Bitdefender®

GravityZone 旗舰版

覆盖威胁全生命周期的智能防护体系

引言

当前企业安全环境正经历结构性变革。高级持续性威胁（APT）、无文件攻击、勒索软件即服务（RaaS）以及攻击者对AI的武器化等新型攻击手段持续演进，安全对抗已从“工具之争”升级为“策略与智能的博弈”。

攻击者正越来越多地依赖零日漏洞利用、合法工具滥用（LOLBins）与供应链攻击等TTPs（战术、技术与程序）绕过传统防御机制，使基于签名和静态规则的防护方式失效。

与此同时，混合办公、多云架构与物联网设备的大规模部署使企业攻击面呈指数级扩展，暴露资产数量激增，边界愈发模糊，风险传导速度加快。传统孤立、被动的安全体系已难以胜任现代威胁环境下的防护与响应需求。

Bitdefender GravityZone 旗舰版 构建于新一代自适应安全架构之上，深度集成多项关键能力，全面覆盖从**预防（Prevention）—检测（Detection）—响应（Response）—预测（Prediction）**的全生命周期防护体系。

平台融合了领先的 EPP（端点防护平台）、EDR（端点检测与响应） 与 XDR（扩展检测与响应） 技术，同时集成 外部攻击面管理、主动攻击面收敛、合规与风险管理 以及 漏洞管理 功能，为企业提供统一、安全、智能的立体式防御体系。

这种高度集成的架构不仅显著提升了跨系统、跨终端的可视性与响应效率，也帮助安全团队从被动防守转向主动防御与预测性分析，构建真正面向未来的网络安全能力。

产品主要优势

→ 全生命周期防护：覆盖预防、检测、响应与预测四大关键阶段，实现从事前防护到事后修复的闭环安全能力。

→ 统一安全架构：深度整合 EPP、EDR、XDR、攻击面管理、风险与合规功能，打破数据孤岛，提升安全运营效率。

→ 主动攻击面收敛：自动识别外部暴露资产与配置风险，持续优化企业攻击面，降低被攻击概率。

→ 高效可视化与快速响应：提供端到端攻击路径分析、MITRE ATT&CK 映射、一键处置等功能，缩短平均检测与响应时间（MTTD / MTTR）。

→ 智能风险与漏洞管理：基于行为分析和上下文评估对终端与用户风险进行量化评分，辅助决策优先修复策略。

→ 云原生设计，灵活部署：支持云端与本地部署模式，单代理、单控制台架构，快速落地，轻松对接现有系统。

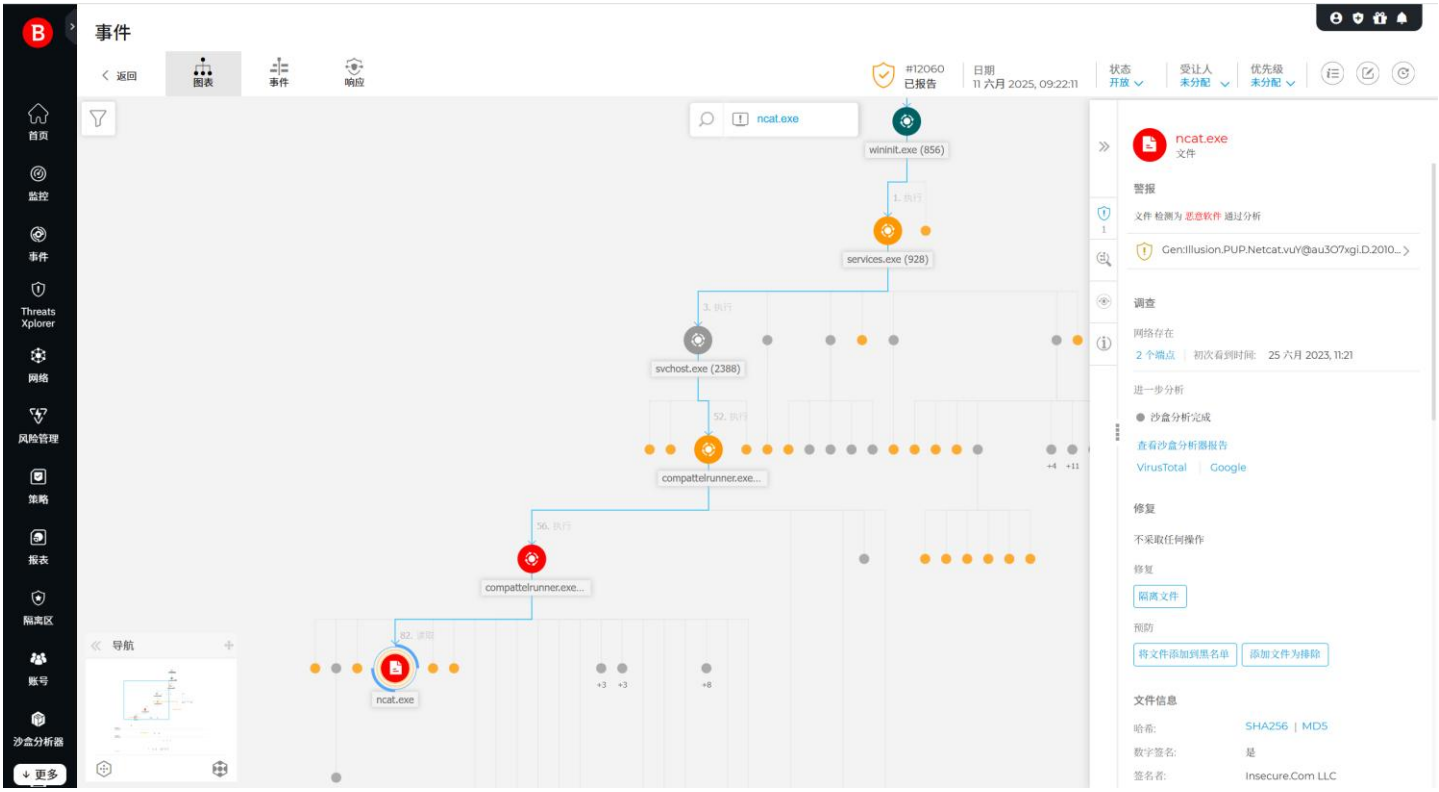
功能模块与防护能力

→ **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本地与云端协同防护
- 全球 5 亿终端威胁情报支持，识别新兴变种与零日攻击
- 机器学习模型每日处理5000亿次安全查询，**检测/阻止率高达99.9%**

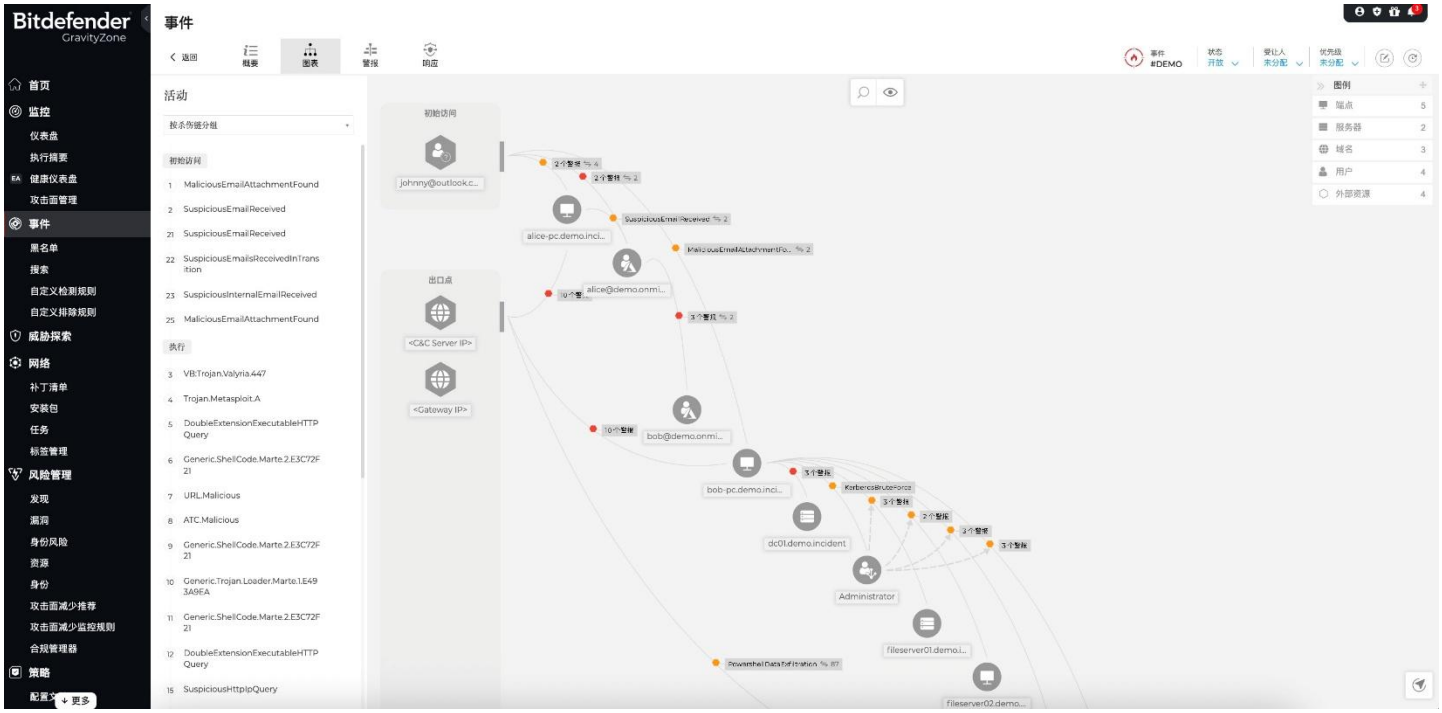
→ **EDR端点检测与响应**：通过先进的 EDR 引擎与交互式攻击链可视化能力，帮助企业精准还原威胁全过程，从行为检测到根因溯源，实现快速、高效的威胁响应闭环。

- 基于MITRE ATT&CK 的智能检测：融合全球权威攻击战术技术框架，自动识别攻击战术、技术与程序（TTPs），告警分类清晰，便于快速研判与应对。
- 连续三年 在MITRE ATT&CK 评估中实现 100% 检测率与最高威胁描述等级
- 攻击路径图谱和Storyline还原全链路攻击：可视化呈现从初始入侵、横向移动、权限提升到数据窃取的完整路径，涵盖进程、文件、注册表、命令、网络连接等多维操作，助力快速定位“谁、从哪来、做了什么”。
- 可视化交互响应闭环：告警节点嵌入上下文详情（如哈希、路径、命令行等），管理员可一键完成隔离终端、终止进程、阻断文件等动作，并自动生成事件报告，助力审计与汇报。



→ **XDR端点检测与响应**：统一关联端点、服务器、容器、AWS/Azure云平台、网络流量、Active Directory、Entra ID、Office 365、Atlassian 等关键系统的安全数据，实现跨域威胁检测与协同响应。

- 自动化威胁关联分析：智能重建攻击链与横向移动路径，快速识别潜在入侵扩散行为
- 多维事件上下文建模：将单点告警与主机行为、账户活动、网络流量等进行深度关联，发现隐藏攻击逻辑
- 原生对接 SIEM / SOAR：无缝整合第三方平台，实现从检测到处置的自动化闭环



→ **XDR 网络流量分析**：攻击者频繁利用网络实施侦察、初始入侵、横向移动及数据窃取。GravityZone XDR通过自动关联网络及多源威胁信号，实现快速精准响应，减轻分析师负担，有效替代昂贵复杂的NDR解决方案。

- 统一威胁可见性：实时分析网络流量，精准识别端口扫描、横向移动和数据外泄等攻击行为。
- IoT威胁检测：监测无代理设备异常流量，主动防御物联网安全风险。
- 低运维成本：原生网络传感器秒级部署，自动整合云端信号，显著降低运营复杂度与成本。

→ **AD/EntraID 身份威胁检测与响应**：全面覆盖本地 Active Directory 和云端 Azure AD（Entra ID），实时监测身份认证与访问行为，识别高危账户活动、凭证滥用和权限提升攻击。

- 本地AD：检测 Kerberos 暴力破解、横向移动、票据重放、伪造域控注册等攻击操作，防止攻击者控制企业身份基础设施。
- Entra ID：识别异常登录、跨地域访问、权限滥用、账户伪装与敏感角色变更，全面保障云端身份安全。

→ **XDR 云传感器**：原生支持 AWS、Azure 与 GCP 三大主流平台，持续监测关键安全事件，及时识别入侵、配置错误与持久化操作。

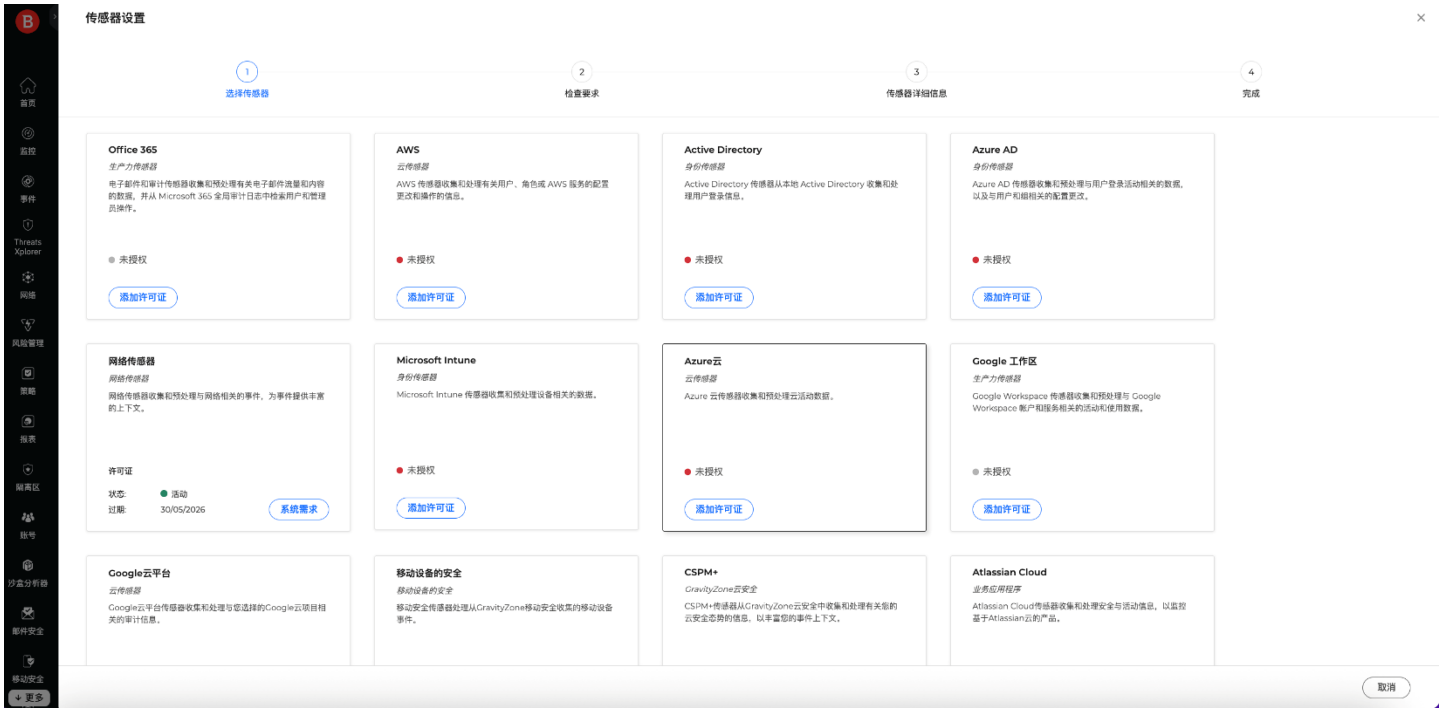
- 全生命周期威胁检测：实时捕捉暴力破解、异常访问、恶意函数执行、日志删除等行为，覆盖侦察、入侵、横向移动与清除痕迹全阶段。
- 行为基线与异常识别：构建云资源正常操作模型，智能识别偏离行为，防范权限滥用、配置泄露与横向渗透，保障多云环境安全可控。

→ **XDR 生产力传感器**：深度集成 Office 365 与 Google Workspace，全面监控邮件、文件和账户行为，保障协同办公平台的使用安全。

- 识别入侵与权限滥用行为：检测钓鱼攻击、异常登录、敏感账户新增、反钓鱼设置被禁用、恶意宏上传、2FA 绕过与批量数据访问等行为，覆盖攻击全生命周期。
- 防止数据泄露与账户劫持：监测邮箱外发异常、文件共享激增、账户批量操作、异常删除等可疑行为，第一时间响应潜在的数据外泄与持久化风险。

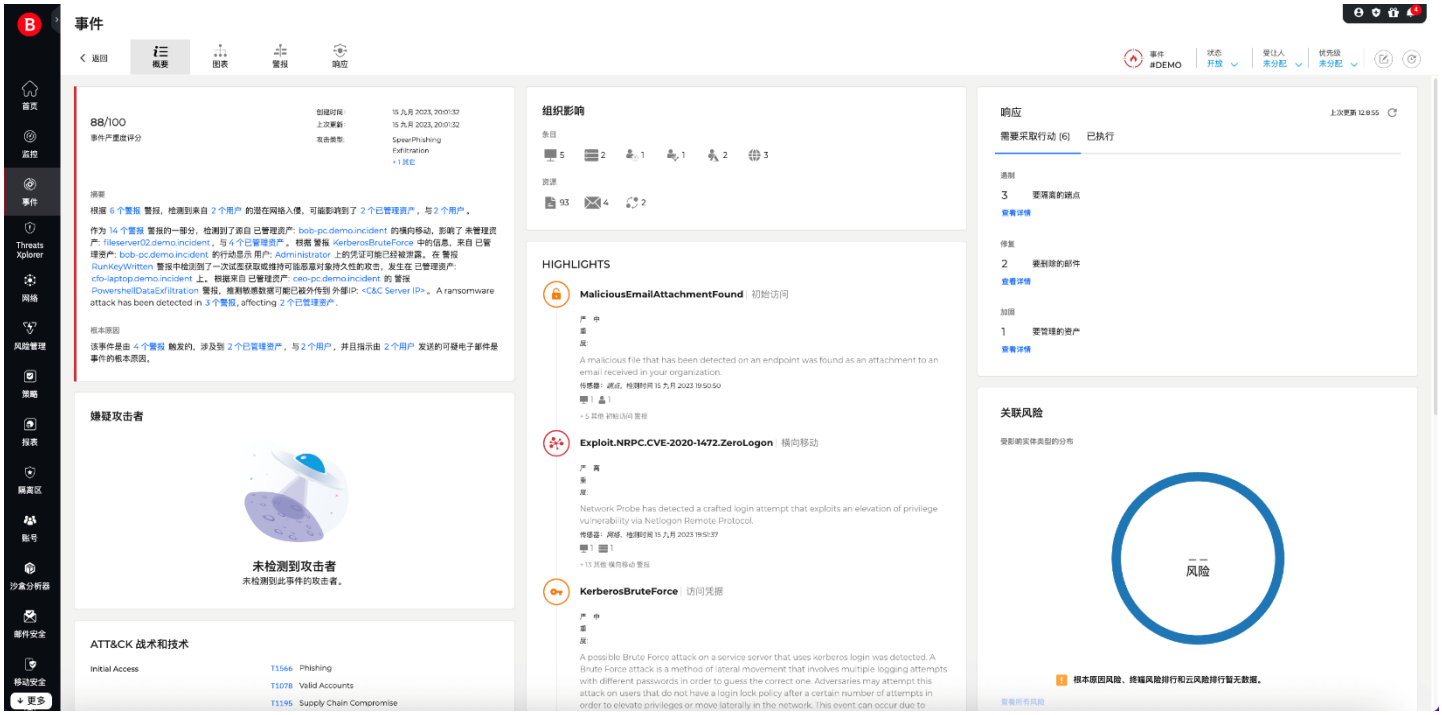
→ **XDR 商业应用传感器**：持续监控 Jira、Confluence 等关键平台，及时发现异常行为、权限滥用与数据泄露风险，确保项目数据与敏感信息安全可控。

- 识别未经授权的账号行为与权限操作：检测暴力破解尝试、可疑令牌创建、权限变更、角色添加或项目删除等行为，防止非法访问与敏感操作。
- 防范数据泄露与破坏行为：监测公共链接生成、空间导出、页面权限调整等潜在外泄操作，阻断数据被窃取或破坏的风险路径。



→ **AI 安全助手**：帮助安全团队在数分钟内完成威胁分析与响应决策，显著降低告警疲劳与响应时间。

- 自动解析攻击全貌：直观展示攻击摘要、影响范围、MITRE ATT&CK 映射、根因分析（RCA）与相关风险，为“发生了什么、为什么发生、影响了什么”提供一目了然的答案。
- 一键式智能响应建议：基于事件上下文，提供覆盖全网的单击响应选项（如隔离终端、封锁账户、清除邮件），辅助用户迅速遏制攻击、最小化业务影响。



→ **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

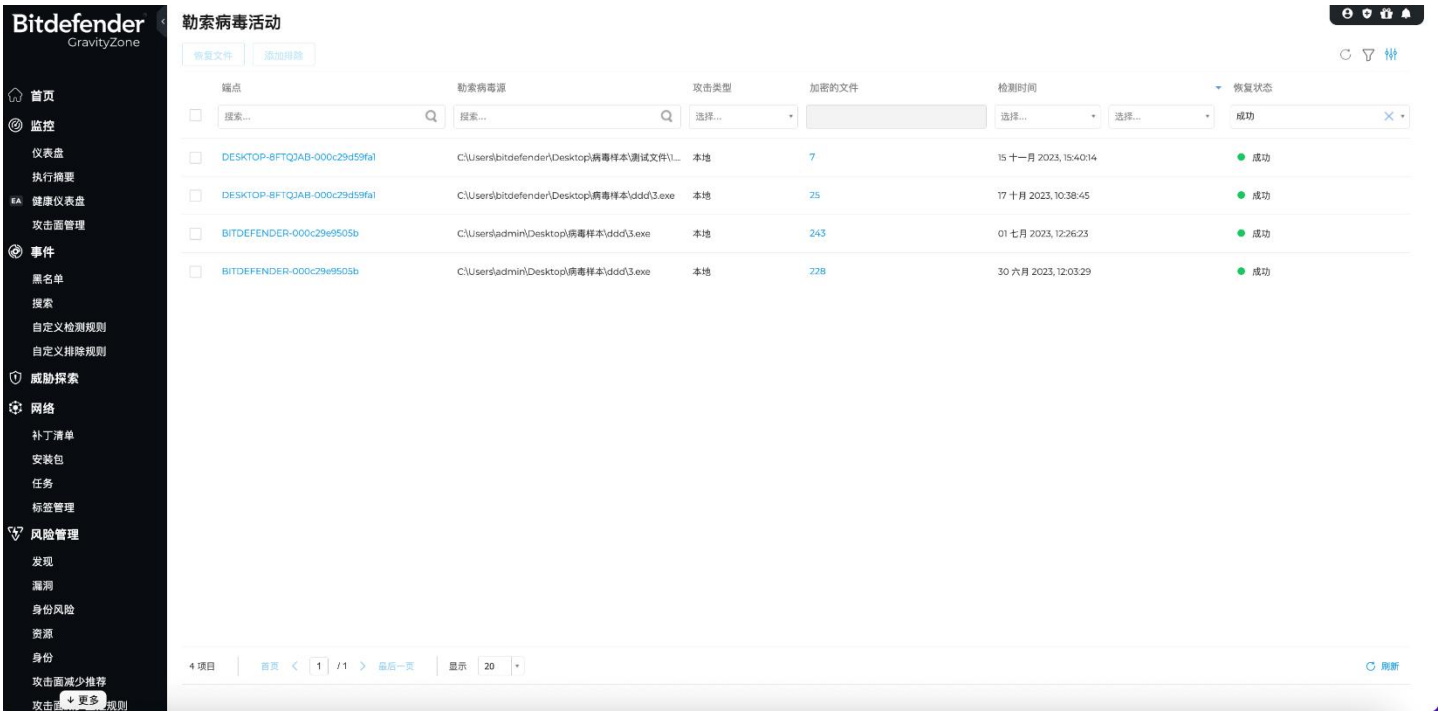
→ **HyperDetect 可调节机器学习**：是一项专为识别APT攻击手法而设计的可调节机器学习技术，它部署在防护链的预执行阶段，通过增强型启发式分析，有效拦截利用合法工具发起的隐匿性攻击。

- 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

→ **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



→ **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。

→ **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

→ **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”。

→ **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。

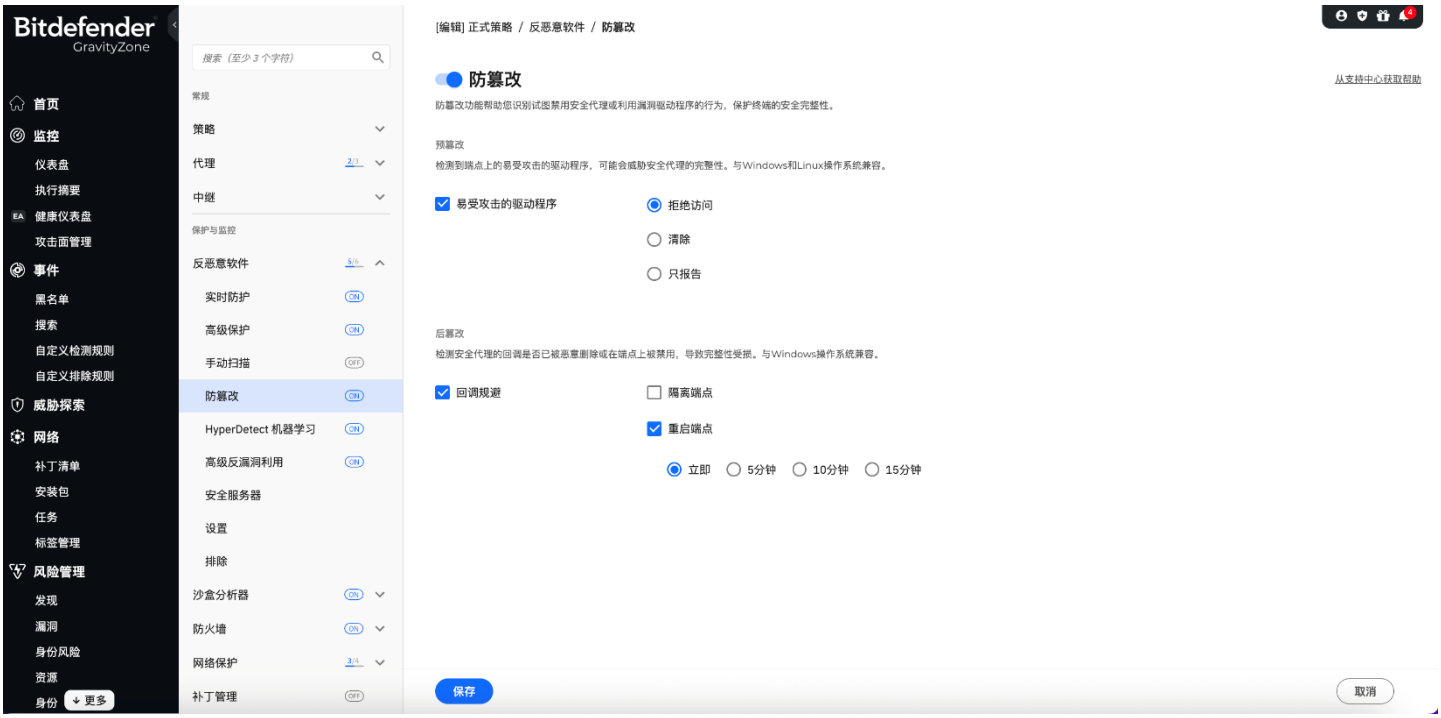
- 拦截暴力破解攻击（如RDP、SSH、SMB暴力破解）
- 拦截网络漏洞利用攻击（如 EternalBlue、Log4j、ProxyShell）
- 拦截横向移动攻击（如 Pass-the-Hash 、Kerberos 票据伪造）恶意C2通信（如僵尸网络、APT远控流量）

→ **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。

→ **应用程序控制：**构建“可信应用”白名单，拒绝未知风险运行

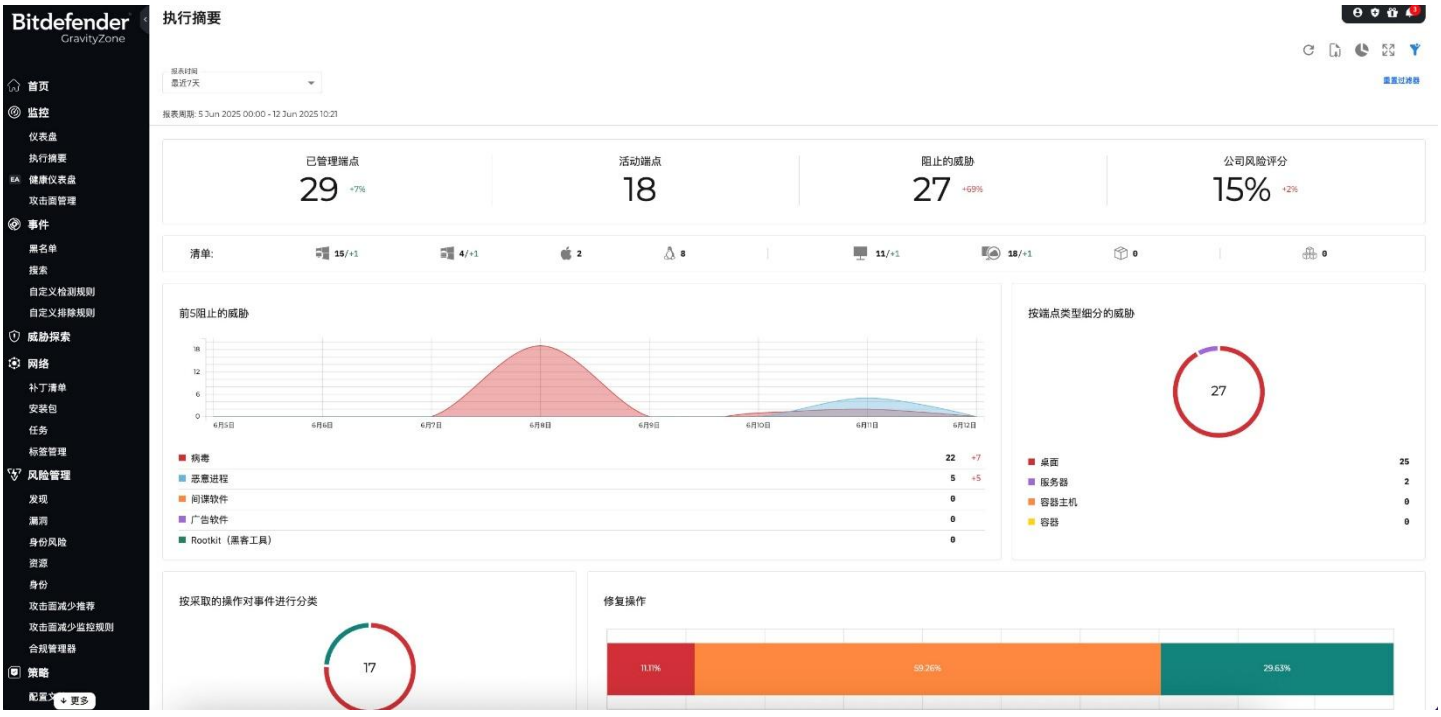
- 通过精细化控制终端上允许运行的应用程序，阻断未经授权或潜在恶意程序的执行，显著降低攻击面。
- 黑名单+白名单机制：仅允许企业批准的程序执行，杜绝未知程序或工具加载

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