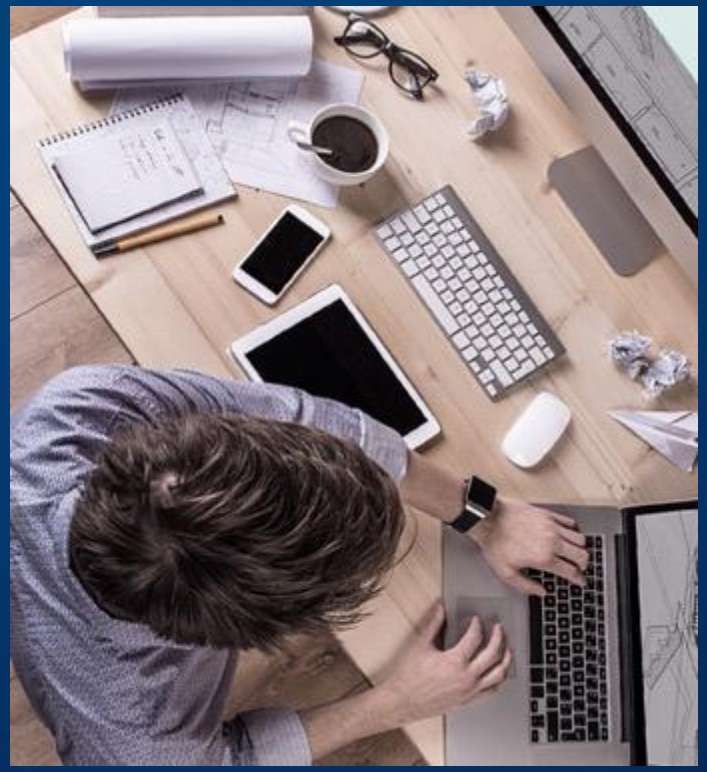
SANGFOR
深信服科技

下一代终端安全平台

深信服终端检测响应EDR

目录

SANGFOR 深信服科技



01

终端安全面临的挑战

越来越多的外部威胁、传统终端安全能力缺失

企业级用户深受其害

威胁形势严峻

WanaCry爆发

150多个国家，30万用户 80亿美元

GlobeImposter 传播

国内医疗、法院、教育等行业均深受其害

勒索病毒频发

- 政府-无法为老百姓提供及时的政务服务
- 医疗-患者无法得到及时的护理和救治
- 公安-警察无法及时响应报警和办理业务
- 金融-导致交易无法进行，银行数据加密
- 企业-无法开展经营行为，导致严重的损失

企业级用户深受其害

相较于个人用户
企业终端、数据等资产价值重要性突出

网络化办公，威胁来源途径多样，高级攻击概率大

针对性的终端安全威胁
造成损失更大、响应要求更快、运维复杂度更高

传统特征杀毒失效

SANGFOR 深信服科技

未知威胁防护能力缺失

弱、被动

基于病毒特征库方式进行杀毒

高级威胁持续产生，呈被动、后知后觉特点

依赖性大

依赖云查杀

杀软依赖云查杀，隔离网环境检测能力骤降

高级威胁层出不穷

特征受限无法应对

天生受限

本地病毒特征库有限

特征库数量与已知病毒样本不匹配

资源加重

特征数量不断增多

加重终端资源以及运算成本

缺乏快速响应机制

SANGFOR 深信服科技

病毒驻留时间长　　业务影响巨大

如何快速响应

手动维护时间过长

高级威胁层出不穷

不可控的进行快速传播
驻留时间长、无法快速响应

人员维护成本巨大

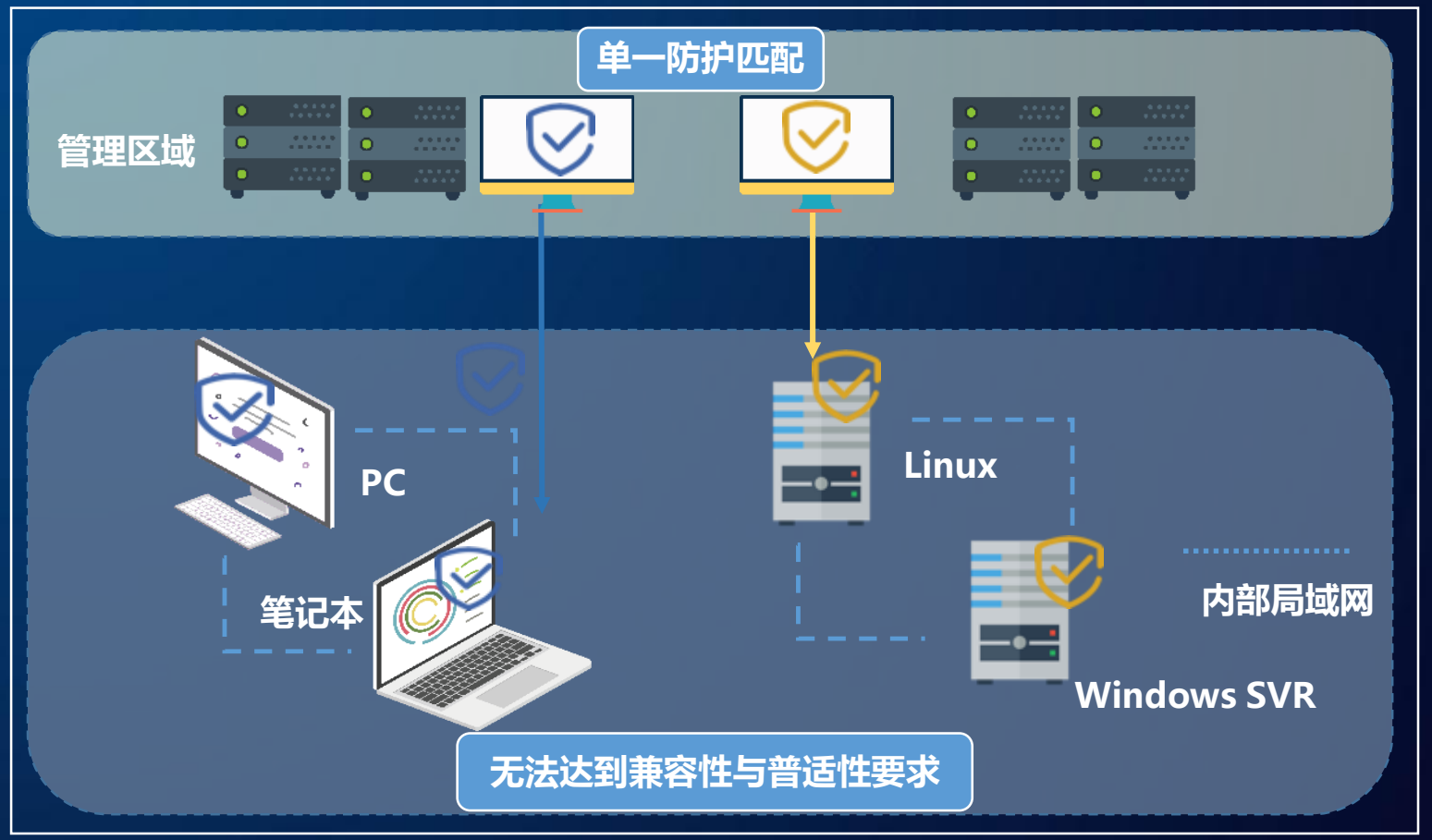
越来越多的外部威胁

分裂的管理端、终端

单一的防护匹配关系

所需防护终端类型多样

不满足普适性与兼容性要求



未实现一体化防护　　管理维护工作量大

02

面向未来，有效保护

人才储备、技术积累

深信服人才储备

SANGFOR 深信服科技

重视研发投入

4

4大研发中心
深圳 北京 长沙 硅谷

20%

营业收入
投入研发

40%
30%

40%研发人员
30%硕博学历

攻防专家

数据科学家

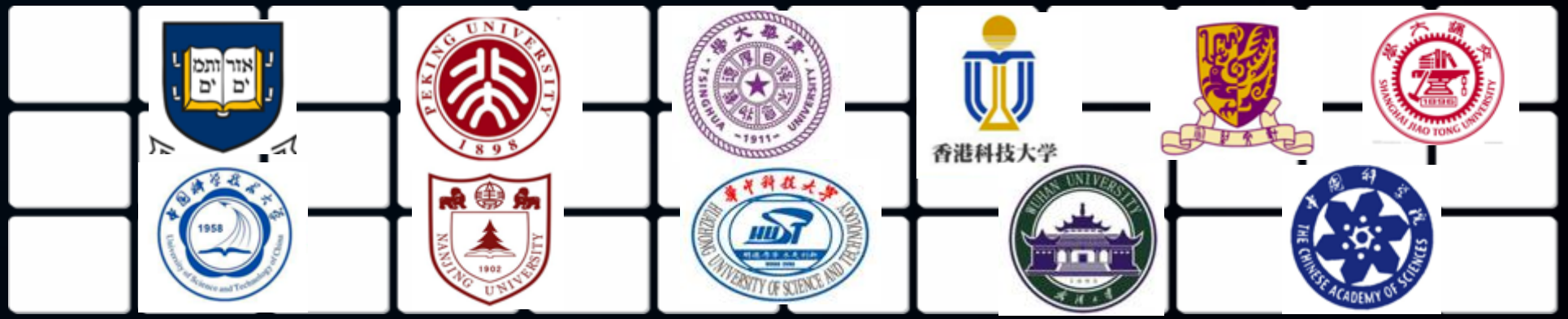
安全分析师

深信服人才储备

SANGFOR 深信服科技

高端人才引进

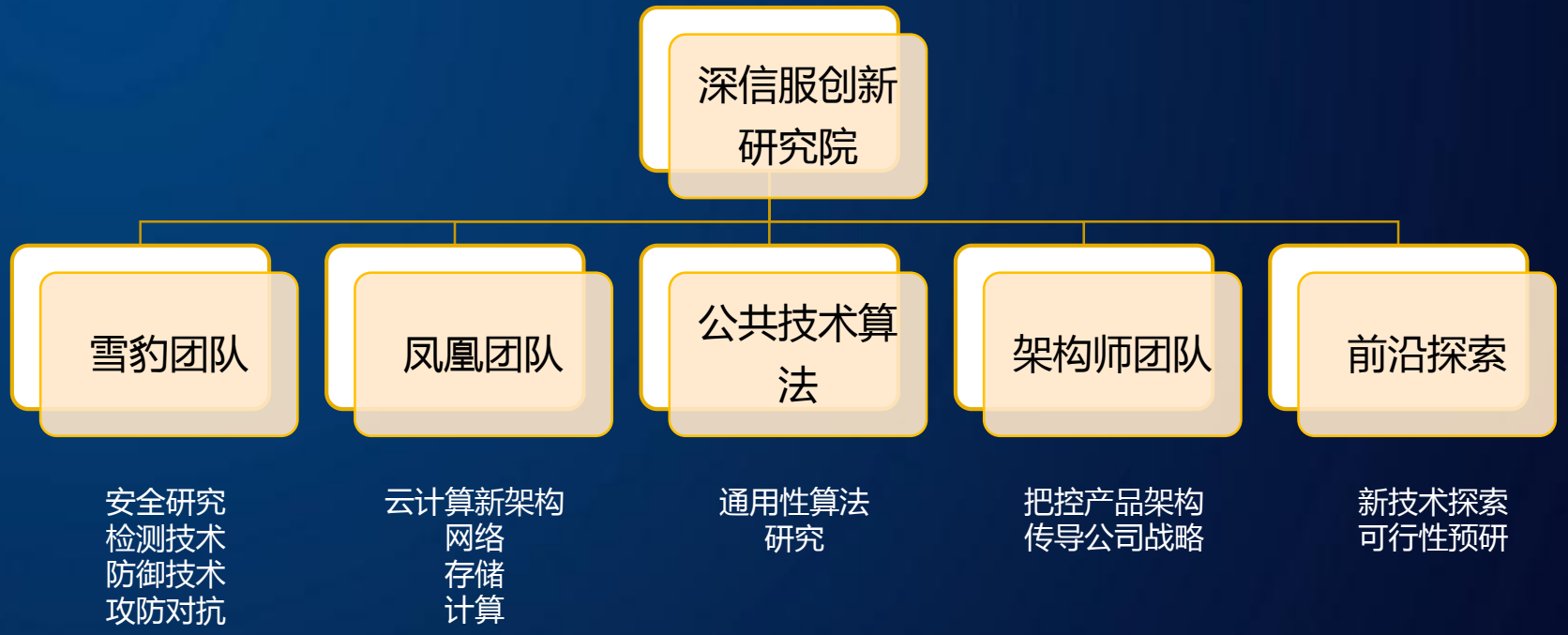
- 目前深信服在职博士30+以上，团队主要成员来自耶鲁大学、北京大学、清华大学、香港科技大学、香港中文大学、瑞士洛桑联邦理工学院、上海交通大学、中国科技大学、南京大学、中国科学院、华中科技大学、武汉大学、大连理工大学、中山大学等。



深信服技术积累

SANGFOR 深信服科技

深信服创新研究院



创新成果——检测能力显著提升

SANGFOR 深信服科技

基于人工智能的研究落地成果显著

- LSTM算法较N-gram有显著提升，僵尸网络检出率达到**99.7%**。
- 帮助某客户每天拦截1万封以上恶意邮件
- 平均每周检出僵尸主机 2301 台
- 单设备最高每天检测出**132626**条黑链

面向未来，有效保护

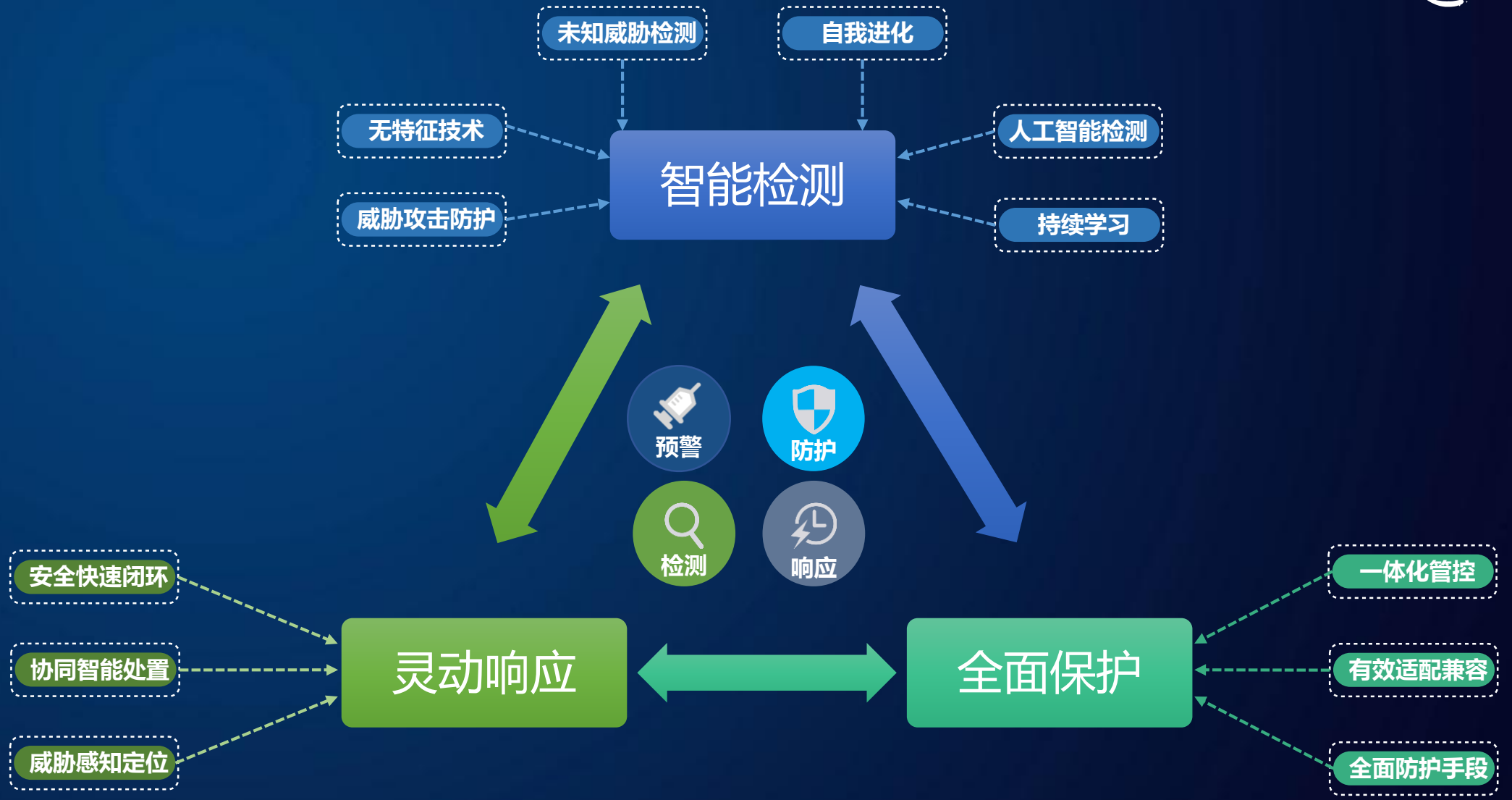
03

下一代终端安全EDR

下一代终端安全框架、智能检测、灵动响应、全面保护

下一代终端安全框架

SANGFOR 深信服科技



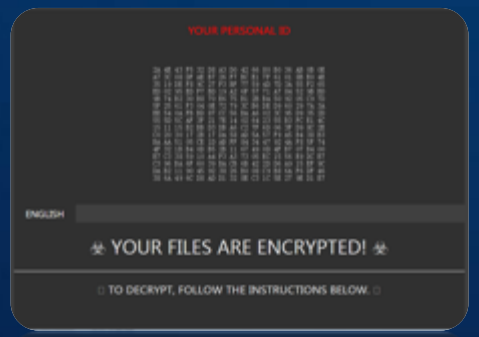
智能检测

SANGFOR 深信服科技

深信服人工智能检测引擎SAVE
Sangfor Anti-Virus Engine

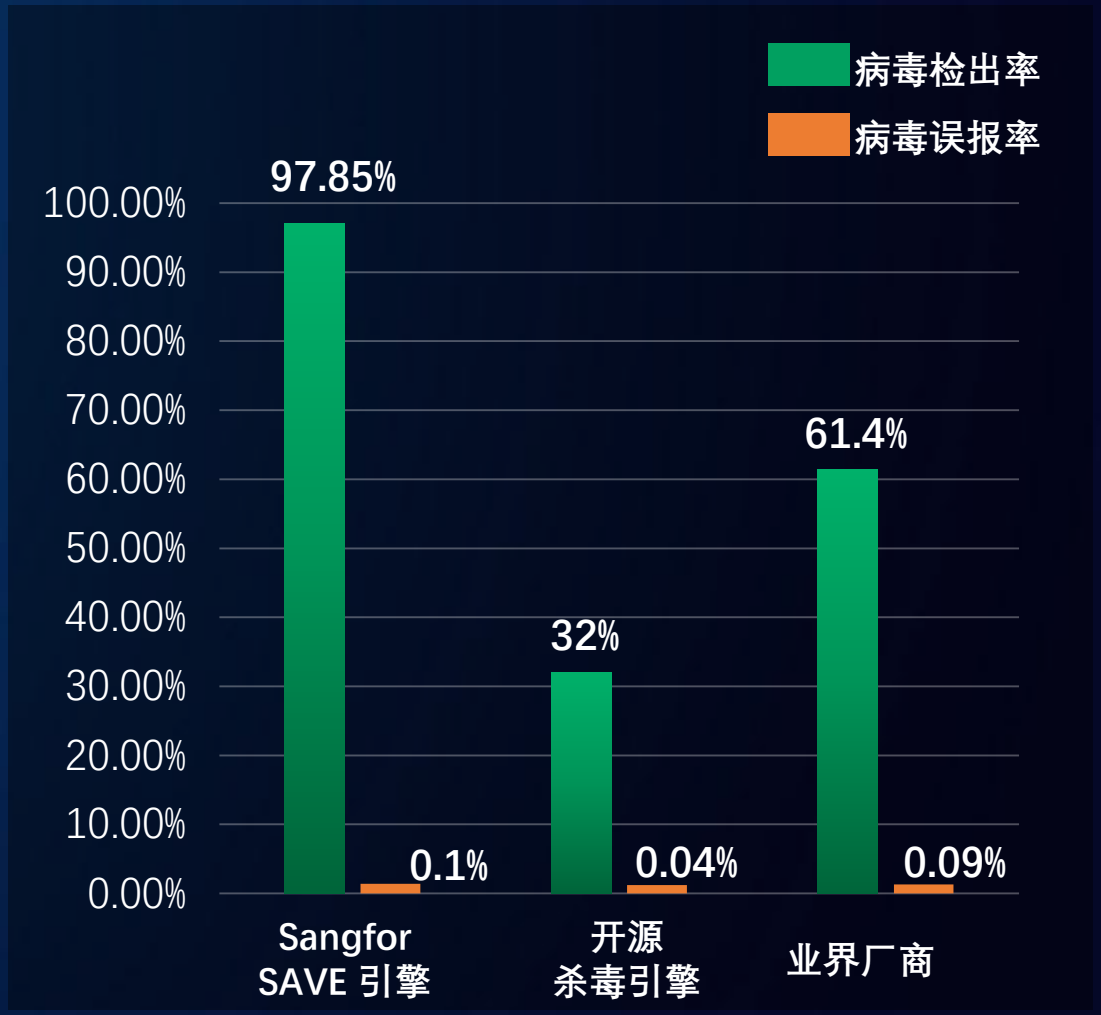
创新人工智能无特征技术
准确检测未知病毒

未知病毒检出率高达97.8%，对已知病毒检出率高于99%



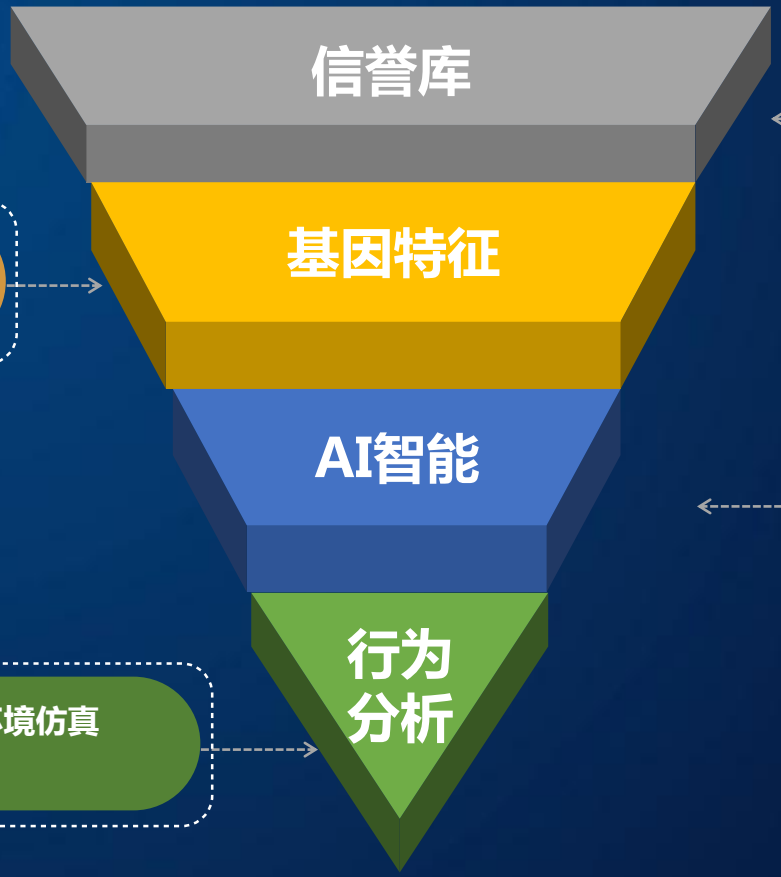
GlobeImposter勒索病毒

查杀成功率 **100%**



智能检测

SANGFOR 深信服科技



本地、全网、安全云脑

基因扫描
速度快、准确率高、误杀操作少

利用深度学习训练数千维度的算法模型
持续学习，自我成长
无特征检测技术

虚拟沙盒、引擎和操作系统环境仿真
解析恶意代码本质

多层级检测，应对百分百安全威胁

灵动响应

SANGFOR 深信服科技

多维度响应处置措施

主机微隔离

一键终端隔离

自动隔离

第三方威胁情报社区协助处置

远程批量脚本执行

一键文件处置

一键文件修复

全局白名单

全局IP黑名单

全网威胁处置

灵动响应

SANGFOR 深信服科技

多维度、快速响应
极大缩短威胁驻留时间

全面保护

SANGFOR 深信服科技

全面保护、减少无效工作、体现运维工作价值

全面检测防护手段

redhat® SuSE ORACLE LINUX 红旗® Linux

04

EDR的典型场景应用

等保合规、一体化、未知威胁防护、快速响应处置、企业级运维

等保合规场景

01 **政策合规**

贴合国家政策法规，满足主机恶意代码防范要求，基线检查，确保终端安全合规

02 **分域保护**

对各区域实施安全保护措施形成立体的安全保护体系

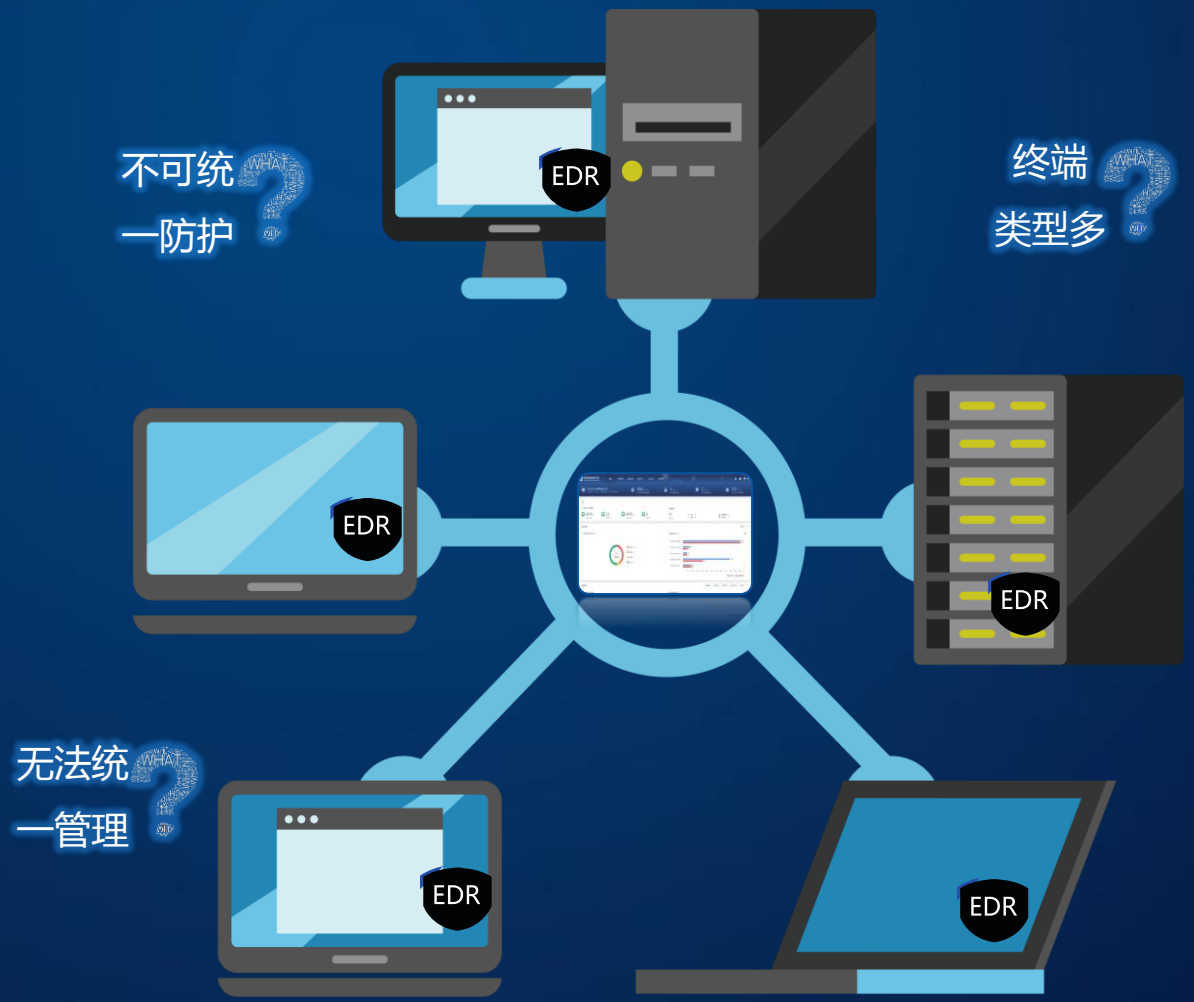
03 **有效防护**

对终端进行全面防护，有效应对已知、未知、高级威胁

04 **能力提升**

安全不止合规，持续输送防护+管控+检测+响应安全能力

一体化防护场景



01 **全面适配**

不区分系统类型，EDR全面适配

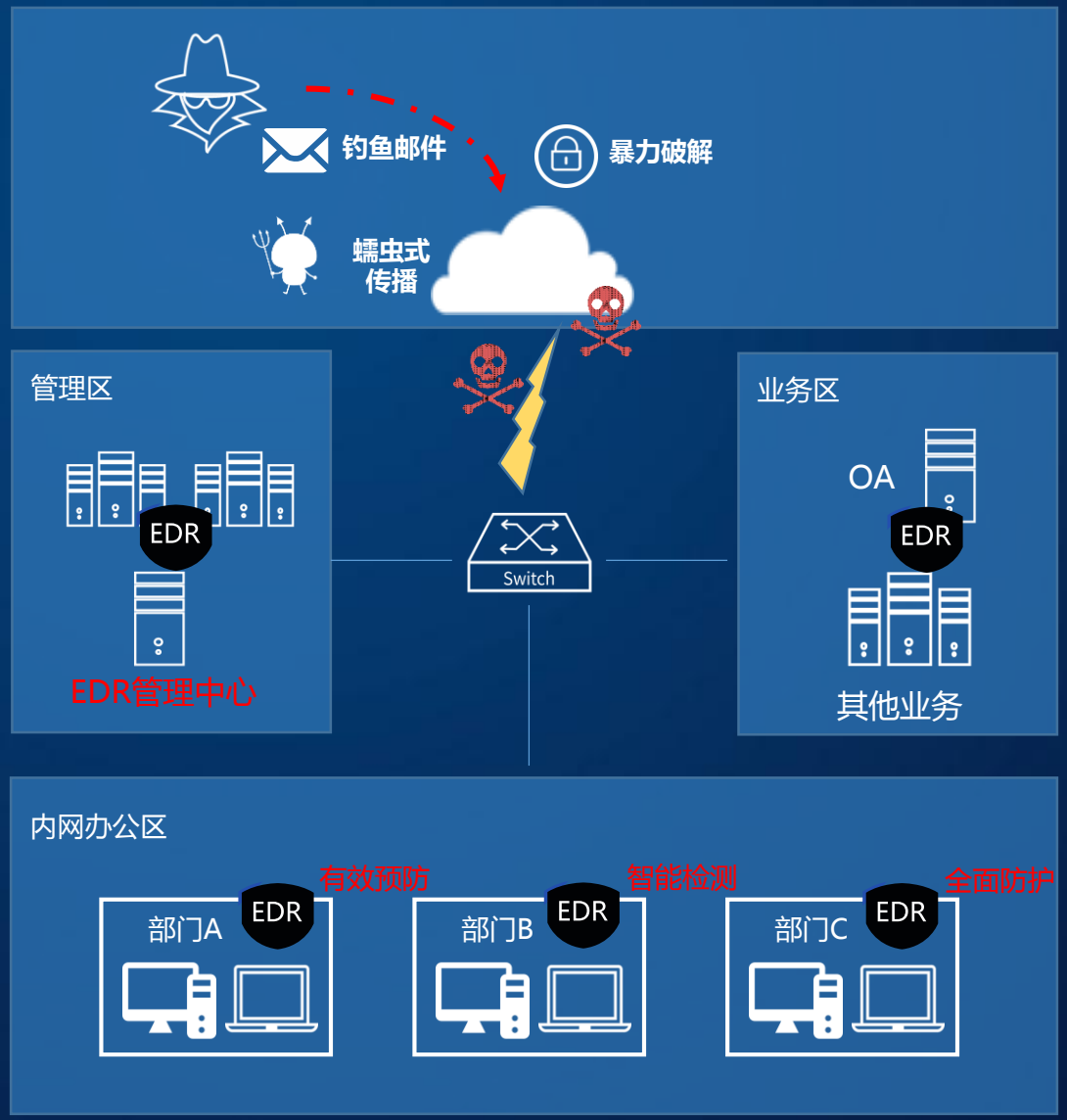
02 **统一防护**

多类型终端，一体化策略配置，统一基线、统一防护

03 **一体化管理**

终端、服务器、虚拟机，不分别对待，一体化管理

未知威胁防护场景



01 **有效预防**

账号及密码策略排查

全网威胁展示与定位

基于最小授权原则，做不同业务、不同终端隔离访问控制

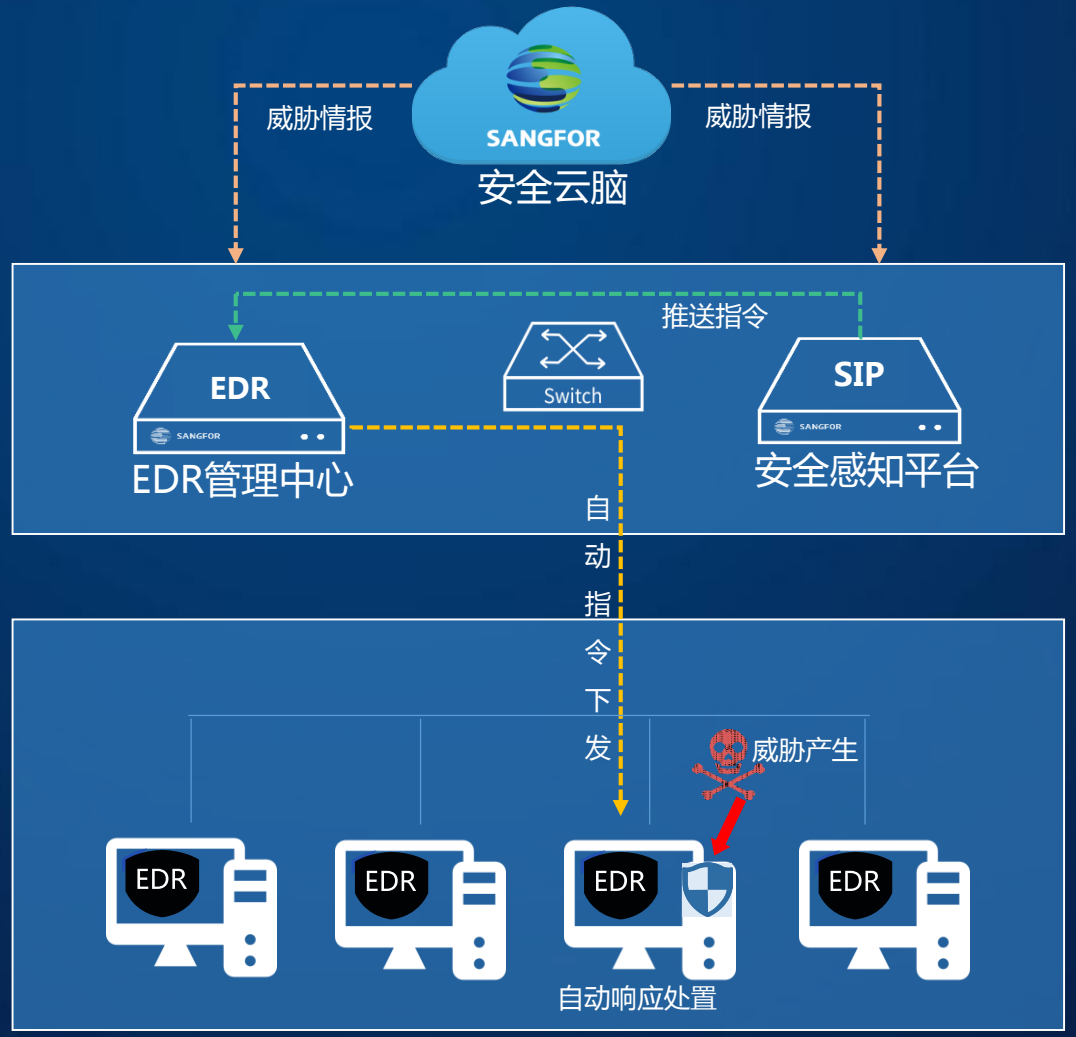
02 **智能检测**

利用人工智能SAVE引擎，无特征技术，对未知威胁进行实时检测

03 **全面防护**

处置暴力破解、WebShell、僵尸网络等威胁

快速响应处置场景



01 **灵动处置**

一键终端隔离、自动隔离

一键文件隔离、修复

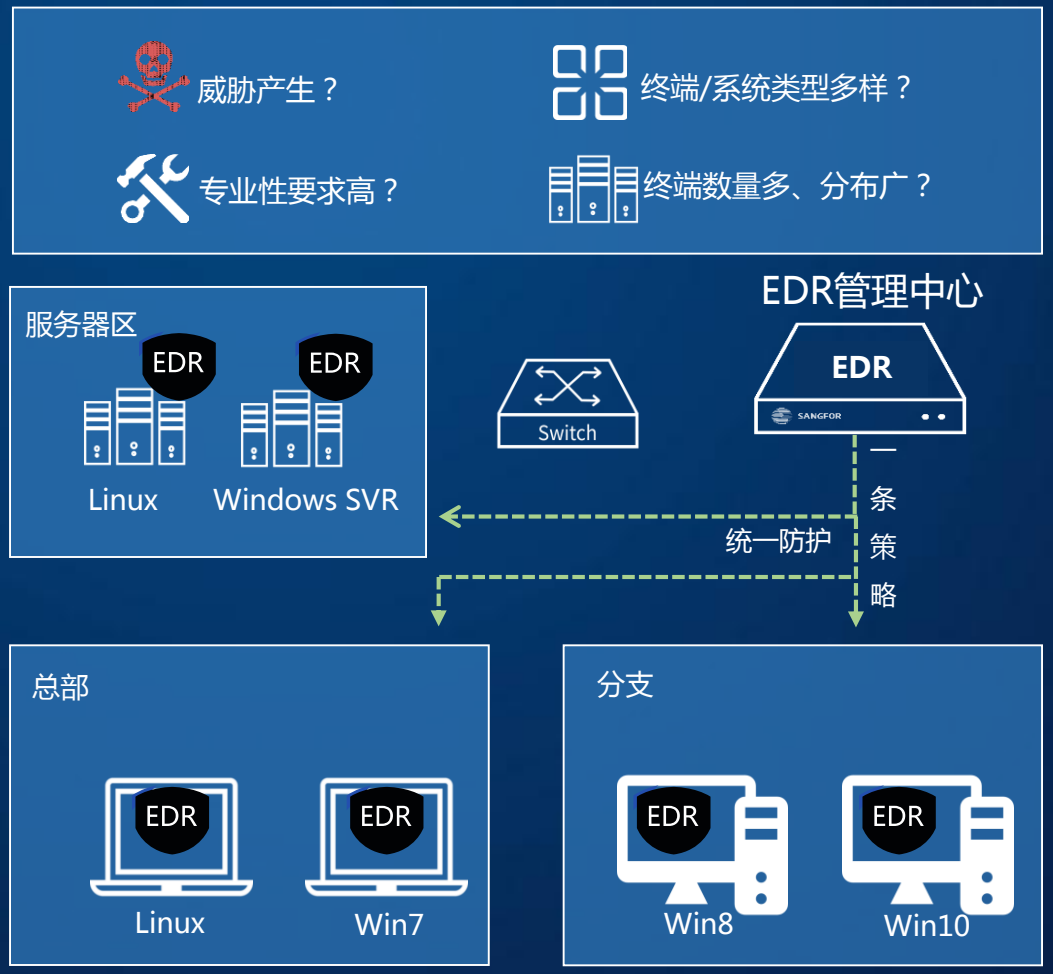
协同联动处置

全局黑名单、全网威胁展示定位

02 **快速响应**

多维度感知、自动响应，快速处置威胁，极大缩短威胁驻留时间

企业级运维场景



01 **全面防御**

多维度持续威胁检测、响应，有效威胁防御，杜绝威胁产生，减免不必要维护成本

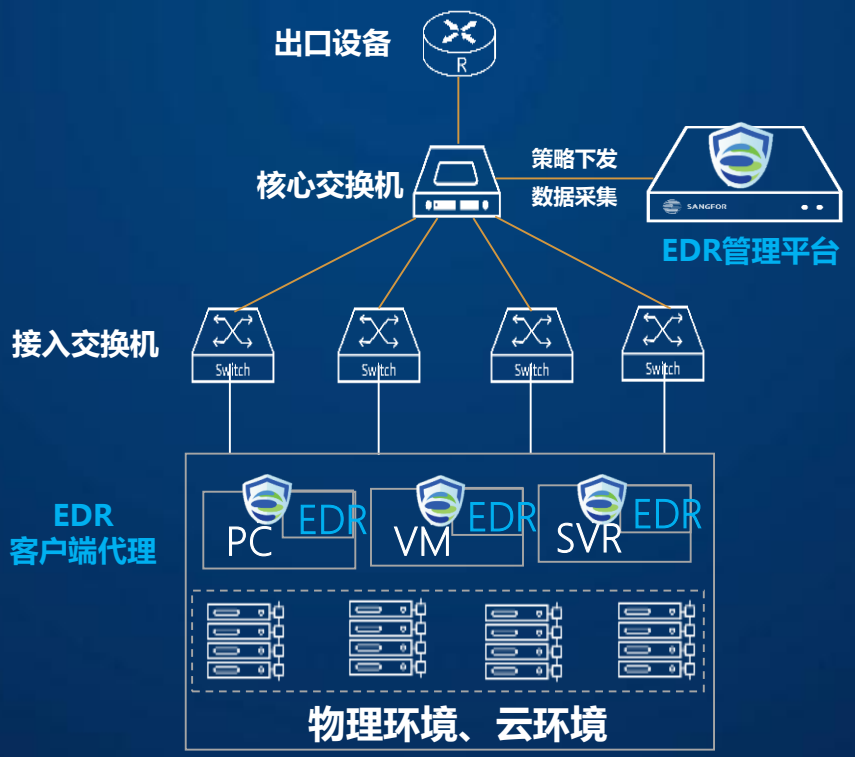
02 **统一维护**

资产统一维护，责任落实到人，风险快速定位

03 **便捷管理**

不区分终端/系统类型，一体化策略下发，自动执行

深信服终端检测响应平台



- EDR=Endpoint Detection Response
  智能检测、灵动响应、全面保护
- 系统为C/S部署、B/S管理方式
  无需对网络进行调整或对网络设备进行配置
- ✓ 运用AI智能、信誉库、基因特征、行为分析全面应对威胁
- ✓ 文件/主机/联动，多维度威胁响应处置
- ✓ 广泛适配辅以多角度防护措施，确保终端全面保护

赋予用户持续进化的预警、防御、检测与响应能力

为IT和业务提供持续保护，让安全建设更有效、更简单！

SANGFOR
深信服科技

谢 谢

Thanks for watching

深圳市南山区学苑大道1001号南山智园A1栋
Shenzhen nanshan district 1001 xueyuan avenue
of nanshan garden A1 building

0755-86627888
market@sangfor.com.cn

www.sangfor.com.cn