Bitdefender

GravityZone AI 安全态势管理

安全使用 AI，无需增加复杂性

AI 应用已经广泛进入企业终端环境，但许多企业仍无法清晰了解正在使用哪些 AI 工具，以及这些使用行为是否正在产生安全风险，并在潜在风险演变为数据泄露事件之前，对潜在风险进行识别、评估和治理。

您并不是唯一面临这一挑战的企业：根据 Bitdefender《2026 网络安全评估报告》，40%的企业认为，降低 AI 使用带来的安全风险暴露，是未来一年最重要的安全工作之一。

GravityZone AI 安全态势管理能够发现企业受管终端中的 AI 使用情况，评估不同 AI 工具带来的安全风险，并提供决策依据，帮助企业决定哪些 AI 应用可以允许使用、需要持续监控，或应该进行限制。

AI 安全态势管理为企业带来的价值：

安全推动企业 AI 应用，降低数据泄露风险

通过集中式 AI 清单，发现您已经管理的终端设备中正在使用的 AI 工具，帮助您识别未经安全团队管理的影子 AI，让您在决定如何处理之前，清楚了解企业环境中有哪些 AI 应用正在运行。

降低最关键的 AI 风险

系统会按照风险类别对发现结果进行分类，并根据严重程度进行排序。每项发现结果都会关联涉及的用户和终端设备，帮助资源有限的安全团队优先处理最关键的问题。

在不增加复杂性的前提下治理 AI 应用

利用 GravityZone 控制台中已有的网页过滤、应用控制和加固策略，根据证据采取行动，无需部署额外工具。

AI 安全态势管理的工作方式：

❶ 发现

通过已部署在终端上的GravityZone代理，发现正在使用的AI。

- 大语言模型与聊天机器人
- AI 助手
- AI Agent
- MCP服务器
- 工具与技能
- 编程助手
- 支持AI的SaaS服务

❷ 评估

判断哪些使用会带来实际风险，以及哪些问题应优先关注。

- 按风险类别归组
- 按严重性和优先级排序
- 关联受影响用户和终端
- 记录来源、置信度及首次/最后发现时间
- 安全证据，不收集提示词内容

❸ 治理

利用 GravityZone 控制台中已有的控制措施，根据证据采取行动。

- Web 访问控制
- 应用控制
- 终端加固策略
- 行为型代理加固（结合PHASR）

作为您现有 GravityZone 平台的附加模块，只需启用即可由已部署的代理开始发现；数分钟内便会出现发现结果。无需集成，无需新建控制台，也无需安排配置项目。

AI安全态势管理工作原理与核心优势

- AI发现基于已经部署在终端设备上的GravityZone Agent，无需新增Agent或调整网络架构，即可发现本地AI运行环境、IDE编程助手、MCP Server和浏览器扩展。
- 覆盖快速增长的AI工具和集成生态，包括 MCP 客户端与服务器、代码助手，以及需要在终端安装本地Agent或客户端的SaaS AI服务。风险发现结果按照风险类别进行分类，并包含严重等级、优先级、服务类型、受影响用户和终端、来源信息、可信度，以及首次和最近发现时间。
- 隐私保护型风险证据。风险发现结果提供足够的信息支持安全决策，同时不会收集提示词内容，也不会收集用户输入AI工具中的数据。审核流程支持状态管理、任务分配和备注记录，帮助资源有限的安全团队建立从风险发现到安全决策的标准化流程。
- 如果同时授权PHASR，安全加固能力可以将AI Agent作为独立行为主体进行管理。例如，一个 AI Agent需要使用 PowerShell，则可以继续允许该Agent使用 PowerShell；但同一设备上的普通用户如果不需要，则可以限制其访问权限，从而减少不必要的攻击面。

为什么 AI 发现需要从终端开始

大多数 AI 使用行为并不会以明显形式经过网络网关。本地 AI 运行环境、编辑器代码助手、MCP Server 和浏览器扩展都运行在终端设备上，而 GravityZone Agent已经部署在那里。因此，从终端开始发现能够获得最真实、完整的 AI 使用情况。

安全使用 AI，而不是默认阻止 AI

“一刀切”限制 AI 使用，会阻碍正常业务工作，用户也容易绕过安全控制。GravityZone只限制真正产生风险的 AI 使用行为。具有PHASR授权后，自适应安全加固能力可以针对每个用户和每个AI工具，缩小其风险访问范围，仅保留实际需要的权限。

拥抱 AI 并不意味着失去控制。
申请 GravityZone AI安全态势管理演示。

查看终端上已经运行哪些 AI。
联系您的 Bitdefender 团队，了解如何扩展 GravityZone 平台。

持续降低 AI 威胁暴露面，减轻响应负担与风险

Bitdefender 是全球网络安全领域的领导者，提供行业顶级的威胁防护、检测与响应解决方案。Bitdefender 为小型企业、中大型企业及个人用户提供具备卓越防护效能、高性能且简单易用的网络安全解决方案。秉持"成为全球最值得信赖的网络安全服务商"的愿景，Bitdefender 致力于守护全球企业与个人用户的数字安全，有效抵御网络攻击，助力优化数字化体验。

中国区联系方式
地址：深圳市龙华区环智中心D座1111室
电话：4000-132-568
邮箱：sales@bitdefender-cn.com

版权所有 © 2026 Bitdefender。 本文所提及的所有商标、商号和产品均归其各自所有者所有。