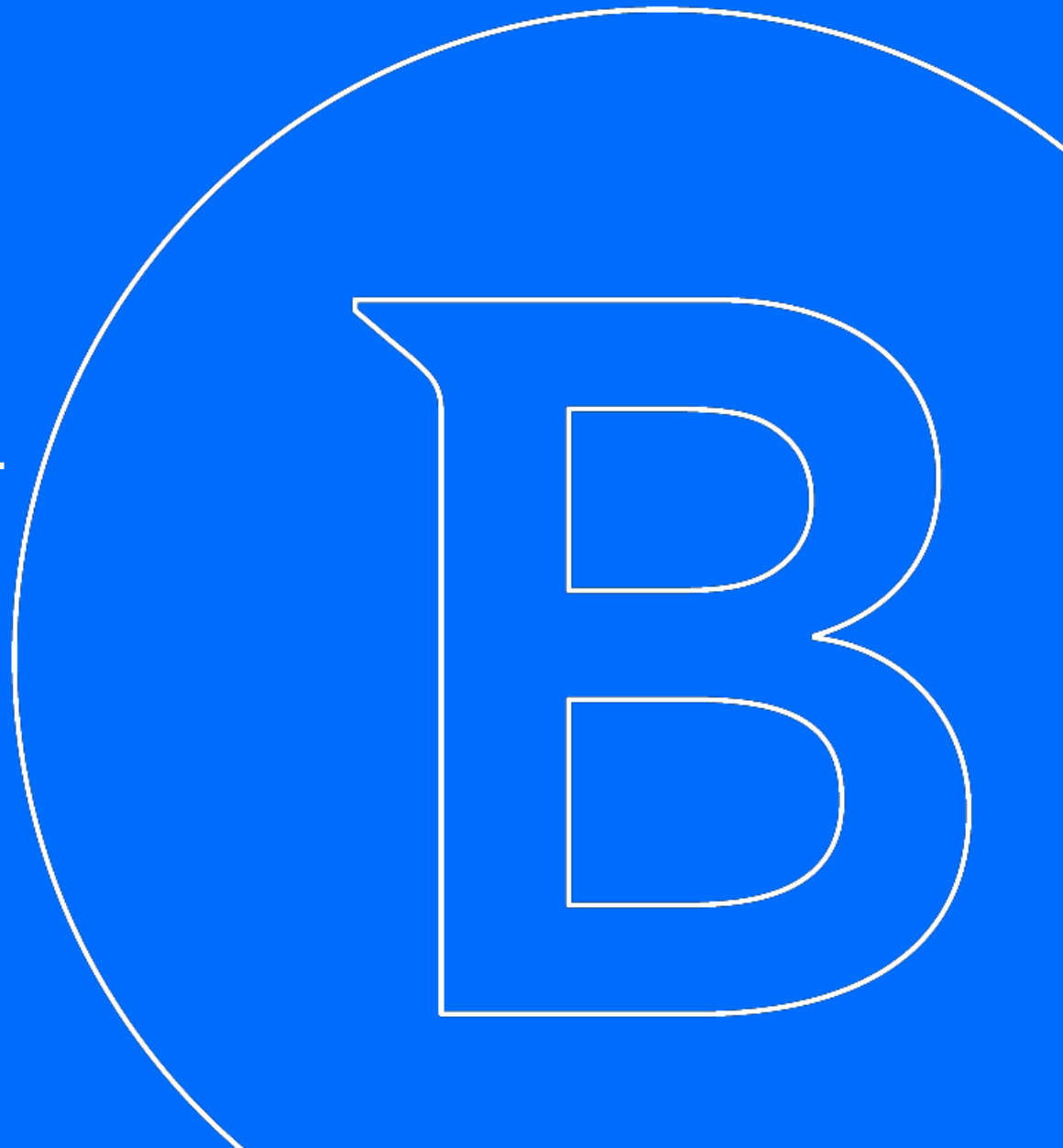
全球网络安全领导者

Bitdefender®

Bitdefender助力企业筑牢信息安全防线



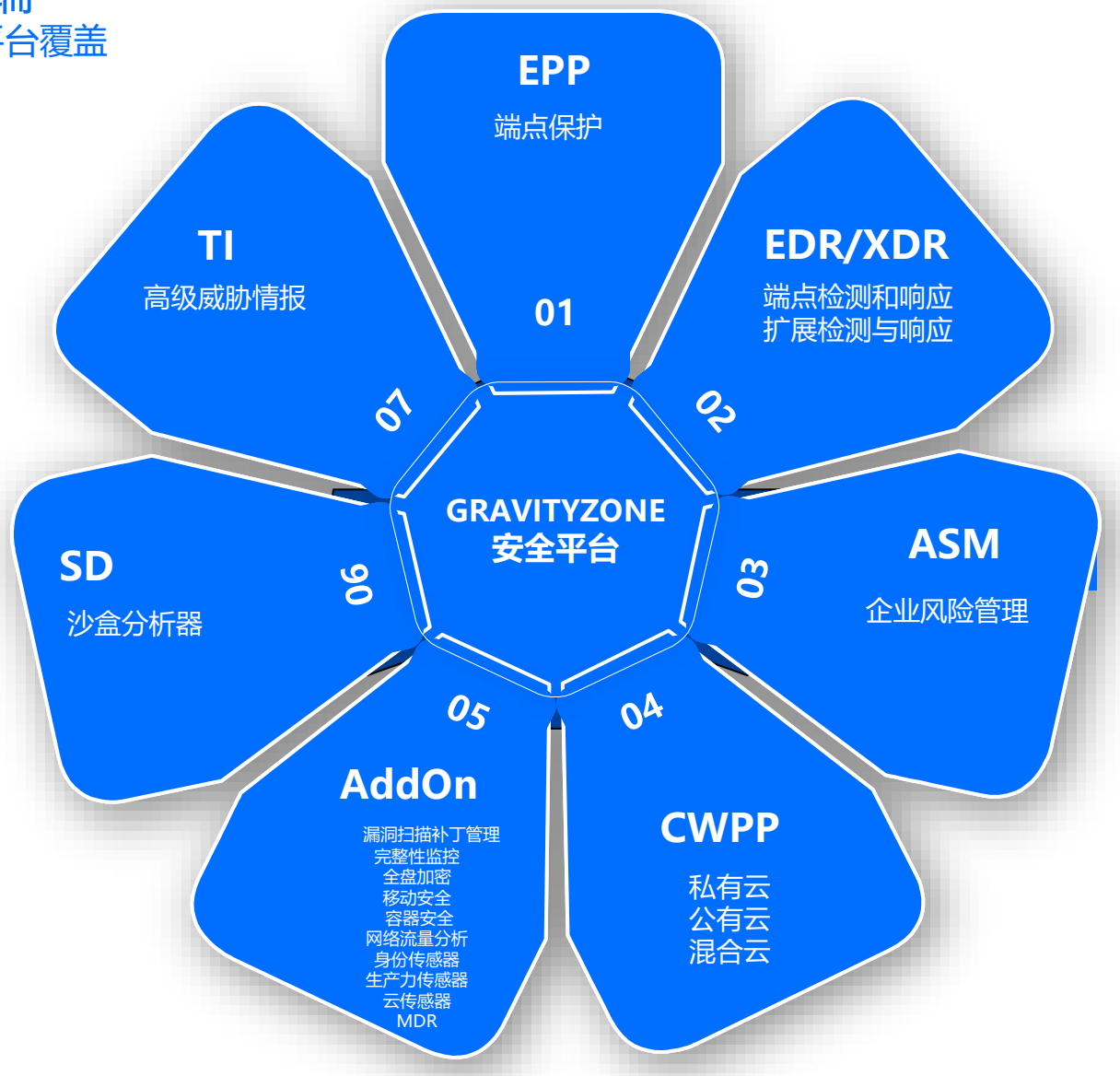
1

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



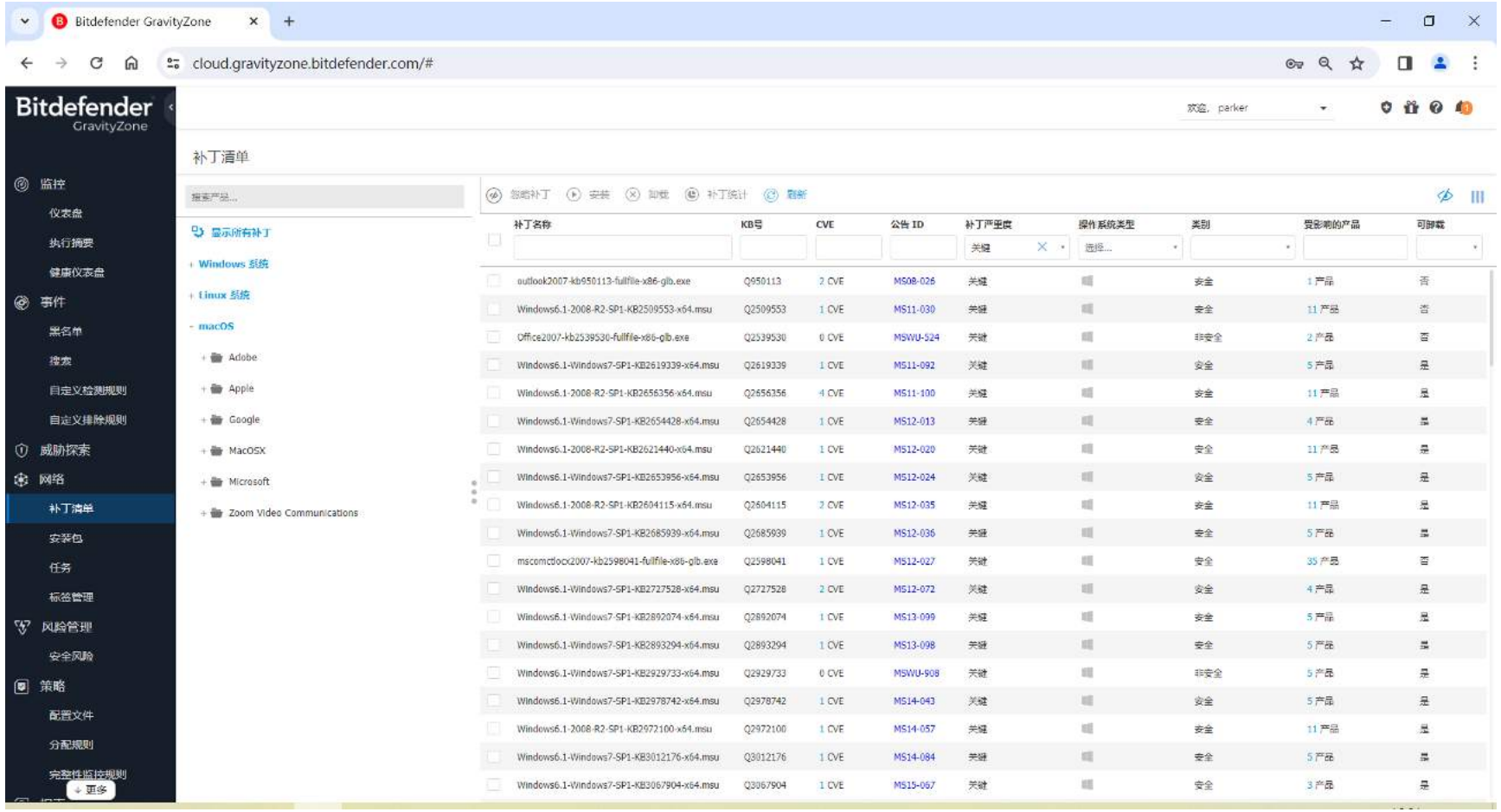
Bitdefender

纵深防护战略

Bitdefender

安全加固 — 漏洞扫描与补丁管理

- 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

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

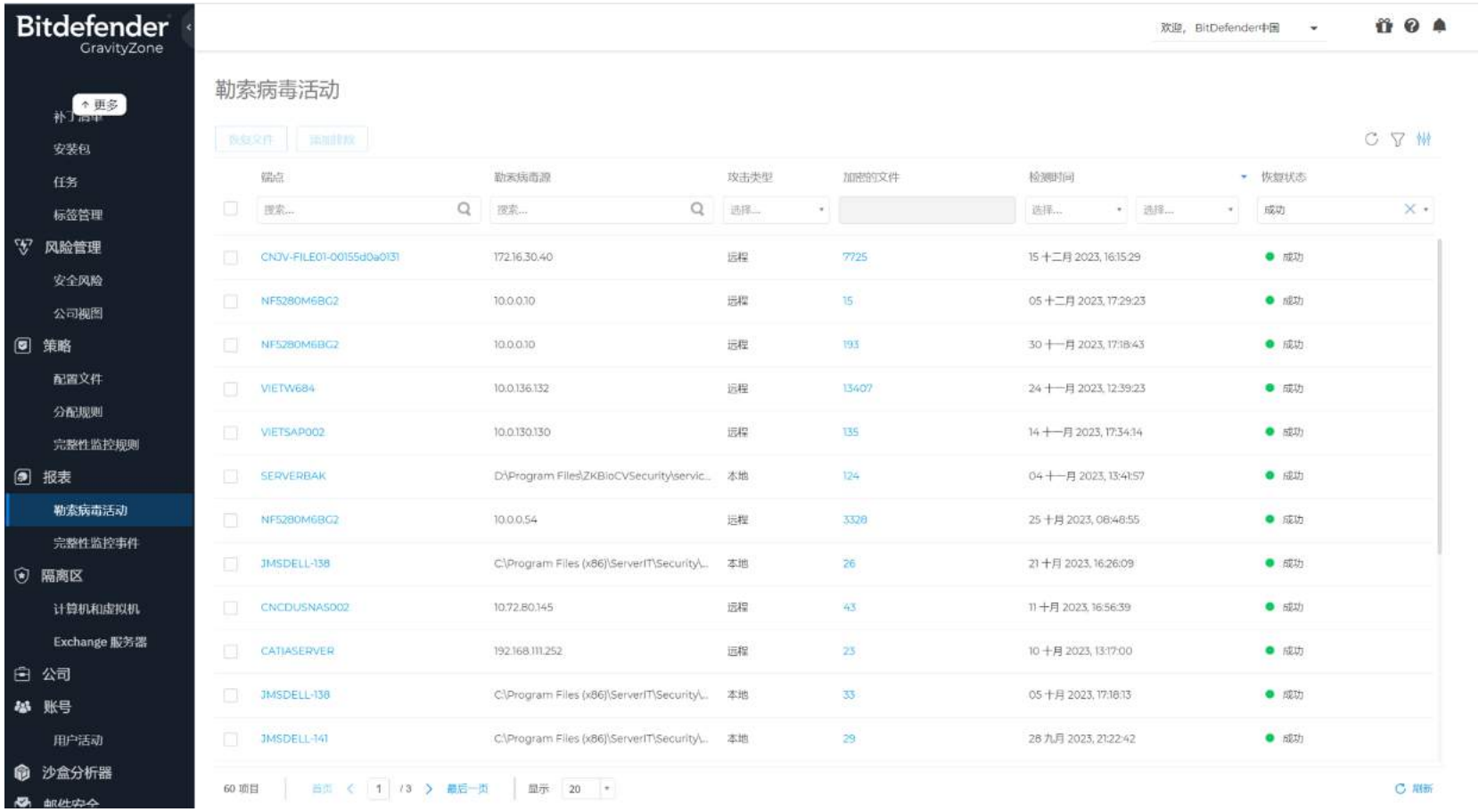
- RDP爆破，SSH爆破，SMB攻击，C2流量，TOR流量，凭据泄露……
- 远程代码执行，PSExec，WMI调用，远程过程调用 (RPC)、远程计划任务和基于分布式组件对象模型 (DCOM) 的执行……
- 网络漏洞利用，如log4J，ZeroLogon、PrintNightmare ，反弹shell…..等等

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@HS	4	04 十二月 2023, 04:53:49	网络攻击防护	网络攻击事件	Exploit.DRSUAPI.DCSync	lateralMovement	10.10.39.75	10.10.8.13
NHSV-STD-ES231	10.10.39.75	nhsv-std-es231	80205911@HS	4	04 十二月 2023, 05:42:36	网络攻击防护	网络攻击事件	Exploit.DRSUAPI.DCSync	lateralMovement	10.10.39.75	10.10.8.14

Bitdefender

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



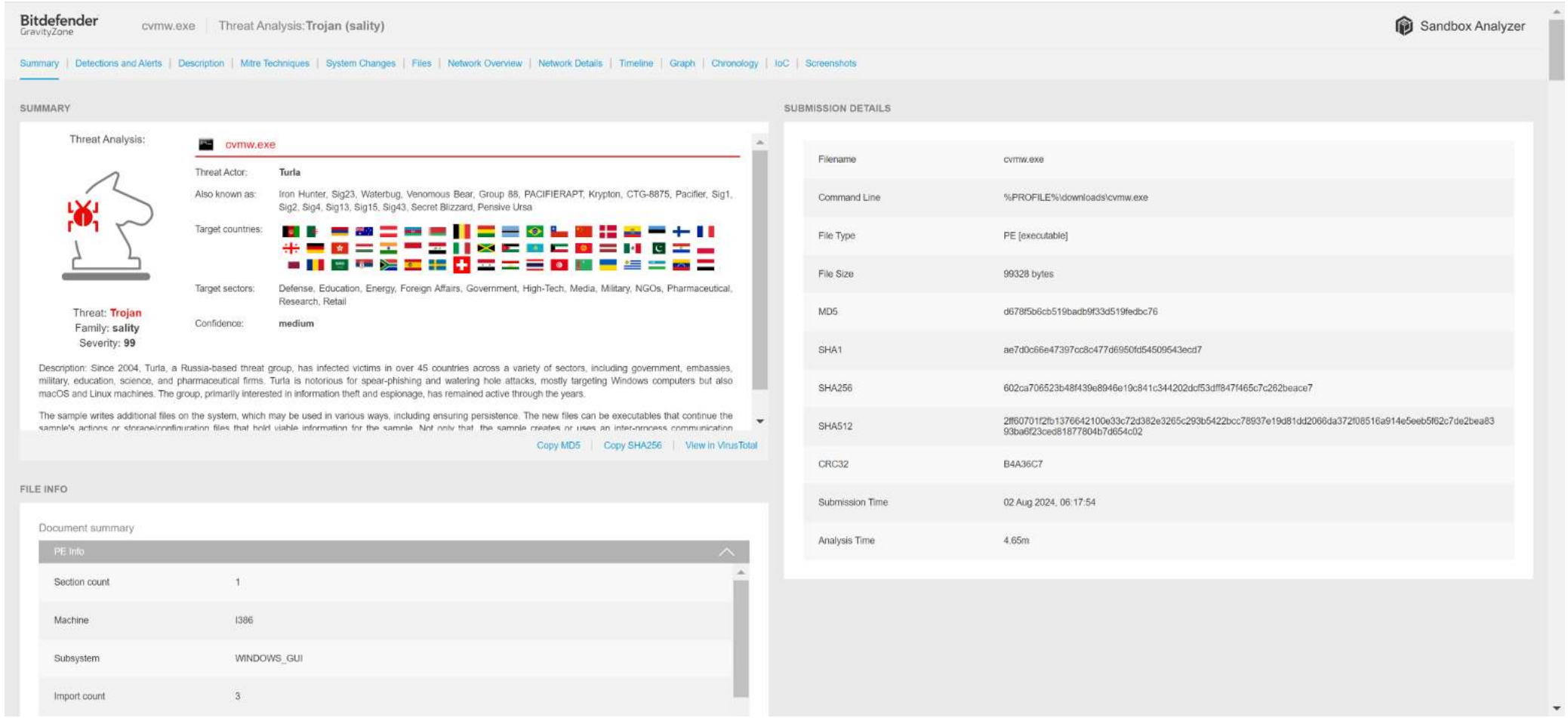
Bitdefender

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

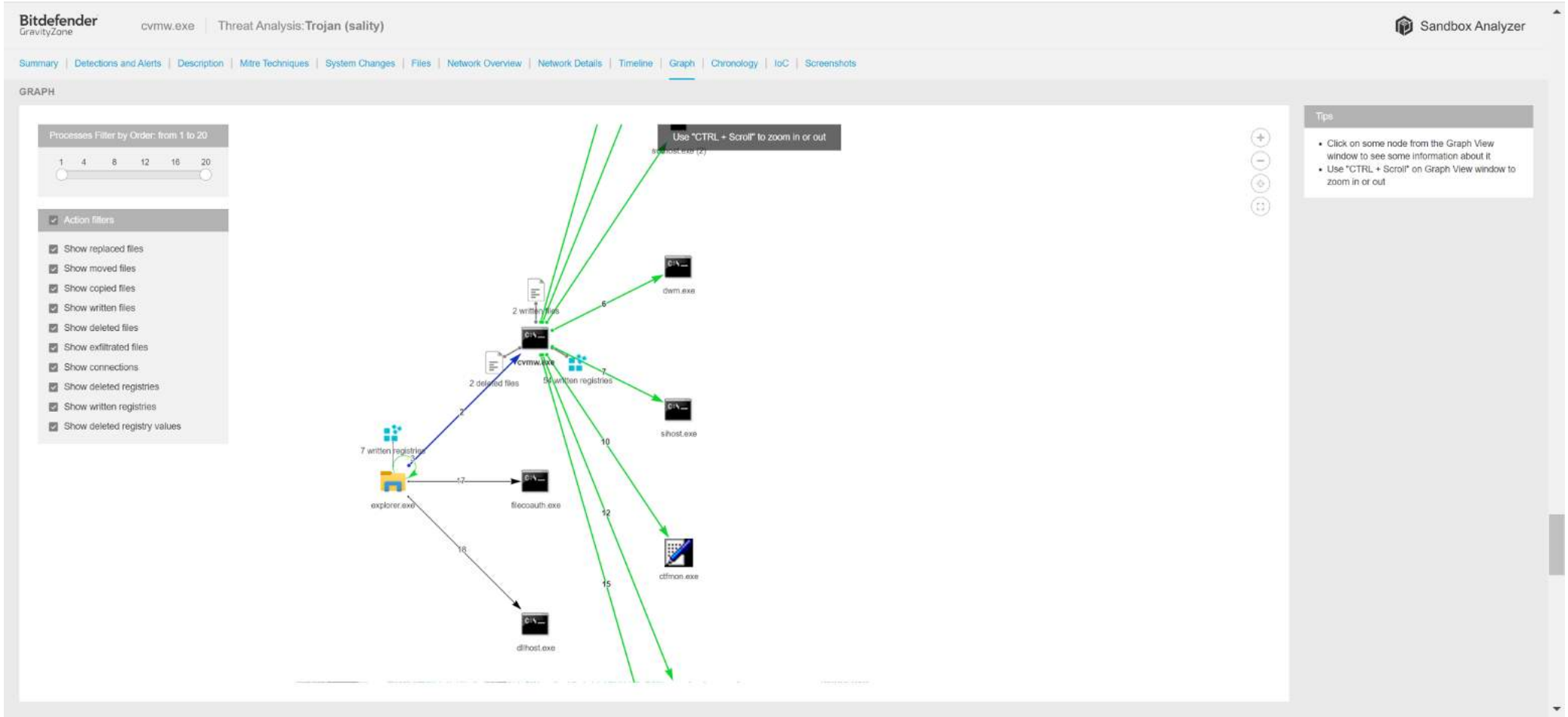
Bitdefender®

完整沙盒分析报告 IOC&IOA



Bitdefender

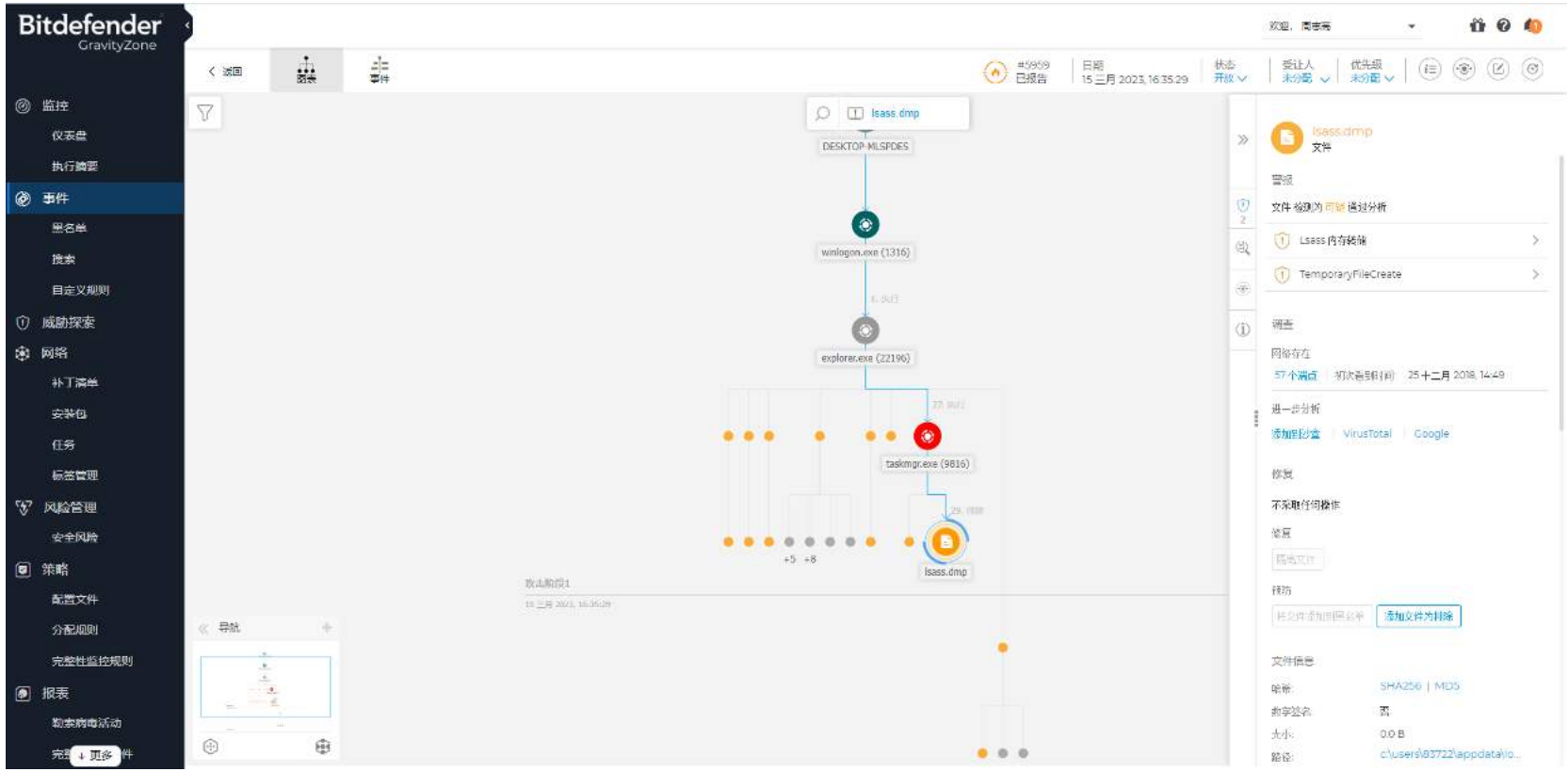
完整沙盒分析报告 IOC&IOA



Bitdefender

EDR 端点检测与响应 全球顶级的 EDR 可视化告警视图

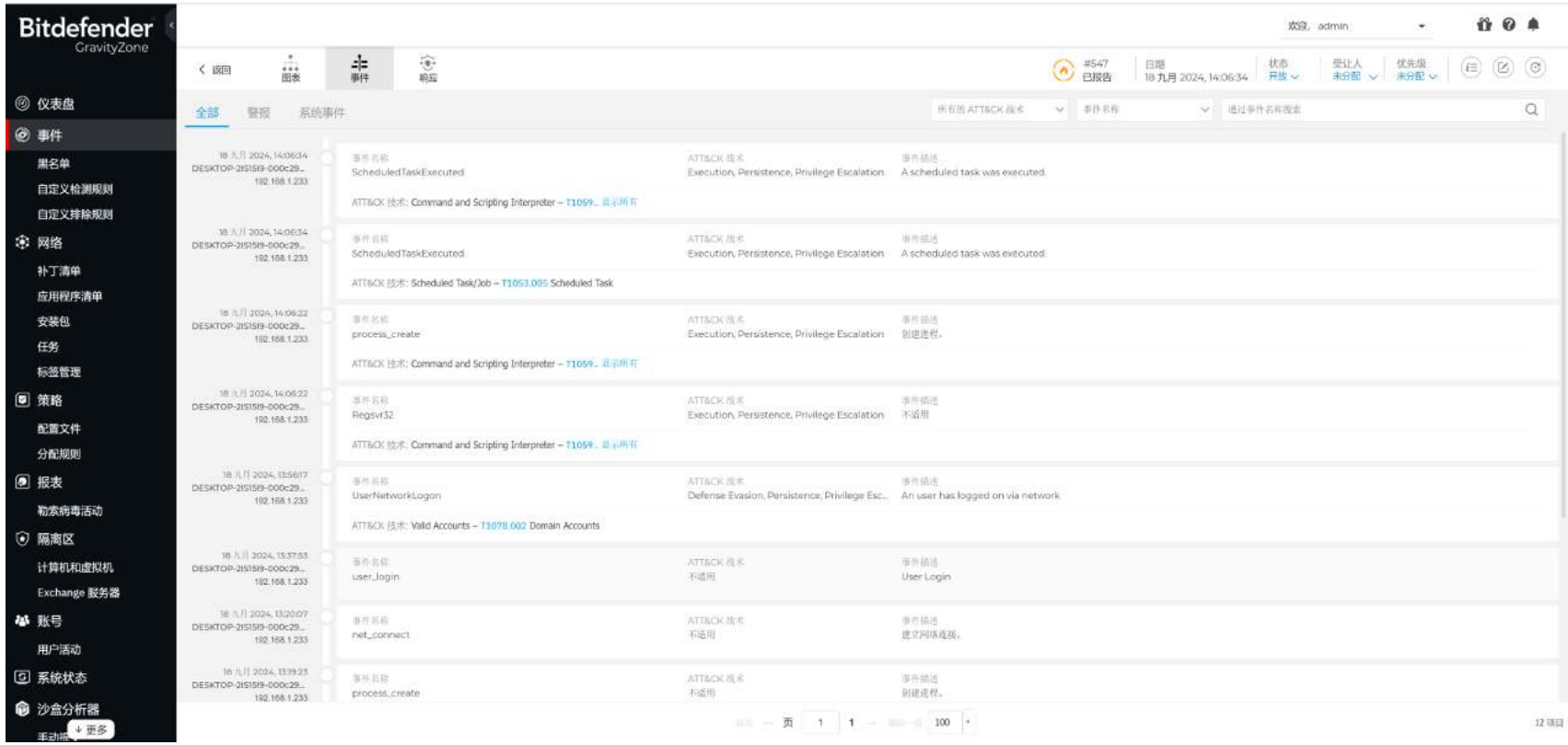
- 行业顶级的EDR，威胁检测模型覆盖完整的MITRE ATT&CK 框架，持续更新。
- 全平台覆盖：Windows，Linux，macOS， 容器环境
- 实时绘测攻击画像，揭示主机上正在进行的可疑活动，大幅度降低攻击者的停留时间
- 简化安全运营：AI自动警报分类、自动危险度评分，引导式调查，缓解建议，深度数据聚合
- 一键响应



Bitdefender

EDR 端点检测与响应 全球顶级的 EDR 时间轴视图

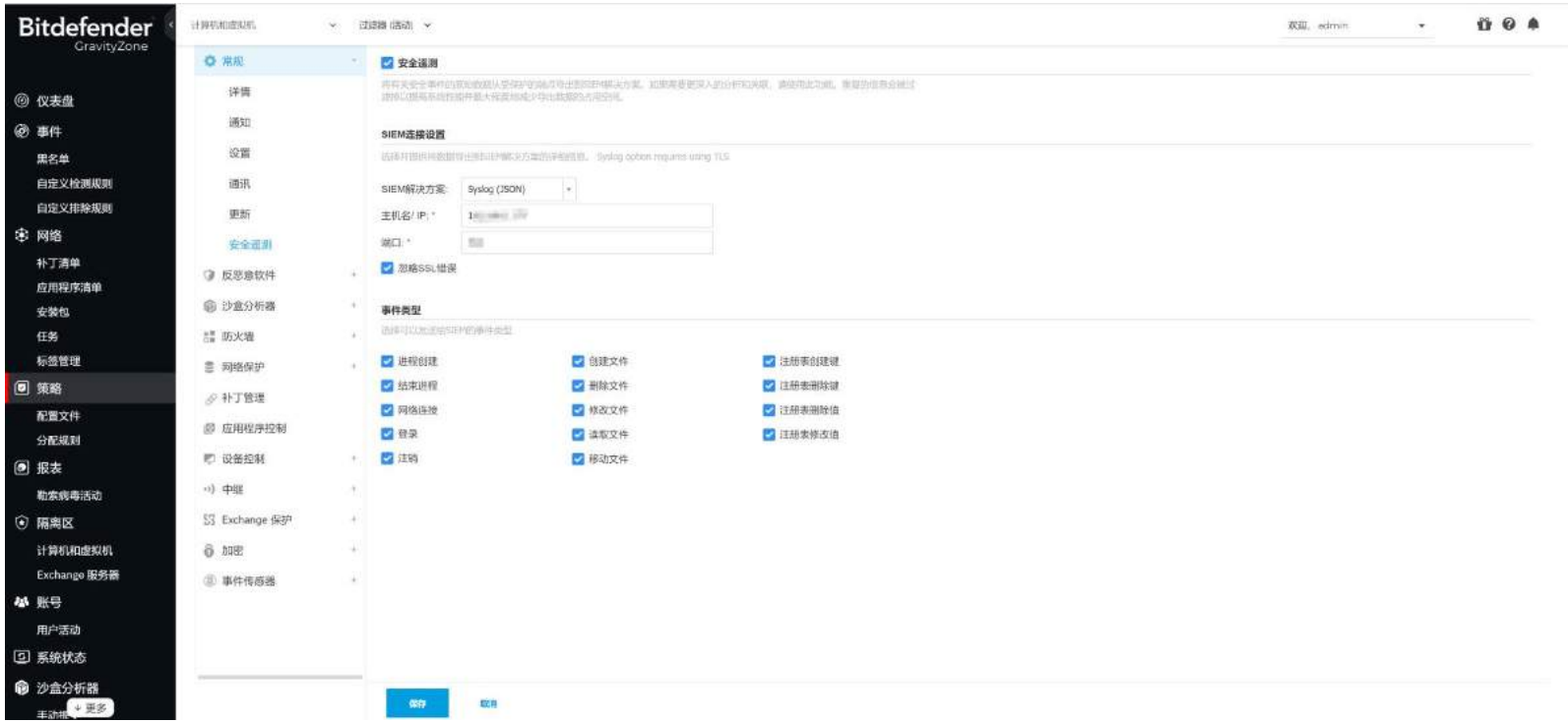
- 行业顶级的EDR，威胁检测模型覆盖完整的MITRE ATT&CK 框架，持续更新。
- 全平台覆盖：Windows，Linux，macOS， 容器环境
- 实时绘测攻击画像，揭示主机上正在进行的可疑活动，大幅度降低攻击者的停留时间
- 简化安全运营：AI自动警报分类、自动危险度评分，引导式调查，缓解建议，深度数据聚合
- 一键响应



Bitdefender

SOC & SIEM 集成

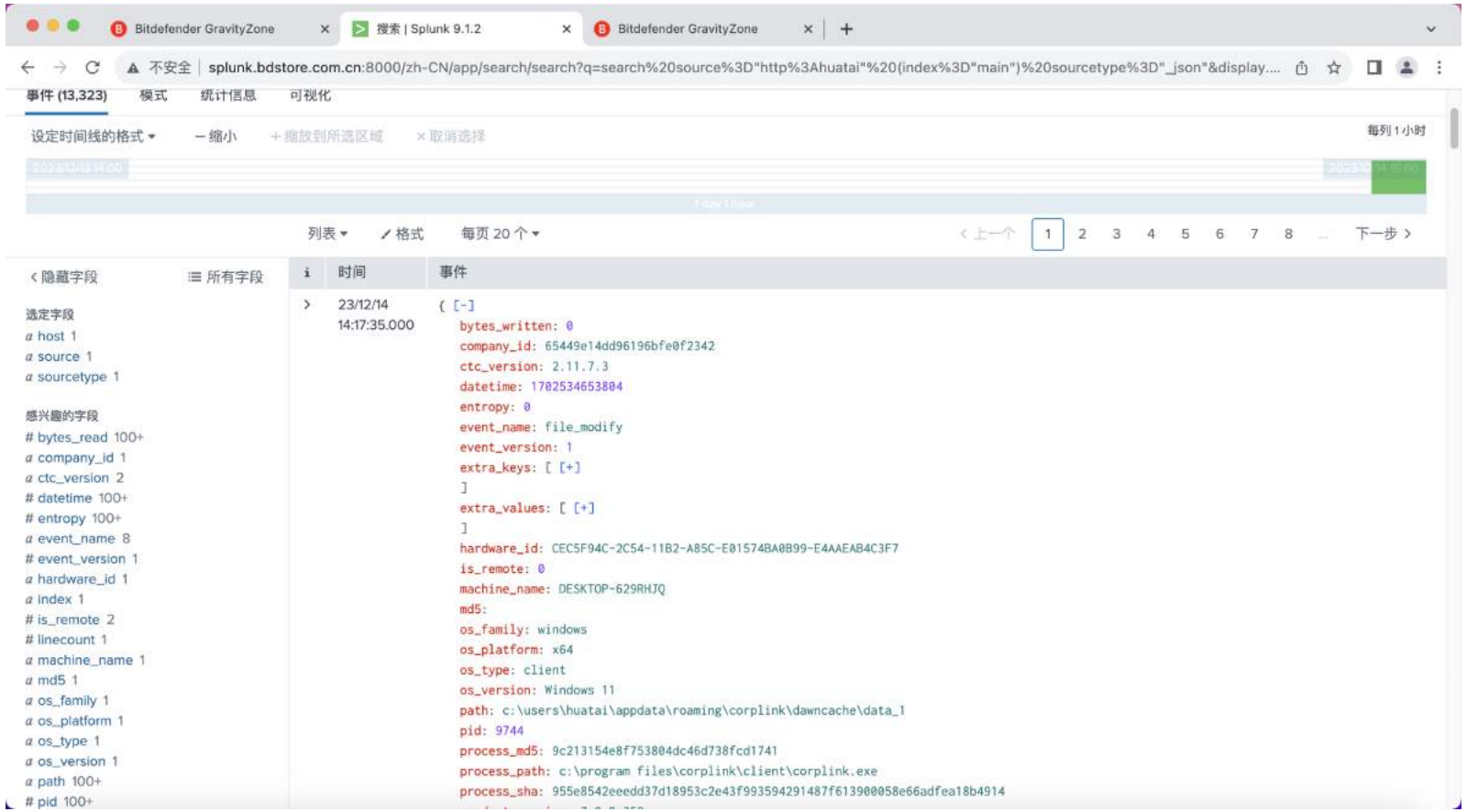
- 支持发送Syslog
- 支持发送Windows，Linux，macOS的EDR全量原始数据：系统登录，文件，进程，网络，注册表，提供原始的证据
- 支持主流的SIEM平台集成：
- IBM QRadar
- Splunk
- Azure Sentinel
- 支持Syslog（Json）发送全量EDR原始数据到SIEM，兼容任何类型SIEM



Bitdefender

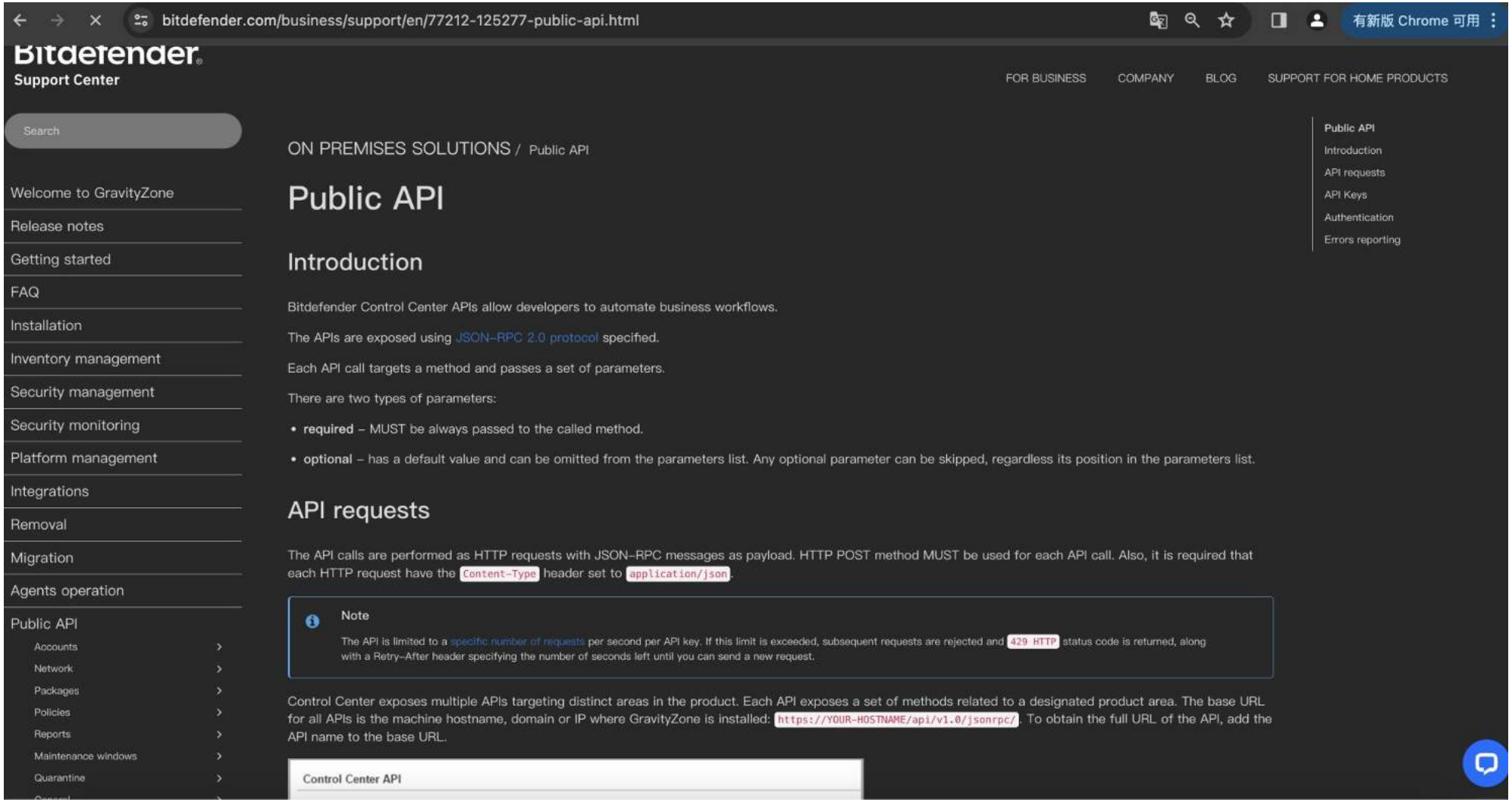
SOC & SIEM 集成

- 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



Bitdefender

支持API 集成

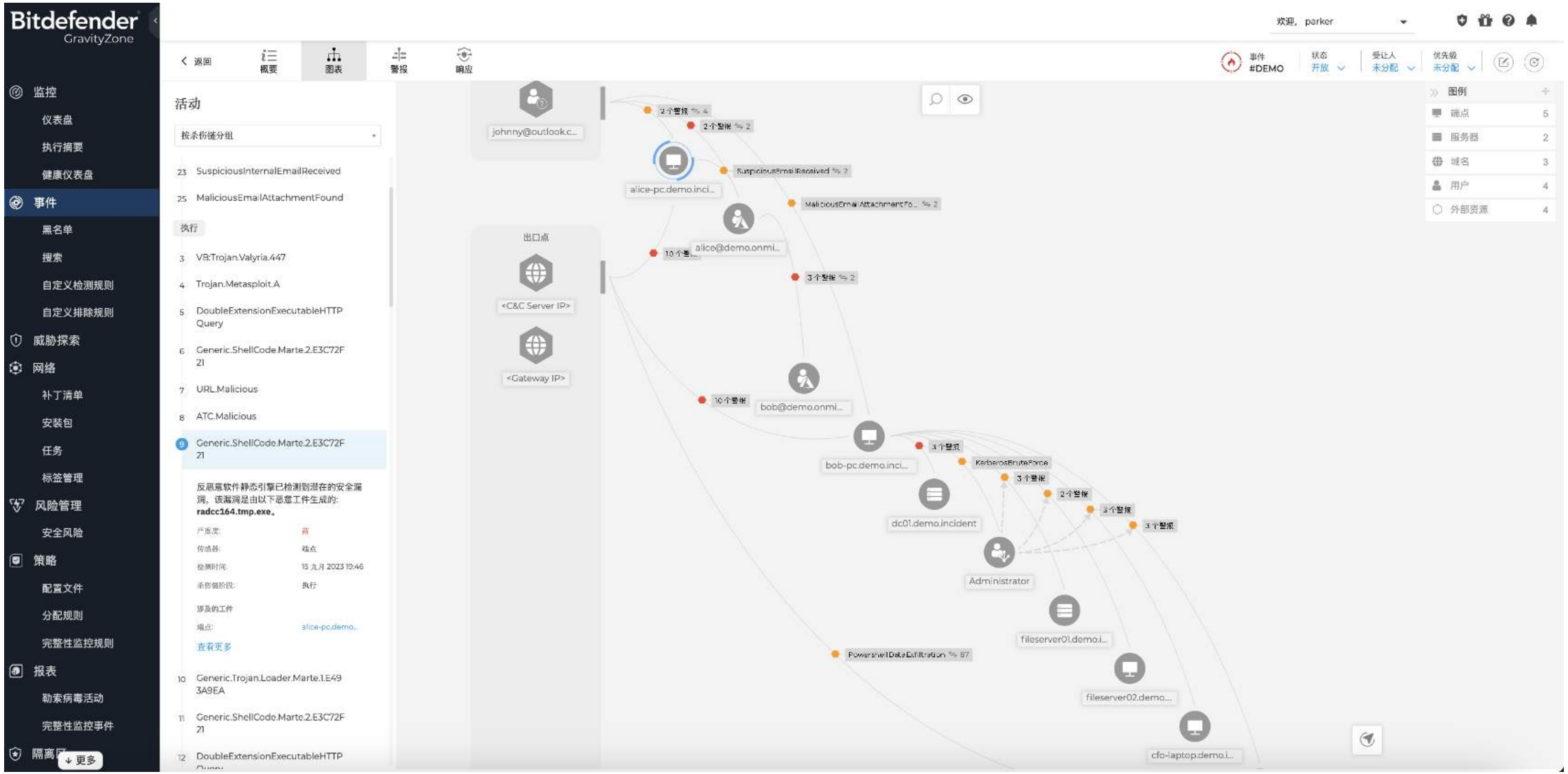


Bitdefender

EDR的下一个飞跃发展　XDR 扩展检测与响应

Bitdefender

XDR 扩展检测与响应

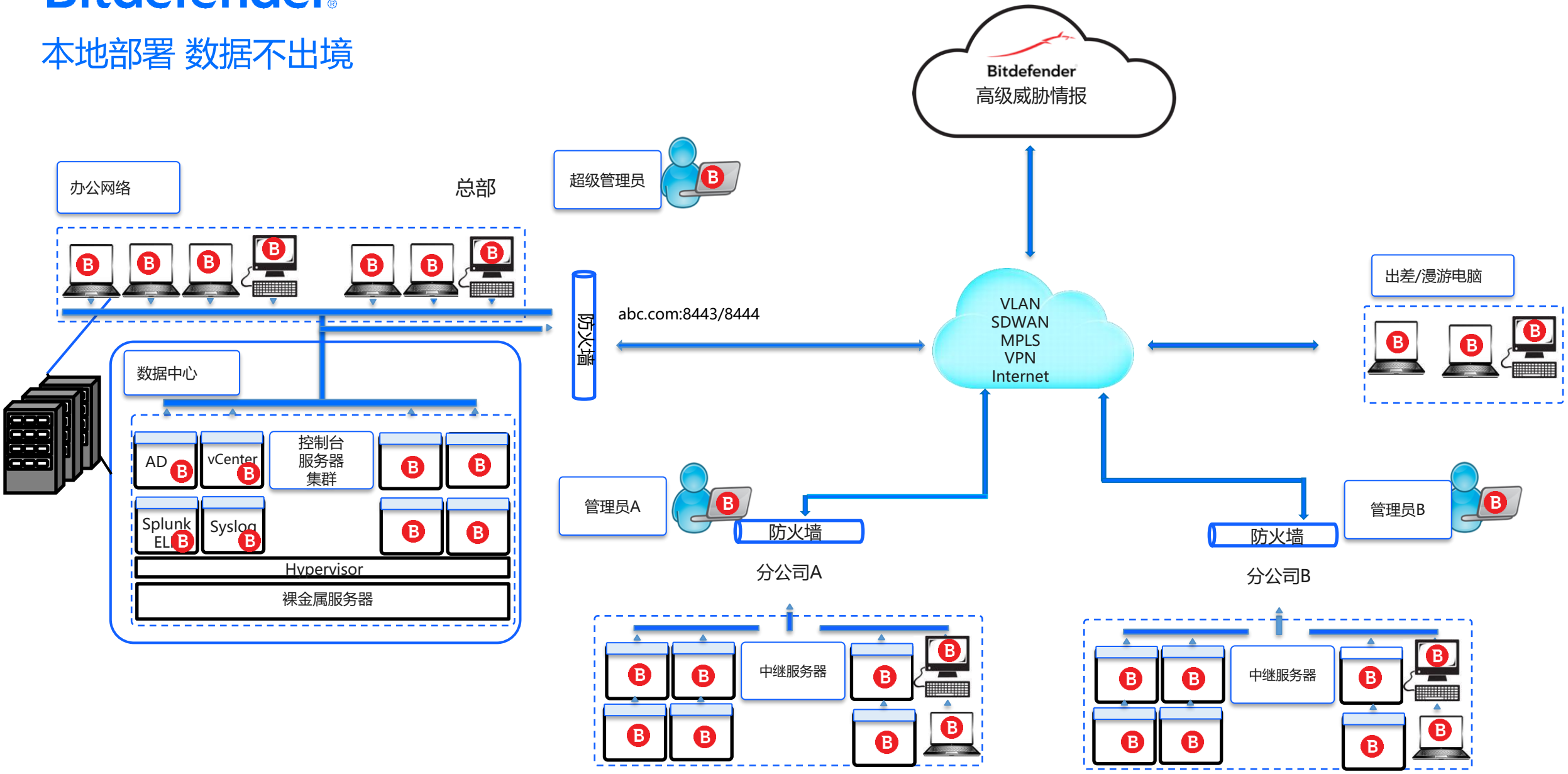


2

方案架构

Bitdefender

本地部署 数据不出境



Bitdefender

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 或在 Ubuntu 20.04 Server上运行脚本安装	厚置被	16	16	200GB	10G 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

Bitdefender

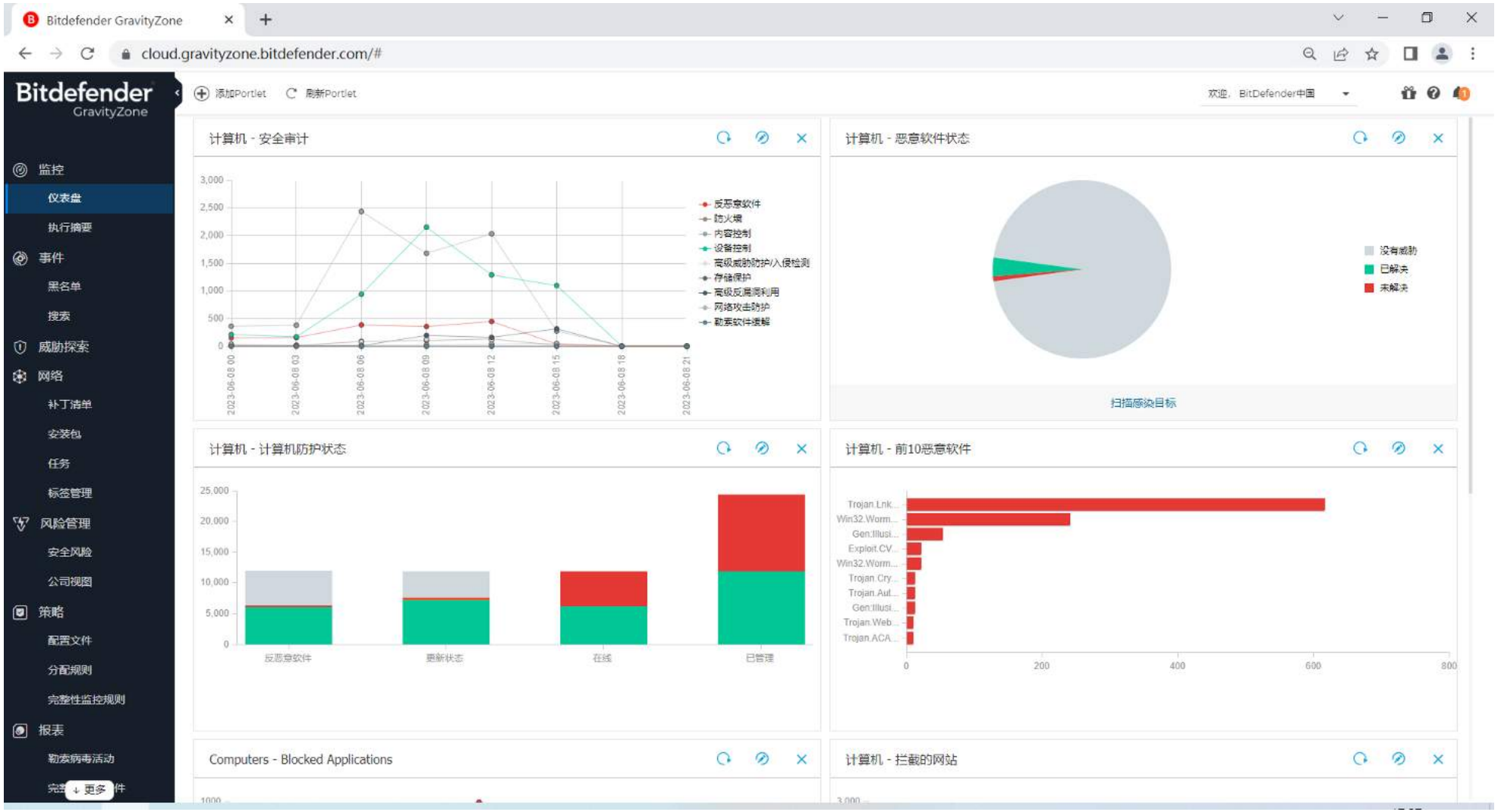
高可用架构 部署资源需求

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1+事件服务器1+更新服务器	导入虚拟化镜像模版 或在 Ubuntu 20.04 Server上运行脚本安装	厚置备	12	16	200GB	10G 或 1G			是，到Bitdefender服务器	
	VM2	BDServer2	数据库服务器 副本成员+Web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+事件服务器2+通讯服务器1			12	16	200GB					
	VM4	BDServer4	负载均衡服务器 均衡对象：Web+通讯服务器+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

Bitdefender

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。

Bitdefender

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
RPM-based		
RHEL 6.10	32-bit, 64-bit	2.6.32-754
CentOS 6.10	32-bit, 64-bit	2.6.32-754
Oracle Linux 6.10 UEK	64-bit	4.1.12-124
Amazon Linux v1 2018.03	64-bit	4.14.x
Debian-based		
Ubuntu 14.04 LTS	32-bit, 64-bit	4.4
Ubuntu 16.04.x	32-bit, 64-bit	4.15

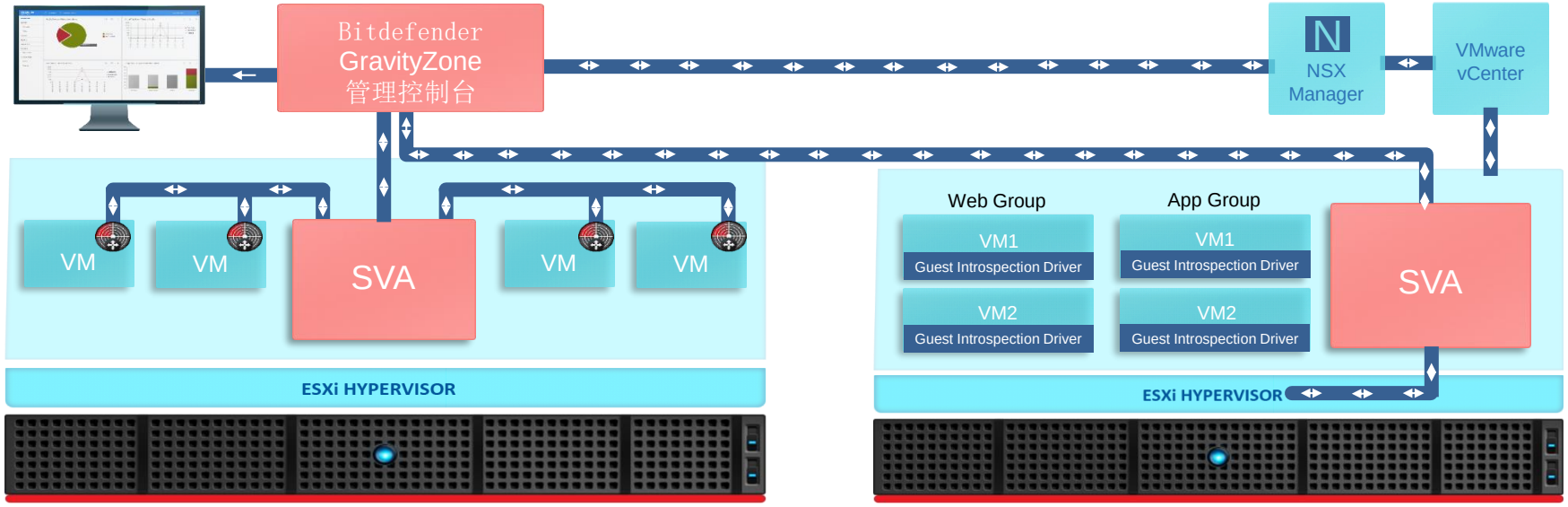
Bitdefender

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。

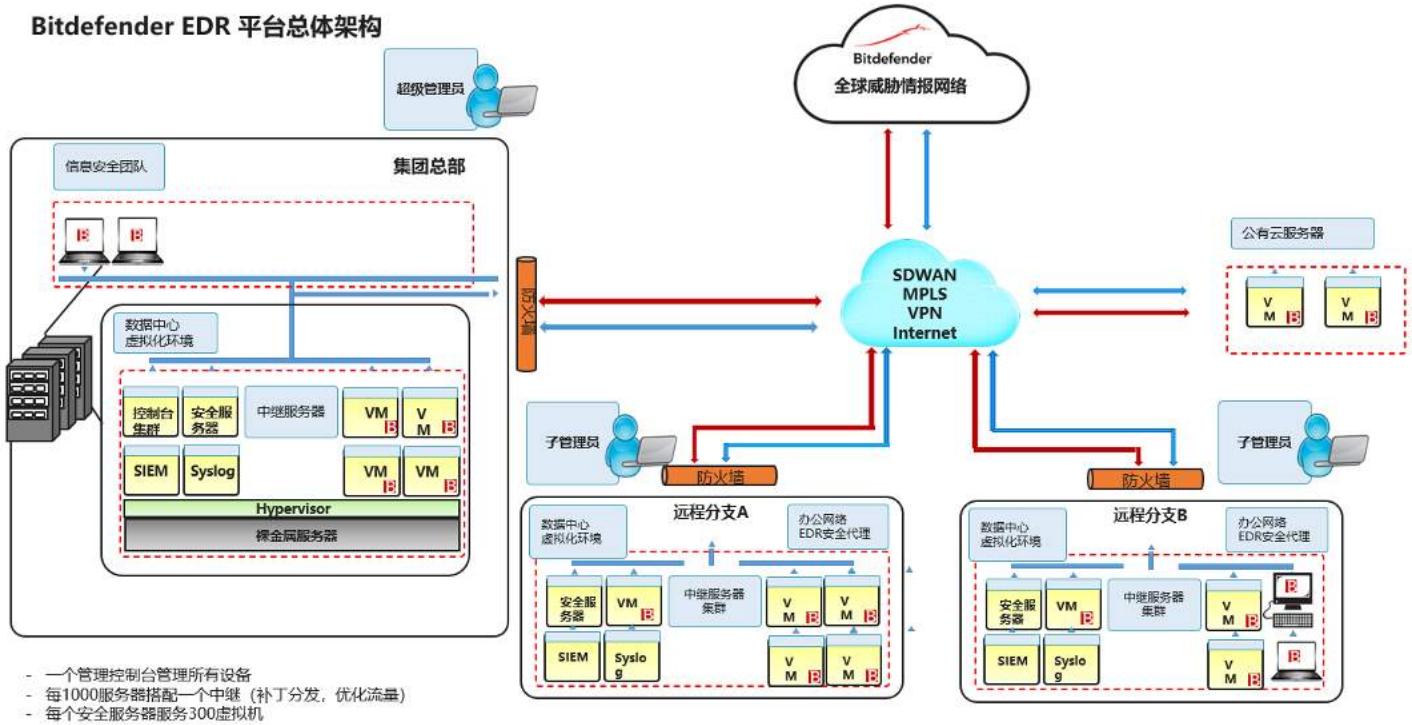


Bitdefender

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

Bitdefender

企业产品案例

为什么选择 Bitdefender

Bitdefender

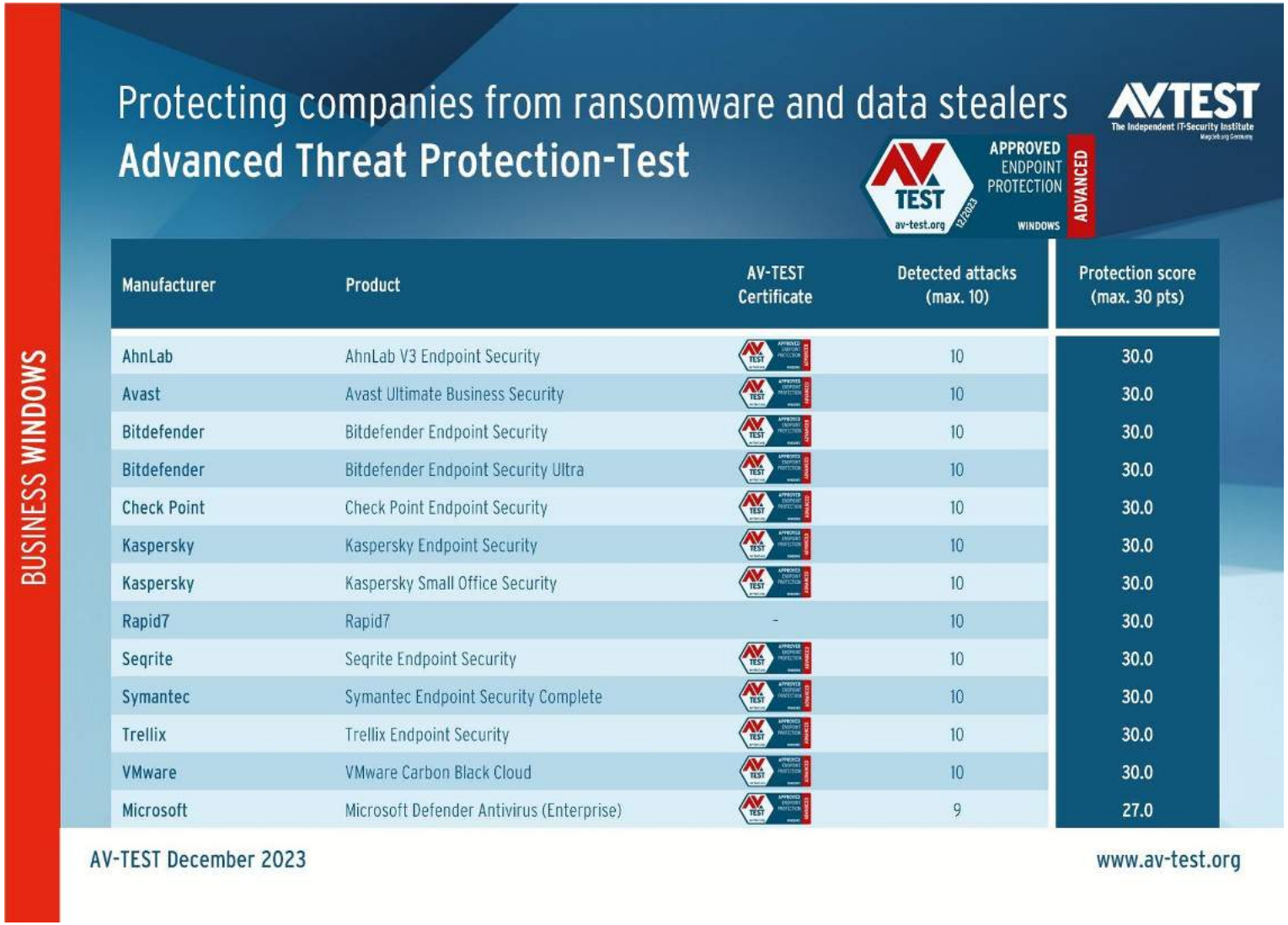
全球顶级的EPP 自动阻止99.5%+ 攻击 AV-Test 2023年度 最佳保护+最佳性能

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

https://www.av-test.org/en/news/av-test-awards-2023-shining-the-spotlight-on-the-best-it-security/

Bitdefender

AV-Test 2024 年2月发布　100% 勒索病毒防护

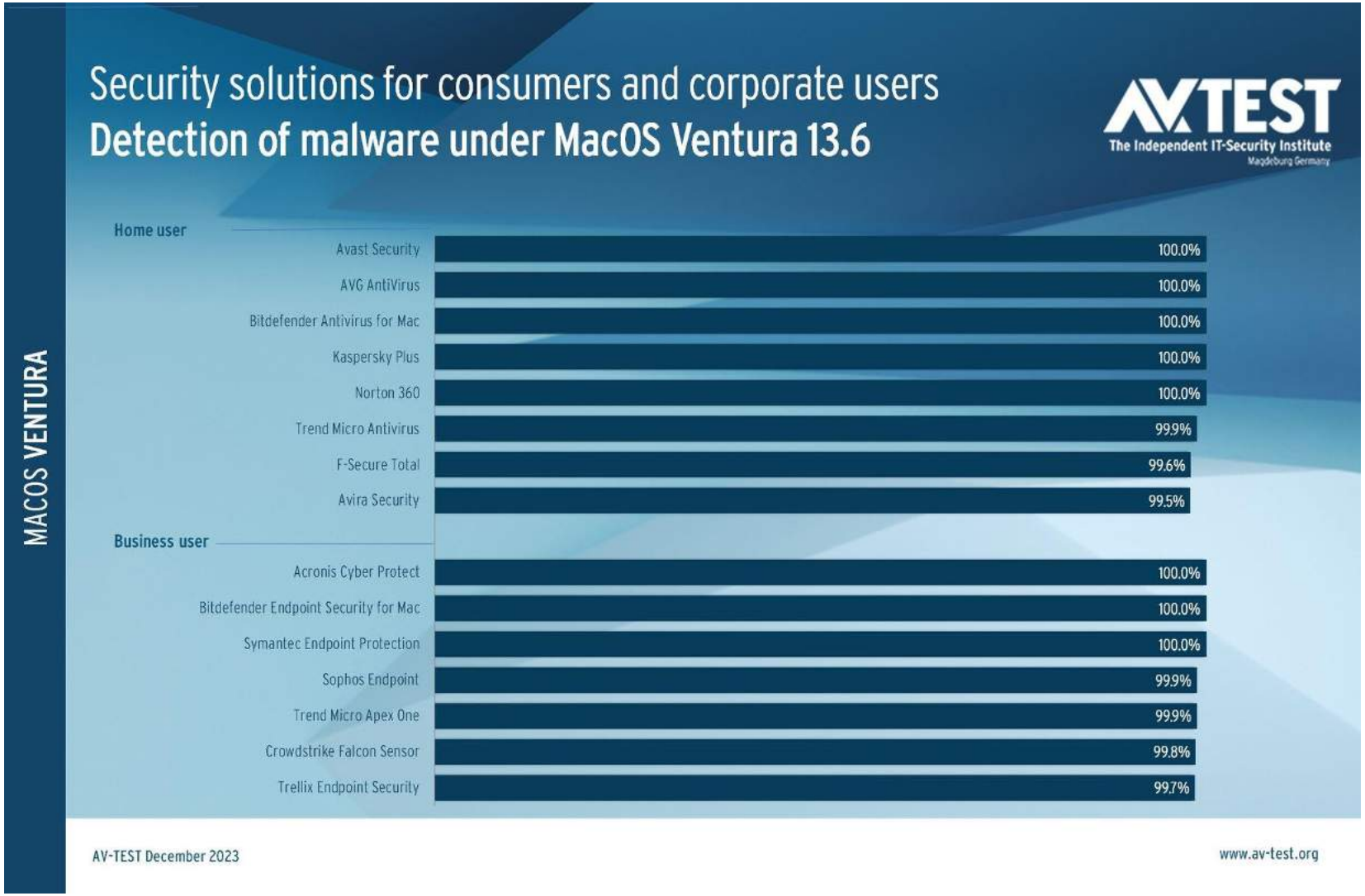


Manufacturer	Product	AV-TEST Certificate	Detected attacks (max. 10)	Protection score (max. 30 pts)
AhnLab	AhnLab V3 Endpoint Security	✓	10	30.0
Avast	Avast Ultimate Business Security	✓	10	30.0
Bitdefender	Bitdefender Endpoint Security	✓	10	30.0
Bitdefender	Bitdefender Endpoint Security Ultra	✓	10	30.0
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

查看完整报告：https://www.av-test.org/en/news/more-protection-against-encryption-and-data-theft/

Bitdefender

AV-Test 2024 MacOS Ventura 13.6 测试成绩



查看报告：https://www.av-test.org/en/news/security-solutions-for-macos-ventura-136-put-to-the-test/

Bitdefender

全球顶级的EPP AV-Comparatives 2023年度报告

	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	***	***	***	***	***	***	***
Bitdefender	***	***	***	***	***	***	***
Avast	***	***	***	**	***	***	***
AVG	***	***	***	**	***	***	***
Avira	***	***	***	*	***	***	***
ESET	***	***	**	***	***	***	*
G Data	***	**	***	**	***	**	***
McAfee	***	***	***		***	**	***
Norton	***	***	**		**	***	**
TotalAV	***	***			***	**	**
Microsoft	*	*	***		***	**	**
Total Defense	**	*	***		***	*	**
F-Secure	**	**	**			**	**
K7		***	**			***	**
Panda		***			*	***	*
Trend Micro		**	*			**	*

Bitdefender

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

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

Bitdefender

行业排名第一的 APT高级持续性威胁防护能力

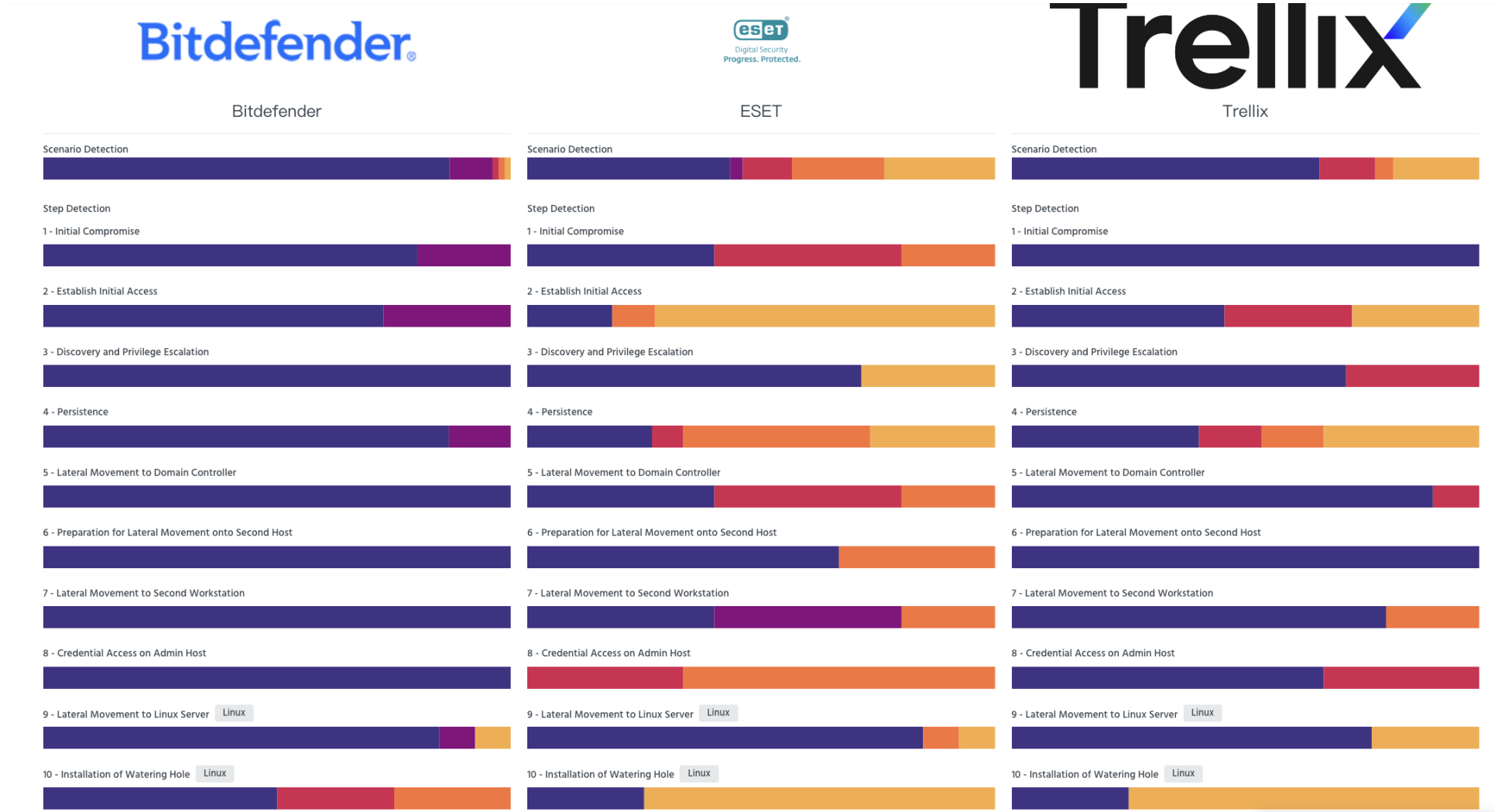
AV-Comparatives 2023 测试报告　HyperDetect 机器学习未开启

	Test scenarios																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	FPs	Score
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/

Bitdefender

Mitre ATT&CK 2023 EDR测评



https://attackevals.mitre-engenuity.org/results/enterprise?vendor=bitdefender&vendor=eset&vendor=trellix&evaluation=turla&scenario=1

Bitdefender

Gartner 2023 端点安全魔力象限　本地私有化部署控制台中最好的厂商

Bitdefender

Forrester Wave™: Endpoint Security, Q4 2023　　端点安全的领导者

Bitdefender

认证

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，并降低安全问题的风险。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的最佳实践建议。

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。

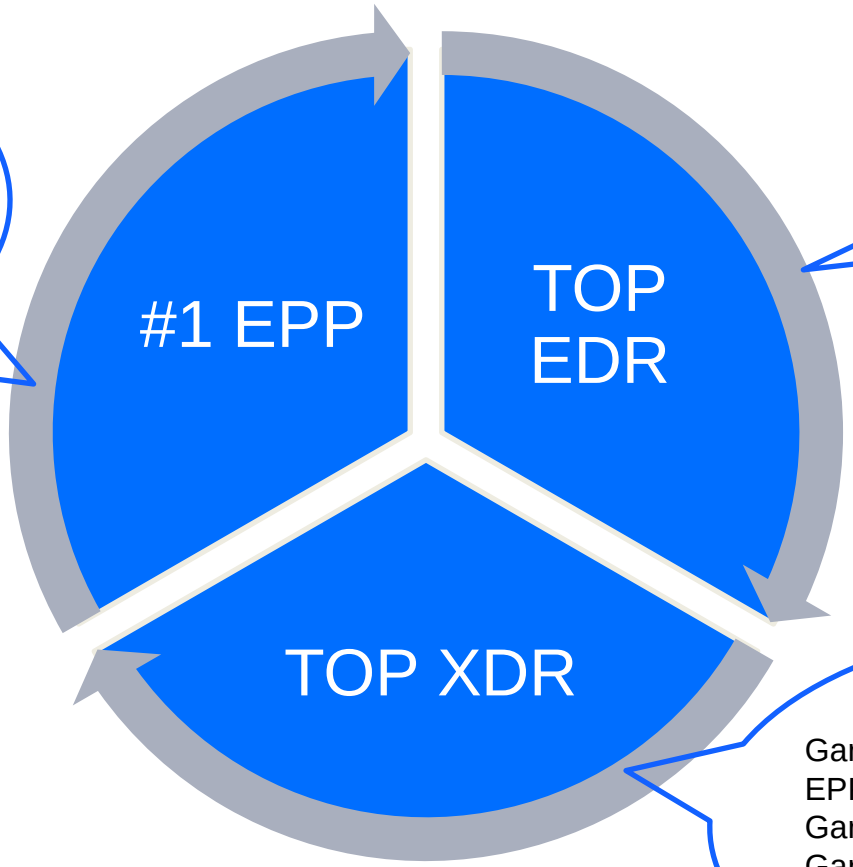
Bitdefender

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



Mitre ATT&CK 连续4年 EDR评估，100%检测

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
Garnter 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