前，客户使用的卡巴斯基杀毒软件，由于较高的资源占用率，已经无法适用客户端生产线上老旧的PC。

解决方案价值

终端轻量级多维度检测：深信服EDR的轻量化设计，能够减少CPU、内存、磁盘IO等计算机资源的消耗，能够适用于客户生产线上很多比较老旧的PC。同时多维度的漏斗型检测机制，通过AI引擎、行为引擎、全网信誉库等保障查杀的精准性。

微隔离与威胁快速处置：微隔离利用应用角色之间的主机流量访问控制的技术，可规范不同主机、不同业务安全域之间的访问行为，通过全局扫描、分析取证，可以溯源攻击主机，帮助用户快速隔离失陷主机。

云网端联动实现大闭环：EDR 可与深信服其他安全产品进行协同联动响应，实现内外部威胁情报实时共享。EDR与AF、SIP 进行关联检测、取证、响应、溯源等防护措施，形成应对威胁的云网端立体化纵深防护闭环体系。



整体拓扑

金汇信托

背景

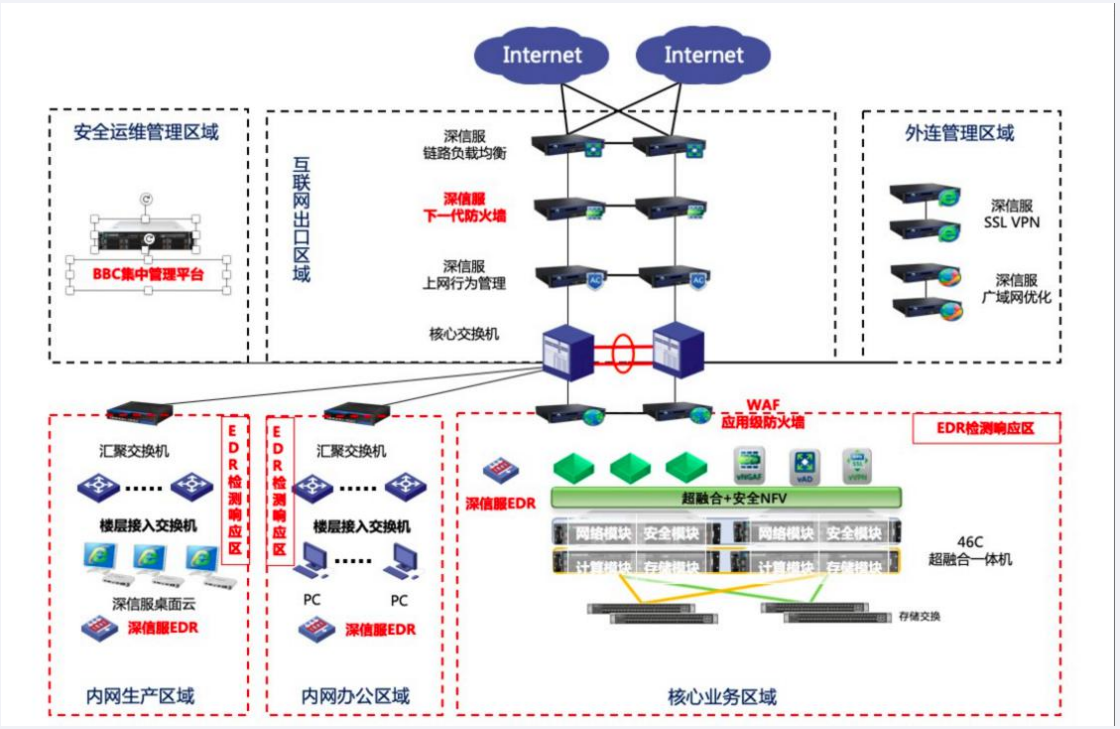
浙商金汇信托股份有限公司是经中国银行业监督管理委员会批准的专业信托理财机构，公司成立于1993年，是一家行业领先、特色鲜明、经营稳健、品牌卓越，能够为当地经济发展提供强大支持的优秀信托公司。公司立足浙江、辐射上海及长三角洲地区，服务于全国经济发达地区，重点服务大型国企、中大型民营企业、上市公司、保险、银行等高端客户群体。

解决方案价值

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。



整体拓扑

银联国际

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。

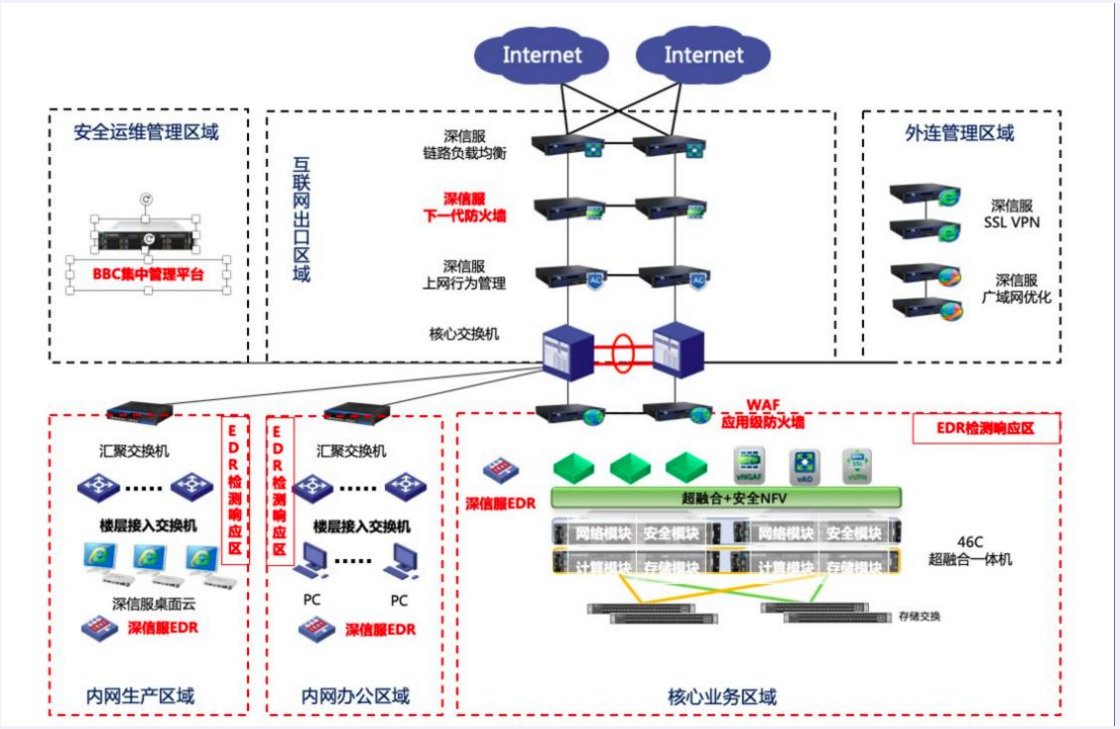
银联国际生产网在去年勒索病毒肆虐的大环境下，客户意识到内网安全建设存在薄弱点，尤其是生产网上跑核心业务的虚拟机安全建设不足，存在勒索病毒等高级威胁入侵的风险，由此开始提出虚拟化安全建设的相关要求。

解决方案价值

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。



整体拓扑

南方科技大学

背景

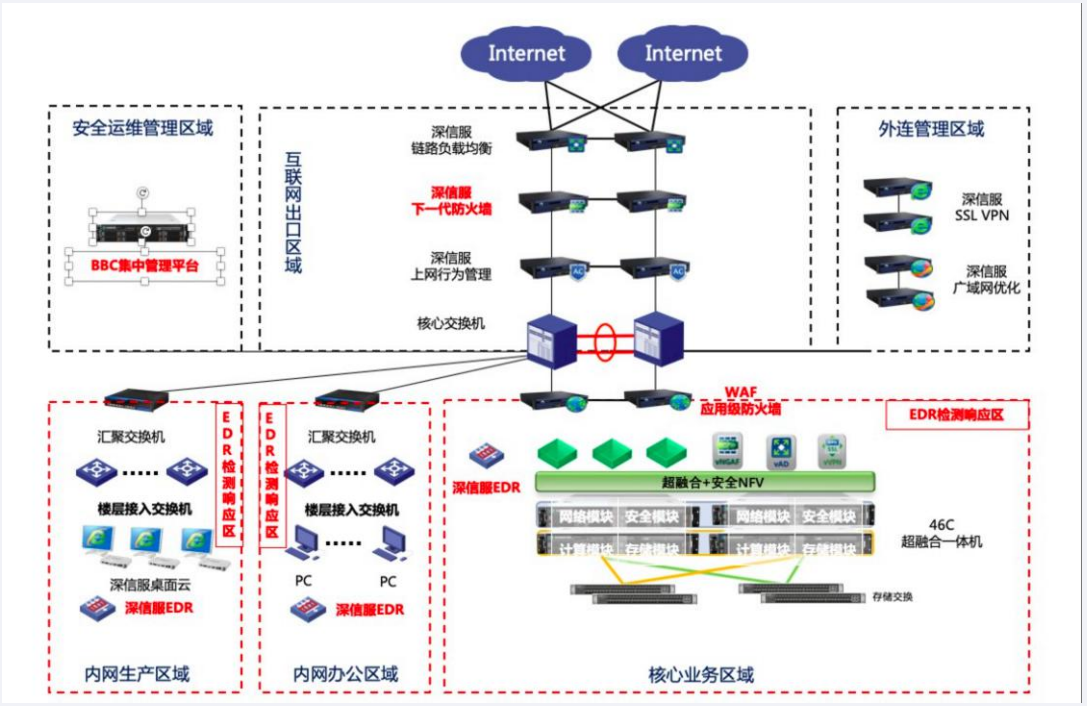
南方科技大学（Southern University of Science and Technology），简称“南科大”，是国家高等教育综合改革试验校、广东省高水平大学重点建设高校，由广东省领导和管理的全日制公办普通高等学校，是深圳市创办的一所创新型大学，目标是迅速建成国际化高水平研究性大学，建成中国重大科学技术研究与拔尖创新人才培养的重要基地。南科大以理学、工学学科为主，兼具部分特色人文社会学科与经济、管理等学科。

解决方案价值

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。



整体拓扑

THANK YOU

2020 深信服科技