

网络检测与响应

常见问题

文档版本 01
发布日期 2025-12-04



版权所有 © 华为云计算技术有限公司 2025。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址：贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址：<https://www.huaweicloud.com/>

目录

1 NDR 服务不同版本插件差异是什么.....	1
2 NDR 服务的威胁检测原理是什么.....	2
3 NDR 服务支持哪些网络协议的威胁分析.....	3
4 NDR 服务支持哪些网络攻击行为的检测.....	4
5 NDR 服务加密流量检测的原理是什么.....	5
6 NDR 支持哪些类型的加密流量威胁检测.....	6

1 NDR 服务不同版本插件差异是什么

NDR提供基础版和专业版两个版本的流量检测插件。

基础版适用于基础的主机流量威胁检测场景，专业版属于威胁检测的进阶，能够识别更多隐藏威胁和实现威胁处置。

- 基础版：支持主机东西向和南北向流量安全检测，威胁告警。
- 专业版：在基础版的基础上，支持加密流量检测与威胁阻断。

2 NDR 服务的威胁检测原理是什么

NDR服务通过在主机上安装检测插件，插件会对流经当前主机网卡的所有流量进行安全检测。

然后综合利用威胁特征，威胁情报，AI模型，综合评分等方式，识别流量中潜在的攻击行为和恶意代码。

安全管理人员可通过管理界面呈现的威胁统计和详情信息，对威胁进行综合分析，对明确的攻击行为进行阻断处置，保证云环境安全。

说明

当前NDR服务检测插件需要依赖HSS主机安全底座，要求检测主机中需先安装HSS并开启防护。

3 NDR 服务支持哪些网络协议的威胁分析

NDR服务支持多种协议的网络威胁检测，具体支持的网络协议如下：

- HTTP
- TCP
- UDP
- DNS
- Telnet
- SMTP
- DHCP
- FTP
- MySQL
- IMAP
- SSH
- SMB
- RDP
- TLS
- MSSQL

4 NDR 服务支持哪些网络攻击行为的检测

NDR预置多种检测和拦截模型，支持以下常见典型攻击的识别与防御：

- 爆破
- 扫描
- Web攻击
- Webshell
- 反弹shell
- 恶意程序
- 异常连接
- 异常协议
- 数据泄密

5 NDR 服务加密流量检测的原理是什么

据不完全统计，企业在互联网中发布的应用，90%以上是通过加密协议发布。企业选择加密协议，主要还是考虑到应用安全和数据安全。

应用加密一定程度上确实保证了安全性，但是也给网络攻击的潜伏带来便利。隐藏在加密流量中的恶意代码，无法被精准识别。

传统的证书解密，中间人代理和大数据/AI技术等，或者有大量额外的准备条件，或者可解释性和准确性很差，因此，加密流量威胁检测成为“老大难”问题。

华为云NDR为了解决上述问题，另辟蹊径采用非证书的解密技术，在保证性能和稳定性的同时，实现了对主机进程中加解密过程的数据还原，此时原本伪装在加密外衣中的恶意代码和攻击行为就暴露出来，轻松被捕获、识别和处置，达成了加密流量检测的根本目的。

6 NDR 支持哪些类型的加密流量威胁检测

NDR当前支持以下类型进程的加密流量威胁检测，加密流量的检测方法请参考[配置流量检测策略](#)。

- java
- tls
- Python
- curl