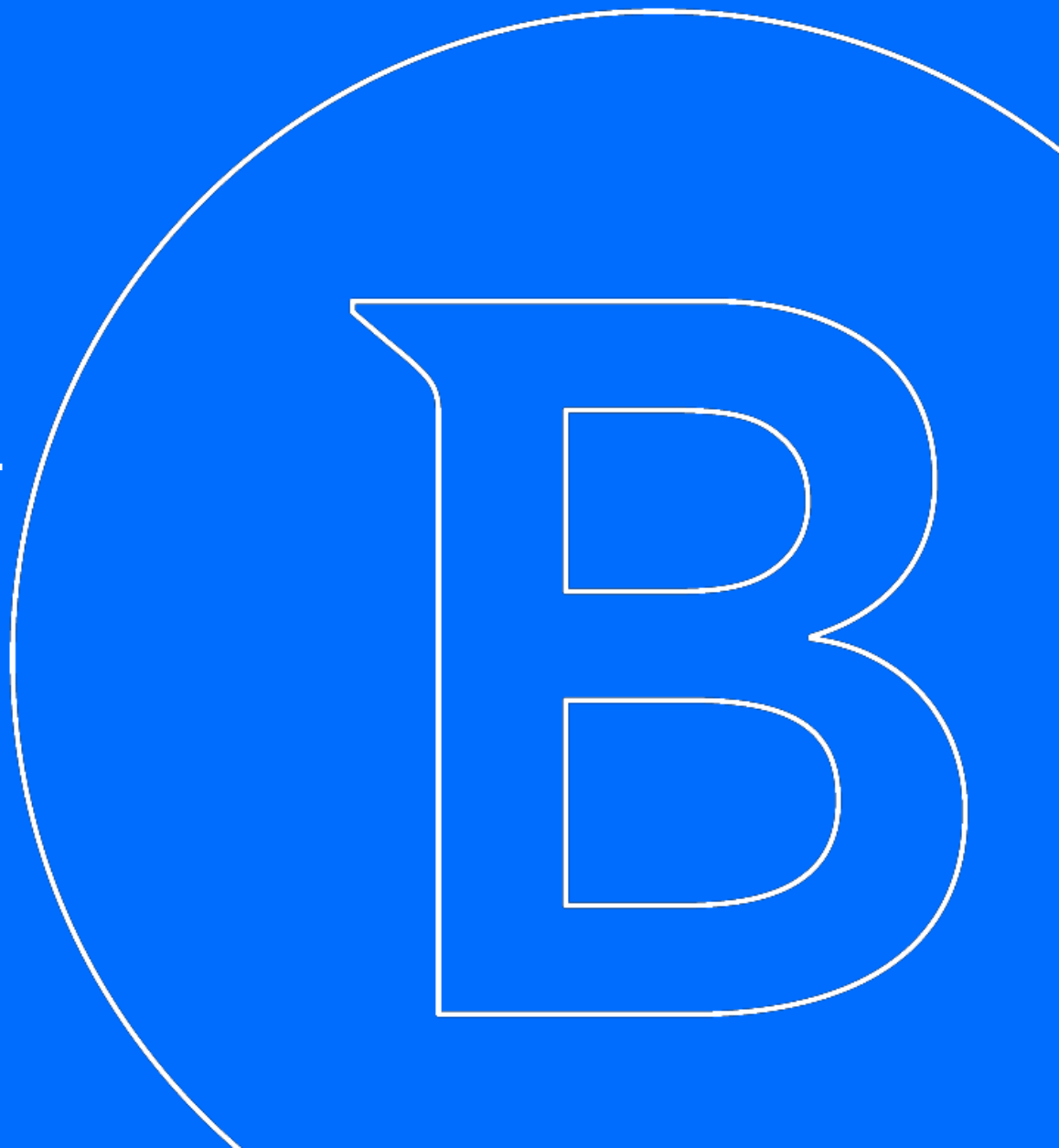
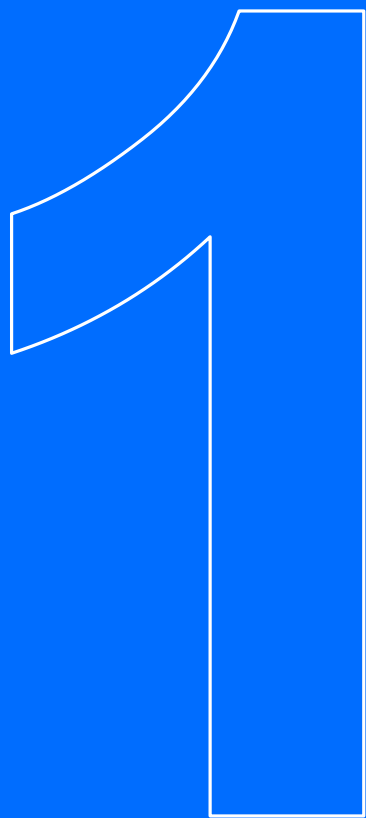


全球网络安全领导者

**Bitdefender**<sup>®</sup>

Bitdefender助力企业  
筑牢信息安全防线





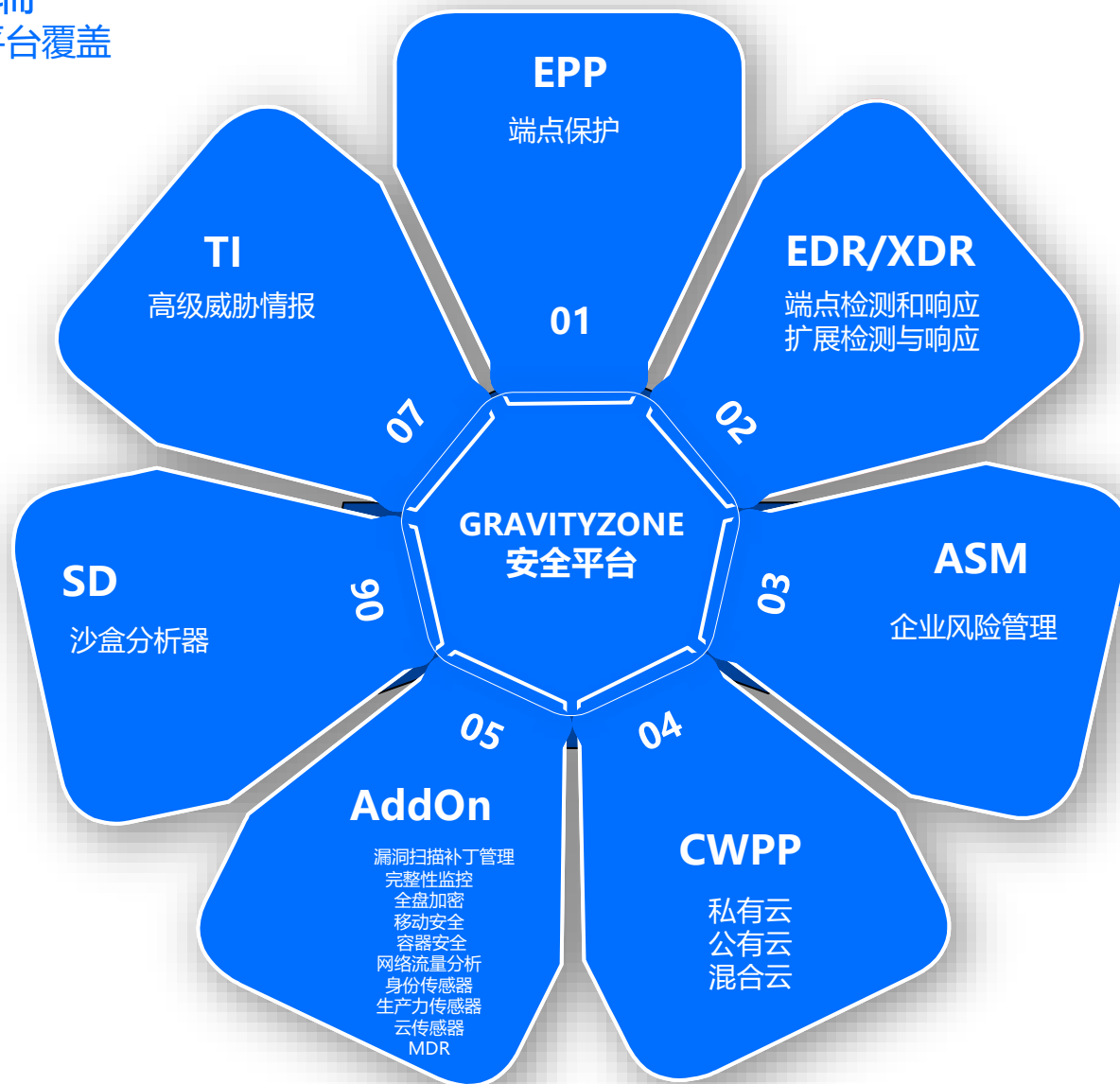
解决方案

# Bitdefender®

一个控制台 一个客户端

Windows、Linux、macOS全平台覆盖

x86、Arm CPU 全平台覆盖





- 修复操作系统、第三方应用程序漏洞
- 主动减少攻击面，预防高级攻击
- 支持自动化、手动修复
- 全平台覆盖：windows, Linux, macOS
- 重要的事情说3遍：打补丁，打补丁，打补丁！

Bitdefender GravityZone

cloud.gravityzone.bitdefender.com/#

补丁清单

| 补丁名称  | KB号      | CVE   | 公告 ID    | 补丁严重度 | 操作系统类型  | 类别  | 受影响的产品 | 可卸载 |
|---|----------|-------|----------|-------|---------|-----|--------|-----|
| outlook2007-kb950113-fullfile-x86-glb.exe   | Q950113  | 2 CVE | MS08-026 | 关键    | Windows | 安全  | 1 产品   | 否   |
| Windows6.1-2008-R2-SP1-KB2509553-x64.msu    | Q2509553 | 1 CVE | MS11-030 | 关键    | Windows | 安全  | 11 产品  | 是   |
| Office2007-kb2539530-fullfile-x86-glb.exe   | Q2539530 | 0 CVE | MSWU-524 | 关键    | Windows | 非安全 | 2 产品   | 是   |
| Windows6.1-Windows7-SP1-KB2619339-x64.msu   | Q2619339 | 1 CVE | MS11-092 | 关键    | Windows | 安全  | 5 产品   | 是   |
| Windows6.1-2008-R2-SP1-KB2656356-x64.msu    | Q2656356 | 4 CVE | MS11-100 | 关键    | Windows | 安全  | 11 产品  | 是   |
| Windows6.1-Windows7-SP1-KB2654428-x64.msu   | Q2654428 | 1 CVE | MS12-013 | 关键    | Windows | 安全  | 4 产品   | 是   |
| Windows6.1-2008-R2-SP1-KB2621440-x64.msu    | Q2621440 | 1 CVE | MS12-020 | 关键    | Windows | 安全  | 11 产品  | 是   |
| Windows6.1-Windows7-SP1-KB2653956-x64.msu   | Q2653956 | 1 CVE | MS12-024 | 关键    | Windows | 安全  | 5 产品   | 是   |
| Windows6.1-2008-R2-SP1-KB2604115-x64.msu    | Q2604115 | 2 CVE | MS12-035 | 关键    | Windows | 安全  | 11 产品  | 是   |
| Windows6.1-Windows7-SP1-KB2685939-x64.msu   | Q2685939 | 1 CVE | MS12-036 | 关键    | Windows | 安全  | 5 产品   | 是   |
| mscomctl2007-kb2598041-fullfile-x86-glb.exe | Q2598041 | 1 CVE | MS12-027 | 关键    | Windows | 安全  | 35 产品  | 是   |
| Windows6.1-Windows7-SP1-KB2727528-x64.msu   | Q2727528 | 2 CVE | MS12-072 | 关键    | Windows | 安全  | 4 产品   | 是   |
| Windows6.1-Windows7-SP1-KB2892074-x64.msu   | Q2892074 | 1 CVE | MS13-099 | 关键    | Windows | 安全  | 5 产品   | 是   |
| Windows6.1-Windows7-SP1-KB2893294-x64.msu   | Q2893294 | 1 CVE | MS13-098 | 关键    | Windows | 安全  | 5 产品   | 是   |
| Windows6.1-Windows7-SP1-KB2929733-x64.msu   | Q2929733 | 0 CVE | MSWU-508 | 关键    | Windows | 非安全 | 5 产品   | 是   |
| Windows6.1-Windows7-SP1-KB2978742-x64.msu   | Q2978742 | 1 CVE | MS14-043 | 关键    | Windows | 安全  | 5 产品   | 是   |
| Windows6.1-2008-R2-SP1-KB2972100-x64.msu    | Q2972100 | 1 CVE | MS14-057 | 关键    | Windows | 安全  | 11 产品  | 是   |
| Windows6.1-Windows7-SP1-KB3012176-x64.msu   | Q3012176 | 1 CVE | MS14-084 | 关键    | Windows | 安全  | 5 产品   | 是   |
| Windows6.1-Windows7-SP1-KB3067904-x64.msu   | Q3067904 | 1 CVE | MS15-067 | 关键    | Windows | 安全  | 3 产品   | 是   |



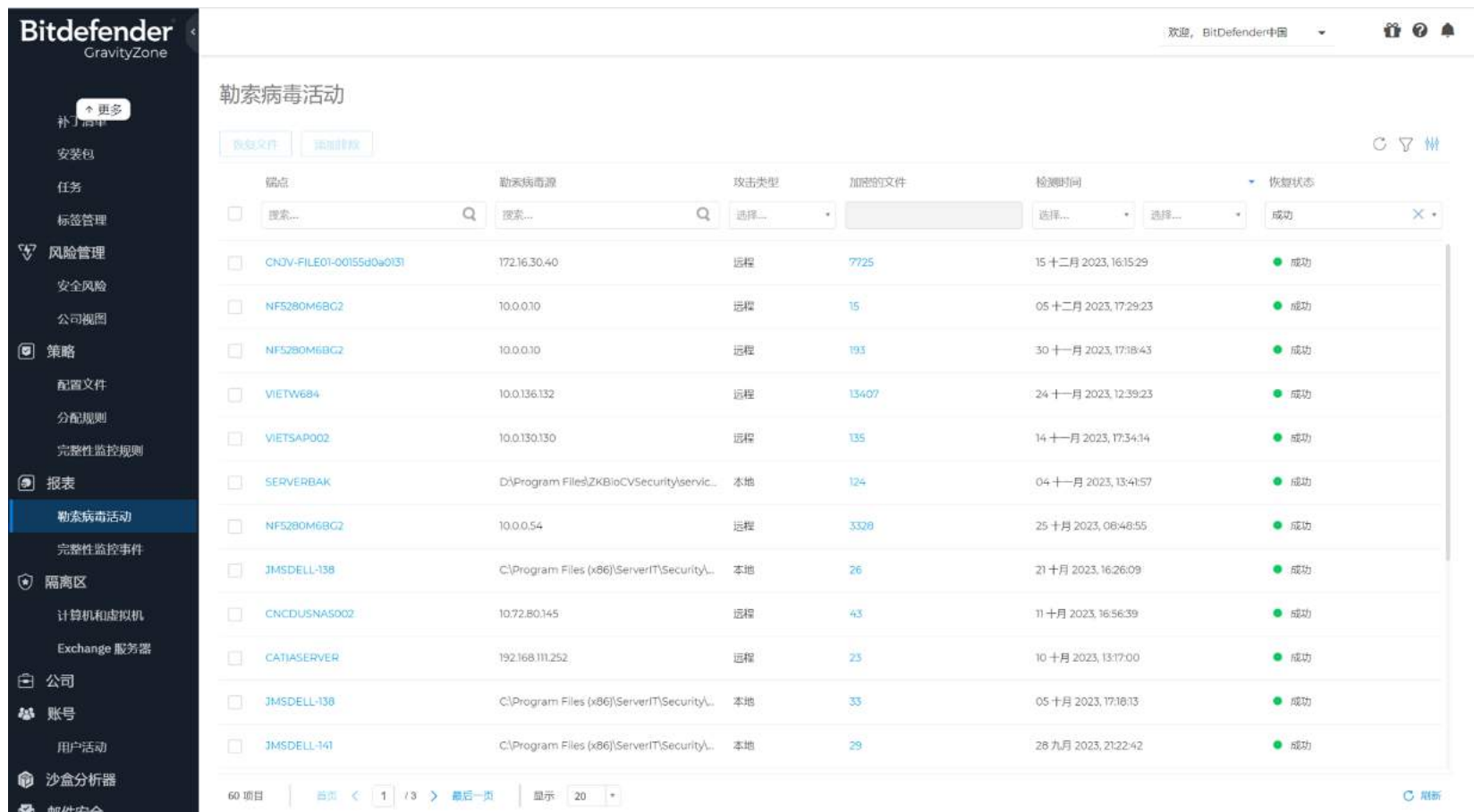
## 网络攻击防护 自动阻止横向移动 Windows, Linux, macOS全平台支持

- RDP爆破, SSH爆破, SMB攻击, C2流量, TOR流量, 凭据泄露.....
- 远程代码执行, PSEXEC, WMI调用, 远程过程调用 (RPC)、远程计划任务和基于分布式组件对象模型 (DCOM) 的执行.....
- 网络漏洞利用, 如log4j, ZeroLogon、PrintNightmare , 反弹shell.....等等

| 端点名称           | Endpoint IP | 端点 FQDN        | 用户           | 出现次数 | Last Blocked          | 模块     | 事件类型   | 详情                      | Attack Technique | Attacker's IP | Targeted IP |
|----------------|-------------|----------------|--------------|------|-----------------------|--------|--------|-------------------------|------------------|---------------|-------------|
| NHSV-STD-ES231 | 10.10.39.75 | nhsv-std-es231 | 80205911@HS4 |      | 04 十二月 2023, 04:53:49 | 网络攻击防护 | 网络攻击事件 | Exploit.DRSUAPI.D CSync | lateralMovement  | 10.10.39.75   | 10.10.8.13  |
| NHSV-STD-ES231 | 10.10.39.75 | nhsv-std-es231 | 80205911@HS4 |      | 04 十二月 2023, 05:42:36 | 网络攻击防护 | 网络攻击事件 | Exploit.DRSUAPI.D CSync | lateralMovement  | 10.10.39.75   | 10.10.8.14  |

## 行业排名第一的勒索病毒防护技术 勒索缓解 自动回滚被勒索病毒加密的文件

- 基于机器学习技术，分析异常行为
- 非诱饵式
- 自动阻止勒索病毒加密本地和远程服务器的数据
- 自动回滚被加密的文件
- 防篡改备份
- 实时告警和邮件通知



The screenshot displays the Bitdefender GravityZone interface. On the left is a dark sidebar with navigation options: 补丁管理, 安装包, 任务, 标签管理, 风险管理, 安全风险, 公司视图, 策略, 配置文件, 分配规则, 完整性监控规则, 报表, 勒索病毒活动 (highlighted), 完整性监控事件, 隔离区, 计算机和虚拟机, Exchange 服务器, 公司, 账号, 用户活动, 沙盒分析器, 邮件安全. The main content area is titled '勒索病毒活动' (Ransomware Activity) and contains a table of logs. The table has columns for 端点 (Endpoint), 勒索病毒源 (Ransomware Source), 攻击类型 (Attack Type), 加密的文件 (Encrypted Files), 检测时间 (Detection Time), and 恢复状态 (Recovery Status). The table lists 13 entries, all with a '成功' (Success) status. At the bottom, there is a pagination bar showing '60 项目' (60 items), page '1' of '3', and a '显示 20' (Show 20) dropdown.

| 端点                       | 勒索病毒源  | 攻击类型 | 加密的文件 | 检测时间                  | 恢复状态 |
|--------------------------|--|------|-------|-----------------------|------|
| CNJV-FILE01-00155d0a0131 | 172.16.30.40                                 | 远程   | 7725  | 15 十二月 2023, 16:15:29 | 成功   |
| NF5280M6BG2              | 10.0.0.10                                    | 远程   | 15    | 05 十二月 2023, 17:29:23 | 成功   |
| NF5280M6BG2              | 10.0.0.10                                    | 远程   | 193   | 30 十一月 2023, 17:18:43 | 成功   |
| VIETW684                 | 10.0.136.132                                 | 远程   | 13407 | 24 十一月 2023, 12:39:23 | 成功   |
| VIETSAPO02               | 10.0.130.130                                 | 远程   | 135   | 14 十一月 2023, 17:34:14 | 成功   |
| SERVERBAK                | D:\Program Files\ZKBioCVSecurity\servic...   | 本地   | 124   | 04 十一月 2023, 13:41:57 | 成功   |
| NF5280M6BG2              | 10.0.0.54                                    | 远程   | 3328  | 25 十月 2023, 08:48:55  | 成功   |
| JMSDELL-138              | C:\Program Files (x86)\ServerIT\Security\... | 本地   | 26    | 21 十月 2023, 16:26:09  | 成功   |
| CNCDUSNA5002             | 10.72.80.145                                 | 远程   | 43    | 11 十月 2023, 16:56:39  | 成功   |
| CATIASERVER              | 192.168.111.252                              | 远程   | 23    | 10 十月 2023, 13:17:00  | 成功   |
| JMSDELL-130              | C:\Program Files (x86)\ServerIT\Security\... | 本地   | 33    | 05 十月 2023, 17:18:13  | 成功   |
| JMSDELL-141              | C:\Program Files (x86)\ServerIT\Security\... | 本地   | 29    | 28 九月 2023, 21:22:42  | 成功   |

# Bitdefender®

## 沙盒分析器 对抗免杀、逃逸型恶意软件

- 攻击者不断改进代码、技术以逃避检测
- 沙盒技术集成在客户端中，可自动化提交、分析、判决和处置
- 全网联动判决，自动阻止
- 短短几分钟出具完整的分析报告，无需手动抓样本
- 支持在控制台手动提交分析文件和网址
- 集成在EDR和XDR事件分析流程中，便于安全分析师分析不确定的可疑文件






Bitdefender GravityZone | cvmw.exe | Threat Analysis: Trojan (sality) | Sandbox Analyzer

Summary | Detections and Alerts | Description | Mitre Techniques | System Changes | Files | Network Overview | Network Details | Timeline | Graph | Chronology | IoC | Screenshots


### SUMMARY

**Threat Analysis:**

 **cvmw.exe**

**Threat Actor:** Turla

**Also known as:** Iron Hunter, Sig23, Waterbug, Venomous Bear, Group 88, PACIFIERAPT, Krypton, CTG-8875, Pacifier, Sig1, Sig2, Sig4, Sig13, Sig15, Sig43, Secret Blizzard, Pensive Urso

**Target countries:** 

**Target sectors:** Defense, Education, Energy, Foreign Affairs, Government, High-Tech, Media, Military, NGOs, Pharmaceutical, Research, Retail

**Confidence:** medium

**Threat: Trojan**  
**Family: sality**  
**Severity: 99**

Description: Since 2004, Turla, a Russia-based threat group, has infected victims in over 45 countries across a variety of sectors, including government, embassies, military, education, science, and pharmaceutical firms. Turla is notorious for spear-phishing and watering hole attacks, mostly targeting Windows computers but also macOS and Linux machines. The group, primarily interested in information theft and espionage, has remained active through the years.

The sample writes additional files on the system, which may be used in various ways, including ensuring persistence. The new files can be executables that continue the sample's actions or store/confirmation files that hold viable information for the sample. Not only that, the sample creates or uses an inter-process communication

[Copy MD5](#) | [Copy SHA256](#) | [View in VirusTotal](#)

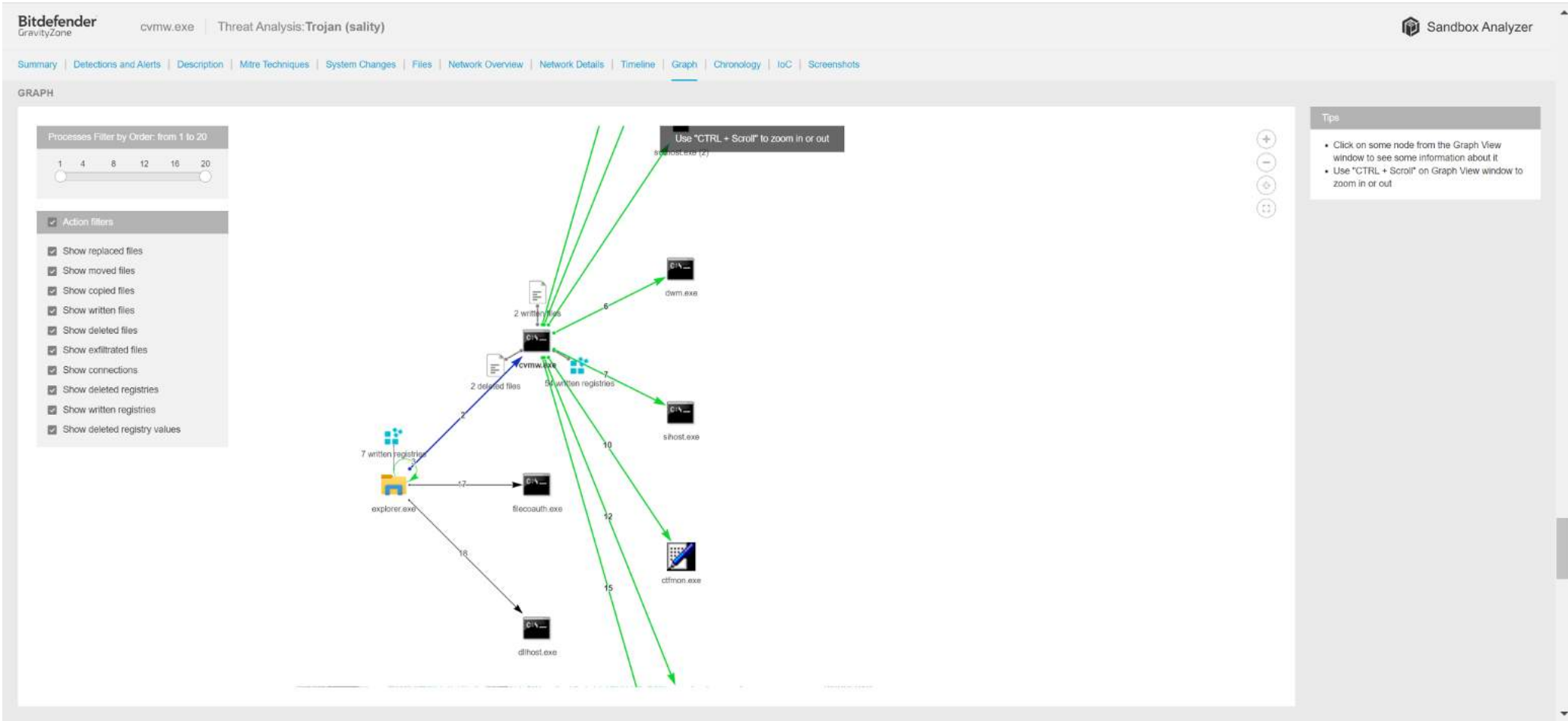
### FILE INFO

Document summary

| PE Info       |             |
|---------------|-------------|
| Section count | 1           |
| Machine       | i386        |
| Subsystem     | WINDOWS_GUI |
| Import count  | 3           |

### SUBMISSION DETAILS

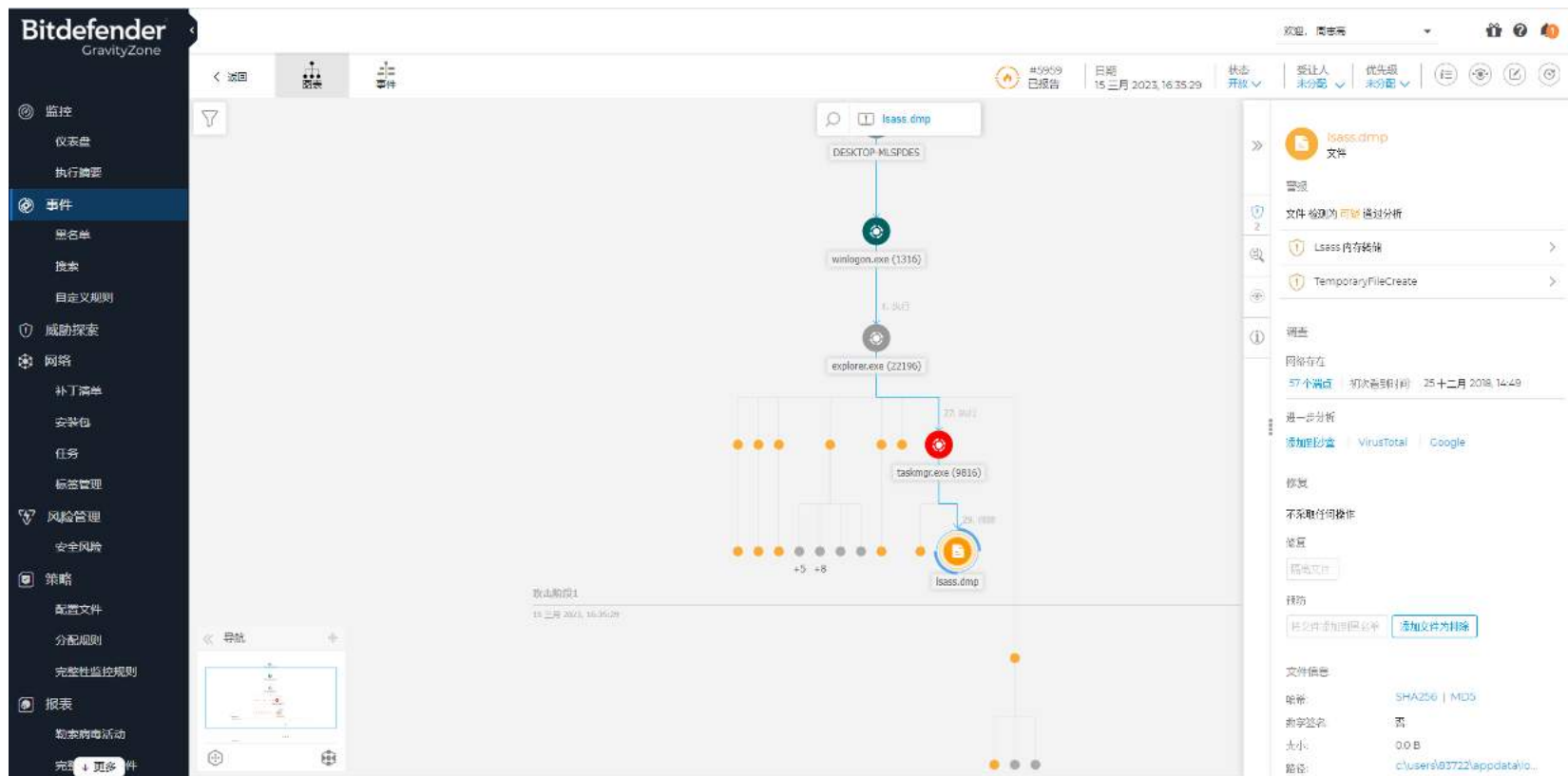
|                 |   |
|-----------------|---|
| Filename        | cvmw.exe  |
| Command Line    | %PROFILE%\downloads\cvmw.exe  |
| File Type       | PE [executable]   |
| File Size       | 99328 bytes   |
| MD5             | d678f5b6cb519ba9f9f33d519fedbc76  |
| SHA1            | ae7d0c66e47397cc8c477d6950fd54509543ecd7  |
| SHA256          | 602ca706523b48f439e8946e19c841c344202df53dff847f465c7c282beace7   |
| SHA512          | 2f60701f2fb1376642100e33c72d382e3265c293b5422bcc78937e19d81dd2066da372f08516a914e5eeb5f62c7de2bea8393ba6f23ce081877804b7d654c02 |
| CRC32           | B4A36C7   |
| Submission Time | 02 Aug 2024, 06:17:54   |
| Analysis Time   | 4.65m   |



# Bitdefender®

## EDR 端点检测与响应 全球顶级的 EDR 可视化告警视图

- 行业顶级的EDR，威胁检测模型覆盖完整的MITRE ATT&CK 框架，持续更新。
- 全平台覆盖：Windows, Linux, macOS, 容器环境
- 实时绘制攻击画像，揭示主机上正在进行的可疑活动，大幅度降低攻击者的停留时间
- 简化安全运营：AI自动警报分类、自动危险度评分，引导式调查，缓解建议，深度数据聚合
- 一键响应



## EDR 端点检测与响应 全球顶级的 EDR 时间轴视图

- 行业顶级的EDR，威胁检测模型覆盖完整的MITRE ATT&CK 框架，持续更新。
- 全平台覆盖：Windows, Linux, macOS, 容器环境
- 实时绘制攻击画像，揭示主机上正在进行的可疑活动，大幅度降低攻击者的停留时间
- 简化安全运营：AI自动警报分类、自动危险度评分，引导式调查，缓解建议，深度数据聚合
- 一键响应

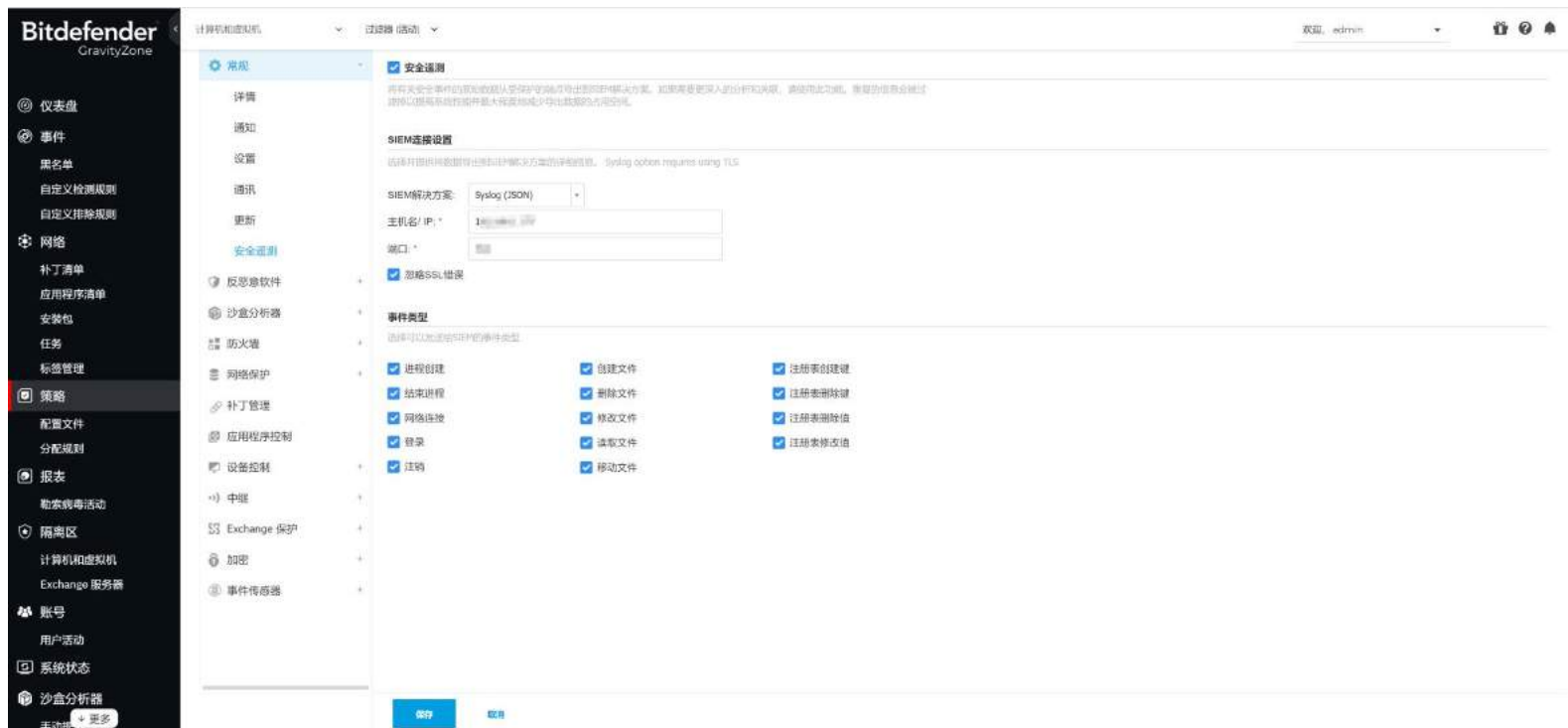
The screenshot displays the Bitdefender GravityZone EDR console interface. The left sidebar contains navigation options: 仪表盘 (Dashboard), 事件 (Events), 黑名单 (Blacklist), 自定义检测规则 (Custom Detection Rules), 自定义排除规则 (Custom Exclusion Rules), 网络 (Network), 补丁清单 (Patch List), 应用程序清单 (Application List), 安装包 (Install Packages), 任务 (Tasks), 标签管理 (Tag Management), 策略 (Policies), 配置文件 (Configuration Files), 分配规则 (Assignment Rules), 报表 (Reports), 勒索病毒活动 (Ransomware Activity), 隔离区 (Isolation Zone), 计算机和虚拟机 (Computers and VMs), Exchange 服务器 (Exchange Servers), 账号 (Accounts), 用户活动 (User Activity), 系统状态 (System Status), 沙盒分析器 (Sandbox Analyzer), and 手动拖拽 (Manual Drag). The main area shows a list of system events for a specific host (DESKTOP-2151519-000c29... 192.168.1.233) on September 18, 2024. The events are categorized by ATT&CK techniques and include details such as event names, descriptions, and associated techniques.

| 时间   | 事件名称                  | ATT&CK 技术  | 事件描述                                    |
|--|-----------------------|--|---|
| 18 九月 2024, 14:06:34<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | ScheduledTaskExecuted | ATT&CK 技术: Execution, Persistence, Privilege Escalation    | 事件描述: A scheduled task was executed.    |
|  |                       | ATT&CK 技术: Command and Scripting Interpreter – T1059. 显示所有 |   |
| 18 九月 2024, 14:06:34<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | ScheduledTaskExecuted | ATT&CK 技术: Execution, Persistence, Privilege Escalation    | 事件描述: A scheduled task was executed.    |
|  |                       | ATT&CK 技术: Scheduled Task/Job – T1053.005 Scheduled Task   |   |
| 18 九月 2024, 14:06:22<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | process_create        | ATT&CK 技术: Execution, Persistence, Privilege Escalation    | 事件描述: 创建进程。                             |
|  |                       | ATT&CK 技术: Command and Scripting Interpreter – T1059. 显示所有 |   |
| 18 九月 2024, 14:06:22<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | Regsvr32              | ATT&CK 技术: Execution, Persistence, Privilege Escalation    | 事件描述: 不适用                               |
|  |                       | ATT&CK 技术: Command and Scripting Interpreter – T1059. 显示所有 |   |
| 18 九月 2024, 13:56:17<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | UserNetworkLogon      | ATT&CK 技术: Defense Evasion, Persistence, Privilege Esc...  | 事件描述: An user has logged on via network |
|  |                       | ATT&CK 技术: Valid Accounts – T1078.002 Domain Accounts      |   |
| 18 九月 2024, 13:37:53<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | User_Login            | ATT&CK 技术: 不适用   | 事件描述: User Login                        |
| 18 九月 2024, 13:20:07<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | net_connect           | ATT&CK 技术: 不适用   | 事件描述: 建立网络连接。                           |
| 18 九月 2024, 13:19:23<br>DESKTOP-2151519-000c29...<br>192.168.1.233 | process_create        | ATT&CK 技术: 不适用   | 事件描述: 创建进程。                             |

# Bitdefender®

## SOC & SIEM 集成

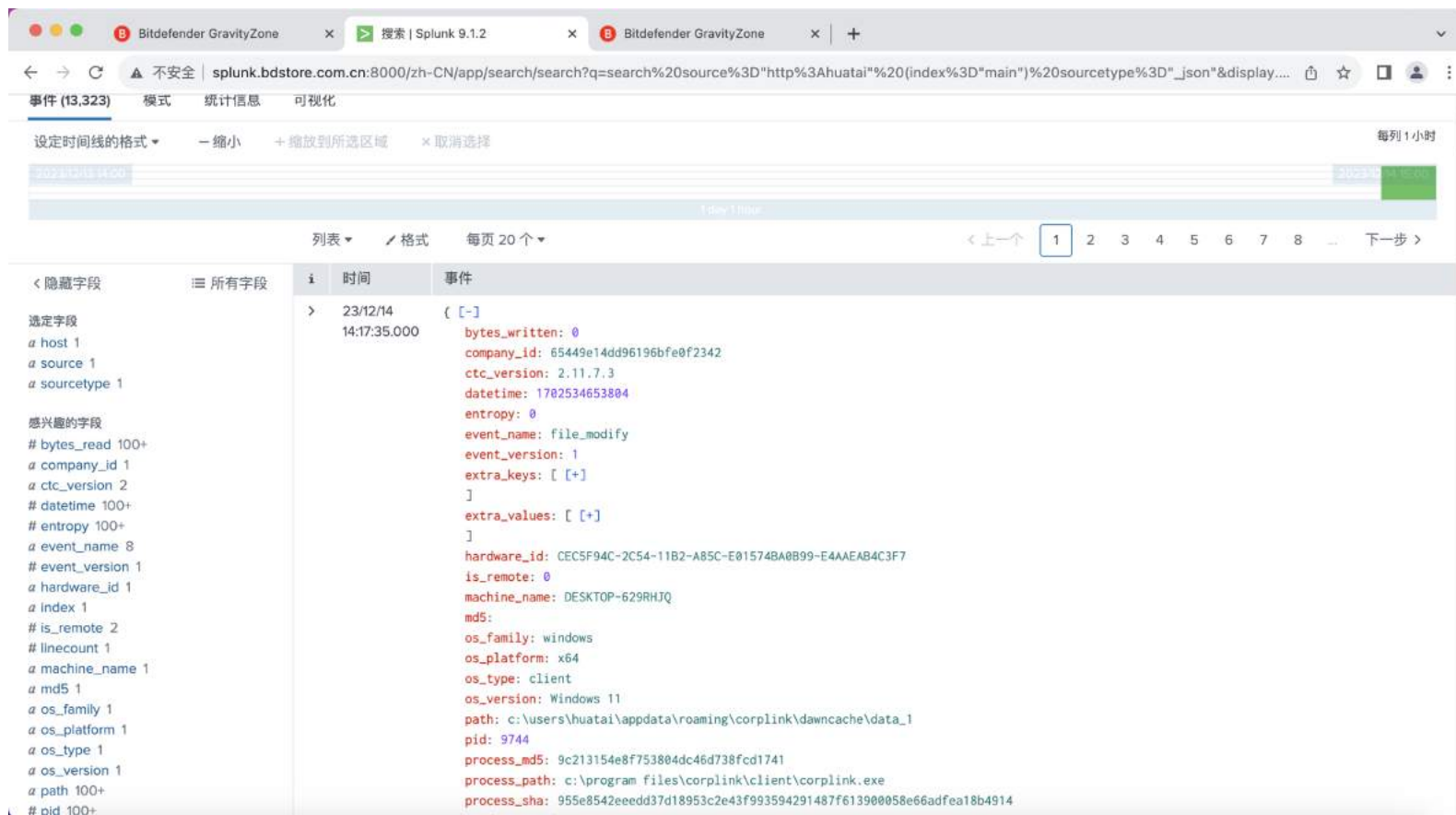
- 支持发送Syslog
- 支持发送Windows, Linux, macOS的 EDR全量原始数据: 系统登录, 文件, 进程, 网络, 注册表, 提供原始的证据
- 支持主流的SIEM平台集成:
- IBM QRadar
- Splunk
- Azure Sentinel
- 支持Syslog (Json) 发送全量EDR原始数据到SIEM, 兼容任何类型SIEM



# Bitdefender®

## SOC & SIEM 集成

- 支持发送Syslog
- 支持发送Windows, Linux, macOS的EDR全量原始数据: 系统登录, 文件, 进程, 网络, 注册表, 提供原始的证据
- 支持主流的SIEM平台集成:
- IBM QRadar
- Splunk
- Azure Sentinel
- 支持Syslog (Json) 发送全量EDR原始数据到SIEM, 兼容任何类型SIEM



The screenshot displays a Splunk search interface with the following details:

- Browser Tabs:** Bitdefender GravityZone, 搜索 | Splunk 9.1.2, Bitdefender GravityZone.
- Search URL:** `splunk.bdstore.com.cn:8000/zh-CN/app/search/search?q=search%20source%3D"http%3Ahuatai"%20(index%3D"main")%20sourcetype%3D"_json"&display...`
- Search Results:** 事件 (13,323). The interface includes options for setting timeline format, zooming, and selecting.
- Table View:** A table with columns for index, time, and event. The selected event is as follows:

| 索引 | 时间                    | 事件  |
|----|-----------------------|---|
| >  | 23/12/14 14:17:35.000 | { [-]<br>bytes_written: 0<br>company_id: 65449e14dd96196bfe0f2342<br>ctc_version: 2.11.7.3<br>datetime: 1702534653804<br>entropy: 0<br>event_name: file_modify<br>event_version: 1<br>extra_keys: [ [+]<br>]<br>extra_values: [ [+]<br>]<br>hardware_id: CEC5F94C-2C54-11B2-A85C-E015748A0B99-E4AAEAB4C3F7<br>is_remote: 0<br>machine_name: DESKTOP-629RHJQ<br>md5:<br>os_family: windows<br>os_platform: x64<br>os_type: client<br>os_version: Windows 11<br>path: c:\users\huatai\appdata\roaming\corplink\dawncache\data_1<br>pid: 9744<br>process_md5: 9c213154e8f753804dc46d738fcd1741<br>process_path: c:\program files\corplink\client\corplink.exe<br>process_sha: 955e8542eeedd37d18953c2e43f993594291487f613900058e66adfea18b4914 |
- Field Lists:** On the left, there are sections for '隐藏字段' (Hidden Fields) and '感兴趣的字段' (Fields of Interest). The '感兴趣的字段' list includes fields like `bytes_read`, `company_id`, `ctc_version`, `datetime`, `entropy`, `event_name`, `event_version`, `hardware_id`, `index`, `is_remote`, `linecount`, `machine_name`, `md5`, `os_family`, `os_platform`, `os_type`, `os_version`, `path`, and `pid`.

The screenshot shows the Bitdefender Support Center website. The browser address bar displays the URL: `bitdefender.com/business/support/en/77212-125277-public-api.html`. The page title is "Public API" under the "ON PREMISES SOLUTIONS / Public API" category. The main content area is titled "Public API" and "Introduction". It explains that Bitdefender Control Center APIs allow developers to automate business workflows and are exposed using the JSON-RPC 2.0 protocol. It lists two types of parameters: required (MUST be passed) and optional (has a default value). A note indicates that the API is limited to a specific number of requests per second per API key, and exceeding this limit results in a 429 HTTP status code. The page also mentions that the base URL for all APIs is the machine hostname, domain, or IP where GravityZone is installed, and provides an example URL: `https://YOUR-HOSTNAME/api/v1.0/jsonrpc/`. The left sidebar contains a search bar and a list of navigation links including "Welcome to GravityZone", "Release notes", "Getting started", "FAQ", "Installation", "Inventory management", "Security management", "Security monitoring", "Platform management", "Integrations", "Removal", "Migration", "Agents operation", and "Public API" (which is expanded to show sub-links like "Accounts", "Network", "Packages", "Policies", "Reports", "Maintenance windows", and "Quarantine"). The right sidebar contains a "Public API" menu with links for "Introduction", "API requests", "API Keys", "Authentication", and "Errors reporting".

bitdefender.com/business/support/en/77212-125277-public-api.html

Bitdefender®  
Support Center

FOR BUSINESS COMPANY BLOG SUPPORT FOR HOME PRODUCTS

Search

Welcome to GravityZone

Release notes

Getting started

FAQ

Installation

Inventory management

Security management

Security monitoring

Platform management

Integrations

Removal

Migration

Agents operation

Public API

- Accounts >
- Network >
- Packages >
- Policies >
- Reports >
- Maintenance windows >
- Quarantine >

ON PREMISES SOLUTIONS / Public API

## Public API

### Introduction

Bitdefender Control Center APIs allow developers to automate business workflows.

The APIs are exposed using [JSON-RPC 2.0 protocol](#) specified.

Each API call targets a method and passes a set of parameters.

There are two types of parameters:

- **required** – MUST be always passed to the called method.
- **optional** – has a default value and can be omitted from the parameters list. Any optional parameter can be skipped, regardless its position in the parameters list.

### API requests

The API calls are performed as HTTP requests with JSON-RPC messages as payload. HTTP POST method MUST be used for each API call. Also, it is required that each HTTP request have the `Content-Type` header set to `application/json`.

**Note**

The API is limited to a [specific number of requests](#) per second per API key. If this limit is exceeded, subsequent requests are rejected and `429 HTTP` status code is returned, along with a `Retry-After` header specifying the number of seconds left until you can send a new request.

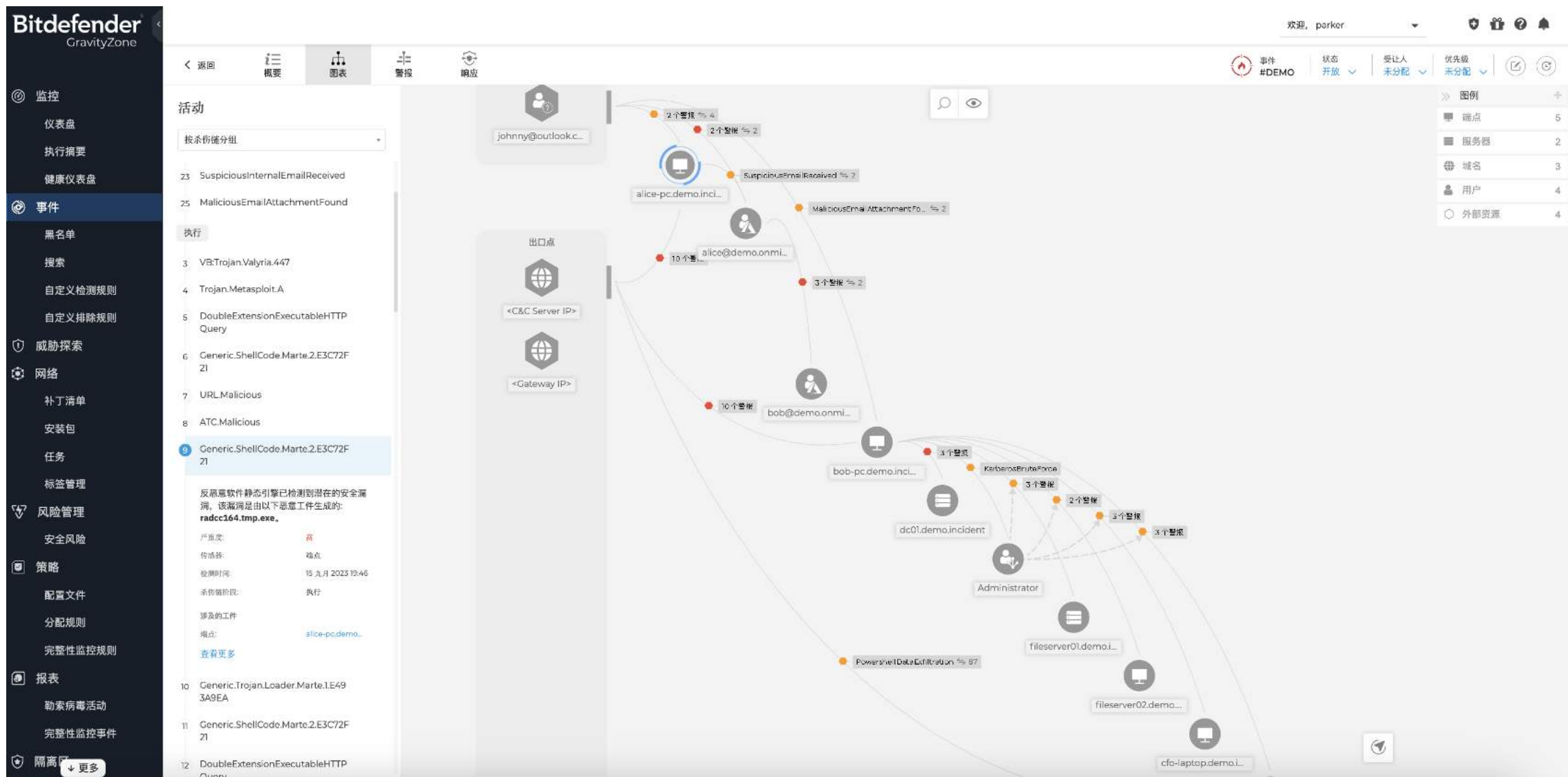
Control Center exposes multiple APIs targeting distinct areas in the product. Each API exposes a set of methods related to a designated product area. The base URL for all APIs is the machine hostname, domain or IP where GravityZone is installed: `https://YOUR-HOSTNAME/api/v1.0/jsonrpc/`. To obtain the full URL of the API, add the API name to the base URL.

Control Center API

## EDR的下一个飞跃发展 XDR 扩展检测与响应





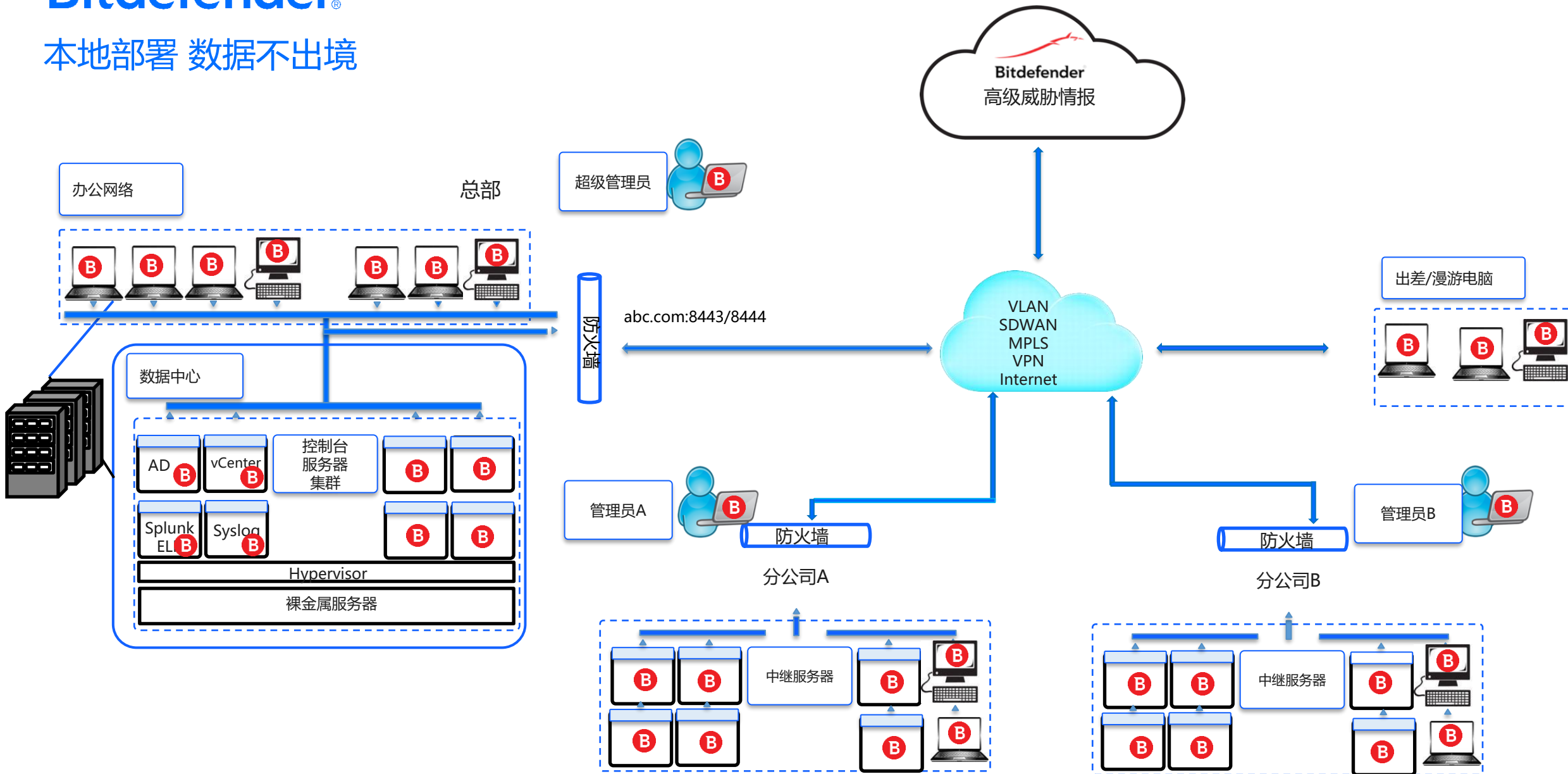


2

方案架构

# Bitdefender®

本地部署 数据不出境



## All in one 部署资源需求

| 服务器 | 主机名设置示例  | 安装角色       | 部署方式                                       | 磁盘置备 | vCPU | 内存 | 磁盘 SSD | 网卡          | VLAN | 静态IP | 互联网访问                | 分配域名 |
|-----|----------|------------|--|------|------|----|--------|-------------|------|------|----------------------|------|
| 管理端 | BDserver | All in one | 导入虚拟化镜像模版<br>或在 Ubuntu 20.04 Server上运行脚本安装 | 厚置被  | 16   | 16 | 200GB  | 10G<br>或 1G |      |      | 是, 到 Bitdefender 服务器 |      |

备注:

— 申请域名: 【web控制台】edr.com.cn 【通讯+事件】bitdefender.com.cn 【更新】bdupdate.com.cn

— 申请SSL证书

## 高可用架构 部署资源需求

| 集群  | 服务器 | 主机名设置示例   | 安装角色                                       | 部署方式  | 磁盘置备 | vCPU | 内存 | 磁盘 SSD | 网卡          | VLAN | 静态IP | 互联网访问                      | 分配域名 |
|-----|-----|-----------|--|---|------|------|----|--------|-------------|------|------|----------------------------|------|
| 管理端 | VM1 | BDServer1 | 数据库服务器 主+Web服务器<br>1+事件服务器1+更新服务器          | 导入虚拟化镜像<br>模版<br><br>或在 Ubuntu<br>20.04 Server上<br>运行脚本安装 | 厚置备  | 12   | 16 | 200GB  | 10G<br>或 1G |      |      | 是, 到<br>Bitdefender服<br>务器 |      |
|     | VM2 | BDServer2 | 数据库服务器 副本成员+Web<br>服务器2+通讯服务器2             |   |      | 12   | 16 | 200GB  |             |      |      |                            |      |
|     | VM3 | BDServer3 | 数据库服务器 副本成员+事件<br>服务器2+通讯服务器1              |   |      | 12   | 16 | 200GB  |             |      |      |                            |      |
|     | VM4 | BDServer4 | 负载均衡服务器<br>均衡对象: Web+通讯服务器+<br>事件服务器+通讯服务器 |   |      | 8    | 12 | 100GB  |             |      |      |                            |      |

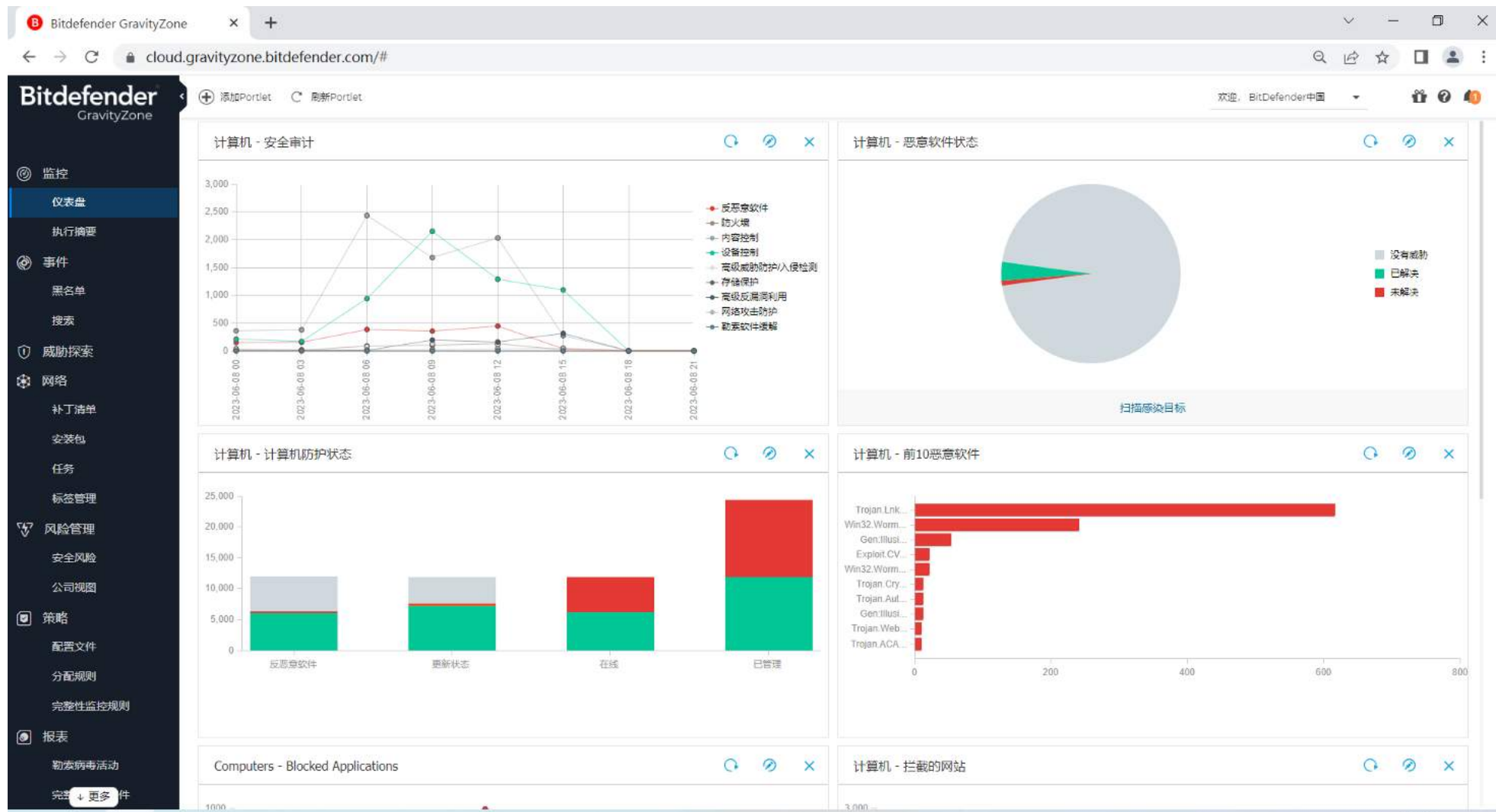
备注:

— 申请域名: 【web控制台】edr.com.cn 【通讯+事件】bitdefender.com.cn 【更新】bdupdate.com.cn

— 申请SSL证书

# Bitdefender®

SaaS 云部署 GCP 非常适合跨国、跨区域部署



3

# 案例介绍

## 案例：某大型制造业防护项目

### 客户需求：

拥有多个生产设施，涵盖从工控系统到日常办公的广泛环境。公司面临着网络安全挑战，需要一种全面的EDR解决方案来保护其复杂的IT和OT环境。

- **工控环境：** 在工控环境中使用多个旧版的工业控制系统和设备，这些系统容易受到网络攻击。现有的安全解决方案无法有效识别和阻止高级威胁，同时也对系统的实时操作造成了干扰。
- **生产环境：** 生产环境中的设备和系统面临恶意软件、病毒和网络攻击，这些威胁可能导致生产停机、设备损坏或数据泄露。需要在保障生产效率的同时提升系统的安全性。
- **办公环境：** 办公环境中的员工设备面临钓鱼攻击、恶意软件和数据泄露的风险。需要保护所有办公设备，同时不影响员工的工作效率。



## 工控环境

### 解决方案：

Bitdefender 提供针对工控系统的高效保护，能够实时监控并保护设备，同时支持常见的工业协议。能在不中断生产过程的情况下运行，并能够与现有的SCADA系统进行集成。支持linux 6.X及win server 2008等老系统，支持ARM平台的各大linux发行版。

#### Supported Linux Legacy Distributions

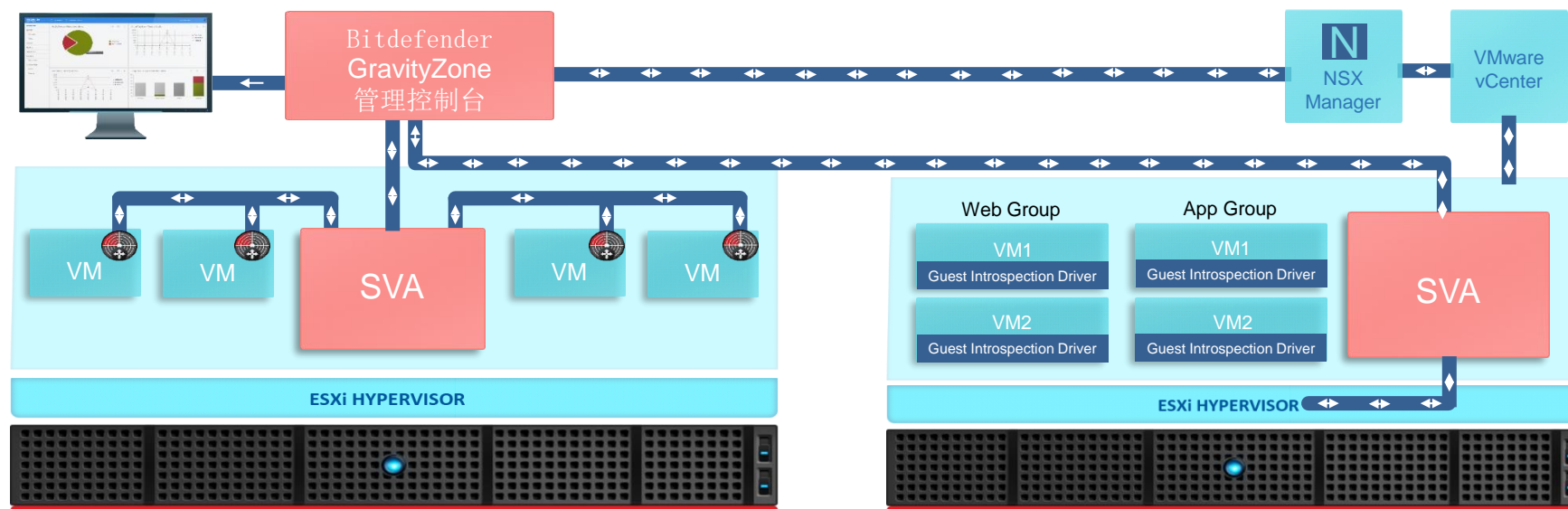
| Distro                         | Architecture   | Kernel Versions |
|--------------------------------|----------------|-----------------|
| <b>RPM-based</b>               |                |                 |
| <b>RHEL 6.10</b>               | 32-bit, 64-bit | 2.6.32-754      |
| <b>CentOS 6.10</b>             | 32-bit, 64-bit | 2.6.32-754      |
| <b>Oracle Linux 6.10 UEK</b>   | 64-bit         | 4.1.12-124      |
| <b>Amazon Linux v1 2018.03</b> | 64-bit         | 4.14.x          |
| <b>Debian-based</b>            |                |                 |
| <b>Ubuntu 14.04 LTS</b>        | 32-bit, 64-bit | 4.4             |
| <b>Ubuntu 16.04.x</b>          | 32-bit, 64-bit | 4.15            |

## 生产环境

### 解决方案：

用户的生产环境全部部署于虚拟化环境中，即有仅vsphere的环境也有NSX-V/NSX-T环境。基于客户的现状，推荐使用轻代理防护和无代理防护相结合的解决方案。

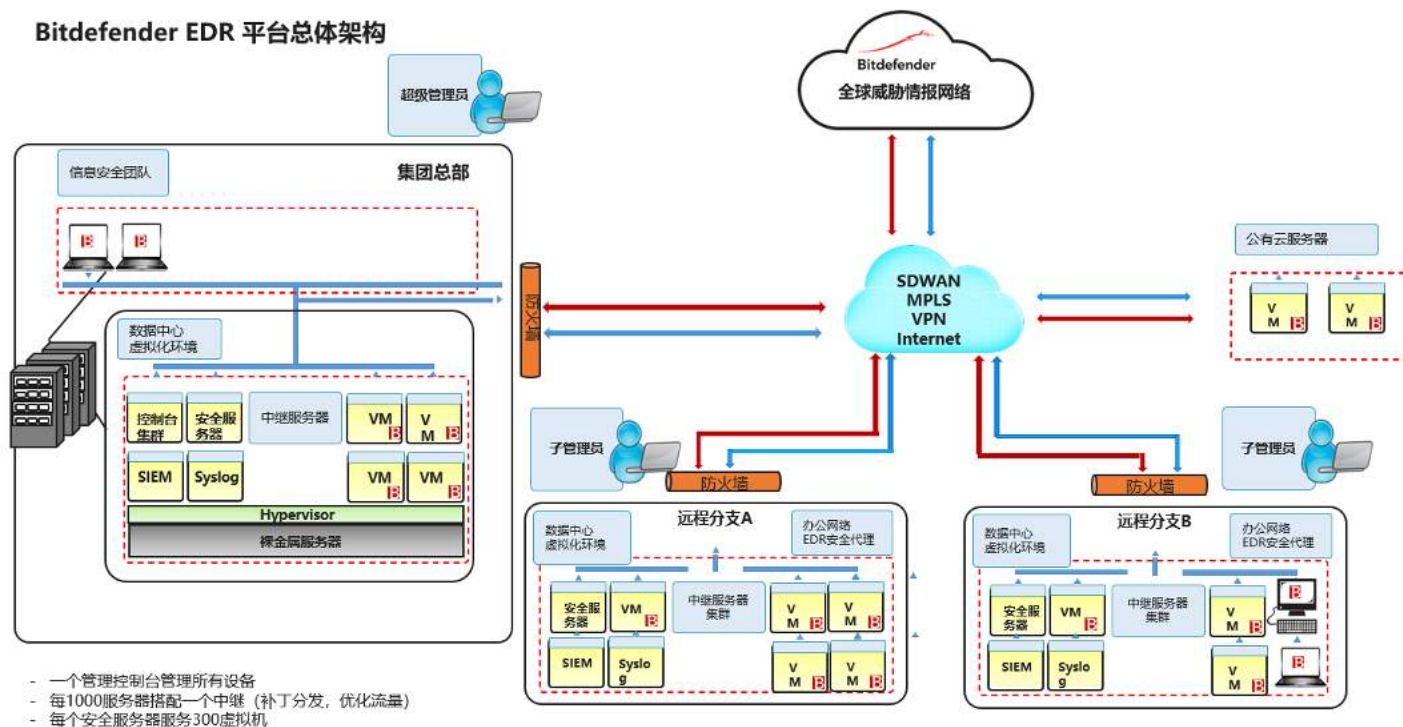
Bitdefender企业防病毒采用特殊优化的虚拟化环境解决方案。轻代理防护通过虚拟机（VM）和安全服务器（SVA）两级缓存，避免冗余扫描，杜绝扫描风暴，显著提高反恶意软件的扫描效率。无代理防护结合NSX-V/NSX-T接口实现针对虚拟系统的安全防护，无需在虚拟机安装Agent程序，通过无代理方式实现病毒防护，无需消耗虚拟机计算资源。



## 办公环境

### 解决方案:

Bitdefender 提供全面的办公环境保护，包括防钓鱼、恶意软件防护和EDR实时防护。具备实时威胁检测和响应能力，能够集中管理Windows、Linux、Mac OS所有办公设备的安全策略，并能够与现有的IT系统进行集成，易于使用和管理的控制台，确保所有办公设备的安全性。

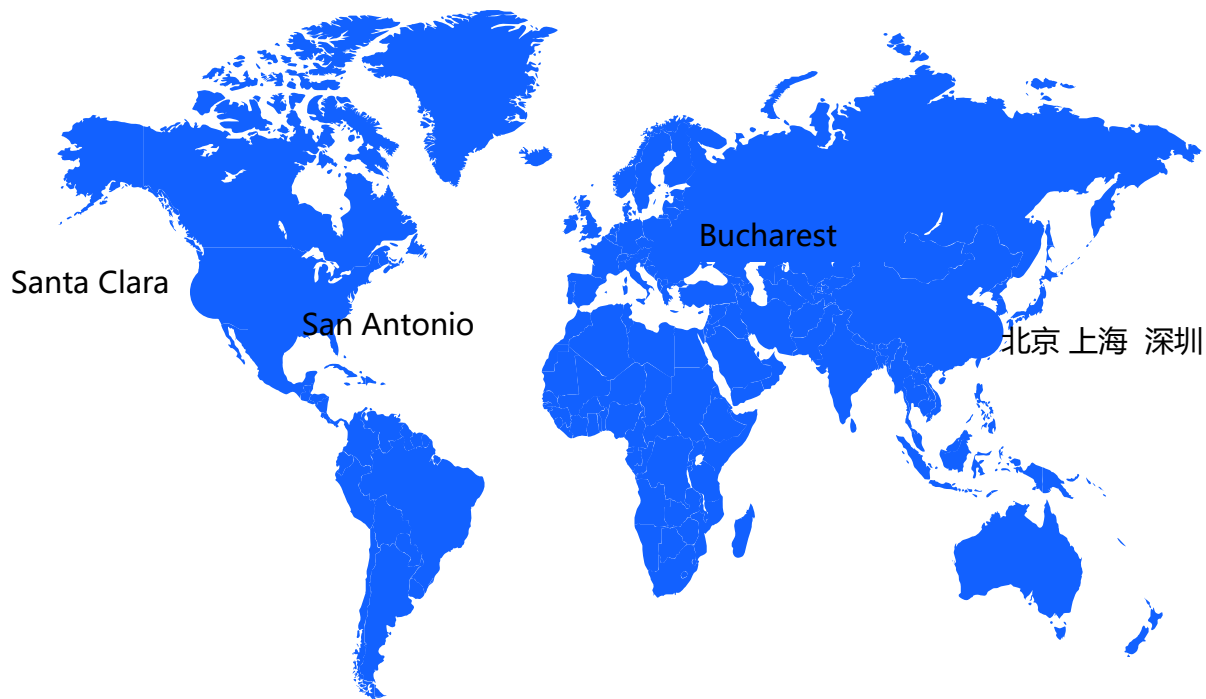




# Bitdefender 公司简介

# Bitdefender®

@防病毒 @EDR @XDR @MDR @CWPP @CSPM @容器安全 @移动安全 @邮件安全



## 2001年

成立，罗马尼亚，欧洲老牌安全厂商

## 5亿

全球5亿用户，遍布180多个国家和地区，具有全球最大的威胁情报网络

## 1800+

员工

## 900+

研发工程师

## 4000亿

每天执行4000亿次威胁查询，海量数据不断训练AI引擎

## 3秒

3秒内响应全球任意位置的最新威胁

## 400+

每分钟发现400+新威胁

Bitdefender® 全球 180+ 公司使用Bitdefender的安全技术 深度覆盖全球和中国网络安全市场



Tencent 腾讯

智慧沟通 灵感无限



PROPRIETARY AND CONFIDENTIAL

Bitdefender®

企业产品案例



Deloitte.



KIOXIA



BORGWARNER



5

为什么选择 Bitdefender



# Bitdefender®

全球顶级的EPP 自动阻止99.5%+ 攻击  
在攻击的早期自动阻止99.5%+的威胁，大幅度降低安全团队日常工作量

AV-Test 2023年度

最佳保护+最佳性能



Protecting companies from ransomware and data stealers

**Advanced Threat Protection-Test**

**AV-TEST**  
The Independent IT-Security Institute  
Magdeburg Germany

**AV-TEST**  
av-test.org  
12/2023

APPROVED  
ENDPOINT  
PROTECTION

ADVANCED

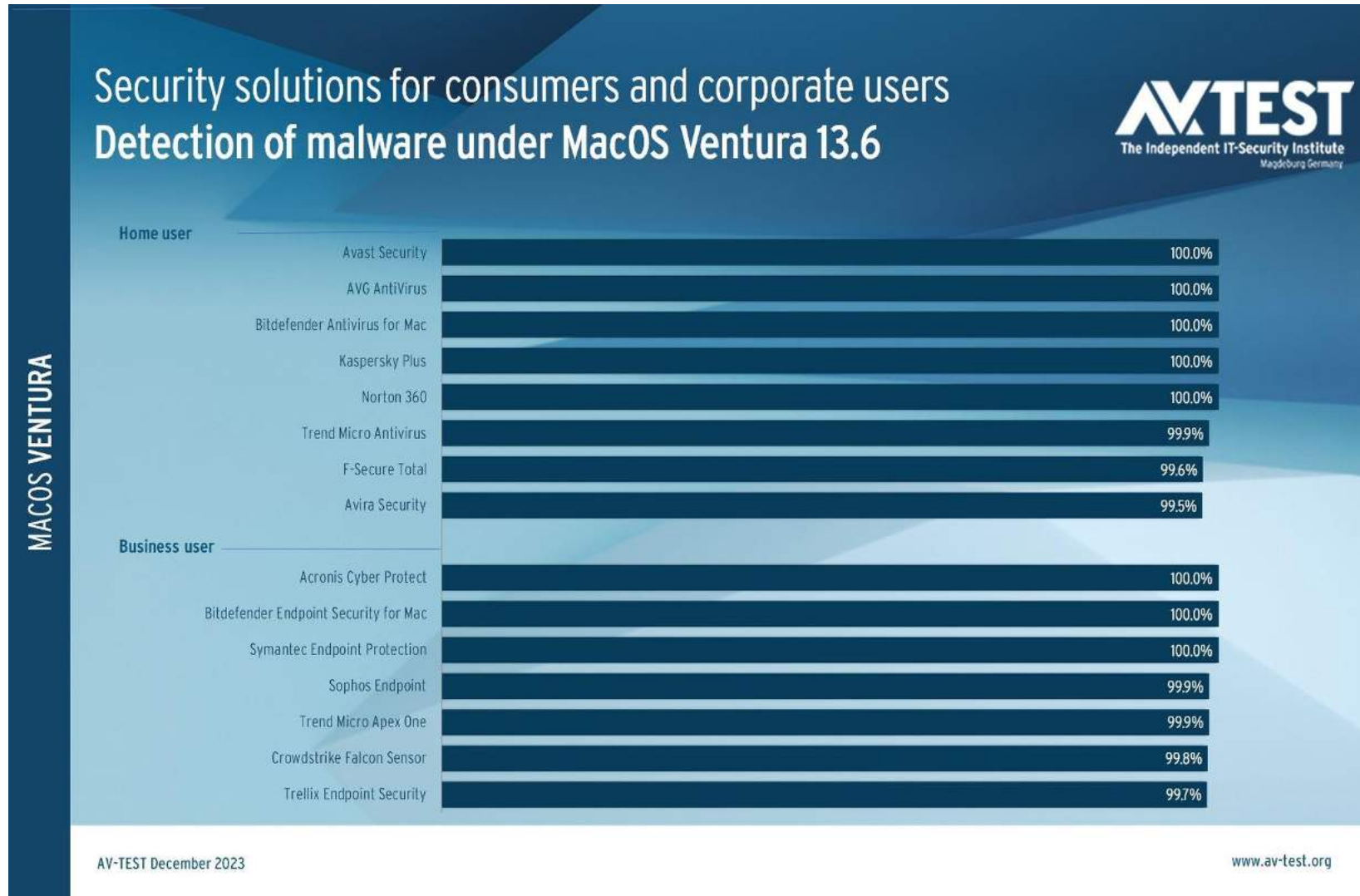
WINDOWS

**BUSINESS WINDOWS**

| Manufacturer | Product                                   | AV-TEST Certificate | Detected attacks (max. 10) | Protection score (max. 30 pts) |
|--------------|---|---------------------|----------------------------|--------------------------------|
| AhnLab       | AhnLab V3 Endpoint Security               |                     | 10                         | 30.0                           |
| Avast        | Avast Ultimate Business Security          |                     | 10                         | 30.0                           |
| Bitdefender  | Bitdefender Endpoint Security             |                     | 10                         | 30.0                           |
| Bitdefender  | Bitdefender Endpoint Security Ultra       |                     | 10                         | 30.0                           |
| Check Point  | Check Point Endpoint Security             |                     | 10                         | 30.0                           |
| Kaspersky    | Kaspersky Endpoint Security               |                     | 10                         | 30.0                           |
| Kaspersky    | Kaspersky Small Office Security           |                     | 10                         | 30.0                           |
| Rapid7       | Rapid7                                    | -                   | 10                         | 30.0                           |
| Seqrite      | Seqrite Endpoint Security                 |                     | 10                         | 30.0                           |
| Symantec     | Symantec Endpoint Security Complete       |                     | 10                         | 30.0                           |
| Trellix      | Trellix Endpoint Security                 |                     | 10                         | 30.0                           |
| VMware       | VMware Carbon Black Cloud                 |                     | 10                         | 30.0                           |
| Microsoft    | Microsoft Defender Antivirus (Enterprise) |                     | 9                          | 27.0                           |

AV-TEST December 2023

www.av-test.org



|                    | Malware Protection Performance |            | Real-World Protection | ATP         | Malware Protection Performance |              | Real-World Protection |
|--------------------|--------------------------------|------------|-----------------------|-------------|--------------------------------|--------------|-----------------------|
|                    | March 2023                     | April 2023 | February-May 2023     | Autumn 2023 | September 2023                 | October 2023 | July-October 2023     |
| Kaspersky          | ***                            | ***        | ***                   | ***         | ***                            | ***          | ***                   |
| <b>Bitdefender</b> | <b>***</b>                     | <b>***</b> | <b>***</b>            | <b>***</b>  | <b>***</b>                     | <b>***</b>   | <b>***</b>            |
| Avast              | ***                            | ***        | ***                   | **          | ***                            | ***          | ***                   |
| AVG                | ***                            | ***        | ***                   | **          | ***                            | ***          | ***                   |
| Avira              | ***                            | ***        | ***                   | *           | ***                            | ***          | ***                   |
| ESET               | ***                            | ***        | **                    | ***         | ***                            | ***          | *                     |
| G Data             | ***                            | **         | ***                   | **          | ***                            | **           | ***                   |
| McAfee             | ***                            | ***        | ***                   |             | ***                            | **           | ***                   |
| Norton             | ***                            | ***        | **                    |             | **                             | ***          | **                    |
| TotalAV            | ***                            | ***        |                       |             | ***                            | **           | **                    |
| Microsoft          | *                              | *          | ***                   |             | ***                            | **           | **                    |
| Total Defense      | **                             | *          | ***                   |             | ***                            | *            | **                    |
| F-Secure           | **                             | **         | **                    |             |                                | **           | **                    |
| K7                 |                                | ***        | **                    |             |                                | ***          | **                    |
| Panda              |                                | ***        |                       |             | *                              | ***          | *                     |
| Trend Micro        |                                | **         | *                     |             |                                | **           | *                     |





## AV-Comparatives 2023下半年 企业安全产品测评 真实世界动态防护

|                               | Blocked | User dependent | Compromised | PROTECTION RATE<br>[Blocked % + (User dependent %)/2]* | False Alarms |
|-------------------------------|---------|----------------|-------------|--|--------------|
| <b>Bitdefender</b>            | 503     | -              | -           | 100%   | 2            |
| <b>Avast</b>                  | 503     | -              | -           | 100%   | 3            |
| <b>Kaspersky</b>              | 502     | -              | 1           | 99.8%  | 1            |
| <b>CrowdStrike</b>            | 502     | -              | 1           | 99.8%  | 16           |
| <b>VIPRE</b>                  | 501     | -              | 2           | 99.6%  | 2            |
| <b>Elastic,<br/>Microsoft</b> | 500     | -              | 3           | 99.4%  | 3            |
| <b>G Data</b>                 | 498     | -              | 5           | 99.0%  | 3            |
| <b>Trellix</b>                | 495     | 4              | 4           | 98.8%  | 10           |
| <b>K7</b>                     | 495     | -              | 8           | 98.4%  | 1            |
| <b>CISCO</b>                  | 494     | -              | 9           | 98.2%  | 7            |
| <b>WatchGuard</b>             | 494     | -              | 9           | 98.2%  | 21           |
| <b>ESET</b>                   | 493     | -              | 10          | 98.0%  | 1            |
| <b>Sophos</b>                 | 491     | 4              | 8           | 98.0%  | 1            |
| <b>Cybereason</b>             | 477     | -              | 26          | 94.8%  | 7            |
| <b>VMware</b>                 | 467     | -              | 36          | 92.8%  | 3            |

查看报告: <https://www.av-comparatives.org/tests/business-security-test-2023-august-november/>

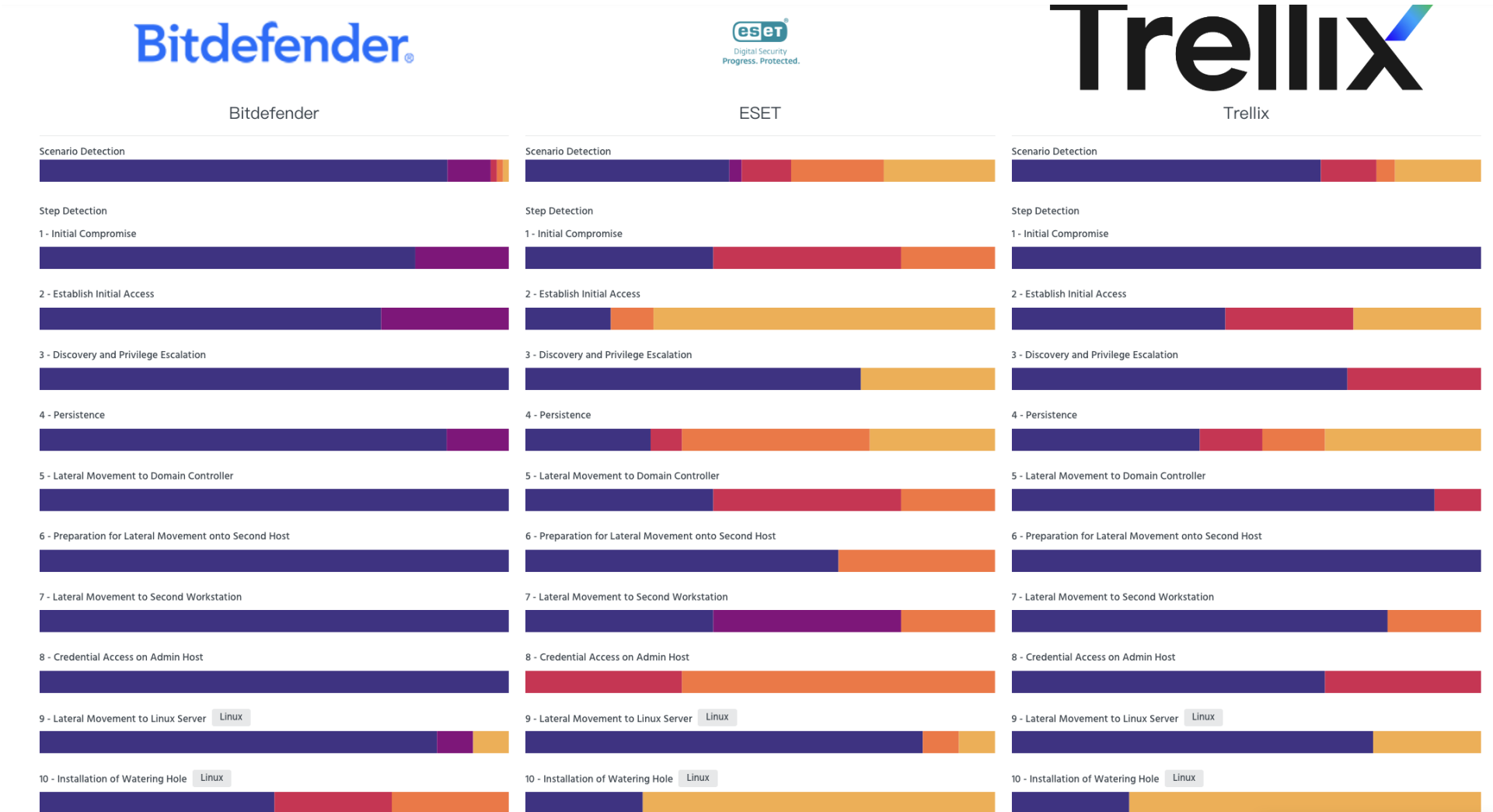


行业排名第一的 APT高级持续性威胁防护能力  
AV-Comparatives 2023 测试报告 HyperDetect 机器学习未开启

|             | Test scenarios |   |   |   |   |   |   |   |   |    |    |    |    |    |    | FPs | Score |
|-------------|----------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|-----|-------|
|             | 1              | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |     |       |
| Avast       | ✓              | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓  | ✓  | ✓  | ✗  | ✓  | ✓  | N   | 13    |
| Bitdefender | ✓              | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓  | ✓  | ✓  | ✗  | ✓  | ✓  | N   | 14    |
| CrowdStrike | ✓              | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓  | ✓  | ✗  | ✓  | ✓  | ✓  | N   | 12    |
| ESET        | ✓              | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗  | ✓  | ✓  | ✓  | ✓  | ✓  | N   | 13    |
| G Data      | ✓              | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓  | ✓  | ✓  | ✗  | ✓  | ✓  | N   | 12    |
| Kaspersky   | ✓              | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | N   | 13    |
| VIPRE       | ✓              | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓  | ✓  | ✓  | ✗  | ✓  | ✓  | N   | 12    |
| VMware      | ✓              | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✓  | ✓  | ✓  | ✓  | ✓  | ✓  | N   | 12    |

查看报告: <https://www.av-comparatives.org/tests/advanced-threat-protection-test-2023-enterprise/>

## Mitre ATT&CK 2023 EDR测评



2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms



COMPLETENESS OF VISION

As of November 2023

© Gartner, Inc

Gartner



# Bitdefender®

Forrester Wave™: Endpoint Security, Q4 2023

端点安全的领导者





### SOC2 Type 2 认证

证明了供应商以有效运营方式密切保护客户数据的承诺。我们的安全控制措施每年都会根据 AICPA SSAE-16 SOC 2 安全性、机密性和可用性原则指南进行审核。完整报告可应要求提供。



### ISO 27017: 云安全控制实践准则

ISO 27017是为云服务提供商和用户开发的安全标准，旨在创建更安全的基于云的环境，并降低安全风险。它是ISO/IEC 27000系列标准的一部分，该系列标准提供了关于信息安全管理最佳实践的建议。



### ISO 27001: 信息安全管理认证

ISO 27000 系列标准可帮助组织确保信息资产的安全。该标准帮助组织管理资产的安全，例如财务信息、知识产权、员工详细信息或第三方委托的信息。



### ISO 9001: 质量管理体系认证

ISO 9001 是全球数百万企业使用的最佳实践管理框架，旨在标准化业务实践并提高业务绩效。该标准帮助组织证明他们有能力始终如一地提供满足客户和适用法律法规要求的产品，并旨在通过系统的有效应用提高客户满意度，包括持续改进系统的过程和保证符合客户和适用的法律法规要求。

## 总结 行业头部厂商 最高的安全水平和安全标准

AV-Test 2019, 2020, 2021, 2023年  
度最佳产品

AV-Comparatives  
2019,2020,2021,2022,2023年度最佳产  
品

自动阻止99.5%+威胁, 100%勒索病毒  
防护

#1 EPP

TOP  
EDR

Mitre ATT&CK 连续4年 EDR  
评估, 100%检测

TOP XDR

Gartner 2022 端点安全技术成熟度曲线,  
EPP、EDR和XDR的推荐供应商  
Gartner 2023 端点安全魔力象限远见者  
Gartner 2023 客户之选  
Forrester 2023 端点安全的领导者

值得信赖 始终如一

# 谢谢!

关注我们



免费试用



联系人: 凌科龙

电话: 18598010128

Email: [Lingkelong@bitdefender-cn.com](mailto:Lingkelong@bitdefender-cn.com)

