圣博润
SBR-info

圣博润恶意代码检测与防御系统

产品概述

圣博润恶意代码检测与防御系统（简称LEDR），采用机器学习及大数据分析技术、高级行为分析技术和漏洞利用检测技术，结合有效的威胁情报信息，针对类似于勒索病毒等高级威胁提供及时检测和快速响应。

产品功能

● 检测和防御0day攻击

通过对操作系统的持续监控，标记和追踪可疑行为，发现针对漏洞利用的行为并进行处置，有效检测和防御0day攻击。

● 未知恶意代码检测与防御

通过对系统行为数据的碰撞和仿真系统行为诱捕，发现系统中存在的异常行为，结合安全事件的关联分析针对未知恶意代码攻击做出响应和处置，针对勒索病毒及其变种均可做到有效检测与防御。

● 黑白名单功能

针对已知的恶意威胁建立黑白名单机制，有效防止威胁的发生和传播，做到事前预防。

● 安全威胁追踪与取证

管理员可通过计算机名、IP地址、用户名等作为关键字追踪系统中安全威胁相关信息，包括可执行文件、域名（IP地址）、可疑用户、IOC扫描威胁。

● 应急响应与处置

◎ 一键隔离功能：快速将威胁主机从网络中隔离，隔离主机仍可与管控服务端保持通讯，隔离可有效避免威胁传播，与管控服务端保持通讯可避免高级恶意软件在网络离线时自毁或掩盖攻击痕迹；

◎ 远程查杀功能：可远程对认定的恶意进程强制灭杀，同时进程对应的恶意程序被自动隔离，以防再次运行。

产品特点

- **轻量级客户端运行与维护**

  系统运行状态下主机CPU占用不超过1%，内存占用小于20M；客户端可一键快速安装和升级。

- **高效准确的威胁发现能力**

  通过检测攻击者的攻击路径和手法及时发现被隐藏的攻击痕迹、行为动作以提升威胁发现能力，同时有效检测病毒以及恶意软件变种。

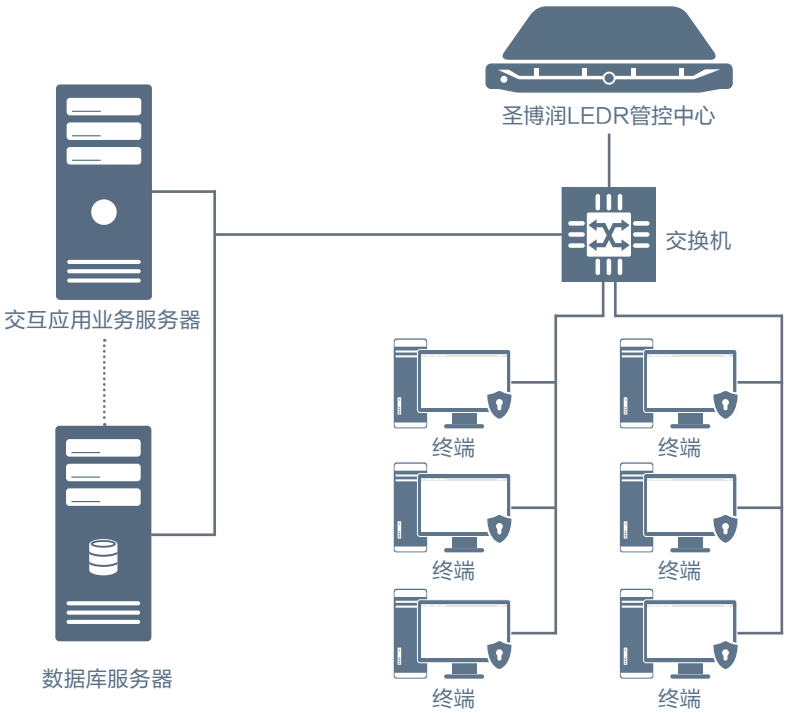
- **有效识别和防范0day、未知恶意威胁**

  通过主动行为检测及安全事件关联分析，有效识别0day、未知恶意威胁，准确定位攻击根源。

- **完整的恶意代码处置——事前防御，事后补救**

  以勒索病毒为例，提供全面的恶意代码识别与检测技术手段，防止勒索病毒侵入被保护的信息系统，做到事前全面防御。对已经发生过勒索病毒事件的网络，能识别、精确定位感染源，并能清除勒索病毒感染源，防止勒索病毒事件再次发生，做到事后积极补救。

产品部署



产品规格

型号规格	配置	性能
LEDR-200	1U，16G 内存，2T 硬盘，单电源，1 个管理口，4 个 100M/1000M 电口	可管理 200 个主机（主机包括终端和服务器）
LEDR-500	1U，32G 内存，4T 硬盘，单电源，1 个管理口，4 个 100M/1000M 电口	可管理 500 个主机（主机包括终端和服务器）
LEDR-1000	2U，32G 内存，4T 硬盘，单电源，1 个管理口，4 个 100M/1000M 电口	可管理 1000 个主机（主机包括终端和服务器）
LEDR-2000	2U，64G 内存，6T 硬盘，双电源，1 个管理口，6 个 100M/1000M 电口	可管理 2000 个主机（主机包括终端和服务器）
LEDR-4000	2U，128G 内存，10T 硬盘，双电源，1 个管理口，6 个 100M/1000M 电口	可管理 4000 个主机（主机包括终端和服务器）

★ 产品规格可能会随市场需求调整，请及时联系以获取最新规格参数。

用户价值

- **主动式免疫保护，有效抵御勒索病毒等恶意软件攻击**
- **获得主动防御0day攻击和未知恶意威胁的能力**

地址：北京市海淀区高梁桥斜街 59 号院 2 号楼 3 层 / 邮编：100044
技术支持热线：800-810-2332 / 400-966-2332 / 电话：010-82138088
技术支持邮箱：support@sbr-info.com / 网址：www.sbr-info.com