Bitdefender®

GravityZone XDR 白皮书

面向中大型企业CSO/CIO的战略级安全解决方案

全域自适应防御体系，让安全成为企业数字化转型的核心支撑

高管摘要 致CSO、CIO及企业决策层

2026年，中大型企业数字化转型进入深水区，云边端融合、IT/OT协同的复杂架构让攻击面呈指数级扩张，勒索软件、APT攻击、供应链威胁已成为企业核心业务的“致命隐患”。

同时，《数据安全法》《关键信息基础设施安全保护条例》等法规的深度落地，让合规从“纸面要求”升级为“实质考核”，2025年企业因安全措施失效导致的合规罚款平均金额同比增长120%。而传统安全体系的碎片化、高级威胁对抗乏力、价值难以量化三大痛点，让企业陷入“高投入、低效能”的安全困境。

Bitdefender GravityZone XDR作为面向中大型企业的**战略级一体化扩展检测与响应平台**，依托全球5亿用户威胁情报库与全栈传感器矩阵，以“全域采集-智能分析-战略运营”三层解耦架构为核心，构建覆盖全威胁生命周期的七大核心能力体系。平台深度适配中国市场合规要求，支持云端SaaS、本地私有化、纯离线三种部署模式，实现**安全与业务协同、成本与效能平衡、合规与防护兼顾**的核心目标。

从商业价值看，GravityZone XDR可实现APT攻击拦截率95%以上、勒索软件加密成功率降至0%、运营效率提升70%以上、合规落地成本降低80%，为不同行业企业带来可量化的安全ROI。

从技术落地看，平台轻量化部署无业务侵入，万台级资产部署周期≤1月，支持与企业现有安全体系无缝集成，保护现有投资。同时，Bitdefender在北京、上海、深圳构建了全链路本地化服务体系，7×24小时中文技术支持与应急响应，确保全球顶尖技术与中国本土需求的深度融合。

本白皮书从CSO/CIO双视角出发，系统阐述GravityZone XDR的技术架构、核心能力、行业落地价值与本地化保障，为中大型企业构建下一代安全防御体系提供**专业、可落地、可量化**的决策参考。

引言

数字化转型已成为中大型企业的核心发展战略，企业IT架构正加速形成“**云边端深度融合、公私网高度交织、IT/OT全面协同**”的复杂格局，业务边界的无限延伸让网络安全攻击面呈指数级扩张。与此同时，网络威胁正朝着**精准化、链条化、产业化**方向迭代，勒索软件的“数据泄露+加密”双重攻击、APT组织的“低慢长”渗透、供应链的源头性污染，正持续威胁企业核心业务连续性、数据资产安全与合规体系有效性。

作为企业安全战略的制定者（CSO）与技术架构的决策者（CIO），您正面临无法回避的三重核心困境：**安全体系碎片化**，多厂商工具各自为战形成数据孤岛，全域威胁联动能力缺失；**高级威胁对抗乏力**，传统特征检测难以应对零日攻击、无文件执行等新型手段，攻击链全环节可视性不足；**安全价值难以量化**，安全投入与业务价值脱节，风险改善与威胁防控成效无法用管理层可理解的指标呈现，预算申请与战略落地面临重重阻力。

安全防御的本质，是从“单点工具堆砌”向“**体系化战略落地**”的升级，是CSO与CIO的协同决策与价值共创。Bitdefender深耕网络安全领域25年，依托全球12大研发中心的技术积累与5亿用户的威胁情报沉淀，专为中大型企业打造GravityZone XDR战略级安全中枢。

平台以“**全栈可视、情报驱动、智能联动、价值量化**”为核心，打通“**采集-分析-运营-响应**”全流程，既承载CSO的安全战略落地，构建全链路防御体系、实现安全价值量化传递；又匹配CIO的技术架构规划，适配云边端混合IT环境、实现轻量化无侵入部署，最终帮助企业实现“安全为业务赋能，合规为发展护航”的核心目标。

一、中大型企业CSO/CIO的核心挑战与战略诉求

1.1 核心挑战：三重困境制约安全体系升级

1.1.1 架构层面：碎片化导致“协同失灵”

企业过往分散采购的终端、网络、云安全工具缺乏统一数据标准与联动机制，形成“数据孤岛”与“管理孤岛”；采集层仅聚焦终端维度，网络、身份、云、应用等关键环节存在严重可视性盲区；多控制台运维模式大幅增加管理成本，无法支撑跨域威胁的快速检测与处置，让企业在高级威胁面前陷入“被动救火”的困境。

1.1.2 防护层面：高级威胁突破“传统防线”

免杀技术、AI驱动攻击、无文件执行等新型手段持续规避传统特征检测；APT攻击以“低慢长”模式渗透企业内网，传统工具仅能识别孤立告警，无法还原完整攻击链；IT/OT融合场景下，老旧工控设备防护薄弱，成为高级威胁的重要“突破口”；供应链攻击从“直接打靶”转向“源头污染”，第三方软件、上游供应商成为企业安全的“隐形风险点”。

1.1.3 价值层面：投入与成效“难以量化”

企业安全投入多以“合规达标”为单一导向，缺乏对核心业务的支撑与价值赋能；风险改善、威胁防控的成效无法通过量化指标呈现，CSO难以向管理层传递安全战略的业务价值，预算申请与战略落地受阻；CIO面临“安全需求与IT架构兼容性”的平衡难题，部分安全工具资源占用过高，成为业务系统的“性能负担”。

1.2 战略诉求：四大核心目标指引平台选型

CSO与CIO的协同决策，要求安全平台必须同时满足**战略适配、技术可靠、运营高效、价值可量化**四大核心诉求，实现安全能力与企业业务发展的深度融合：

决策者	核心诉求	具体期望
CSO	战略落地与价值传递	构建全链路防御体系，实现高级威胁精准对抗；安全成效可量化，向管理层呈现 ROI；满足等保 2.0、数据安全法等合规要求。
CIO	架构兼容与高效运维	采用分层解耦架构，适配云边端混合 IT 环境；轻量化部署，无侵入业务系统；支持多模式部署，兼顾数据本地化与运维便捷性。
共同诉求	能力协同与弹性扩展	全维度采集无盲区，支持跨域威胁联动处置；能力模块可按需扩展，匹配企业业务发展节奏；保护现有安全投资，实现生态无缝集成。

二、中大型企业CSO/CIO的核心挑战与战略诉求

2.1 战略定位

GravityZone XDR 是**Bitdefender 为中大型企业量身打造的战略级安全中枢**，以 “全栈可视、情报驱动、智能联动、价值量化” 为核心，打通 “采集 - 分析 - 运营 - 响应” 全流程，实现从 “单点防护” 到 “体系化防御” 的升级。

平台既是 CSO 的 “安全战略指挥中心”，通过七大核心能力落地风险管控与威胁防御战略；也是 CIO 的 “安全技术底座”，通过三层解耦架构与全栈传感器矩阵，无缝融入企业现有 IT 架构，支撑安全能力的弹性扩展。

2.2 核心设计原则

GravityZone XDR 的设计全程围绕 CSO/CIO 的双重诉求，遵循六大不可动摇的核心原则：

1. **全栈采集，无死角可视**：突破单一终端采集局限，构建覆盖终端、网络、云、身份、应用的传感器矩阵，实现攻击链全环节信号无遗漏；
2. **分层解耦，高弹性扩展**：采用 “采集 - 分析 - 运营” 三层解耦架构，各层组件独立迭代、按需部署，适配企业业务扩张与 IT 架构升级；
3. **情报驱动，精准化防御**：依托全球 5 亿用户威胁情报，实现 “威胁出现即防御”，情报深度融合于检测、响应、治理全环节；
4. **轻量化部署，无业务侵入**：所有传感器与组件均采用轻量化设计，终端资源占用极低，网络与云传感器无旁路部署，不影响核心业务运行；

5. **多元部署，强合规适配**：支持云端、本地私有化、纯离线三种部署模式，全面满足中国市场 “数据本地化” “数据不出域” 的严苛合规要求；
6. **价值量化，强决策支撑**：内置价值量化引擎，将安全成效转化为管理层可理解的量化指标，为 CSO/CIO 的战略决策与预算申请提供数据支撑。

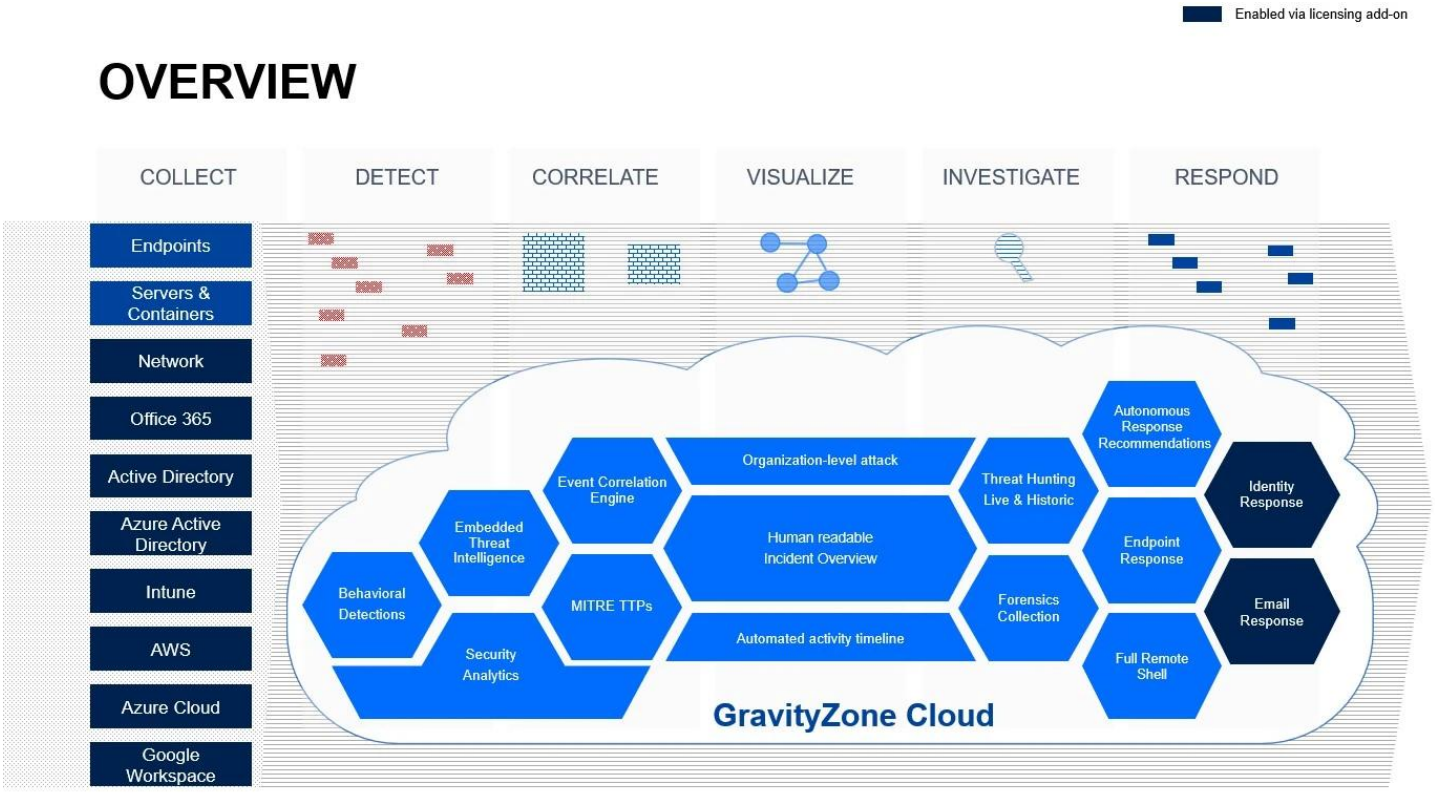
三、Bitdefender GravityZone XDR 三层技术架构设计

GravityZone XDR 采用 “全域采集层 - 分析引擎层 - 智能运营层” **三层解耦技术架构，核心解决 “采集不全面、分析不协同、运营不统一” 的行业痛点。该架构仅聚焦**技术实现逻辑、组件构成与部署特性 **，不涉及具体安全能力的功能细节，为七大核心安全能力的落地提供坚实技术支撑，完全匹配中大型企业云边端融合的混合 IT 架构需求。

3.1 架构设计核心逻辑

三层技术架构遵循 “全域多源传感器归一化采集、分布式引擎协同智能化分析、战略级控制台统一化运营” 的核心逻辑，通过 “解耦” 实现各层组件的独立扩展与迭代，通过 “聚合” 实现跨层数据的无缝流转与能力的协同联动。

架构的核心突破在于两大设计：一是**全栈传感器矩阵**，覆盖攻击链全环节，彻底消除可视性盲区；二是**中央关联引擎**，实现多源数据的跨域关联分析，还原完整攻击链。这一设计既满足 CIO 对 “架构兼容性、弹性扩展性” 的技术要求，又为 CSO 的 “全域威胁对抗、体系化风险治理” 战略提供底层支撑。



3.2 第一层：全域采集层 —— 全栈传感器矩阵，捕获攻击链全环节信号

作为架构的数据入口，全域采集层的核心目标是**实现企业全域 IT/OT 基础设施的无死角数据采集，覆盖终端、网络、云、身份、应用五大维度，同时保障采集过程的轻量化与业务无侵入性**，为上层分析引擎提供标准化、全维度的基础数据。

3.2.1 核心组件：Bitdefender 全栈传感器矩阵

依托 Bitdefender TechZone 定义的全维度检测传感器体系，采集层整合七大核心采集组件，构建 “无死角、全链路” 的信号采集网络：

传感器类型	核心部署形态	采集核心信号	应用场景
终端传感器	轻量级代理（Bitdefender Agent），部署于终端、服务器、容器、云工作负载	进程行为、文件操作、注册表交互、网络连接、漏洞信息、内存注入、无文件执行	终端全生命周期防护，覆盖 Windows、Linux、macOS、容器设备
网络传感器	镜像流量采集 / 探针模式，部署于核心交换机、DMZ 区、内网骨干节点	南北向 / 东西向流量、端口扫描、暴力破解、横向移动、数据外溢、恶意协议交互	网络层威胁检测，补齐终端采集的网络视野盲区
云传感器	API 原生集成，适配 AWS、Azure、GCP	云资源配置变更、身份访问异常、云函数异常执行、存储桶权限篡改、日志销毁	云原生环境防护，覆盖公有云、混合云、私有云场景
身份传感器	对接 AD、Azure AD、LDAP 等身份系统	特权账号滥用、异常登录、多地域同时登录、权限越权变更、账号生命周期异常	身份层风险防控，从攻击源头识别账号劫持与内部威胁
生产力应用传感器	API 对接，适配Office 365、Google Workspace等	钓鱼邮件、恶意附件、敏感信息外传、异常文件共享、协作平台恶意链接	应用层攻击防护，覆盖员工日常办公的高频攻击入口

3.2.2 核心技术特性

1. **全栈覆盖，无视野盲区**：五大维度传感器协同工作，实现从 “初始入侵（应用 / 身份）→横向移动（网络）→终端驻留（终端）→云环境渗透（云）” 的攻击链全环节信号采集；
2. **轻量化设计，零业务侵入**：终端传感器 CPU 占用率≤5%、内存占用≤600MB；网络传感器采用无旁路部署，不影响网络带宽；云 / 身份 / 应用传感器通过 API 集成，无需改造业务系统；

3. **边缘智能，分布式算力**：所有传感器均具备本地轻量化分析能力，可在边缘侧实现已知威胁的快速拦截与异常行为初步筛选，减少核心算力消耗与数据传输量；
4. **快速部署，低运维成本**：支持一键批量部署、域推送、云镜像、API 自动对接等多种方式，中大型企业万台级资产与多类型传感器的部署周期可缩短至 72 小时内；
5. **离线兼容，高可用性保障**：终端与网络传感器支持本地缓存与离线检测，断网状态下仍可完成基础威胁防护与数据采集，网络恢复后自动同步数据，满足纯离线部署场景需求。

3.3 第二层：分析引擎层 —— 分布式多引擎协同，实现智能化研判

作为架构的核心算力层，分析引擎层的核心目标是**对采集层所有传感器上报的标准化数据进行深度分析与智能研判，实现威胁精准识别、风险量化评估与响应指令生成**，是平台安全能力的 “算力核心” 。

3.3.1 核心组件：解耦式智能分析引擎矩阵

分析层采用 “核心引擎 + 专项引擎” 的解耦设计，确保各分析能力独立迭代、协同工作，核心组件包括：

1. 全球威胁情报引擎

作为分析层的 “数据大脑” ，实时同步 Bitdefender Labs 全球威胁情报库（每分钟更新数百个新型威胁，每日验证数十亿次威胁查询），为所有分析组件提供最新的威胁特征、IoC 指标、MITRE ATT&CK 战术技战法、APT 组织攻击策略与行业专属威胁情报。支持云端实时同步、本地私有化部署、纯离线情报包更新三种模式，满足不同合规需求。

2. 多维度检测引擎

融合四大子引擎，实现 “已知威胁精准拦截、未知威胁提前预警” ：

- 特征检测引擎：基于海量威胁特征库，快速拦截已知恶意软件；
- 行为检测引擎：建立资产与用户的正常行为基线，识别异常行为；
- HyperDetect 机器学习引擎：通过无监督学习，精准识别零日攻击、无文件攻击等未知威胁；
- 沙箱分析引擎：对可疑文件进行动态执行分析，还原恶意行为全貌。

3. 中央关联引擎

Bitdefender 核心技术壁垒，主动采集所有传感器的原始事件与告警，通过机器学习驱动的关联算法，识别事件间的时序关系与因果关联，将分散的孤立告警整合为统一的高阶事件，自动还原完整攻击链与攻击时间线，解决传统工具 “见树不见林” 的检测痛点。

4. 风险量化分析引擎

基于 “资产价值 + 风险严重程度 + 影响范围 + 处置难度” 四维模型，对资产漏洞、配置缺陷、用户行为异常进行量化评分，生成企业全域风险全景数据，为风险治理提供精准依据。

5. 自动化响应决策引擎

基于预设规则、威胁情报与分析结果，自动生成精细化处置指令，支持 “终端处置、网络封禁、身份冻结、云资源隔离” 等跨域联动处置，实现威胁的秒级响应，同时支持与上层运营层的人工决策联动。

3.3.2 部署模式适配

分析引擎层支持**云端 SaaS、本地私有化、纯离线**三种部署模式，CIO 可根据企业合规要求与 IT 架构规划灵活选择，核心组件实现 “按需下沉、全域协同”：

部署模式	核心部署架构	适用企业	核心优势
云端 SaaS 部署	所有分析引擎部署于 Bitdefender 全球云平台	中小企业、轻量化运维需求的中大型企业	快速上线、零本地算力投入、引擎与情报实时自动更新
本地私有化部署	全量分析引擎与情报节点落地企业内网	金融、能源、等需 “数据本地化” 的企业	数据全程本地流转、自主管控、适配行业专项监管
纯离线部署	分析引擎与离线情报包全量部署于企业内网，支持 U 盘更新	银行等高敏感金融机构等需 “数据不出域” 的企业	完全离线运行、无外部网络依赖、最高等级数据安全

3.4 第三层：智能运营层 —— 战略级指挥中心，实现统一化管控

作为架构的人机交互层，智能运营层的核心目标是**将分析引擎层的技术分析结果，转化为 CSO/CIO 可理解、可决策、可呈现的战略级信息**，实现企业安全运营的统一化、智能化与价值化。

3.4.1 核心组件

1. 云原生智能控制台

作为 CSO/CIO 的 “安全战略指挥中心”，整合资产管控、策略配置、威胁监控、风险治理、合规审计、价值量化等全功能模块，支持 PC 端、移动端多终端访问。核心亮点是**Incident Advisor 视图**，以可视化攻击链图谱呈现关联告警，让决策者 “一眼掌握威胁全貌”。

2. AI 安全助手组件

基于大语言模型的智能化运营插件，深度适配中文场景，实现 “报告自动生成、合规分析、指令解读、威胁溯源问答” 等功能，替代 90% 以上的人工运营工作，降低对专业安全人才的依赖。

3. 开放 API 网关

提供全面的 REST API 接口，支持与企业现有 SIEM、ITSM、日志管理系统、工单系统无缝集成，实现数据互通与能力联动，保护企业现有安全投资，构建专属安全生态。

4. 权限与审计组件

支持多租户管理、细粒度权限分配（按角色 / 业务线 / 区域）与操作日志全记录，适配中大型企业 “总部统管、分支自治” 的管理架构，满足GDPR、数据安全法的合规审计要求。

3.4.2 核心运营特性

1. **单控制台统一管理**：彻底消除 “多控制台疲劳”，实现企业全域传感器、资产、策略、事件、风险的一站式管控，大幅降低运维成本；
2. **可视化态势呈现**：通过企业级仪表盘、资产拓扑图、攻击链图谱、风险热力图等形式，直观展示安全态势，让决策者 “一眼掌握全局风险”；
3. **敏捷决策支撑**：整合 “自动化响应 + 人工决策”，支持 “一键处置、批量操作、跨域联动”，大幅提升应急响应效率，缩短 MTTR；
4. **全流程可追溯审计**：所有操作、事件、处置记录全程留痕，支持按时间、用户、资产、事件类型等维度精准追溯，满足合规审计的全流程要求。

四、Bitdefender GravityZone XDR 七大核心能力体系

基于三层技术架构的坚实支撑，GravityZone XDR 构建了覆盖 ** “预防 - 检测 - 响应 - 治理 - 运营 - 价值” **全链路的七大核心能力体系。该部分完全聚焦**CSO 的战略诉求与业务价值 **，不涉及技术架构的组件细节，各能力模块边界清晰、层层递进、无功能重叠，为中大型企业 CSO 落地安全战略提供可量化、可落地的核心支撑。

4.1 核心能力体系总览

七大核心能力围绕 CSO “**控风险、防威胁、提效率、降成本、显价值**” 的核心工作目标设计，形成闭环协同的安全能力矩阵，精准匹配中大型企业的安全战略需求：

能力维度	核心定位	核心量化价值
情报驱动防御能力	战略级防御底座，为全能力提供精准情报支撑	实现 “威胁出现即防御”，新型威胁识别时效缩短至分钟级，APT 攻击拦截率提升 99% 以上
攻击面主动收缩能力	前置风险管控，从源头降低威胁发生概率	安全事件减少 85% 以上，攻击面最高收缩 95%，核心资产高危漏洞修复率提升至 100%
高级威胁精准检测能力	全域威胁识别，破解高级威胁隐蔽性难题	实现 100% 攻击步骤检测率，零日攻击预警时效提前至 24 小时内，误报率降低至 1% 以下
威胁极速联动	应急处置核心，快速遏制威	平均响应时间（MTTR）缩短 50% 以上，勒索软件加密成功

能力维度	核心定位	核心量化价值
响应能力	胁扩散	率降低至 0.1% 以下
全域安全风险治理能力	体系化风险管控，实现风险可视可控可追溯	企业整体安全风险评分降低 40% 以上，漏洞修复周期缩短至 72 小时内
AI 智能安全运营能力	运营效率引擎，降低人工与合规成本	运营效率提升 70% 以上，合规落地成本降低 80%，安全团队人力投入减少 50%
安全价值量化呈现能力	战略价值支撑，向管理层传递安全投入价值	安全 ROI 精准量化，核心业务损失降低 90% 以上，为预算申请提供数据支撑

4.2 核心能力详解

4.2.1 情报驱动防御能力：战略级情报底座，实现威胁 “先见先知”

威胁情报是中大型企业抵御高级威胁的核心战略资产，GravityZone XDR 将全球威胁情报与企业防御体系深度融合，而非简单的特征叠加，为所有核心能力提供 “精准导航”。

1. **全域实时情报支撑**：依托 Bitdefender 全球 5 亿用户的威胁数据，实现分钟级威胁情报更新，确保企业防御体系与全球威胁趋势同步；
2. **行业定制化情报适配**：针对金融、制造、零售、政企等不同行业，推送专属威胁情报，包括行业攻击趋势、针对性防御策略、典型攻击案例，让防御更具针对性；
3. **多模式情报部署保障**：支持云端实时同步、本地私有化部署、纯离线情报更新，彻底解决中国市场 “数据不出域” 与 “情报实时性” 的双重诉求；
4. **全链路情报融合应用**：情报直接驱动检测规则更新、响应策略优化、风险治理重点识别、威胁狩猎方向制定，实现 “情报 - 防御 - 运营” 的全链路贯通，让每一项防御动作都有精准依据。

4.2.2 攻击面主动收缩能力：前置防御核心，从源头切断攻击路径

针对 CSO “降低整体安全风险” 的核心诉求，该能力聚焦 **“风险识别 - 分级 - 加固 - 收敛” ** 全流程，将安全防御前置至威胁发生之前，彻底改变传统 “被动救火” 的防御模式。

1. **全域无死角风险扫描**：依托全栈传感器矩阵，对企业终端、服务器、云资产、网络设备、身份系统进行持续自动化扫描，全面识别配置漏洞、应用脆弱性、高风险权限、异常用户行为等全维度风险；
2. **业务关联式风险分级**：基于 “风险严重程度 + 影响范围 + 业务核心度” 三维模型，对风险进行高、中、低三级分级，让安全团队优先处置核心业务（如交易系统、产线控制系统）相关的高等级风险；

3. **自动化终端加固落地**：针对中低等级常见风险，实现无人干预的自动化加固（如自动开启防火墙、修复配置缺陷、推送补丁提醒、禁用高风险应用），大幅提升风险修复效率；
4. **精细化攻击面收敛**：通过应用白名单、端口封禁、设备接入管控、权限最小化配置等手段，关闭无用攻击入口、限制高风险操作，实现攻击面的精细化收缩，从源头降低威胁入侵概率。

4.2.3 高级威胁精准检测能力：全域关联识别，破解 “见树不见林” 痛点

针对 APT 攻击、供应链攻击、勒索软件等 “攻击链长、隐蔽性强” 的高级威胁，该能力依托中央关联引擎，实现从 “单点检测” 到 “全域关联识别” 的升级，精准还原威胁全貌。

1. **全链路威胁检测**：整合终端、网络、云、身份、应用五大维度的检测信号，实现攻击链每一个环节的精准识别，避免单一维度检测的局限性；
2. **全网攻击关联分析**：将分散的孤立告警整合为统一的高阶事件，自动还原威胁的初始入侵点、横向移动路径、权限提升方式、数据窃取 / 加密行为，生成可视化攻击链报告；
3. **MITRE ATT&CK 战术匹配**：将检测到的威胁行为与 MITRE ATT&CK 框架深度匹配，结合全球情报，精准研判攻击者所属组织、攻击意图、惯用战术技战法，为反制策略提供依据；
4. **主动式威胁狩猎**：提供低门槛的可视化狩猎工具，支持基于 IoC 指标、MITRE ATT&CK 战术的自定义规则，让安全团队主动发现隐藏的、躲避自动化检测的高级威胁。

4.2.4 威胁极速联动响应能力：自动化 + 联动化，实现威胁 “秒级遏制”

针对 CSO “快速降低业务损失” 的应急诉求，该能力构建 “**智能分级 - 自动处置 - 一键操作 - 跨域联动**” 的全流程响应体系，最大限度缩短威胁处置时间，遏制威胁横向扩散。

1. **智能告警分级归并**：基于 AI 算法与威胁情报，对告警进行 “业务关联度 + 威胁严重程度” 双重分级，归并同源告警，过滤 90% 以上的无效告警，仅推送高价值核心告警；
2. **秒级自动化处置**：内置针对勒索软件、横向移动、权限提升、数据外溢等常见威胁的开箱即用规则，检测到威胁后自动执行进程阻断、文件删除、网络封禁、身份冻结等操作，无需人工干预；
3. **一键式全域应急操作**：通过单控制台实现跨分支机构、跨区域的一键隔离、远程查杀、系统恢复、云资源隔离等操作，无需现场介入，大幅提升应急处置效率；
4. **跨域设备联动封禁**：与企业现有防火墙、邮件网关、云安全网关无缝联动，自动同步恶意 IoC 指标，实现全域威胁封禁，阻止威胁在企业内部扩散。

4.2.5 全域安全风险治理能力：体系化管控，实现风险 “可视可控可追溯”

安全风险治理是 CSO 落地安全战略的核心环节，该能力构建 “**全景可视 - 分级管控 - 闭环修复**” 的体系化机制，让企业风险治理从 “零散处置” 升级为 “标准化管控” 。

1. **企业级风险全景可视**：通过统一风险仪表盘，按资产类型、业务线、分支机构、风险等级多维度展示风险分布，让 CSO 实时掌握企业全域安全风险态势；
2. **风险分级精准管控**：建立 “高等级风险专人负责、限时整改，中低等级风险自动化处置” 的管控机制，确保核心业务风险得到优先处置；
3. **漏洞修复全流程闭环**：自动生成漏洞处置工单，明确责任人、整改时限与步骤，支持工单派发、跟踪、验收、归档全流程管理，确保每一个漏洞都能闭环解决；
4. **安全态势量化评估**：基于风险等级、攻击面大小、漏洞修复率等核心指标，对企业安全态势进行量化评分，对比历史数据展示风险改善趋势，衡量风险治理成效。

4.2.6 AI 智能安全运营能力：降本提效，释放安全团队战略价值

针对 CSO “降低运营成本、减少人才依赖” 的诉求，该能力以 “单控制台统一管理 + AI 安全助手” 为核心，实现安全运营的自动化、标准化，让安全团队从繁琐工作中解放，聚焦战略级工作。

1. **单控制台全域统一管控**：整合所有安全能力于单一控制台，实现资产、策略、事件、风险、合规的一站式管理，彻底解决 “多控制台切换、数据不通” 的痛点；
2. **AI 安全助手自动化运营**：一键生成日常运营、风险分析、威胁事件、合规审计等多类型中文报告，支持 Word/Excel/PDF 一键导出，替代 90% 以上的人工报告制作工作；
3. **合规审计全流程自动化**：内置等保 2.0、数据安全法、GDPR、行业专项监管等全球主流合规模板，自动采集合规数据、识别不合规项、提供可执行的整改建议，实现合规审计的自动化闭环；
4. **开放生态无缝集成**：通过全面的 REST API 接口，与企业现有 SIEM、ITSM 等系统集成，实现数据互通与能力联动，保护企业现有安全投资，构建专属安全生态。

4.2.7 安全价值量化呈现能力：ROI 可视化，向管理层传递安全战略价值

向企业管理层 “量化呈现安全价值” 是 CSO 争取预算、落地战略的关键，该能力通过价值量化 dashboard 与定制化报表，将安全工作成效转化为管理层易理解的量化指标。

1. **安全 ROI 精准量化**：通过 “安全事件减少比例、核心业务损失降低金额、运营成本节约、合规成本降低” 等指标，精准计算安全投入的投资回报率，直观展示安全投入的实际价值；
2. **威胁防控成效可视化**：统计威胁事件的数量、类型、严重程度变化趋势，展示高级威胁检测率、处置成功率等核心指标，直观呈现威胁防控能力的提升；
3. **风险改善成效量化呈现**：展示攻击面收缩比例、高等级风险数量下降幅度、漏洞修复率提升趋势，量化呈现安全团队的风险治理工作成效；
4. **定制化战略价值报表**：根据管理层关注重点，定制化生成安全价值报告，将合规达标、风险降低、成本节约等核心价值转化为量化数据，为 CSO 的战略决策与预算申请提供支撑。

五、核心竞争优势

作为面向中大型企业的战略级安全平台，GravityZone XDR 凭借 “**分层解耦的技术架构 + 全栈传感器矩阵 + 边界清晰的核心能力**”，形成显著的差异化竞争优势，彻底解决传统安全方案 “能力重叠、体系碎片化、价值难量化” 的核心痛点：

竞争优势	CIO 技术价值	CSO 战略价值
全栈传感器矩阵，全域可视无盲区	覆盖终端、网络、云、身份、应用五大维度，无缝适配混合 IT 架构	实现攻击链全环节检测，破解高级威胁 “隐蔽性” 难题
架构与能力深度解耦，弹性扩展强	三层解耦架构，组件独立迭代，支持按需部署，保护现有投资	能力模块可随业务发展扩展，支撑安全战略长期迭代
全球情报全链路融合，防御更精准	情报驱动引擎迭代，无需人工频繁更新规则，降低运维成本	实现 “威胁出现即防御”，构建战略级防御壁垒
全部署模式适配，合规能力领先	支持云端、本地私有化、纯离线部署，满足中国市场所有合规要求	彻底解决 “数据本地化” “数据不出域” 的合规痛点
AI 驱动智能运营，降本提效显著	单控制台管理，AI 助手替代人工，降低对专业人才的依赖	运营效率提升 70% 以上，合规成本降低 80%
价值量化能力闭环，决策支撑强	量化数据支撑架构优化，实现安全与 IT 架构协同发展	安全 ROI 可视化，为预算申请与战略落地提供数据支撑
中国本地化服务完善，落地有保障	北京、上海、深圳本地团队，7×24 小时中文技术支持	专属行业解决方案，确保安全战略贴合中国市场实际

六、中大型企业典型行业落地场景与战略价值

GravityZone XDR 的 “三层技术架构 + 七大核心能力” 可根据不同行业的业务特点与 CSO/CIO 核心诉求，实现灵活适配与组合应用，打造定制化的落地解决方案，彰显战略级安全价值。

6.1 金融行业：APT 防护 + 纯离线合规，守护核心数据安全

行业核心诉求

- CSO：精准对抗 APT 攻击、勒索软件，保护核心交易数据与客户信息；满足 “数据不出域” 的严苛合规要求。
- CIO：本地/纯离线部署，无外部网络依赖；轻量化传感器，不影响交易系统性能。

架构与能力适配

- **技术架构**：本地/纯离线部署模式，全域采集层传感器支持离线工作，分析引擎层全量组件与离线情报包落地内网，智能运营层实现本地统一管控。
- **核心能力**：重点启用情报驱动防御（本地情报节点）、高级威胁精准检测、威胁极速联动响应、AI 智能安全运营。

战略价值

- 实现 APT 攻击、勒索软件的 100% 检测与全链路溯源，核心交易数据零泄露；
- 合规落地成本降低 80% 以上，彻底满足金融行业专项监管要求；
- 交易系统性能无影响，保障业务连续性。

6.2 制造行业：勒索软件防御 + IT/OT 融合防护，保障产线稳定

行业核心诉求

- CSO：防御勒索软件攻击，避免产线停工；实现跨区域工厂统一风险治理。
- CIO：传感器适配 ICS/OT 设备，轻量化无侵入；本地私有化部署，保障生产数据安全。

架构与能力适配

- **技术架构**：本地私有化部署，全域采集层终端传感器适配 ICS 设备低资源需求，网络传感器覆盖 IT/OT 融合网络，分析引擎层实现 IT/OT 数据独立分析与联动。
- **核心能力**：重点启用攻击面主动收缩、高级威胁精准检测（勒索软件专项检测）、威胁极速联动响应、全域安全风险治理。

战略价值

- 从源头降低勒索软件攻击风险，产线停工风险降低至 0；
- 安全事件数量减少 85% 以上，实现跨区域工厂统一安全管控；

- IT/OT 融合场景无防护盲区，保障智能制造转型。

6.3 集团型企业：跨区域管控 + 体系化运营，提升整体安全韧性

行业核心诉求

- CSO：实现跨区域分支机构统一安全战略落地；量化呈现全集团安全价值。
- CIO：云端 + 本地混合部署，兼顾统一管控与本地响应；开放 API，与现有 SIEM/ITSM 集成。

架构与能力适配

- **技术架构**：云端 + 本地混合部署，总部部署核心运营控制台，分支机构部署采集层传感器与边缘分析节点，实现 “全域统一管控 + 本地快速响应” 。
- **核心能力**：重点启用 AI 智能安全运营（单控制台统一管理）、全域安全风险治理（企业级风险全景）、高级威胁精准检测、安全价值量化呈现（集团定制报表）。

战略价值

- 实现跨区域资产的统一管控与策略标准化，消除防护盲区；
- SOC 团队工作效率提升 80% 以上，运营成本降低 50%；
- 集团级安全价值量化报表，为 CSO/CIO 的战略决策提供数据支撑。

七、Bitdefender 品牌实力与中国本地化支撑

Bitdefender 成立于 2001 年，是全球领先的网络安全企业，二十余年深耕威胁防御技术研发与应用，为全球 170 多个国家和地区的数百万消费者、企业与政府机构提供安全防护解决方案，是**全球 5 亿用户的网络安全守护者**。其品牌实力与本地化服务能力，为 GravityZone XDR 在中大型企业的落地提供了坚实保障。

7.1 全球顶尖的技术研发实力

1. **威胁情报能力行业领先**：Bitdefender Labs 在全球拥有 12 个研发中心，每分钟发现数百个新型威胁，每日验证数十亿次威胁查询，构建的全球威胁情报库覆盖已知与未知威胁；
2. **权威测评屡获殊荣**：检测引擎在 AV-Test、AV-Comparatives 等国际权威测评中连续斩获 “最佳保护” 大奖，2024 年 MITRE Engenuity ATT&CK 评估中实现 100% 攻击步骤检测率，入选 2025 Gartner 端点安全魔力象限唯一 “远见者”；
3. **核心技术壁垒深厚**：在机器学习、全网攻击关联分析、勒索软件缓解、无文件攻击检测等领域开创多项突破性技术，核心技术被全球 200 余家知名科技品牌授权使用。

7.2 完善的中国本地化服务体系

为深度适配中国中大型企业的需求，Bitdefender 在中国构建了 “研发 - 销售 - 服务” 全链路本地化体系：

1. **本地化团队布局**：在北京、上海、深圳设立三大核心机构，拥有专业的中文售前咨询、技术支持、应急响应与行业解决方案团队；
2. **7×24 小时本地化服务**：提供 7×24 小时中文技术支持热线（4000-132-568）、邮件支持与现场服务，确保问题快速响应与解决；
3. **中国市场合规适配**：满足等保 2.0、数据安全法、个人信息保护法等中国合规要求，确保产品完全符合中国监管规定；
4. **行业专属解决方案**：针对金融、制造、零售、医药、能源等重点行业，组建专属解决方案团队，结合行业特点打造可落地的安全战略方案。

八、总结

数字化转型背景下，中大型企业的安全防御已从 “单点工具堆砌” 升级为 “体系化战略落地”，CSO 与 CIO 的协同决策，要求安全平台同时具备**技术可靠性、战略适配性、运营高效性与价值可量化性。**

Bitdefender GravityZone XDR 凭借 **“全域采集 - 分析引擎 - 智能运营” 三层解耦的技术架构 **，构建了以全栈传感器矩阵为核心的技术底座，实现了企业全域 IT/OT 基础设施的无死角采集、多引擎协同的智能化分析、战略级统一化的运营管控；基于该架构，进一步打造了**边界清晰、闭环协同的七大核心能力体系**，覆盖情报驱动、攻击面收缩、高级威胁检测、联动响应、风险治理、智能运营、价值量化全链路。

从 CSO 视角，GravityZone XDR 能够承载安全战略落地，构建 “预防为先、全域防护” 的安全体系，通过价值量化能力向管理层清晰传递安全投入的 ROI；从 CIO 视角，平台采用分层解耦设计，适配云边端混合 IT 架构，支持多模式部署，兼顾合规要求与运维便捷性，保护现有安全投资。

凭借独有的技术优势、清晰的能力定位与完善的本地化服务，Bitdefender GravityZone XDR 已成为中大型企业 CSO/CIO 制定安全战略、落地安全体系、提升企业安全韧性的首选战略级安全平台。

Bitdefender 将以全球顶尖的技术实力、深厚的威胁研究积累与完善的本地化服务能力，成为中大型企业的**战略安全合作伙伴**，助力企业在数字化转型浪潮中筑牢网络安全防线，实现安全与业务的协同发展。

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。

2025 端点安全魔力象限 “远见者”

AV-Test 连续5年 “年度最佳保护”

Gartner 2026 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