NDR 网络威胁检测系统

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：2025-04-14 15:18:42

什么是 NDR 网络威胁检测系统

NDR 网络威胁检测系统（Network Detection and Response），是网络威胁检测、分析、溯源和阻断的一体化解决方案。在网络边界处采用镜像流量和旁路检测的方式，对流量进行协议解析、文件还原和全量信息存储，通过有机结合规则引擎、哈勃沙箱、威胁情报和 AI 算法等技术，帮助企业发现恶意攻击和潜在威胁，协助客户对攻击事件进行分析、溯源和阻断。

产品功能

网络入侵检测

木马、蠕虫及漏洞利用等攻击手段在网络入侵中仍占据很大比例，NDR 网络威胁检测系统提供完善的网络入侵规则集，高度覆盖已知入侵场景。

文件威胁检测

对于从流量中还原的样本，运用自研的哈勃沙箱和腾讯反病毒引擎TAV技术，以动态行为检测、静态行为检测以及漏洞检测方式，发现恶意文件并洞察恶意文件一切行为。

威胁情报失陷感知

黑客往往会通过远程控制已攻陷的系统，挂马企业信息资产，此类行为会使外联 C&C 服务器产生相应的网络流量。因此，网络边界是从全局感知失陷资产的极佳位置。NDR 网络威胁检测系统基于腾讯的威胁情报，可精准识别网络主机产生的失陷流量。

全流量数据溯源分析

在攻击发生后，用户往往要对安全事件进行溯源分析，了解安全事件的来龙去脉，对于较大的安全事件，甚至需要进行深入复盘。NDR 网络威胁检测系统提供流量日志存储功能，通过“检索”可进行流量日志交互式分析，回溯攻击发生时刻的流量信息，同时还可提供告警流量的 PCAP 包下载功能。

安全专题运营分析

基于腾讯安全的运营经验，NDR 网络威胁检测系统提供了密码安全、勒索病毒、组件安全、攻击 IP 分析、数据泄露、登录行为分析、邮件安全和域名解析的专题场景，每个专题下会提供多种角度的安全分析视图，供安全运营管理人员重点关注及分析。

资产发现及管理

NDR 网络威胁检测系统的资产管理包括资产列表和资产发现。用户能够便捷快速的管理资产，从列表页中快速识别风险信息，洞察资产风险分析结果，迅速从资产维度处理安全事件，提升管理和运维效率。

产品优势

最近更新时间：2024-09-19 09:51:31

强大流量分析引擎

内置安全规则和机器学习算法模型，能够快速准确地发现已知和未知的各类攻击事件，具有强大的威胁识别能力。

腾讯哈勃沙箱技术

具备高可疑行为监控、网络发包监控、隐私窃取监控等能力，可以全方位监控动态行为，多方面精准识别勒索病毒和漏洞行为。

集成威胁情报服务

对网络恶意流量进行精准判定。依托海量的高质量威胁情报服务，大幅提升检测与溯源能力，使告警有据可依，有源可查。

检索系统高效易用

PB 级别的数据存储和检索，支持平行扩容。对全流量、告警、协议、报文和资产等数据进行快速有效地检索，助力客户调查取证及溯源。

AI 安全检测能力

运用基于 AI 的分析和检测技术，使用传统规则引擎与机器学习智能算法相结合的分析技术，配合丰富的业务场景与安全场景，最终实现风险发现和威胁检测的能力，即安全感知。

应用场景

最近更新时间：2025-04-14 15:18:42

深度检测

传统检测手法对高级威胁基本无效。NDR 网络威胁检测系统大量应用人工智能、机器学习，行为分析，统计模型等高级检测方法来识别网络中潜伏的威胁。检测效果明显优于传统检测方法，有效识别高级威胁、未知威胁。

失陷感知

边界是对用户网络中失陷流量进行感知的主要位置，NDR 网络威胁检测系统集成腾讯威胁情报，通过情报匹配，能协助用户精准定位失陷资产，及时感知资产受害信息。

常见安全场景调查

提供安全交互分析工具，内置腾讯域名解析、勒索病毒检测、密码安全、组件安全、邮件安全、登录行为分析等丰富安全运营专题分析，助力安全调查与分析。

秒级响应

结合腾讯网络入侵防护系统旁路阻断能力，毫秒级实时拦截攻击。适配IPv4、IPv6场景，提供基于IP和URL的阻断能力。轻松应对亿次攻击。开放阻断能力API供第三方检测设备调用，帮助企业快速响应安全事件，构建流量威胁响应中心。