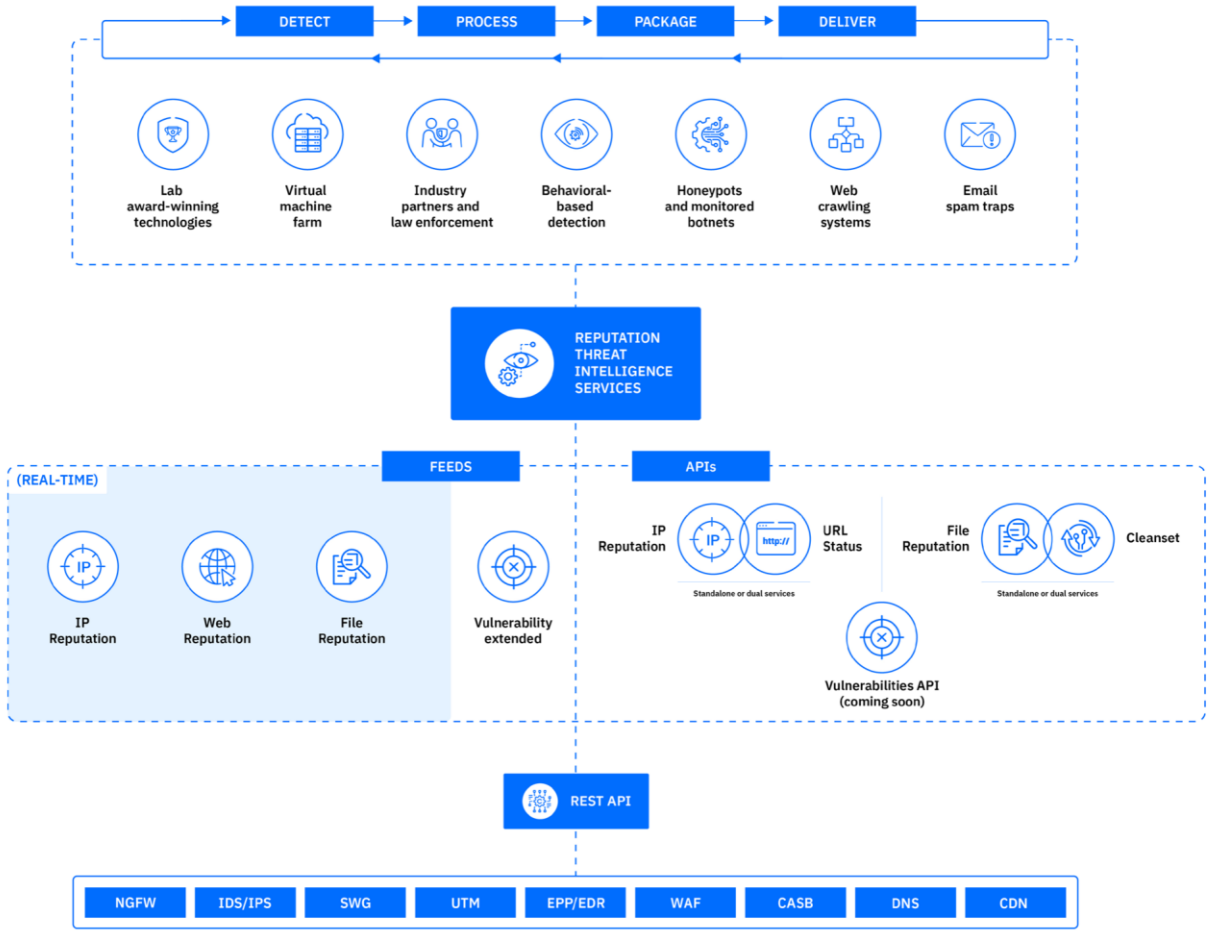
Bitdefender

GravityZone TI 信誉威胁情报

引言：实时信誉情报的新价值

随着全球化的网络攻击快速演变，恶意软件、钓鱼、欺诈、垃圾邮件与潜在有害应用（PUA）传播速度越来越快，攻击方式也日益多样与复杂。传统的安全防护手段（如终端、网络、服务器、移动与云端的防护）在面对未知与隐蔽威胁时往往力不从心，导致企业面临极高的安全与运营风险。

为了应对这一挑战，企业需要具备“超视距”能力，能够实时接收来自全球领先安全厂商的验证过的威胁情报。Bitdefender 信誉威胁情报（Reputation Threat Intelligence）正是为此而生，帮助企业安全体系快速接入最新的恶意域名、IP、URL、文件哈希信誉和漏洞数据，提升检测与阻断能力。



产品主要优势

→ 全球化威胁覆盖

- 数据来源覆盖：终端遥测、蜜罐系统、垃圾邮件陷阱、沙箱分析、深网监控、受控僵尸网络、合作厂商与执法机构
- 每日处理 5000 亿+ 威胁事件，实时提炼高价值 IoC

→ 实时与高性能

- IoC 检测后 5 分钟内即可进入信誉数据库
- API/Feeds 支持毫秒级查询响应，满足高并发场景

→ 高精度与低误报

- 自动化与人工双重校验
- 每条 IoC 附带置信度、严重度、首次发现时间、TTL、类别等上下文信息，避免“盲目阻断”

→ 快速无缝集成

- 支持 JSON、STIX 2.0、MISP、JSONL 等标准格式
- 兼容 SIEM、SOAR、EDR/XDR/EPP、防火墙、DNS/WAF、零信任、HIDS、网络威胁检测与响应、CASB 等平台
- 分钟级上线，无需额外开发

→ 可视化与分析支持

- IntelliZone 门户提供仪表盘、趋势分析与 IoC 检索
- 支持威胁溯源、MITRE TTP 映射与攻击链可视化

用户使用场景

1. SOC 威胁检测与响应

- 场景：SOC 团队每日处理海量告警，缺乏高置信度情报。
- 应用：将 Bitdefender RTI Feeds 接入 SIEM/SOAR，自动校验告警涉及的域名/IP/文件哈希信誉度。
- 价值：告警降噪 60%+，缩短事件响应时间，减少分析师疲劳。

2. 集成到业务系统，保障业务安全

- 大型企业（金融、电商、互联网、能源等行业）面临海量网络连接请求与文件交互场景，如邮件附件、文件下载、内部共享。攻击者常通过恶意文件（木马、勒索软件、后门）配合钓鱼链接或恶意域名，绕过单点防护，渗透到核心业务系统。企业需要在现有安全架构中，对 **域名/IP/URL** 和 **文件哈希** 进行全方位信誉校验。
- 应用：
    - **IP/URL 信誉情报**
        - 集成到 邮件安全网关，拦截钓鱼邮件和恶意附件中的恶意链接
        - 集成到 企业 DNS 服务器，阻止用户访问恶意域名
        - 集成到 防火墙/UTM/WAF，实时拦截高风险通信
        - 集成到 HIDS（主机入侵检测）/NDS（网络检测系统），用于告警验证与溯源
    - **文件信誉情报**
        - 在 邮件网关与安全邮件系统中，校验附件文件哈希，阻止勒索软件和木马型恶意文件进入企业网络
        - 在 EDR/XDR 平台中，通过文件哈希信誉查询，快速识别零日恶意样本，减少沙箱分析压力
        - 在 文件共享与协作平台（如网盘、文档系统）中集成 File Reputation API，防止恶意文件在企业内部传播
        - 在 SOC 与 SOAR 系统中，利用文件信誉情报对告警文件进行自动化分类，优先阻断高危恶意文件
- 价值：
    - 全链路覆盖：从网络流量到文件流转，实现对恶意链接与恶意文件的双重拦截
    - 降低入侵风险：阻止钓鱼、勒索软件、木马在初期渗透阶段得手
    - 提升响应效率：SOC 能快速基于信誉数据对文件与连接进行处置，减少人工分析负担
    - 保障核心业务：防止恶意文件进入交易、结算、内部办公系统，保障交易安全和用户体验

3. ISP / CDN / 云服务商的网络安全增强

- 场景：运营商与 CDN 服务商需对客户流量做恶意阻断。
- 应用：利用 RTI 提供的实时黑名单，将恶意域名/IP 自动推送至 DNS 层与 CDN 边缘节点。
- 价值：快速阻断恶意流量传播，提升网络整体安全性。

4. 漏洞与补丁管理优先级排序

- 场景：企业 IT 面对数百条 CVE 难以决定修复顺序。
- 应用：通过 Vulnerabilities Feed/API，获取漏洞的攻击活跃度与利用代码信息。
- 价值：基于实际攻击情况进行补丁优先级排序，提高安全资源利用效率。

5. 安全产品厂商与 OEM 集成

- 场景：安全厂商需增强产品的检测能力。
- 应用：将 Bitdefender RTI 作为内嵌信誉引擎，增强防火墙、EDR、邮件安全网关的检测效果。
- 价值：快速提升产品竞争力，缩短研发周期，降低自建情报平台的成本。

技术部署与集成

模块	内容
数据交付	Feeds（实时流式数据）、APIs（云端信誉查询）
格式支持	JSON、JSONL、STIX 2.0、MISP
兼容性	已验证集成：Splunk、QRadar、ThreatConnect、Anomali、TIP 平台
可视化	IntelliZone 门户，支持搜索、溯源、趋势分析
性能指标	IoC 延迟 < 5 分钟；API 毫秒级响应；每日新增数十万 IoC
支持	提供免费试用与技术支持，分钟级部署

免费试用

产品介绍：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