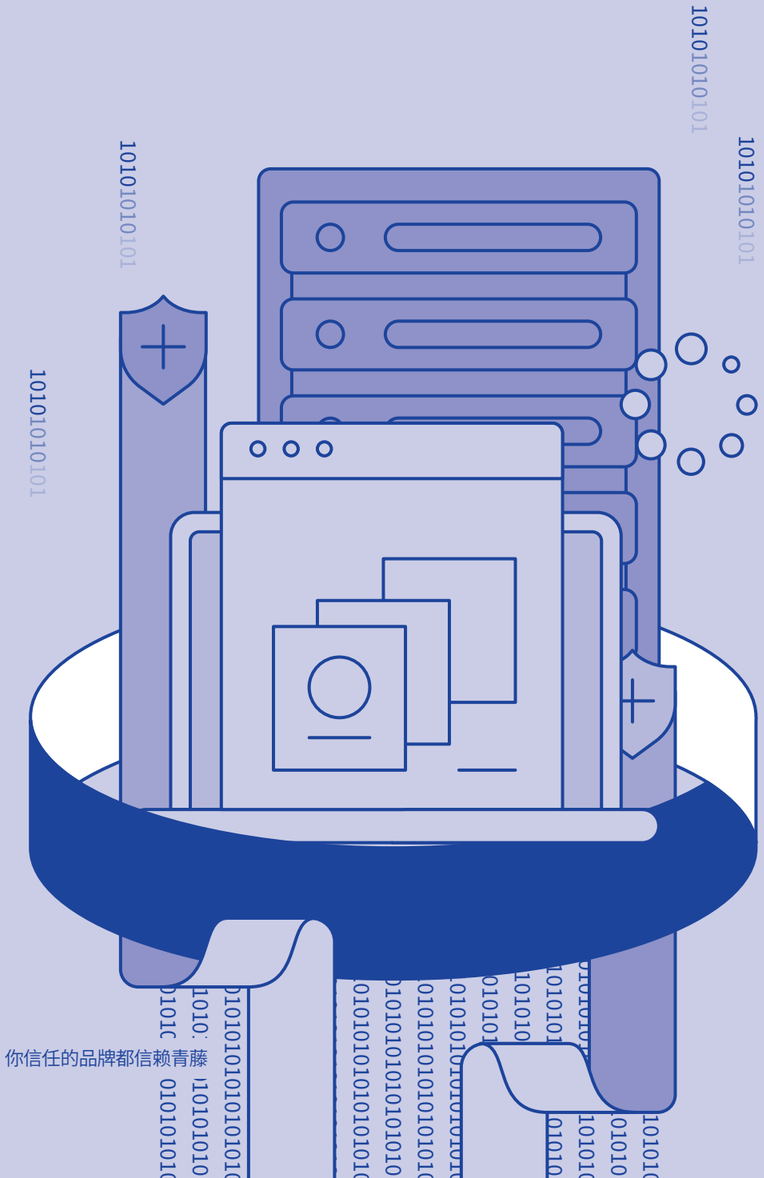
互联网行业
Internet Industry



260 余家

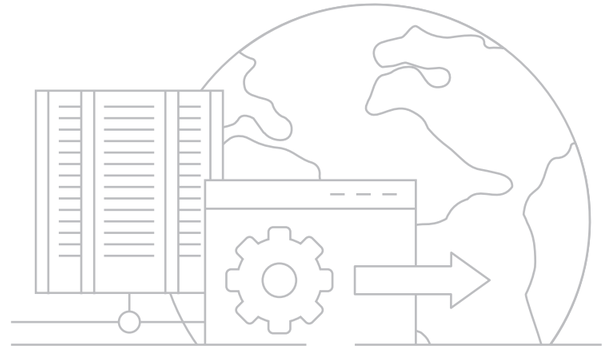
顶级主流互联网企业

40,000+

运营漏洞数

970,000+

行业Agent 部署量



互联网企业网络安全的好坏可能会对业务效益、商业竞争、品牌形象、安全合规这几个方面产生重要影响。现在互联网行业的安全要求越来越严格，《网络产品安全漏洞管理规定》《个人信息保护法》等相关信息安全的法律也在不断完善。如果互联网企业能够做好安全合规、数据安全保护、主机威胁防御等安全工作，将进一步保障和促进公司业务的发展。

青藤 部署灵活适应互联网业务频繁变化，弹性扩容

全面的入侵防护：

依靠实时的检测和全面的数据分析，及时发现威胁并全面溯源分析，降低安全风险。

高价值数据保护：

青藤通过全面的安全防护及安全服务，保护互联网企业最核心的客户数据安全。

有效的合规管理：

青藤从整体国家和行业层面监管要求出发，助力互联网企业满足监管合规要求。

某互联网视频公司智能、灵活、联动的安全防御方案

背景概述

某互联网视频公司 2018 年在美国纳斯达克上市，经过十年多的发展，构建了一个源源不断产生优质内容的生态系统，并入选“ BrandZ ”报告 2019 最具价值中国品牌 100 强。

> 安全负责人：“通过与青藤的合作，我们快速地解决了过去资产不清晰、安全状态不透明的问题。在产品改进和售后服务方面，青藤针对安全部门不断提出的问题，一直保持着耐心倾听和快速迭代，这十分难得。”

客户需求

网络攻击、勒索、安全漏洞等事件令人惴惴不安，敏感信息保护更是互联网企业安全建设的重中之重。在安全建设初期，客户一直被以下问题困扰。

资产庞杂，梳理不够明晰

客户应用架构庞大、数据庞杂，业务应用间交互性、数据的多样性，导致IT资产混乱，相关人员无法系统地了解资产的具体情况。

缺少掌控整体安全态势的能力

各种潜在威胁层出不穷，客户需要主动发现潜在安全风险，及时知道谁、什么时间、做过什么样的攻击、攻击是否成功、目标系统受影响程度等安全问题。

缺少入侵感知和灵活响应能力

客户需要强化主机入侵攻击的监控能力，在遭遇攻击时可以通过便捷的工具查询主机相关信息，快速定位风险，灵活响应处理。

解决方案

通过独立部署模式实现约2.5万台服务器的安全防护，全方位自动清点客户已有资产，并通过资产扫描发现边缘灰色资产，扫清主机资产盲点。

通过风险发现功能及时发现客户Web中间件中出现的远程控制、命令执行漏洞，并推进客户修复漏洞并验证。

通过实时的入侵检测分析，快速发现系统入侵威胁，并提供灵活的应急工具箱，及时响应处理威胁。

客户收益

01 实时智能的资产安全分析，提高风险发现处置能力

青藤万相帮助客户打造一个智能化、可视化、可自服务的资产分析管理平台，提升了客户的实时感知威胁、自动响应攻击的信息安全能力。

02 通过安全风险闭环管理，强化数据安全保护水平

客户的风险发现和自动化安全运维监测等能力进一步增强，对核心的主机系统和敏感数据安全实现全方位保护。

03 强大的入侵检测响应能力，提升红蓝对抗的防御水平

内部红蓝对抗时，青藤的产品在主机层发挥出很好的效果，蓝队借助产品也取得了极佳的防守成果，红队面对强大的监测能力束手无策。

新东方全面提升网络安全成熟度方案

背景概述

新东方作为中国著名私立教育机构，是以科技为驱动力的综合性教育集团，于2006年在美国纽约证券交易所成功上市。自成立以来，新东方累计面授学员2000万人次。

> 新东方安全负责人杨宁：“青藤的主机自适应安全平台为我们在系统入侵防护方面提供了事前的风险识别、事中的监控告警、事后的分析取证，帮助我们在主机安全层面建立起了一个实时有效的防护体系，拓展了我们在远程分支机构及公有云端的系统安全防护能力。”

客户需求

随着IT技术不断发展，网络攻击的方式和手段越来越多样，让企业防不胜防。当前，新东方在信息安全领域主要面临 4 个难题。

传统防护体系失效

受网络虚拟化和BYOD的趋势影响，企业安全防护的边界越来越模糊，通过网关实现安全防护越来越难。

攻击复杂度增大

攻击复杂度越来越高，攻击成本和门槛越来越低，黑客工具越来越智能，给企业带来巨大的安全压力。

难以应对高级威胁

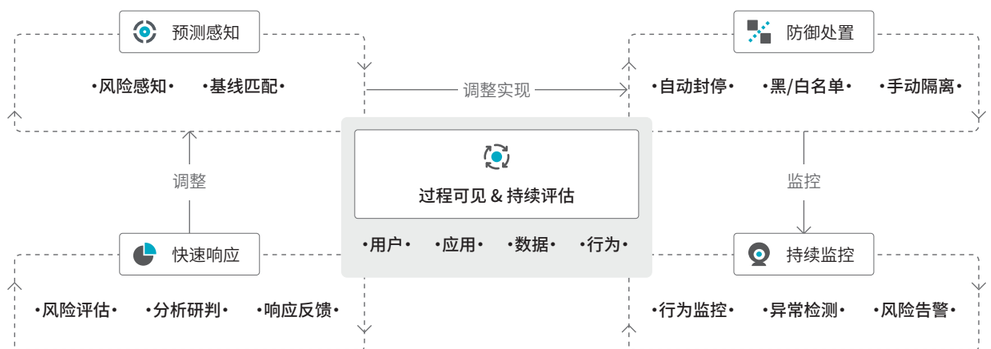
单一的安全检测产品难以应对多态病毒、零日攻击、高级持续性威胁等各类安全威胁。

安全合规压力大

由于《网络安全法》、欧盟 GDPR 的实施，对企业的合规要求越来越高，企业安全合规压力越来越大。

解决方案

- 通过自适应主机安全解决方案，提升客户主动防御能力，达到安全的可管、可控、可视、可调度、可持续。
- 对客户系统进行持续监控分析及定期安全巡检，凭借详实的操作日志与堡垒机关联，强化威胁溯源分析能力。
- 青藤万相的服务接口多样化并可集成，实现安全能力的协同联动，通过风险发现和合规基线能力全面掌握客户系统的风险和配置漏洞等问题。



客户收益

01 实时动态分析，自适应优化防御机制

青藤万相可对客户系统细粒度、多角度、持续化的实时动态威胁分析，并自动适应变化的网络和威胁环境，优化自身的防御机制。

02 全面溯源分析精准定位威胁

青藤的主机安全产品，将客户入侵事件人工调查取证时间降低了80%，而且入侵过程和行为识别更加精准，极大提升了客户的应急响应的效率。

03 深度漏洞检测和基线检查能力

客户通过青藤提供的资产分析能力，对主机部署的系统组件、服务、端口、账号进行深度识别和全面分析，发现各种安全漏洞和基线配置问题，并及时修复满足合规要求。

春雨医生互联网医疗平台一体化威胁风险管理方案

背景概述

春雨医生互联网医疗平台创立于2011年7月，是世界上最大的移动医患交流App。截止到2015年7月份春雨医生已拥有 6500 万用户、20 万注册医生和 7000 万条健康数据，每天有 11 万个健康问题在平台上得到解答。

> “作为一家互联网医疗公司，我们在利用网络的同时也饱受网络攻击的困扰，使我们扩展业务和保障安全首尾不得兼顾。青藤的主机安全产品保障了我们全部服务器的安全运行，为我们解决了后顾之忧。”

客户需求

该客户作为互联网医疗的典型代表，上线了越来越多的数据平台和信息化系统，在网络安全建设中存在诸多问题挑战。

实现合规基线管理

一旦发生维护人员误操作，或采用一成不变的初始系统设置而忽略了安全控制的要求，就可能会带来极大的安全隐患。客户需要实现服务器的配置基线管理。

全面实时掌握系统风险情况

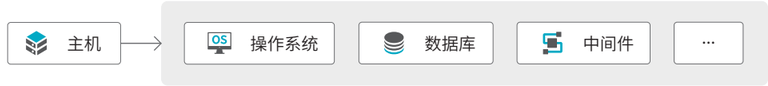
医疗行业的网络安全隐患普遍存在，同时医疗行业是勒索病毒的高发行业。新的漏洞和风险层出不穷，客户需要全新的解决方案，全面掌握现有IT系统的风险情况。

加强威胁入侵检测和数据保护能力

医疗系统中记录了患者个人信息及医疗情况，这对攻击者来说价值巨大。客户需要建立威胁发现能力避免黑客入侵，保护医疗机构核心数据的安全。

解决方案

- 利用合规基线产品快速进行医院内部风险自测，发现问题并及时修复，以满足监管部门要求的安全条件。
- 发现应用配置缺陷、新型漏洞、弱口令等风险，从“识别、分析、处置、验证”全流程对风险进行闭环管理。
- 结合威胁情报、机器学习等方法，对主机实时监控，发现未知手段的黑客攻击，保护最核心的数据资产安全。



深度资产清点

- **主机管理** - 操作系统版本、配置、系统账号及权限等
- **进程管理** - 进程运行及分布情况等
- **网络及端口清点** - 网络板卡清点等
- **Web层管理** - web应用、web站点、web框架及版本清点等
- **数据库资源配置清点**

风险分析

- **主机安全综合分析** - 账号安全分析、弱口令分析、端口暴露性分析等
- **支持主机、数据库及Web的安全基线检查及分析**
- **主机操作审计** - 规则制定、审计、回溯
- **Web安全深度检测** - Web统一识别管理、分析漏洞及风险，并提供修复意见
- **暴力破解** - 实时监控，迅速通知并阻断

入侵诊断

- **威胁实时监测** - 检测异常登录、异常文件及本地权限，并提供报警功能
- **后门诊断** - rootkit及 bootkit查杀、识别监控后门
- **动态蜜罐** - 自定义白名单、实时捕获、报警

客户收益

01 全面的合规管理，满足监管要求

青藤通过合规基线功能，及时为客户发现不满足等保标准的配置项，并提供详细修复建议。之后，通过定时复测并协助客户进行安全规划与设计，使客户满足等保合规要求。

02 安全风险定期扫描，跟踪风险修复进度

每天对全量服务器的安全风险进行体检，帮助客户发现多处业务应用和操作系统存在的组合型弱口令。客户根据风险提示，下发安全整改任务，并实时跟踪每台主机的漏洞修复进度。

03 实时入侵检测，大幅缩短攻击响应时间

客户成功发现了多次反弹Shell及提权攻击，捕获多次非法端口扫描行为。发现威胁后，安全工程师配合客户进行应急处置，帮助客户快速定位攻击来源，截断攻击连接。

游族网络公司主机安全态势感知平台建设方案

背景概述

游族网络股份有限公司成立于2009年，并在2014年6月正式登陆A股主板。公司立足全球化游戏研发与发行、大数据应用、IP管理工程、泛娱乐产业投资四大业务板块，发行范围遍及欧美、中东、亚洲及南美等230多个国家及地区，全球化优势显著。

> “随着互联网行业的发展，我们越来越意识到安全的重要性，青藤产品全面的入侵检测和强大的溯源能力，真实解决了我们遇到的安全问题，现在我们对青藤的主机安全产品更加信赖。”

客户需求

安全无小事，一旦互联网公司被成功“入侵”，其后果将不堪想象，客户需要建设以下安全能力。

加强主机安全感知能力

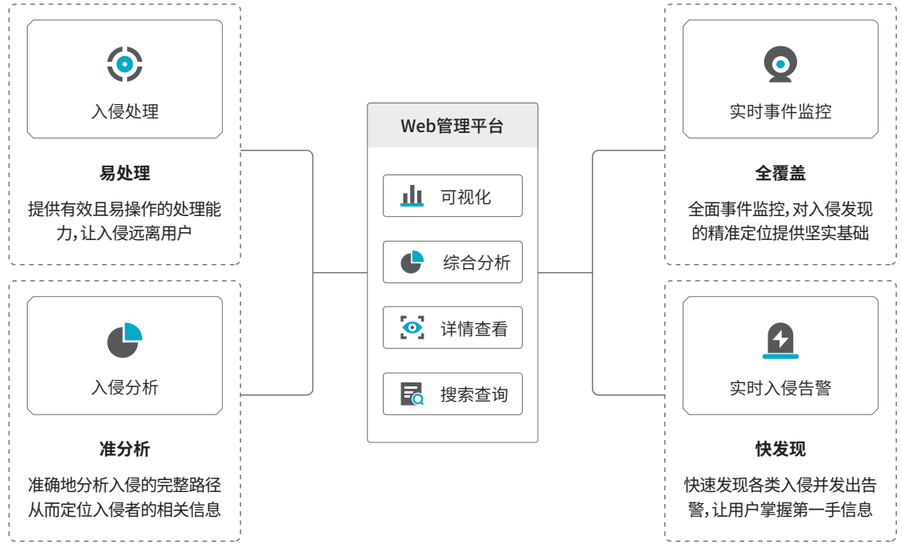
客户在主机层面的防护薄弱，对主机上所承载的资产掌握不清，对内网的整体安全态势无感。客户需要建立态势感知能力，并获得态势感知信息的处理建议。

加强入侵检测和分析能力

流量侧的告警像雪花一样，攻击噪声多，检查成功落地的攻击过程繁琐，且效率低下。客户需要建立主机入侵持续检测能力，准确发现可疑威胁，并快速响应。

解决方案

- 通过资产清点能力，对服务器上承载的业务全面梳理，清晰可视化展示，让安全人员摸清家底，并获得详细的安全威胁感知信息。
- 通过入侵检测能力和流量侧的告警做校验，快速地排查误报，对告警进行降噪，让安全人员将更多的精力聚焦在真正落地的攻击上。



客户收益

01 全面感知网络安全态势

通过资产感知、漏洞感知、攻击感知这三个维度和安全态势总览，帮助客户把庞大复杂的态势感知信息处理体系进行不同维度的理解和构建。

02 提升威胁告警准确率和快速响应能力

青藤的安全产品从全局发现问题，可以相对准确地发现黑客攻击和入侵行为，提供主机侧可靠的攻击防护能力，快速响应威胁使客户免受黑客持续攻击。