安全湖

产品简介

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

产品简介
产品概述

最近更新时间：2024-01-17 10:10:41

安全湖（Security Lake）是一款基于云原生技术打造的高性能、低成本、纯自研、国产的安全大数据分析平台，为企业提供一体化的泛安全数据接入、加工、存储、分析、告警、可视化等服务，具备“插件化”应用开发能力，助力企业构建云原生湖仓一体安全分析平台。

产品功能

腾讯安全主应用

安全湖中的腾讯安全 App 为主应用，腾讯安全 App 内置安全检测和威胁狩猎规则，支持腾讯威胁情报和多源情报管理，可配置自动化情报回扫任务对每日新增数据和长周期历史数据进行情报回溯，并可视化风险呈现情报碰撞趋势和风险排名。

安全场景化 App

基于安全湖的高性能数据底座，构建丰富的安全场景化 App，包括流量检测、零信任、AD 域安全、数据库审计、API 安全、DNS 安全等 App，通过 API/SDK 方式构建完整的安全数据应用生态体系。

高性能底层引擎

自研数据底层引擎，符合国产信创要求；采用云原技术，支持弹性扩容、存算分离，“无索引“架构避免索引带来的成本开销、”列存储”提供10~20倍的数据压缩比、“支持对象存储”可降低存储成本，解决海量数据存储和使用成本问题，实现海量安全数据实时分析。

一体化智能分析引擎

包含准实时分析引擎、流处理引擎、机器学习/AI 引擎，具备可视化 BI 仪表盘和报表、检索语句兼容 SQL 和 SPL，提供一站式泛安全数据采集、治理、存储、应用，可扩展 IT 运维与应用性能检测、安全运营与合规管理、可视化 BI 智能数据分析等方向的安全场景。

产品优势

最近更新时间：2024-01-17 10:10:41

安全检测分析

对全流量实时检测、原始主机日志实时分析、海量数据进行威胁情报匹配碰撞，支持发现各类风险问题，如 SQL 注入、代码注入、命令执行、僵尸网络、勒索、挖矿、DGA、木马、后门等。

安全态势可视化

预置流量安全、终端安全、API 安全、数据库审计、DNS 安全、AD 域等安全专题可视化仪表板，支持自定义各类图表统计和交互组件，提供丰富图表自定义配置。

威胁狩猎

通过 ATT&CK TTP 对全量安全日志进行威胁狩猎，在日常运营和攻防对抗场景下，主动发现高级威胁、APT、以及潜伏的高危安全事件，提供完整上下文以提升威胁溯源工作效率。

泛安全场景应用

预置流量安全、终端安全、API 安全、数据库审计等安全应用，实现安全数据深度洞察，提高安全运营工作效率。

云原生

采用云原生架构，具有高可扩展性，支持弹性伸缩、秒级扩缩容，低成本，支持无限量存储。

平台化

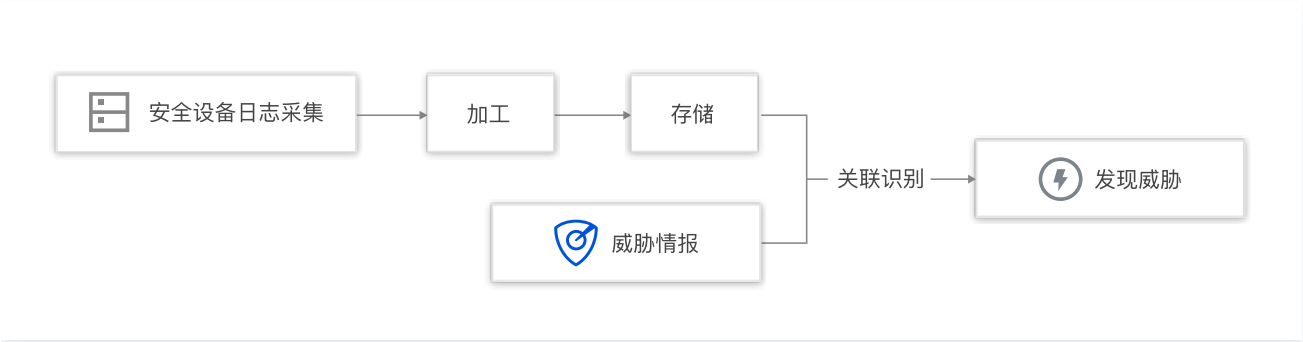
搭建数据市场，提供 Rest API 及 SDK，实现“插件化”的场景组装构建安全功能和数据应用。

应用场景

最近更新时间：2024-01-17 10:10:41

安全分析

具备 PB 级数据秒级分析能力，集成威胁情报，可对全流量实时检测、原始主机日志实时分析、以及海量数据威胁情报分析。支持丰富的安全检测，如 SQL 注入、代码注入、命令执行、XSS、CSRF、WebShell、僵尸网络、勒索、挖矿、DGA、木马、后门、APT 等。

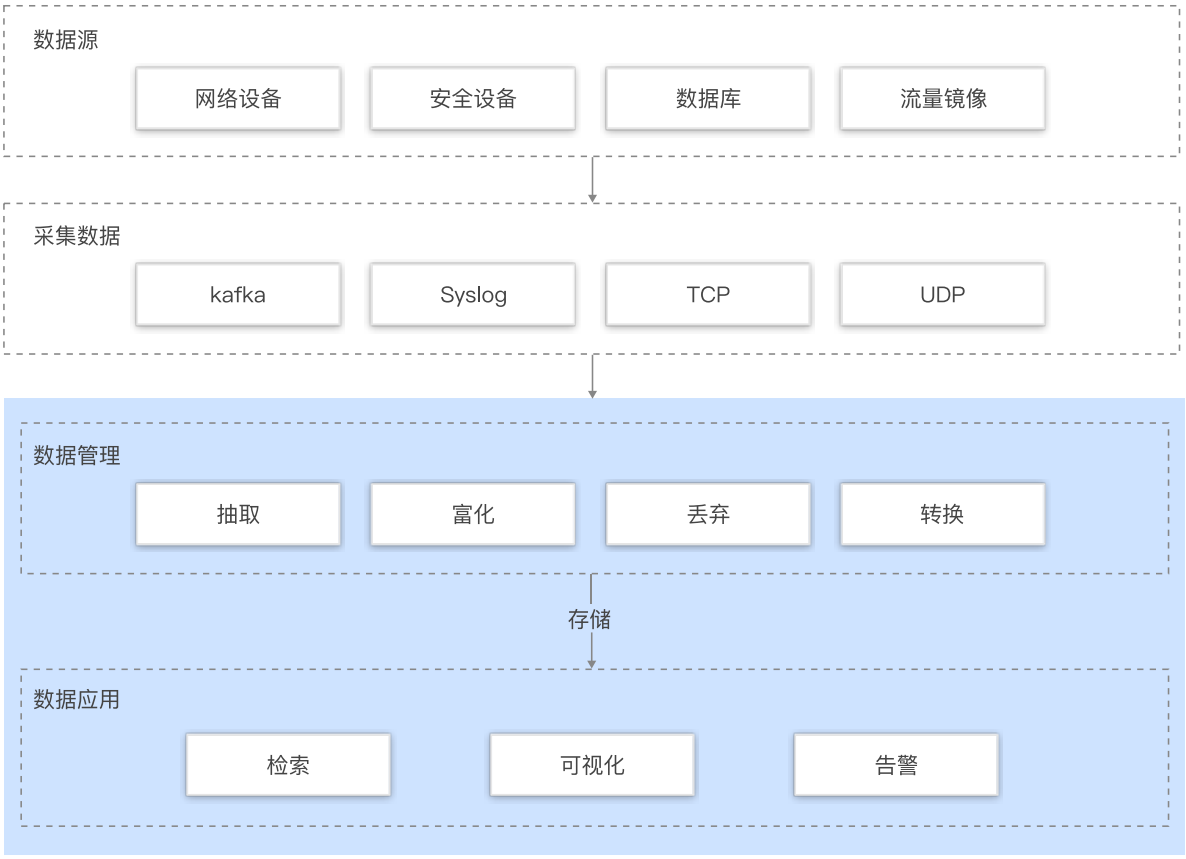


威胁狩猎

支持 PB 级数据低成本存储、万亿记录秒级分析能力。将全流量、原始主机日志、应用日志、安全产品告警等海量数据进行长周期存储。通过 ATT&CK TTP 对以上数据进行威胁狩猎，在日常运营和攻防对抗场景下，主动发现高级威胁、APT、以及潜伏的高危安全事件，还原其上下文（全流量、主机行为），构建完整性溯源取证和事件定损。

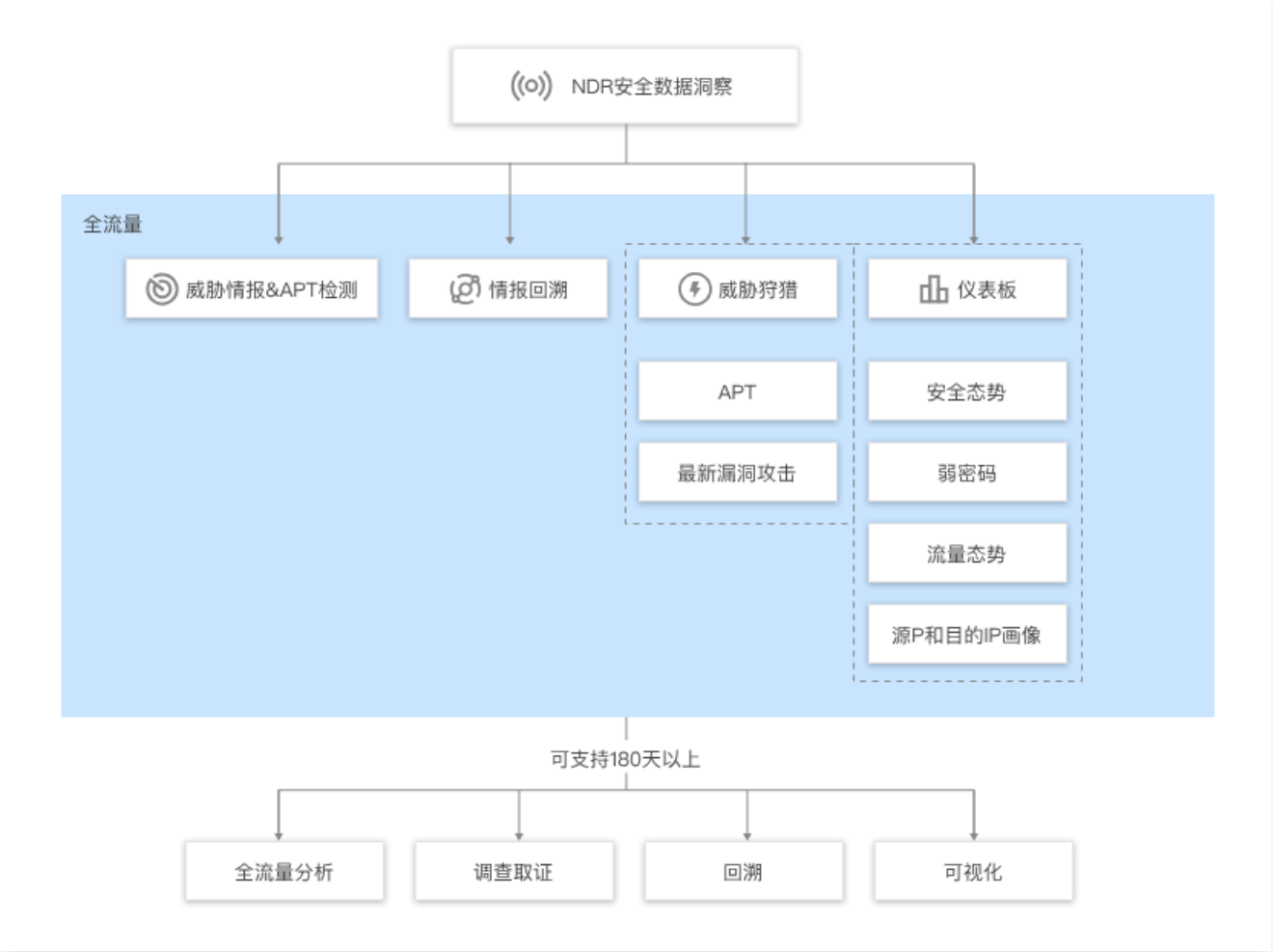
合规审计

支持 PB 级数据低成本存储、秒级检索查询。将网络设备日志、安全设备日志、数据库审计日志、流量日志、以及其他系统日志等进行长周期存储，存储周期可达180天以上，符合安全合规审计。



流量安全洞察

NDR 安全数据洞察，包括基于全流量的威胁情报&APT 检测、情报回溯、威胁狩猎（APT、最新漏洞攻击）、仪表板（安全态势、弱密码、流量态势、源 IP 和目的 IP 画像等）。可支持180天以上的全流量分析、调查取证、回溯和可视化。



终端安全洞察

IOA 安全数据洞察，支持180天以上的安全洞察，包括合规态势、准入态势、安全态势、漏洞态势，支持基于全量终端日志的威胁情报&APT 检测、情报回扫、威胁狩猎、行为审计、事件溯源等。