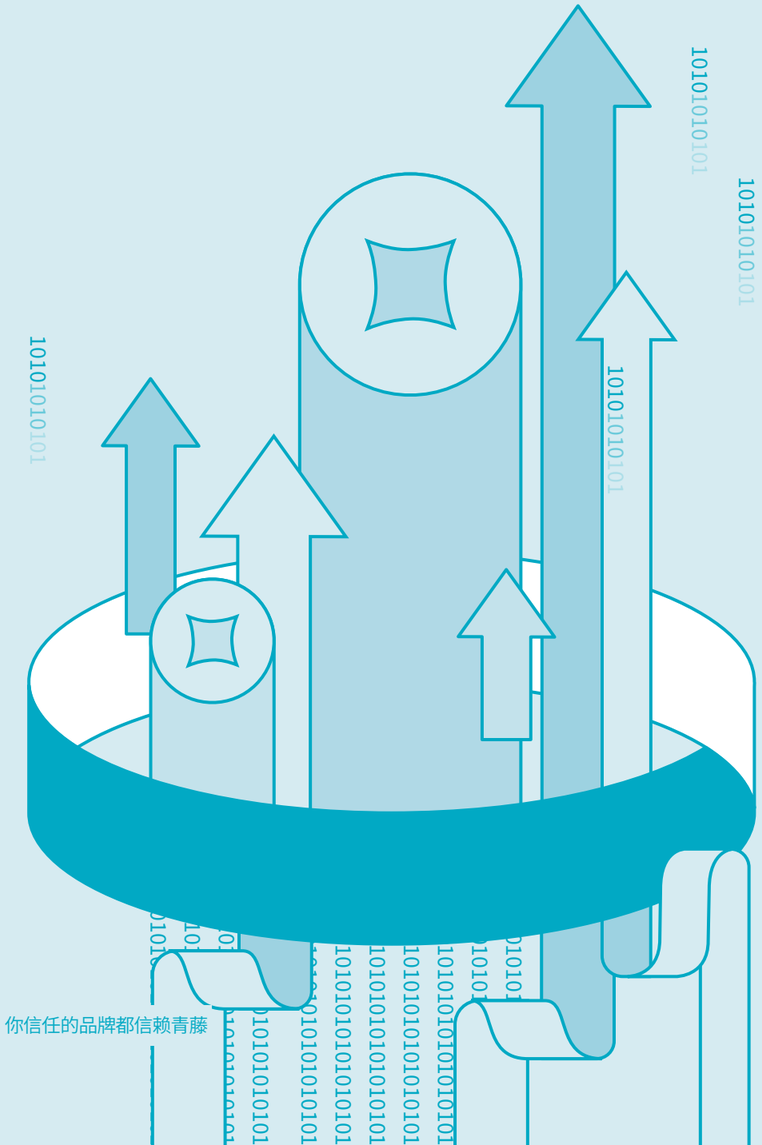
金融行业
Financial Industry



3家

大型国有银行

全部12家

全国性股份制商业银行

150,000+

最大客户安装Agent数量

第1

金融行业主机安全占有率

金融行业的信息安全是重中之重，行业本身对数据完整性、可用性、不可否认性有区别于一般行业的特殊要求，《金融等保2.0》《金融数据安全 数据安全分级指南》《金融数据安全 数据生命周期安全规范》等一系列金融行业的安全政策标准作为支撑，金融行业信息安全逐渐从概念走向了政策体系化的落地。金融机构要尽快地去学习法规标准，调整自身的行为，组织适应的越快、经营风险越低、未来的竞争力越强。

青藤 主动防御方案解决金融机构高级攻击，精准高效

部署方便可扩展：
一个轻量级Agent，只需一条命令就能完成安装，确保无中断部署和可扩展性。
解决复杂攻击：
结合业务对数据进行深度分析，帮助金融企业发现复杂攻击行为，提升快速响应能力。
守护重保安全：
通过安全技术和服务，协助客户提升重保及攻防演练活动安全能力，减轻安全团队的压力。

某大型银行混合多云统一安全管理平台建设方案

背景概述

某大型银行是一家全国性的股份制商业银行，2002年挂牌上市，在境内外分支机构 1800 余家，辐射全国 130 余个经济中心城市，拥有员工 7 万余人。

> “银行信息化快速发展，云计算、虚拟化等新型技术应用大大提升业务信息化水平，但管理众多IT资产面临巨大挑战。我们通过和青藤深度合作，利用主机安全解决方案，获得了实时可视的详细资产信息，以此为基础，风险发现和响应速度持续提升，解决了大量入侵威胁。”

客户需求

混合多云的业务环境，缺乏全面的资产可见性

随着银行逐步推进业务上云战略，越来越多的基础系统、业务、平台部署到云端，业务环境极为复杂，主机资产数量庞大。在此背景之下，如何对资产实现全面的可见性成为了一大难题。

全面发现系统脆弱性，提高攻击门槛

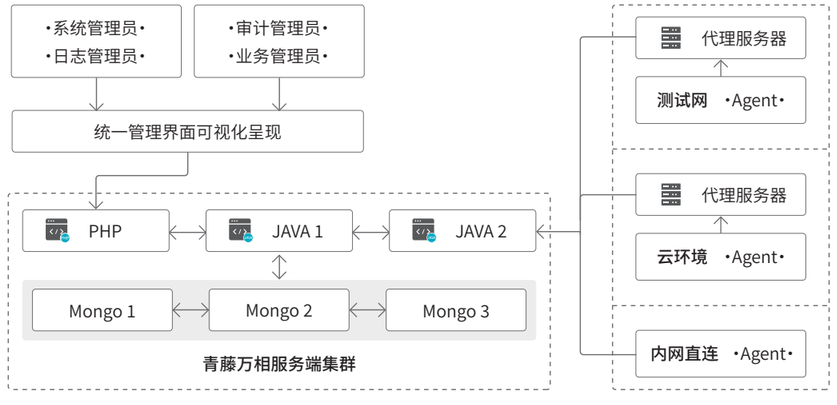
网络安全威胁层出不穷，为了提高攻击门槛，需要全方位检测IT系统存在的脆弱性，获得风险状况视图，先于攻击者发现安全问题，及时进行修补。

未知威胁层出不穷，传统检测产品形同虚设

传统基于规则的安全检测产品，在面对未知威胁时，无法进行及时响应。如何提高应急响应的效率，有效阻止黑客进一步入侵是该银行当下亟需解决的问题。

解决方案

- 青藤提供基于 Agent 底层技术的主机解决方案，采用分布式高可用部署架构，一天时间完成总行和各分支机构的约 22000 台服务器的部署工作。
- 通过Agent为银行任何地方的工作负载提供持续地可视化监控，覆盖互联网应用、交易等多个关键业务区域，部署过程业务无影响，快速实现安全能力。
- 持续检测分析服务器上的各种行为，追踪各种细微的活动，及时发现外部和内部的各种入侵攻击行为。



客户收益

01 实时可视化掌握服务器资产信息

客户对本地环境、虚拟环境、云环境等混合业务架构实现集中管理，并获得清晰可视化的安全监测和分析结果，全面了解主机、业务、风险等关键信息。

02 实时入侵检测，第一时间发现黑客攻击行为

入侵检测功能已实现与客户日志系统实时联动，一旦发现主机层面入侵行为，便可以第一时间发送通知到日志平台，极大地提高了应急响应的效率。

03 各安全模块智能协同，实现风险事件快速响应

青藤万相实现各安全模块的智能协同，对设备日志、资产漏洞和威胁情报进行自动化关联分析，帮助客户发现本地威胁和异常，并对攻击进行追踪溯源。

某金融服务集团多元化业务的主机安全管理方案

背景概述

某金融服务集团是国内第一家以保险为核心,集证券、信托、银行、资产管理、企业年金等多元金融业务为一体的综合金融服务商,集团旗下拥有银行、证券、寿险等业务种类子公司。

> “我们在总部和子公司全面部署青藤的主机安全产品，实现了对总部和所有子公司资产的统一管理，革新了传统的安全防护体系，并通过风险发现功能持续细粒度分析系统内潜在的风险，让整个集团的安全管理清晰可衡量。”

客户需求

该客户作为综合金融服务集团，业务遍布全国，资产分布广，安全管理难度极大，主要问题表现在以下几个方面。

子公司众多、业务多样，统一安全管理难

客户需要花费大量的资源来实现动态的、复杂的安全策略管理。在此背景之下，如何对集团及子公司安全风险统一管理，成为了一大难题。

入侵攻击不断增多，现有防御体系能力不足

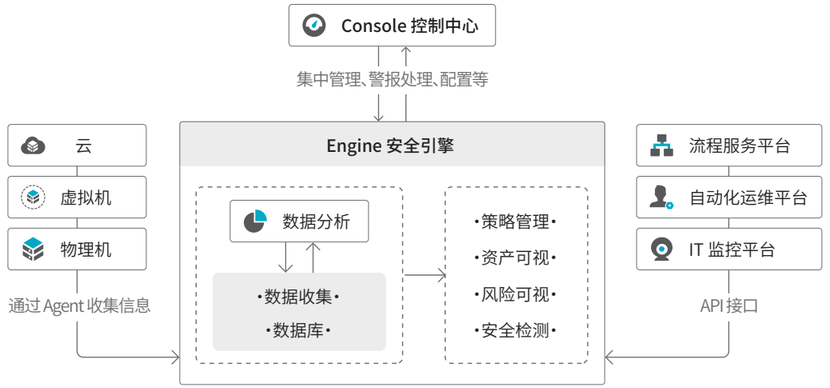
木马、病毒、黑客等安全威胁越来越频繁，客户针对当前的网络安全现状，需要在现有网络架构下建立一套可靠的威胁入侵防御体系。

主机侧资产数据细粒度不足，安全响应不及时

客户缺乏全面详细的主机侧资产信息，出现风险事件时，很难确定受影响的资产范围，不能及时有效响应处理，导致威胁损失持续扩大。

解决方案

- 采用部署 6 台服务端方案，其中生产环境服务端设计要求支持 5000 台 Agent，通过自动化运维工具批量安装，对集团及各子公司主机快速完成 Agent 部署，实现全面统一安全管理。
- 资产清点作为数据支撑平台，与风险发现和入侵检测全面关联，通过动态防护，打造全面立体的防御体系。
- 通过青藤万相提供的 API 接口与客户现有运维系统和 CMDB 系统关联，主机层检测日志统一推送到现有日志管控平台，补充主机侧资产信息。



客户收益

01 集中统一管理安全风险

客户通过集中管理的安全工具，实时获得所有防护资产的各项安全监测和分析结果，更方便进行系统配置和管理、安全响应等相关操作。

02 发现服务器内部高危漏洞，减少攻击风险

青藤基于Agent 的持续监测与分析机制，并迅速与庞大的漏洞库进行比对，精准高效地检测出客户系统内部多个高危漏洞，并及时进行修补，减少漏洞攻击风险。

03 基于细粒度资产信息，快速定位响应风险

青藤帮助用户从安全角度自动化构建资产信息，并支持与CMDB 系统关联，有效补充系统的资产数据。在发现入侵事件时，客户凭借全面的资产数据信息，快速定位响应风险。

某证券公司攻防演练安全防护方案

背景概述

某证券公司是国内开展证券通信业务最早的公司之一，是全面服务深交所的技术公司，是资本市场数字化基础设施和金融科技创新应用的赋能者。

> “青藤的安全产品让资产态势和系统风险完全可视化，它基于行为的分析，无需依赖于对漏洞和黑客工具的了解，能够有效发现未知攻击。这些独特的产品功能为公司筑牢了主机安全防护网。”

客户需求

根据行业监管需求，客户积极向行业发展方向靠拢，需要用新型网络安全技术，提高重要网络安全威胁应对能力。

建立主机侧资产梳理和风险管控能力

主机是所有攻击最后的着陆点，客户需要清晰地了解主机内存在什么样的应用、组件、进程等资产，获得可视化的主机安全风险信息，建立主机维度的资产清点和风险分析能力。

收集全面的主机安全日志信息

客户需要收集全面的主机安全日志信息，并将其纳入整体态势感知体系，多维度监控和分析当前面对的安全威胁和风险。

提升真实威胁的发现响应能力

客户需要持续智能的入侵检测分析，在重保活动或攻防演练中，解决真实的攻击问题。

解决方案

对客户约2600台服务器部署Agent，通过自动化运维工具一条命令快速完成部署，全面对接资产清点及风险发现功能，Agent 可持续扩展其他能力。

对系统进行持续检测，收集主机侧信息，对告警信息进行快速研判，发现异常行为立即上报，并结合威胁狩猎能力进行溯源，输出溯源报告。

目前在客户生产网和办公网各部署了一套万相产品，在生产网部署了一套青藤猎鹰·威胁狩猎平台，建立纵深的安全防御体系，对真实攻击快速溯源响应。

客户收益

01 全面清点资产发现风险脆弱性，收窄暴露面

客户利用青藤万相定期检查漏洞、补丁、弱密码、应用风险等情况。在攻防演练期间，共修复了弱密码 20 个、应用风险 3 项共 38 个。

02 扩展了大数据分析平台日志的宽度

青藤主机Agent能提供很多日志和采集信息，并可通过标准syslog接口发往大数据态势感知平台，帮助客户扩大数据信息广度，提升威胁情报收集、管理、使用能力。

03 快速威胁研判响应，高效解决真实攻击

出现威胁告警时，客户结合以往该主机是否有此类行为、该行为影响范围，以及利用威胁狩猎查询告警期间主机对外连接及进程启动的情况等，确保不放过任何真实攻击。

某基金公司真实攻击溯源分析能力建设方案

背景概述

某基金管理公司是业内Top30的基金管理公司，旗下拥有多家子公司，拥有公募基金管理、社保基金境内委托投资管理人、基本养老保险基金证券投资管理机构、特定客户资产管理等业务资格，是具备综合资产管理能力的大型基金管理公司。

> “随着国家对网络安全的重视，基金行业也日益加强了对网络安全的建设，我们通过青藤的主机安全解决方案，全面梳理资产信息准确识别系统漏洞，有效解决了许多复杂的入侵攻击，在重保活动及日常安全运营中安全防御能力大幅提升。”

客户需求

面对复杂攻击快速溯源分析定位影响

金融行业面对日益增多的复杂入侵攻击，急需建立威胁溯源能力，快速定位风险，及时响应威胁，尽可能减少风险损失。

清晰梳理资产信息减少风险暴露面

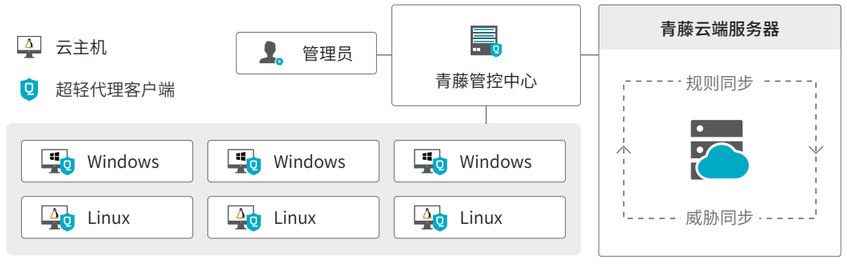
客户业务种类多，系统架构复杂，需要清晰梳理资产信息，全面识别高危漏洞和各种系统脆弱性风险，减少攻击风险。

在重保活动期间提高风险响应能力

客户重保活动多，在活动期间需要全天候的安全保障和快速有效的应急响应流程，以便及时发现风险，并快速分析溯源确定影响范围，实现重保期间的业务安全。

解决方案

- 对客户业务系统全面部署青藤Agent，部署量大约覆盖8000台服务器，全面对接青藤万相·主机自适应安全平台，并接入威胁狩猎能力。
- 全面梳理资产，提供必要的技术力量为客户做好前期的风险排查，包括互联网暴露的未知资产排查、内部访问控制策略排查、非法外连排查。
- 在重保活动期间，严格执行7*24小时的监控工作。一旦发现异常情况，立刻启动安全应急响应预案进行事件处理，确保将事件影响控制在最小范围。



客户收益

01 0 day 漏洞快速排查，降低入侵风险

某次同行业内爆出0day漏洞，该基金公司使用威胁狩猎功能对内部系统进行语句查询，查找出含有0day的主机，并快速进行安全修复，降低了漏洞利用风险。

02 提高风险发现和漏洞整改效率

客户使用青藤万相平台进行高危漏洞清点，生成主机报表，并关联相关主机管理员，从而快速进行漏洞整改，大大提高了安全工作效率。

03 提升分析溯源能力和威胁处理效率

在重保活动中，客户现场发生一起真实入侵事件，为确定失陷范围，使用青藤威胁狩猎功能对失陷主机网络连接日志以及进程日志进行查询，快速确定影响范围，及时处理威胁。