QINGTENG

2020
青藤产品白皮书

V 3.4.0

青藤万相，让主机稳定又安全

www.qingteng.cn

青藤万相·主机自适应安全平台

ADAPTIVE SECURITY PLATFORM

随着云时代的来临，业务变得越来越开放和复杂，固定的防御边界已经不复存在，而黑客的手段却越来越多样化。大多数企业在安全保护方面，还是优先使用拦截和防御以及基于策略的防御控制手段将危险拦截在外，但高级定向攻击总能轻而易举地绕过传统防火墙和基于黑白名单的预防机制，安全威胁已防不胜防。

青藤万相·主机自适应安全平台，采用 Gartner 在 2014 年提出的自适应安全架构，有效解决传统专注防御手段的被动处境，为系统添加强大的实时监控和响应能力，帮助企业有效预测风险，精准感知威胁，提升响应效率，保障企业安全的最后一公里。自适应安全架构核心理念：

1. 持续监控与分析

当前的防护功能难以应对高级定向攻击或持续攻击，“应急响应”已不再是正确的思维模式，企业或组织要持续、动态地监控自身安全，并加强快速分析和响应能力。

2. 安全能力协同联动

自适应安全体系的构架覆盖防御、监控、回溯和预测这四项关键能力，并且各项安全能力以智能、集成和联动的方式应对各类攻击。

产品体系
FEATURES

青藤万相·主机自适应安全平台，通过对主机信息和行为进行持续监控和分析，快速精准地发现安全威胁和入侵事件，并提供灵活高效的问题解决能力，将自适应安全理念真正落地，为用户提供下一代安全检测和响应能力。

青藤产品体系采用模块化的组织形式，实现了各功能的智能集成和协同联动。“资产清点”可主动识别系统内部资产情况，并与风险和入侵事件自动关联，提供灵活高效的回溯能力；“风险发现”可主动、精准发现系统中存在的安全风险，提供持续的风险监测和分析能力；“入侵检测”可实时发现入侵事件，提供快速防御和响应能力；“合规基线”构建了由国内信息安全等级保护要求和 CIS（Center for Internet Security）组成的基准要求，帮助用户快速进行企业内部风险自测，发现问题并及时修复，以满足监管部门要求的安全条件；“病毒查杀”集成小红伞、ClamAV、T-Sec-反病毒引擎等主流病毒查杀引擎，并具备自研发的病毒检测引擎，提供全面的病毒检测和防护能力。

同时，运行在底层的青藤核心平台架构，是下一代主机安全能力引擎。其插件化的构建方式，不仅具备灵活的扩展能力，同时能实现各功能模块之间无缝联动；其分布式的部署方式，能够应对客户大量任务下发和大型攻击来临的海量数据分析处理，并始终保持稳固的性能。

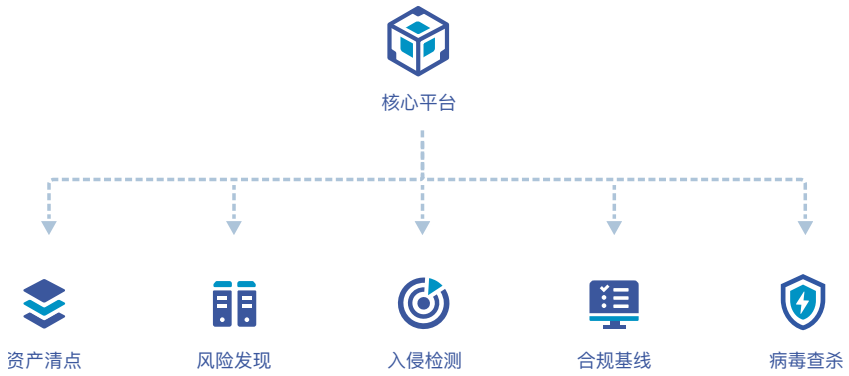

图 1 – 青藤万相 ·主机自适应安全平台产品体系

核心架构

青藤的核心平台架构，主要由 Agent，Server，Web 三部分构成，为产品服务提供基础的、灵活的、稳固的核心能力支持。

图 2 – 持续监控和分析的安全联动平台

1. Agent – 主机探针

Agent 只需一条命令就能在主机上完成安装，且自动适配各种物理机、虚拟机和云环境。运行稳定、消耗低，能够持续收集主机进程、端口、账号、应用配置等信息，并实时监控进程、网络连接等行为，还能与 Server 端通信，并执行其下发的任务，主动发现主机问题。

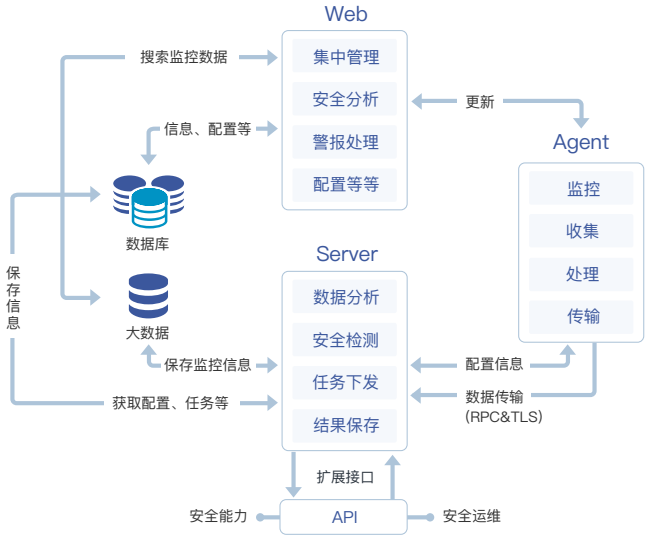

图 3 – 核心架构

2. Server – 安全引擎

Server 作为核心平台的信息处理中枢，支持横向扩展分布式部署，能够持续分析检测从各个 Agent 上接收到的信息和行为并进行保存，可从各个维度的信息中发现漏洞、弱密码等安全风险和 Webshell 写入行为、异常登录行为、异常网络连接行为、异常命令调用行为等异常行为，从而实现对入侵行为实时预警。

3. Web – 控制中心

以 Web 控制台的形式和用户交互，清晰展示各项安全检测和分析的结果，并对重大威胁进行实时告警，帮助用户更好更快地处理问题，提供集中管理的安全工具，方便用户进行系统配置和管理、安全响应等相关操作。

Agent 运行保障

安全

- 对 Agent 进行加壳防护，防止被篡改
- 采用加密传输与服务端通信，保证数据安全

稳定

- 通过 50000+ 台服务器的运行实践，稳定性高达 99.998%
- 2 分钟内离线自动重启机制，保障系统始终处于监测状态

消耗低

- 正常的系统负载情况下，CPU 占用率 <1%，内存占用 <40M，消耗极低
- 在系统负载过高时，Agent 会主动降级运行（CPU 占用率 <1%），严格限制对系统资源的占用，确保业务系统正常运行

01 资产清点
ASSET INVENTORY

越来越多的公司在数字化转型过程中采用混合数据中心架构，包括本地环境、虚拟环境、云环境等；同时随着业务规模与生产环境变化，企业配套 IT 设施也在随时发生改变；这些无疑对企业体系化安全建设提出严峻挑战。对资产“看得全，理得清，查得到”，已经成为企业在日常安全建设中首先需要解决的问题。同时在发生安全事件时，全面且及时的资产数据支持，也将大大缩短排查问题的时间周期，减少企业损失。

青藤资产清点（Asset Inventory），致力于帮助用户从安全角度自动化构建细粒度资产信息，支持对业务层资产精准识别和动态感知，让保护对象清晰可见。使用 Agent–Server 架构，提供 10 余类主机关键资产清点，800 余类业务应用自动识别，并拥有良好的扩展能力。

1. 自动化构建资产信息，资产清晰可见

通过安装 Agent，可在 15 秒内，从正在运行的环境中，反向自动化构建主机业务资产结构，上报中央管控平台，集中统一管理。青藤独特的主机发现系统，随时发现网络环境内没有纳入安全保护的主机，确保安全覆盖无死角；此外，对 Web 资产与数据库资产等高价值高敏感业务资产，进行了针对性资产建模，能够与风险发现和入侵检测功能配套提供安全保护。

2. 资产变化实时通知，安全不再落后于业务

生产环境下，业务服务器需要随着业务变化随时扩容或减配，业务资产也随之相应变化。传统安全方案无法完全匹配业务变化，其对资产实施保护的时间往往滞后甚至遗漏，这就给黑客组织可乘之机。平台在清点资产后，将保持对资产持续监控，保证监控数据与实际业务数据的一致， 对一些需要特殊关注的敏感资产(如:账号、进程、端口、数据库、Web 站点等)发生变化，将提供实时或定时通知，客户安全团队可进行针对性处理，实现资产动态保护。

3. 灵活的检索方式，快速定位关键

在企业安全检查时，通常需要提供针对性的信息，但面对庞大分散的主机数据，信息梳理效率极低。在发生安全事件时，通常需要获得多角度、跨时间段的数据综合分析，获取这类数据需要横跨多个机构、多个系统，且数据结构杂乱无章，分析难度极大。青藤资产清点参考大量国外先进产品经验，结合通用安全检查规范与安全事件的数据需求，形成细粒度资产清点体系，利用多维度的视图，引导用户轻松获得需要的资产信息。同时，借助多角度的搜索工具，帮助用户快速定位关键资产信息。

资产清点特色功能
FEATURES

1. 主机发现

通过设置检查规则，系统自动检查已安装探针主机，所在网络空间未纳入安全管理的主机，自动排除普通网络设备。针对不同网络状况，提供多种探查方法，包括“ARP 缓存分析”、“Ping 扫描”、“Nmap 扫描”、“连接记录分析”等，客户可基于实际业务环境，灵活选择对应功能发现主机，减少无意义网络资源消耗，保证探测与被探测主机正常运转。

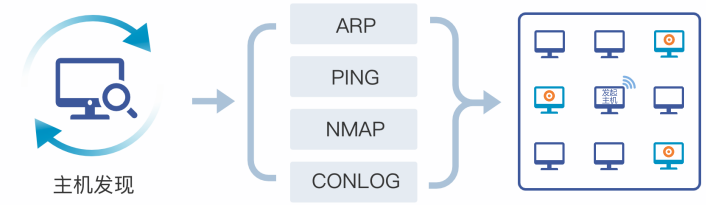

图1 – 主机发现

2. 应用清点

自动化清点进程、端口、账号、中间件、数据库、大数据组件、Web 应用、Web 框架、Web 站点等十余类安全资产，覆盖通用资产。根据每个服务器业务特点，系统针对性识别应用，目前可识别业务应用已覆盖 800 余类，例如Nginx、Apache、JBoss、Mysql、Memcached、Redis、Hbase等。每个应用在风险发现与入侵检测中，均提供对应安全策略保护。未来版本中，将允许自定义清点对象，可根据业务需要，自助清点数据。针对不同清点对象均采用单独模块管理，模块间保持一定联动性，确保同时运行的清点单元最小化，瞬时性能消耗最低。

3. 资产快速检索

对于每类业务资产，系统提供“主机视角”和“资产视角”两种通用维度，聚合展示数据，每个数据表格列均允许搜索与排序。每个表格额外提供大量可选列（不常用的数据列被默认隐藏），客户可根据需求灵活显示的数据，定义自己的表格显示。在复杂搜索场景下，例如横跨多种资产联合搜索，系统已提供关键资产（主机、账号、进程等）全系统关联，未来还将提供全局搜索工具。

图 2 – 资产快速检索

4. 资产面板

在获得资产信息后，将结合业务情况，形成“概览视图”与“分级视图”，展示企业整体资产状况。“概览视图”使用图形化的方式展示企业的关键资产状况，帮助用户直观的了解资产。“分级视图”通过树状结构逐层展示资产信息，并显示关键资产的数值，引导用户找到需要的信息。针对每种特定业务资产，产品提供“分析板”功能，多维度剖析单一资产，详细分析内部情况。此外资产面板功能还提供一些从安全角度出发的特殊资产视角，引导客户从安全维度发现一些问题。

图 3 – 资产清点概览视图

5. 报表导出与 API 支持

所有数据均提供报表导出功能，可任意选择导出的数据列与数据行，形成自定义报表。所有资产均提供基础 API，可结合自身业务情况，获得清点的数据，进行二次开发。

资产清点产品特点
HIGHLIGHTS

1. 从安全角度出发，重新定义资产

传统意义上的资产，被定义为服务器和 IT 设备，仅限于从物理层清点资产，但青藤资产清点从安全角度出发，结合通用安全检查规范与安全事件数据的需求，构建业务型资产对象（包括 Web 服务、Web 站点、数据库、大数据组件等），更加契合基于安全对资产的实际需求。这种转变，正是基于青藤多年积淀的自适应安全理念，从“安全角度重新定义资产”。

2. 细粒度构建系统内部资产，有效弥补 CMDB 缺失信息

传统运维平台的 CMDB 系统，主要用于存储和管理 IT 设备的各种配置属性，但对于与业务安全相关系统内部资产，无法有效管理。平台可清点 10 余类主机关键资产，识别 800 余类常见业务应用，并支持与 CMDB 系统关联，有效补充缺失的数据，提高管理者对整体资产把控能力。

3. 为风险发现和入侵检测，提供资产关联能力

资产清点作为数据支撑平台，已与青藤万相·主机自适应安全平台中的风险发现和入侵检测系统全面关联，实现一键查看，如漏洞风险关联对应的软件应用状态，账号风险关联到对应的系统账号，反弹 Shell 关联对应的端口进程等。用户也可使用资产 API 系统，将相关数据导入风险发现或入侵检测等其他系统，获得更为准确的信息。

4. 支持不同业务系统，复杂业务环境主机的统一平台管控

支持绝大部分主流 Linux/Windows 系统，支持本地环境、虚拟环境、云环境等混合业务架构环境的主机，平台采用集式管理模式，统一平台管控。同时提供各种结合业务的资产管理功能，用户可以基于公司自身的组织架构创建多级业务组，将主机按资产等级、管理部门、负责人等灵活分组管理。

02 风险发现
VULNERABILITY DISCOVERY

事实证明，90% 的攻击事件都利用了未修补的漏洞，且攻击者的手段不断变化，网络安全状况也在随着安全漏洞的增加变得日益严峻。而传统的漏洞扫描器仅为按季度或按年的周期性扫描，在未进行检测期间，新的漏洞很容易被黑客利用入侵。因此，企业需要能够实现风险持续性地监测与分析产品，能够化被动为主动，深入发现内部暴露的问题和风险，持续有效地对风险进行处理，从而提高攻击门槛，缩减修复窗口期。

青藤风险发现（Vulnerability Discovery）致力于帮助用户精准发现内部风险，帮助安全团队快速定位问题并有效解决安全风险，并提供详细的资产信息、风险信息以供分析和响应。

1. 提高攻击门槛，有效缩减 90% 攻击面

在资产细粒度清点的基础上，持续、全面透彻地发现潜在风险及安全薄弱点。根据多维度的风险分析和精确到命令行的处理建议，帮助用户及时处理重要风险，限制黑客接触系统、发现漏洞和执行恶意代码，从而大大提高系统的攻击门槛。

2. 企业风险可视化，安全价值清晰可衡量

持续性监测所有主机的安全状况，图形化展现企业风险场景。为安全决策者动态展示企业安全指标变化、安全走势分析，使安全状况的改进清晰可衡量。为安全运维人员实时展示风险分析结果和风险处理进度，提供专业可视化的风险分析报告，使安全管理人员的工作价值得到可视化呈现。

3. 持续性监控分析，及时发现最重要的风险

主动、持续性地监控所有主机上的软件漏洞、弱密码、应用风险、资产暴露性风险等，并结合资产的重要程度进行风险分析，准确定位最急需处理的风险，帮助企业快速有效解决潜在威胁。另外，安全团队持续关注国内外最新安全动态及漏洞利用方法，不断推出最新漏洞的检测能力，实现紧急安全事件快速响应。

风险发现特色功能
FEATURES

1. 发现未安装的重要补丁

持续更新的补丁库以及 agent 探针式的主动扫描，能及时、精准发现系统需要升级更新的重要补丁，第一时间帮助用户发现潜在可被黑客攻击的危险。深入检测系统中各类应用、内核模块、安装包等各类软件的重要更新补丁，结合系统的业务影响、资产及补丁的重要程度、修复影响情况，智能提供最贴合业务的补丁修复建议。

2. 发现应用配置缺陷导致的安全问题

自动识别应用配置缺陷，通过比对攻击链路上的关键攻击路径，发现并处理配置中存在的问题，大大降低可被入侵的风险。如下图中黑客利用 redis 应用漏洞的攻击链路，针对黑客的每一步探测，系统均会进行持续性的检测，及时发现并处理了某个配置缺陷后，将有效解决潜在安全隐患、阻断黑客的进一步活动。

图1 – Redis 应用配置缺陷检测

3. 快速发现系统和应用的新型漏洞

青藤持续关注国内外最新安全动态及漏洞利用方法，不断推出最新漏洞的检测能力，至今已积累达 37000+ 的高价值漏洞库，包括系统 / 应用漏洞、EXP/POC 等大量漏洞，覆盖全网 90% 安全防护。同时，基于 Agent 的持续监测与分析机制，能迅速与庞大的漏洞库进行比对，精准高效地检测出系统漏洞。

图 2 – 持续性漏洞检测

4. 智能化的弱口令检测，支持多种应用

精准检测几十种应用弱密码，覆盖企业常用应用如 SSH、Tomcat、MySQL、Redis、OpenVPN 等。识别方法以离线破译优先，且识别弱口令后会对没有发生变化的离线弱口令文件哈希入库，如口令未发生新的变更，不再重复对弱口令进行检测。通过分布式的 Agent 对全量主机的弱口令检测，一方面极大的提高工作效率，另一方面对流量及业务的影响也降到了最低。同时，结合企业特征，系统能智能识别更多的组合弱口令，支持用户自定义口令字典以及组合弱口令字典，能有效预防被黑客定向破译的风险。

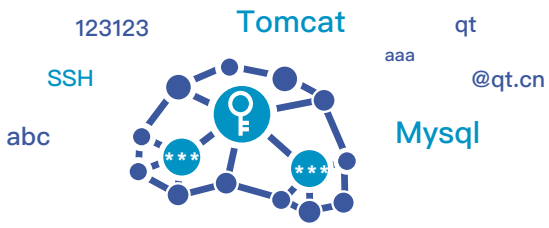

图 3 – 智能化的弱口令检测

5. 发现运维人员的违规操作

发现由于运维人员的违规操作引起的安全风险，如修改重要配置文件、未设置密码复杂度、/etc/shadow 权限检查、网卡处于混杂模式检查等，并结合黑客的攻击手段，持续检测并暴露这些可能存在威胁的安全隐患，及时通知相关人员进行处理。

6. 发现资产暴露性风险

监测暴露在外的资产风险，如 Web 风险文件、危险进程端口对外、不必要的进程服务、不必要的系统账号等。建立多维分析模型，结合资产重要程度及资产上所有风险进行关联分析，综合分析出最易受攻击的资产。

风险发现产品特点
HIGHLIGHTS

1. 全面系统脆弱性发现

全方位检测 IT 系统存在的脆弱性，发现信息系统存在的安全补丁、安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，为企业提供无死角的风险状况视图，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

2. 白盒角度发现风险，比黑盒角度更准

Agent 探针式的扫描机制，建立了自内而外的白盒视角。这种扫描机制能以极低的误报率精准发现软件漏洞，发现更多更全的弱密码账户等，比如能探测到系统内核模块的软件漏洞，能读取 MySQL 数据库文件中包括系统账号在内的更多业务账号，这比从主机外部建立扫描的方式更加准确、全面。

3. 比传统扫描器更快、更方便

传统的扫描器每次扫描均需要将远程安全评估系统接入各级网络，部署相对麻烦且不能持续性扫描防护，同时无法与资产数据进行关联，扫描后风险整改困难。而基于 Agent 由内而外的扫描方式，一条命令即可一键部署，部署成功后即可持续为企业安全保驾护航。

4. 资产数据自动关联

在主机环境资产全面清点的基础上进行的持续性风险扫描，能对主机环境资产进行持续性防护。风险扫描后自动关联资产数据，如主机 IP、端口、进程、账号、应用、Web 站点、主机负责人等资产详细信息。支持在风险发现之后，一键查看对应的资产情况，为风险的下一步处理提供有效信息。

03 入侵检测
INTRUSION DETECTION

传统的入侵防护方案能够很好地抵御已知的攻击，但是对于未知和迅速变化的攻击手段则缺乏相应的检测能力。因此，如何实现有效的入侵检测并提供实时的告警和响应手段已经成为安全建设急需解决的问题。当前的攻击手段千变万化，但是攻击成功后要做的事情却是归一化的。因此，青藤将视角从了解黑客的攻击方式，转化成对内在指标的持续监控和分析，无论多么高级的黑客其攻击行为都会触发内部指标的异常变化，从而被迅速发现并处理。

入侵检测（Intrusion Detection）提供多锚点的检测能力，能够实时、准确地感知入侵事件，发现失陷主机，并提供对入侵事件的响应手段。

1. 多锚点的检测能力，实时发现失陷主机

攻击者通常会同时采用多种手段来攻击用户主机。入侵检测通过多维度的感知网络叠加能力，对攻击路径的每个节点都进行监控，并提供跨平台多系统的支持能力，保证能实时发现失陷主机，对入侵行为进行告警。

2. 不依赖对漏洞和黑客工具的了解，有效发现未知黑客攻击

传统的入侵检测能力往往依赖于对已知的漏洞和黑客工具的了解，通过基于特征的检测来发现攻击。该方法对于突发新型漏洞和未知的攻击手段缺乏有效的发现能力，导致许多入侵行为不能被实时发现，从而造成无法挽回的损失。青藤入侵检测结合专家经验，威胁情报、大数据、机器学习等多种分析方法，通过对用户主机环境的实时监控和深度了解，有效发现包括“0Day”在内的各种未知黑客攻击。

3. 对业务系统“零”影响

通常情况下，需要进行安全监控的主机，往往也都承载着用户的核心业务系统，比如数据库、Web后台等。因此，安全监控对主机性能和业务系统的影响是非常重要的指标。青藤Agent以其轻量高效的特性，在保证对用户主机安全监控的前提下，不对其业务系统产生影响，为用户的主机安全提供了高效可靠的保护。

4. 结合资产信息，为响应提供最准确的一线信息

发现入侵事件只是入侵检测的第一步，提供入侵的详情信息和响应手段，才能真正帮助用户解决问题。在独有的资产管理能力的支持下，青藤不仅能发现入侵，还能够提供详细的入侵分析和响应手段，从而让用户精准有效地解决问题。

入侵检测特色功能
FEATURES

图 1 –多维度入侵感知系统

1. 暴力破解监控

通过实时监控登录行为，可以及时且自动化地发现黑客使用不同服务尝试暴力破解用户登录密码的攻击行为，并进行自动化封停处理，使得黑客不能进行更多的尝试。

2. Web 后门监控

自动化地监控关键的Web 目录，结合恶意样本库、正则库、相似度匹配等多种检测方法，实时感知文件变化，从而能够及时发现Web 后门，并对后门的恶意代码内容进行清晰标注。

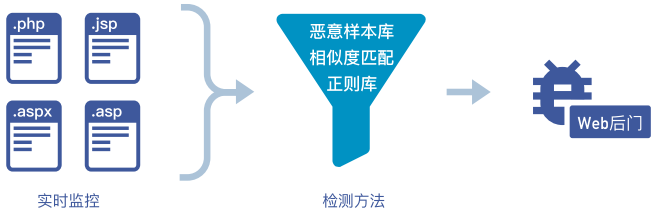

图 2 – Web 后门监控

3. 反弹 Shell

通过对用户进程行为进行实时监控，结合行为的识别方法，及时发现进程的非法 Shell 连接操作所产生的反弹 Shell 行为， 有效感知“0Day”漏洞利用的行为痕迹，并提供反弹 Shell 的详细进程树。

4. 本地提权监控

通过对用户进程行为进行实时监控，结合行为识别技术，我们能及时发现进程的提权操作并通知用户，并提供提权操作的详细信息。

5. 系统后门监控

区别于传统的特征分析，我们通过对进程关联信息的分析，结合模式识别和行为检测，提供了不依赖 Hash 的自动化 系统后门检测方式，能够实现在多系统中进行多维度、高准度、快速度的后门发现，能够对包括 Linux 下的 Rootkit、 Bootkit，还有 Windows 下的可疑进程、可疑线程等多种后门。

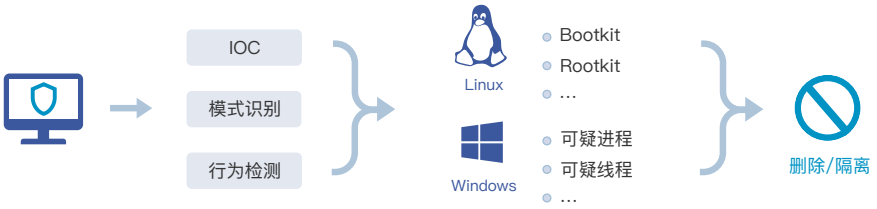

图 3 – 系统后门监控

6. 挖矿木马检测

通过分析挖矿木马程序的行为特征，青藤针对挖矿常见的特征研制多种检测模型，对挖矿进程执行的命令、挖矿在主机中的行为、挖矿文件的信息以及挖矿本身具备的属性都设置了相应的锚点进行监控，提供用户全方位挖矿检测和防护能力。云端+客户端的双重检测模式，让挖矿程序的每一个特征和行为，都会被实时发现并上报告警，同时给出青藤专业角度的安全分析。不仅支持对挖矿进行隔离、删除、修复验证等多种处理方式，同时也提供检测规则的高度自定义能力，方便用户对挖矿木马进行快速响应和预防。功能实现了从监控发现、检测分析、响应处理、设置预防的安全闭环能力，为用户提供稳定持续高效的安全服务。

图 4 – 挖矿木马检测

7. Web RCE 监控

通过分析常见的远程命令漏洞利用实例，利用模式识别的方式，实时监控用户进程行为的各项特征，对主机中进程异常的执行行为和执行命令内容进行精确匹配，能有效发现黑客利用漏洞执行命令的行为痕迹，并及时进行告警。告警信息提供整个漏洞利用过程的进程树信息，帮助用户准确分析黑客的入侵路径和目的，功能同时也支持用户自定义规则进行检测，可帮助适应客户多样化的业务流程，精准覆盖各类 RCE 攻击的监控场景。

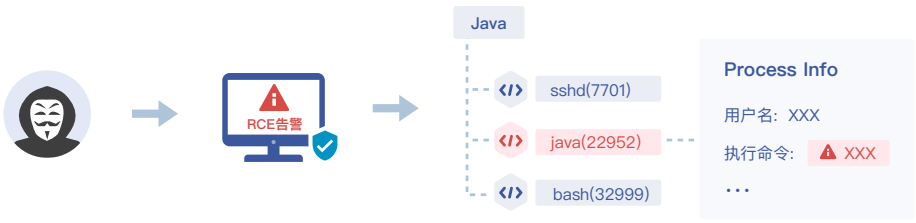

图 5 – Web RCE 监控

8. 自研雷火 Webshell 检测引擎

雷火引擎（代码推导与计算引擎）是青藤自研发的 Webshell 检测引擎，不依赖正则匹配，而是通过对 Webshell 代码内容中恶意函数和调用参数的精确检测，发现 Webshell 中存在的可疑内容。经过多轮公开的对抗测试，青藤自研的雷火引擎都能有效发现各式企图绕过一般检测引擎的 Webshell。适用范围广，不论是 PHP 或是 JSP 类型的后门，均能发现其内容中隐含的恶意特征；检测精度深，独具的特征挖掘角度让后门难以绕过，无处遁形。

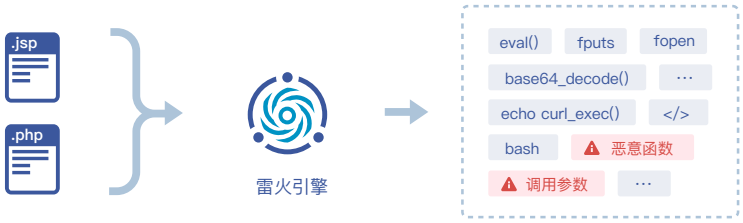

图 6 – 自研雷火 Webshell 检测引擎

入侵检测产品特点
HIGHLIGHTS

图 7 – 入侵检测产品特点

1. 全方位攻击监控

通过对攻击路径的每个节点进行深入的监控，提供了多平台、多系统的全方位、高实时的攻击监控，对进程变化、文件变化、 登录登出等事件了如指掌，做到了实时监控“全”方位。

2. 高实时入侵告警

在 Agent 的深入探针能力支持下，结合 IoC、大数据、机器学习等多种分析方法，保证了对入侵事件的实时检测，并提 供包括短信、邮件等多种方式在内的通知手段，让用户第一时间知道入侵发生，做到了入侵“高”实时。

3. 可视化深度分析

基于对攻击时间和攻击维度的深度分析，整理入侵事件的来龙去脉，以可视化方式完整呈现。让用户对于整体环境的入侵情况和需要处理的入侵事件有清晰的了解，使得入侵分析“深可见底”。

4. 多样化处理方式

根据入侵场景不同，提供了包括自动封停、手动隔离、黑 / 白名单和自定义处理任务等多种处理方式，让用户从根本上 解决入侵事件，让处理从此“高效多样”。

5. 易扩展配置灵活

面对多变的入侵行为，提供针对其本源行为特征的自定义检测规则，实现检测能力高度可扩展。若有突发入侵需快速响应，掌握必要情报，便能通过扩展规则来快速排查，以“随机应变”巧妙应对各种攻击。

04 合规基线
COMPLIANCE

合规标准让运维人员有了检查默认风险的标杆，但是面对网络中种类繁杂、数量众多的设备和软件，如何快速、有效地检查设备，又如何集中收集核查的结果，以及制作风险审核报告，并且最终识别那些与安全规范不符合的项目，以达到整改合规的要求，这些是网络安全运维人员面临的新的难题。

青藤合规基线（Compliance）构建了由国内信息安全等级保护要求和CIS（Center for Internet Security）组成的基准要求，涵盖多个版本的主流操作系统、Web应用、数据库等。结合这些基线内容，一方面，用户可快速进行企业内部风险自测，发现问题并及时修复，以满足监管部门要求的安全条件；另一方面，企业可自行定义基线标准，作为企业内部管理的安全基准。

1. 持续关注监管政策，助力企业达到监管要求

紧跟监管政策，不断推出与等级保护、CIS标准对应的基线。企业可使用该合规基线模块，一键自动化进行检测、并可视化基线检查结果，根据产品提供的修复建议进行修复，以满足企业监管要求。

2. 自定义检查标准，满足不同检查基准场景

对于上级或有关监管部门的检查，可以根据产品自定义基线功能，对于不同的检查基准，灵活制定不同检查强度的标准，提前自行制定策略自查，及时整改，以满足不同检查场景的需求。

3. 提供企业基线定制服务，支撑企业日常运维及管理要求

根据不同行业的相关基线规范，结合企业个性化的应用场景，青藤可为用户提供基线定制开发服务，以快速匹配各行业、各企业安全配置需求。

合规基线特色功能
FEATURES

1. 支持等保/CIS等多重标准、覆盖各类系统/应用基线

安全研究人员持续研究国家等级保护政策、CIS基线标准，不断推进更多基线标准的支持。产品目前支持Centos、Debian、RedHat、SUSE、Windows Server 2008、Windows Server 2012等常用操作系统，同时覆盖Apache、MongoDB、MySQL等10余种数据库类、Web服务类应用。

2. 结合资产清点，自动识别服务器需检查的基线

在资产细粒度清点的基础上，根据所选服务器的操作系统、软件应用等信息，自动筛选出该服务器上需要检查的系统和应用基线。同时支持一键批量创建基线任务，操作简单易用。

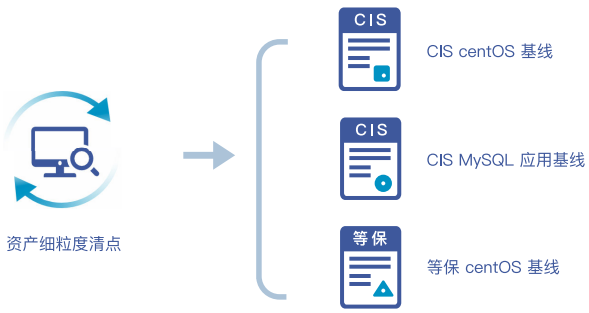

图 1 – 自动识别服务器需检查基线

3. 一键任务化检测，基线检查结果可视化呈现

合规基线功能设计了灵活可配置的任务式的扫描机制，用户可快捷创建基线扫描任务。根据检测需要，自行选择需要扫描的主机和基线。在完成检测后，检查结果将以“检查项视图”和“主机视图”两种方式可视化呈现，满足企业个性化的检测需求。

图 2 – 一键任务化检测

4.开放企业自定义基线检查项能力

企业可根据实际的使用场景，自行定义基线的检查项，如自定义检查阈值、自定义检查目录、自定义检查结果展现模板、 自定义检查项整改方案等，以满足企业多样化的内部监管要求。

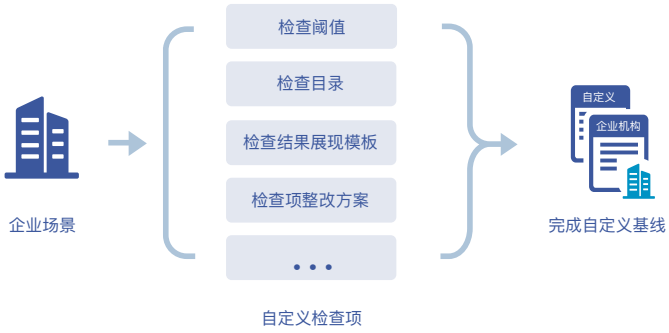

图 3 – 自定义基线检查项

合规基线产品特点
HIGHLIGHTS

1. 一站式的安全合规解决方案

构建了从扫描到处理的一站式安全合规解决方案，自动化的任务式基线扫描，可视化的服务器合规情况，有效针对每一条不合规的Checklist提供精确到命令行的修复建议，并提供基线导出、白名单功能，为基线整改提供更便捷的管理方式。

2. 不断丰富完善的Checklist知识库

支持1500+的Checklist知识库，同时安全研究人员持续关注国内外基线标准，不断丰富基线配置检查系统Checklist知识库。同时可根据不同行业相关基线规范，对知识库实现定制管理，匹配各行业安全配置需求。

3. 与安全管理平台的无缝整合

提供API下发基线检查策略，同时返回检查结果信息，与企业安全管理平台进行无缝对接。安全管理平台可以针对安全基线的不同检查规范和不同检查目的，对检查结果进行全过程管控，全面了解基线检查配置弱点的整改过程，为安全管理工作提供更有利的过程管控信息。

4. 基于Agent的白盒探测，扫描更智能准确

基于Agent白盒探测机制，可自动探查被核查的操作系统、应用的类型及版本，并自动发现中间件及数据库安装路径，让扫描更智能、更准确。

05 病毒查杀
ANTI VIRUS

传统的病毒查杀大多数为 Windows 上的各类杀毒软件，针对 Linux 环境下实用且可方便统一管控的病毒查杀工具非常之少。传统病毒扫描占用资源消耗大且耗时长，病毒库的频繁更新也时常导致云环境下存在的流量下发问题。众多杀毒软件也没有能够还原病毒入侵后主机环境的能力，如何解决删除完病毒的后一步：恢复业务，也是安全运维管理非常头疼的问题。如今 GB/T 22239–2019《信息安全技术网络安全等级保护基本要求》中，安全计算环境的二级以及三级要求，对恶意代码防范（即病毒查杀）能力也提出了明确的要求。因此，可统一管控的病毒查杀工具已成为企业中必不可少的安全要求，如何快速部署病毒查杀，高效地对病毒进行检测和发现，保护主机环境免受攻击，并符合等保的要求，都将会是企业需要面对的问题。

病毒查杀（Anti Virus）结合多个病毒检测引擎，能够实时准确地发现主机上的病毒进程，并提供多角度分析结果，以及相应的病毒处理能力，对病毒能够快速、准确、高效地实现从检测分析到处理修复的安全工作闭环。

1. 多引擎病毒检测能力，实时发现病毒

病毒流传后变种很快，单一检测库容易被针对性绕过。青藤病毒查杀通过集成多个病毒检测引擎，并定期更新检测库，有效防止病毒绕过，并通过实时监控的检测方式帮助用户及时查杀主机上运行的病毒。

2. 部署方便快捷，轻量查杀，业务“零”负担

青藤Agent通过一行命令即可完成安装部署，并自动适配系统开启监控。以轻量高效的特性，结合“客户端监控+云端查杀”的模式，在保证对用户主机安全监控的前提下，避免了各种不必要的下发更新，保证不对其业务系统产生影响，为用户的主机安全提供了高效可靠的保护。

3. 深入剖析等保要求，满足各项具体规定

青藤的病毒查杀贴合用户的常见使用场景和等保要求，在众多强大功能的支持下，对等保2.0中恶意软件防范二级和三级要求的具体规定项，均能够完美符合，能够帮助企业通过等保审查。

病毒查杀特色功能
FEATURES

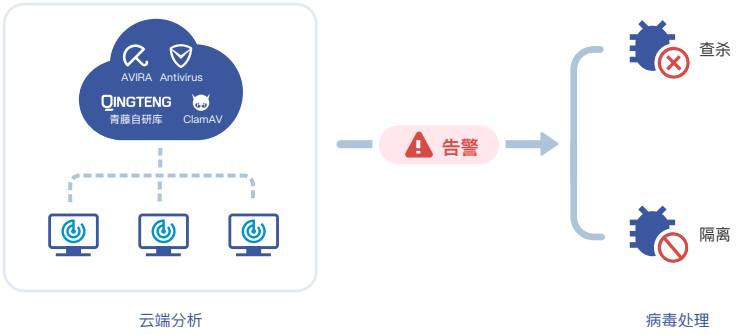

图 1 – 病毒查杀特色功能

1. 多引擎病毒检测

青藤病毒查杀结合多个杀毒引擎，查杀率高，对多种病毒木马程序都能进行检测。杀毒引擎目前已集成：小红伞 Avira 引擎、腾讯 T-Sec-反病毒引擎、ClamAV 引擎和青藤自研引擎。其中青藤自研引擎是由青藤自主研发的杀毒引擎，对挖矿木马、蠕虫病毒、勒索病毒及黑客工具等都能进行有效的检测。

图 2 – 多引擎病毒检测

2. 实时监控告警

采用云端 + 客户端双重检测机制，客户端实时地监控用户各类进程的运行状态，在客户端检测和云端分布式检测引擎的加持下，一旦判定为病毒，立即进行上报，通过邮件、短信等多种方式向用户告警，并提供各项病毒文件静态和进程动态的详细信息帮助用户分析病毒。被确认病毒的源文件也会立即上传服务端备份，用户随时可下载分析。

3. 主动病毒阻断

对确认的病毒可进行主动的病毒阻断，病毒会被自动进行隔离，在安全的目录下被加密压缩，并进行备份。隔离后的病毒将不具备启动运行和传播的能力，不会再感染其他主机，有效抵御病毒的攻击。

4. 配置防御策略

支持对各个主机配置其特定的防御策略，在确认易受攻击的主机上开启自动隔离，使病毒可被自动查杀；在确认免受攻击的主机上则可不开启自动处理，避免误杀。因此可适应客户多样化的主动防范需求。

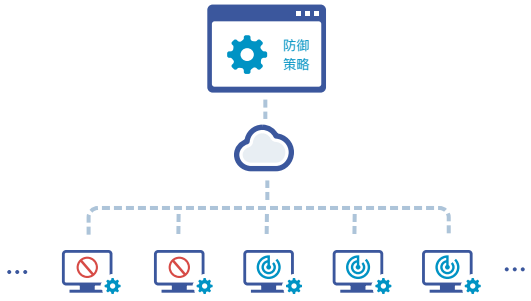

图 3– 配置防御策略

5. 支持多种处理

青藤产品提供丰富的病毒处理能力，包含：支持对病毒进行进程阻断、文件隔离和文件删除；确认为非病毒时可将其加为受信任；修复后可将病毒事件标记为已修复等。隔离后的文件还可以点击进行一键还原，快速恢复用户的受影响业务。

6. 沙箱验证修复

通过青藤自研的沙箱，可对检测发现的病毒进行快速验证，发现并分析其入侵的路径，从而得出查杀病毒的正确方法和手段。沙箱还可以自动生成对应的修复工具，帮助用户还原其对主机的恶意修改内容，修复病毒造成的影响。

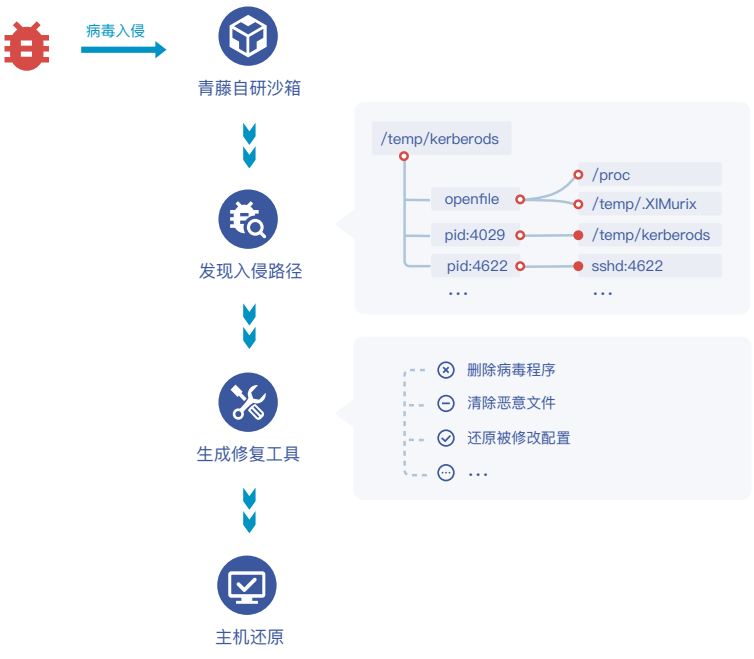

图 4 – 沙箱验证修复

病毒查杀产品特点
HIGHLIGHTS

1. 精准查杀

通过实时监控的方式监控病毒进程，对病毒的检测更加精准和针对化。结合多引擎病毒检测引擎，查杀率高。多方分析“实锤”病毒信息，检测结果一站化体现，坚实可靠。

2. 轻量稳定

青藤Agent程序占用空间小，仅只需一条命令就能在主机上完成安装，且自动适配各种物理机、虚拟机和云环境，可快速在客户环境中完成部署工作。经多家客户验证使用，通过 50000+ 台服务器的运行实践，稳定性高达 99.998%。其云查杀的模式，也同样避免了病毒库频繁下发的流量问题，实现日常维护成本的最小化消耗。

3. 集中管控

通过服务端与Agent的联系，统一、集中管理企业终端，对环境所有的主机，可统一接收和查看其病毒告警，并下发到具体的终端进行处理，高效且易用。对各台主机的防御策略配置可统一管控，方便快捷地实现对主机上策略的调整，解决企业常见管理难题。

4. 处理简单

用户仅通过界面点击即可实现对病毒的各项处理，并自动完成对病毒在主机上的修复验证，一键下发，简单易用。通过在主机运行沙箱生成的自动化专杀工具，不仅能彻底清除病毒，还能相应地还原正常的主机配置，消除病毒影响，让恢复主机不再成为难题。

5. 符合等保

提供对各类恶意软件例如挖矿、勒索、蠕虫等病毒的检测和主动防御能力，病毒库也支持进行定期的更新，完全满足等保 2.0 的相关要求。

QINGTENG

青藤云安全是国内首家自适应主机安全公司，运用独创的下一代安全技术，为企业提供精准、 高效、可扩展的主机安全产品和专业服务；以服务器安全为核心，构建基于业务端的安全联动平台，为用户提供稳固、持续性的安全防护。

中国第一也是唯一入选 Gartner 全球安全市场指南的安全初创公司

B+ 轮融资获大湾区共同家园领投 3 亿元人民币

标杆用户

斗鱼 DOUYU.COM

中国平安 PING AN 保险 · 银行 · 投资

借贷宝

91金融 91jinrong.com