Bitdefender®

GravityZone 精英版

AI驱动的可视化威胁检测与响应平台

引言 从防御到响应，企业需要更全面的安全能力

在面对日益复杂的网络攻击时，传统防护手段已难以满足现代企业的安全需求。勒索病毒、无文件攻击、APT渗透、漏洞武器化利用等高级威胁不断演化，安全能力不仅要“防得住”，更要“看得见、控得住、应得快”。

Bitdefender GravityZone 精英版是面向进阶企业的全栈安全平台，集成先进的EPP + EDR能力，融合AI、行为分析与攻击可视化技术，全面提升终端防护、威胁检测、事件响应与取证分析能力，为企业构建“零盲区、快响应”的安全运营体系。

产品主要优势

→ 全栈防护，一体集成：集成AV、EDR、沙箱、补丁、CWPP、Exchange邮件服务器安全、硬盘加密、攻击面管理等，构建统一终端安全平台

→ AI赋能，智能检测：每天处理5000亿次威胁查询，检测率达99.9%，支持自动响应与溯源分析

→ 攻击链可视化，响应提速：攻击路径自动还原，支持隔离、回滚等操作，一站式处置威胁

→ 跨平台支持与快速部署：支持Windows、macOS、虚拟机和云环境，5分钟快速上线

功能模块与防护能力

→ **反恶意软件**：基于AI驱动的多层检测引擎，实时扫描并清除病毒、木马、勒索病毒、APT威胁等恶意软件。

- 静态与动态启发式分析，结合全球5亿终端的威胁情报库
- 机器学习模型每日处理5000亿次安全查询，**检测率高达99.9%**

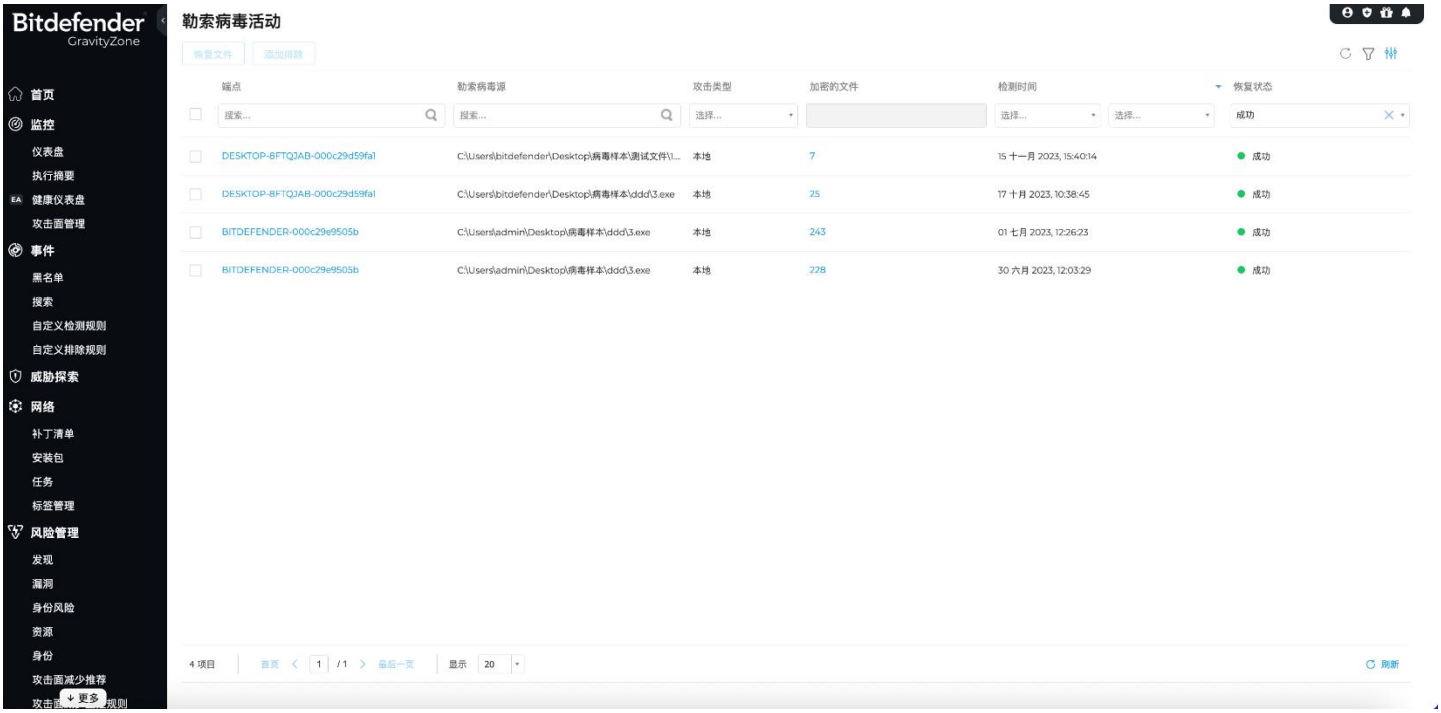
→ **高级威胁防护**：基于行为分析而非特征码，实时监控进程活动，精准识别未知威胁。

- 实时监测300+恶意行为特征
- 机器学习分析340+进程特征，降低误报率
- 深度检测内存攻击和DLL劫持

- 内核级防护，有效对抗高级攻击工具
- 全面监控关键系统操作

→ **勒索病毒防护**：实时检测加密行为并自动恢复文件，阻断本地/远程勒索攻击，提供主动防御+精准回滚双重保障：

- 实时阻断攻击：通过行为监控精准识别加密行为（如大规模文件篡改），立即终止恶意进程
- 一键回滚被勒索病毒加密的文件：立即回滚被加密的文件，支持自动恢复和手动恢复
- 防篡改备份：采用专利非VSS（卷影复制）技术，为关键数据构建独立于系统的安全副本，彻底规避勒索软件对备份链的破坏行为



→ **HyperDetect 可调节机器学习**：是一项专为识别APT攻击手法而设计的可调节机器学习技术，它部署在防护链的预执行阶段，通过增强型启发式分析，有效拦截利用合法工具发起的隐匿性攻击。

- 高级启发式检测：在文件执行前识别恶意行为，拦截利用合法工具发起的攻击，如：Rclone（数据窃取工具）、Gsudo（提权工具）、远控管理框架、Sysinternals 套件（常被APT用于隐蔽操作）
- 恶意打包识别能力：识别使用未知或恶意倾向的加壳方式打包的可执行文件，以及使用 Visual Studio、VS Code、Delphi 等编译的可疑程序
- 可疑行为与路径识别，检测异常行为与结构：可执行文件存在于异常目录、文件名异常、进程之间的父子关系异常（如非预期的进程调用链）、可疑执行路径或关联命令行为

→ **无文件攻击防护**：通过分析内存行为与命令执行路径，在恶意代码运行前实现精准阻断，有效拦截不落地、不留痕的高级攻击。

- 拦截内存型攻击， 阻止利用 PowerShell、WMI、CMD 、Python 等工具直接在内存中运行恶意代码，杜绝传统杀软无法识别的威胁。
- 防范命令行滥用，识别恶意命令模式、异常执行路径和脚本注入行为，保护终端免受脚本型、自动化攻击链侵害。
- 构建多平台防护体系，结合 AMSI 与命令行分析引擎，覆盖 Windows、macOS、Linux 等操作系统，形成统一的无文件攻击防御能力。

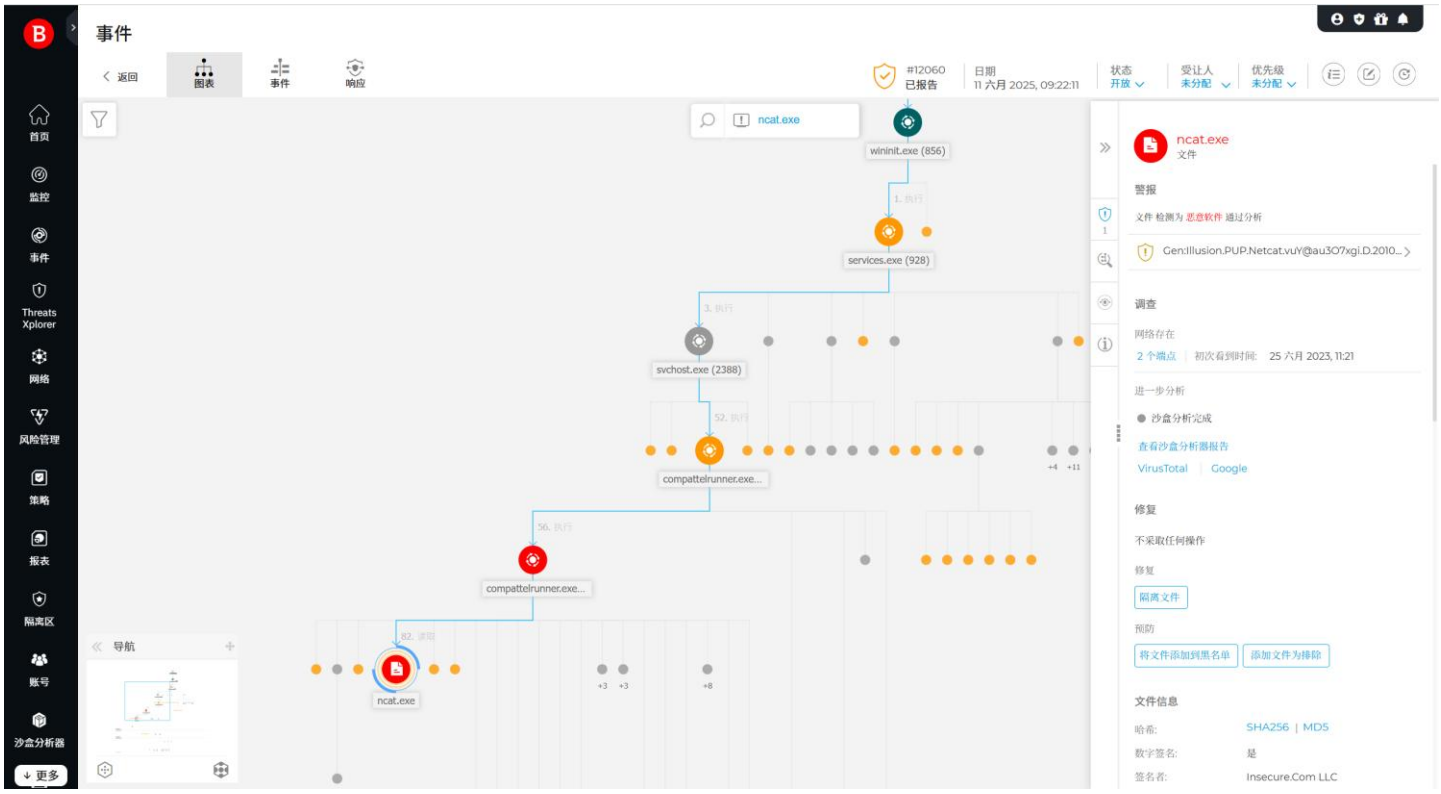
→ **沙盒分析器**：是一项基于云端的动态行为分析技术，在隔离的虚拟环境中“引爆”可疑文件，精准识别逃逸型、免杀型、高复杂度恶意软件，构建终端防护的最后一道防线。

- 精准识别未知威胁与绕过型攻击，有效对抗企图规避防御（AV/EDR）的攻击行为
- 可疑文件自动提交沙箱，无需人工抓样本或等待，分析结果智能判决，自动阻断威胁，无需安全专家介入，提供详细报告与可视化分析图，辅助快速理解与溯源
- 威胁情报共享与自动化防护升级，分析结果同步至网络中的其它电脑，确保一旦某一电脑识别出威胁，所有电脑即刻获得防护，无需重复“引爆”。

→ **攻击实时可视化**：提供交互式图谱视图，帮助安全团队直观理解攻击链条、溯源威胁来源，并快速做出响应，极大提升检测效率与处置速度。

- 还原完整攻击链，辅助快速溯源，自动绘制攻击路径图，包括初始入口、恶意进程行为、文件创建、注册表操作、命令执行、网络连接等，帮助安全人员快速定位“谁、从哪、怎么来”的威胁路径。
- 提升威胁理解与响应决策效率，每个事件节点附带详细上下文信息（如哈希、文件路径、命令行、相关进程等），结合 MITRE ATT&CK 技术标签，实现知识化威胁分析，有助于判断是否为误报、是否需要隔离或阻断

- 支持协作与应急响应闭环，管理员可直接在可视化界面发起终端隔离、进程终止、文件封锁等响应动作，提升响应闭环效率，并生成事件报告辅助复盘、审计或汇报。



→ **高级反漏洞利用**：主动防护系统内存及应用程序漏洞，拦截零日攻击和权限提升行为，防御APT攻击、漏洞武器化利用及内存注入攻击。

- 监控进程内存操作（如API调用、ROP攻击），保护LSASS等关键进程。
- 防止0day漏洞、未知武器化利用

→ **Web威胁防护**：实时过滤恶意URL，阻止恶意软件下载及C2通信。

- 云端URL信誉库动态更新，覆盖TOR/暗网威胁。
- 防御水坑攻击、恶意广告及僵尸网络通信。

→ **反钓鱼**：拦截钓鱼网站及商业欺诈（BEC）行为，保护企业数据与资金安全。

- SSL流量解密扫描，识别仿冒登录页面。
- 识别仿冒页面与商业欺诈（BEC）

→ **智能防火墙**：精细化控制网络访问策略，检测入侵行为。

- 基于行为的应用联网管控（如限制RDP外联、禁用445端口）

- 实时拦截网络扫描等异常活动

→ **网络攻击防护**：实时监控网络流量，检测并阻断恶意连接、网络漏洞利用及异常行为。

- 拦截暴力破解攻击（如RDP、SSH、SMB暴力破解）
- 拦截网络漏洞利用攻击（如 EternalBlue、Log4j、ProxyShell）
- 拦截横向移动攻击（如 Pass-the-Hash 、Kerberos 票据伪造）恶意C2通信（如僵尸网络、APT远控流量）

→ **风险管理**：持续识别、分析和缓解端点、用户和云环境中的潜在安全风险，帮助企业主动防御、减少攻击面、提升安全韧性。

- 可视化风险全景，提升决策效率，提供公司级风险评分与趋势图，快速定位高风险用户、终端、漏洞或配置错误
- 支持计划扫描与按需扫描，持续扫描 + 自动加固，降低攻击面

→ **防篡改**：从用户态到内核态的全链条保护，防止攻击者破坏安全软件

- 自我保护：自动保护安全进程、文件和注册表，防止终止或修改，防止安全软件被攻击者关闭、卸载、绕过
- 回调逃逸检测：实时监控关键系统回调（如进程创建、驱动加载），发现篡改立即告警和拦截
- 漏洞驱动防护：识别并阻断利用合法驱动漏洞的攻击

→ **设备控制**：防止数据外泄与恶意设备接入

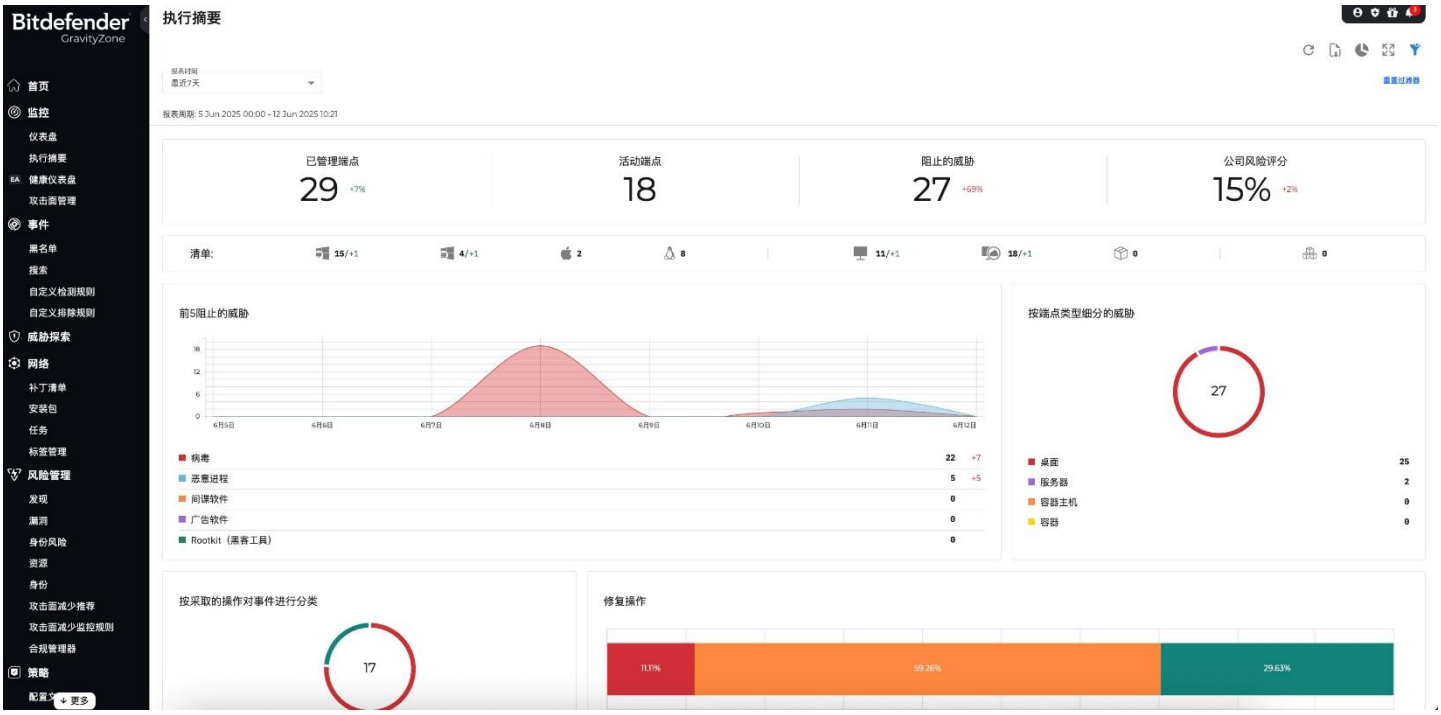
- 设备类型识别与分组管理：可识别并分类控制各类设备（如U盘、移动硬盘、打印机、手机、调制解调器等），支持不同用户组分配不同策略。
- 按权限授予访问级别：可配置只读、完全禁止、读取等多种访问级别，满足合规性与办公便利性之间的平衡。
- 按设备ID授权白名单：支持根据设备ID定义可信USB设备，防止非法设备伪装接入。

部署与管理

→ 支持云端控制台与本地私有化部署，5分钟即可完成快速上线。

→ 支持 Windows、macOS、服务器系统、VMware、Citrix数据中心，Azure、阿里云环境等

→ 中文化界面，管理简洁直观



权威认证

Bitdefende被独立测试组织和行业顶级咨询公司公认为全球网络安全的领导者。

2024 端点安全魔力象限 远见者

AV-Test 2024 年度最佳保护产品

Gartner 2025 客户之选

免费试用

欢迎体验，试用申请：https://www.bitdefender-cn.com/free-trial.html

联系电话：4000-132-568

联系邮箱：sales@bitdefender-cn.com

关于Bitdefender

Bitdefender 是全球领先的网络安全公司，保护全球 5 亿多设备，覆盖 170 多个国家。其安全技术被全球超过220+公司集成并采用，深受客户与行业认可。

扫一扫 关注我们