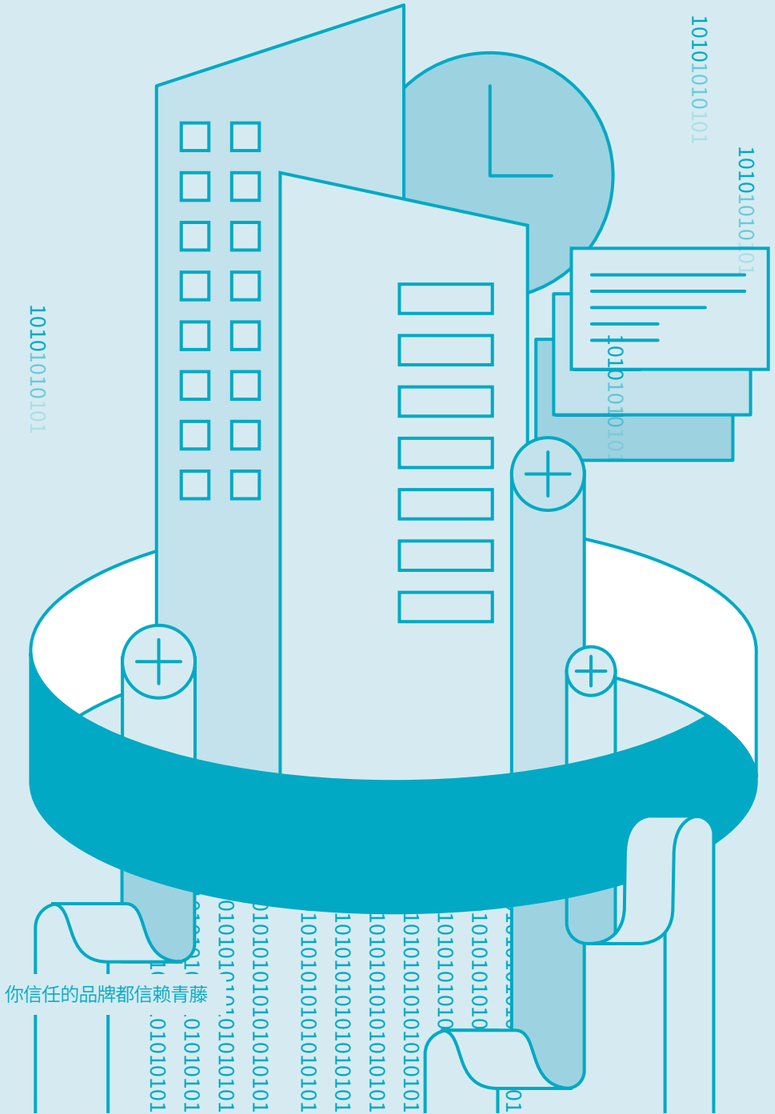
大型企业
Enterprises



300 余家

大型企业客户

2 分钟/百台

Agent静默部署无需重启

240,000+

行业Agent 部署量

现代攻击手段层出不穷，不法分子通过服务器入侵窃取客户重要信息，甚至攻击Web应用服务器，导致系统瘫痪，严重影响企业形象和长期发展。目前，信息安全已经上升到国家安全层面，这对大型企业安全能力提出了更高的要求。从国家层面的《网络安全法》，到行业内的《2021年电力安全监管重点任务》《交通运输行业信息系统安全等级保护基本要求》等，相关监管部门推出一系列政策标准，要求加强大型企业安全能力建设。

青藤 自适应安全提升企业数字化业务韧性，主动防御

威胁感知：
通过持续监控，增强企业的未知威胁感知能力，让企业的安全能力处于行业领先地位。

风险溯源：
结合威胁狩猎能力，快速定位攻击、还原攻击路径和追溯攻击者，从源头上控制安全风险。

安全服务：
青藤通过“产品+服务”帮助大型企业客户提升安全防护能力，减轻安全人员压力，提升安全投资回报。

某石化企业总部、区域中心统一化安全运营能力建设方案

背景概述

某石化企业作为上、中、下游一体化的大型能源化工公司，主要从事石油与天然气勘探开采、石油炼制、石油化工等工作，经营范围遍布全球 76个 国家和地区，拥有员工 84.5 万人。

> “通过青藤安全产品的支持，我们加强了总部、区域中心、企业三位一体的安全运营能力，实现对全集团安全态势的统一管控，整体提升了安全运营系统的效能。”

客户需求

作为能源石化大型企业，客户业务信息系统复杂度极高，信息系统从模块化的分层架构，向容器化的微服务敏捷架构转变，这些转变给网络安全运营带来新的挑战。

对众多资产建立全面管控能力

客户整体网络延伸到 5 大洲、30 余个国家，国内 32 个省自治区直辖市，150 余个企业，需要全面清晰梳理所有资产信息，并实现统一资产管理。

全面收敛面向互联网的攻击暴露面

作为关键信息基础设施企业，石化行业是各种攻击组织的重点目标。客户需要持续开展系统风险脆弱性排查，全面收敛面向互联网的攻击暴露面。

加强数据分析和威胁溯源能力

对于系统中发现的恶意事件，如何了解事件的来龙去脉，以及如何提升对恶意事件的检测能力，是摆在客户安全人员面前的一大难题。

解决方案

- 在资产管理方面，形成资产清点与态势感知相结合的自动化监测能力，通过开展资产清点，明确资产归属，形成台账，及时下线废弃或无主系统。
- 结合全面实时的资产信息和持续的系统监控，对客户系统进行风险排查，及时发现配置错误及弱口令等安全风险，并快速改进，收窄风险暴露面。
- 采用大数据分析技术，融合汇聚主机防护设备情报源、企业威胁情报源、情报联盟情报源等多源数据，开展威胁、情报关联分析，精确完成威胁溯源定位。

客户收益

01 全面快速资产清点

客户利用资产清点功能，十五分钟完成全部资产的细粒度清点，并可从正在运行的机器上反向生成 CMDB，安全人员可实时获得最新资产信息，减少了复杂的管理操作。

02 创建层次清晰、手段丰富的纵深防御体系

客户利用入侵检测及微蜜罐功能建立自动化防护系统，并依托青藤威胁狩猎能力，解决安全数据汇集、数据挖掘、事件回溯、安全能力整合等各类问题，对攻击行为进行感知、辨识、追溯、取证，建立起纵深防御体系。

中广核主机安全纵深防御管理方案

背景概述

中国广核集团有限公司是伴随我国改革开放和核电事业发展逐步成长壮大起来的中央企业，由核心集团公司和直属管理 26 家主要成员公司组成的国家特大型企业集团，是我国核电发展的主力军、可再生能源发展的排头兵和节能减排、核技术应用产业发展的重要力量。

> “我们构建了一套以青藤万相主机安全为视角的大数据分析系统，确保中广核各分子公司信息系统的资产全面纳入内网安全框架，并利用青藤万相的安全能力快速定位存在高危漏洞的资产及应用组件，及时修复收窄攻击面，在攻防演练期间结合青藤威胁狩猎系统实现入侵看得见、防得住、能溯源。”

客户需求

当前中广核安全团队正在面对各种国家、行业、地区的重大保障任务，需要建立起“实战化、体系化、常态化”攻防演练机制，实现安全风险的快速响应和有效处置。

建立起覆盖各分支机构的统一安全防御体系

中广核作为大型清洁能源中央企业，各分支机构众多，安全资产分散，未实现集中管理，分支机构风险暴露面带来极大的安全隐患，需要对各分支机构建立起统一的安全管理体系。

清晰梳理资产信息，全面发现安全风险

客户需要将分子公司资产全部纳入内网安全体系，全面清晰梳理资产信息，发现系统安全风险，收窄风险暴露面，降低业务安全风险。

提升重保活动期间的威胁溯源能力

重保活动时期，系统可能在短时间内涌现大量安全告警，客户需要提高威胁溯源能力，提高风险事件的研判、溯源和响应处置的效率。

解决方案

客户全区域部署多套青藤万相主机安全产品，通过青藤万相主机安全系统统一管理平台，实现集团总部和各分子公司的全面防护，并在各区域对接青藤威胁狩猎系统，构筑纵深的安全防御体系。

利用青藤万相资产清点能力，实现全部主机细粒度数据的集中采集管理，自动化构建资产信息，资产态势可视化。

通过威胁狩猎系统对威胁建模，循环执行检测个性化用例，监测系统的各类业务变化，在最短的时间内完成威胁判定和溯源分析，快速定位失陷主机及影响范围。

客户收益

01 建立起统一的主机安全防御管理体系

青藤 Agent全面覆盖客户集团总部及各分支机构的重要系统，客户通过统一管理平台，实现全部资产的集中管理，及时发现风险、定位威胁、防止扩散。

02 深度资产清点发现系统漏洞

通过深度资产梳理，客户发现了主机中存在的大量风险点，包括软件漏洞、弱口令，同时发现了多个历史遗留的系统后门和 Web 后门文件。

03 建立最佳的内网研判和溯源能力

发现可疑的入侵后，进一步配合青藤威胁狩猎系统和安全服务人员的专业深度分析，验证威胁存在，收集/保存黑客行为记录，加强了深度的内网研判和溯源能力。

某手机厂商多数据源分析主机精准防护实践方案

背景概述

某知名手机厂商是一家全球性的智能终端制造商和移动互联网服务提供商，业务覆盖中国、美国、俄罗斯、欧洲、东南亚等市场，月活用户超过 3 亿。

> “我们通过青藤的主机安全产品，建立起了有效的安全防御体系，通过多数据源关联分析全面感知系统风险，快速定位系统漏洞并有效处置，提升精准防御能力。”

客户需求

客户的主营业务是实体移动电子产品，智能手机覆盖了全球40个国家和地区，而移动端作为全球网络的最大载体，目前仍然存在一些安全隐患。

发现系统漏洞并进行安全修复

互联网业务使用了大量 Nginx 等开源技术，优势是这些技术非常先进且性能优越，为支撑业务的快速发展与变更提供了很好的服务。但不足的是，如果第三方文件库或开源软件出现安全漏洞，就会对整个体系造成连锁影响。所以在出现漏洞时，客户需要准确的漏洞定位和安全修复能力。

建立有效的入侵防御能力

大量的服务器、网络设备以及服务器上运行的开源软件，都运行在IT基础设施上，客户需要加强入侵的主动检测和实时防御能力，保障整个基础设施环境的安全性。

解决方案

通过青藤万相为客户建立起主机安全防护体系，系统平台部署在6台服务器集群上，支持7200 个 Agent 同时在线运行。

利用风险发现功能，细粒度分析系统内潜在的漏洞风险与合规问题，生成分析报告并给出详细的修复建议，让安全管理清晰可衡量。

通过Agent采集主机上的事件，并将数据信息对接给SOC、态势感知等产品，从主机侧提供关键基础分析数据，并通过持续的入侵检测发现威胁准确溯源。

客户收益

01 结合细粒度资产清点信息，快速定位漏洞

青藤万相针对每台主机都能进行自动化、细粒度的资产清点，依托详细的资产信息，可对安全漏洞快速定位，并及时修复。

02 持续监测分析，发现内外风险

青藤提供的风险快速分析和响应能力，帮助客户持续监测暴露在外的资产风险,弥补了传统边界防护的不足，让客户从单纯的“应急响应”升级到全周期的“持续响应”管理。

03 安全日志无缝对接其他平台，实现关联分析

青藤产品支持多种安全日志输出格式，包括 API 、SYSLOG 、CSV 等，可快速对接客户的运维工具和安全运营平台，帮助客户实现威胁风险关联分析。

理想汽车主机安全风险发现及处置方案

背景概述

理想汽车是一个豪华智能电动车品牌，以创造移动的家、创造幸福的家为使命。2020年7月30日，理想汽车在美国纳斯达克证券市场正式挂牌上市。2020年12月18日，理想汽车累计交付量突破30000辆。

> 客户安全负责人评价说：“青藤提供专业安全技术团队随时给予支持，帮助我们进行等保基线检查，快速地梳理资产，全面地评估威胁，通过安全产品和安全服务，以智能、集成和联动的方式应对各类攻击。”

客户需求

人们希望把网络和人工智能有机的结合，并应用于汽车中，通过车机系统、传感器等实现车与人、车与车、车与路、车与云的互联。然而，当边界消失，汽车更加智能化的时候，更多的安全威胁也伴随而至。

加强主机安全防御能力

云端主机是“大脑”，如果控制了主机就相当于控制了大脑，所以客户十分重视云端的安全防护，需要对资产进行梳理，建立主动发现漏洞的机制，保护主机的安全。

通过持续监控分析第一时间发现威胁

客户需要加强持续监控防御能力，通过持续的监控分析第一时间发现入侵行为并快速响应，保障企业损失最小化。

统一安全策略管理提升自动化水平

客户需要进行统一的安全策略管理，通过统一的管理平台，提升自动化运维能力，释放人员压力，减少人力成本。

解决方案

通过青藤万相·主机自适应安全平台以主机安全为核心，构建基于主机端的安全态势感知平台，加强主机安全防御能力。

通过连续的预测、防御、检测、响应闭环循环，实现主机持续地监控和分析，以智能、集成和联动的方式应对各类攻击，为客户建立起主动的威胁防御能力。

通过统一的安全管理平台为客户提供持续的安全监控、分析和快速响应能力，并自动关联资产清点信息与风险和入侵事件。

客户收益

01 提高精准感知主机威胁的能力

青藤利用与客户真实业务结合构建的业务行为模型，能够检测出高级攻击所引起的异常主机行为，大幅提升了客户对主机恶意事件的检测和响应能力。

02 持续监控分析，自适应调整防御机制

客户通过青藤万相实现细粒度、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，不断优化自身防御机制。

03 实现统一资产管理，提高响应效率

客户通过统一的管理平台实现自动化运维，节省人力。并且通过青藤专业技术团队随时给予安全服务支持，提高客户的威胁溯源响应能力。