Bitdefender®

勒索病毒防护技术简介

勒索软件概述

勒索软件是一种恶意软件，旨在加密数据、盗窃数据以勒索钱财。 勒索软件受害者必须向攻击者付费，才能获得解密密钥，重新获得数据的访问权。通常需要支付无法追踪的加密货币。不过，付款后也仍然有可能拿不到解密密钥。

对于个人而言，图片、视频或重要文件如果被泄露可能会引起焦虑，但对于公司而言，被勒索的内容包括专有信息、客户信息、账户和支付详细信息或其他有价值的公司数据。

勒索软件几乎总是以金钱为动机，但是高级勒索软件攻击可能具有更广泛的目标，并对公司造成巨大伤害。例如：勒索软件攻击会导致公司无法开展正常业务，导致生存问题。 在极端情况下，甚至会危及人的生命。

最近备受瞩目的勒索软件攻击案例造成了巨大的金钱损失和负面社会影响：
• 2022 年 3 月 1 日，日本丰田汽车公司因零部件供应商受到“勒索软件”攻击,决定停止日本全国所有工厂运行)
• 2022 年 02 月 20 日，全球十大物流公司 Expeditors 遭勒索软件攻击致全球业务受损
• 2022 年 03 月 8 日，三星证实源代码被窃取,科技巨头频陷勒索软件泥潭，黑客组织声称对芯片制造巨头英伟达进行了网络攻击，表示已窃取近 1TB 数据，并公开索要赎金。由于英伟达未满足其勒索要求，Lapsus$公布了包含英伟达 GPU 驱动、挖矿锁算力软件源代码等高度机密数据。

勒索软件可以多种方式出现在受感染的笔记本电脑、台式机或服务器上，通常会拒绝用户访问数据或系统，直到支付赎金：
- 加密敏感和个人文件，无法解密
- 威胁公开发布敏感和个人文件
- 锁定计算机屏幕拒绝完全访问系统
- 阻止某些应用程序运行，从而削弱用户的工作效率

勒索软件适应性强，经过精心设计，可避免被安全软件检测到。 即使是很小的延迟检测，也可以为潜在的不可逆文件加密提供足够的时间。

勒索软件是如何攻击过来的?

勒索软件有许多可行的途径入侵公司，网络犯罪分子在利用技术和人类漏洞方面非常有创意。 尽管进行了多年的安全意识培训，但危险的用户行为仍以极高的比率持续存在，导致对可疑链接的危险点击和考虑不周的应用程序/文件下载。

- 带有恶意链接和恶意文件附件的针对性的网络钓鱼邮件
- 恶意文档下载，无论是用户发起的还是偷渡式下载触发的
- 恶意程序/可执行文件下载，包括虚假软件和虚假产品更新
- 从浏览器发起的内存空间无文件攻击，无需落地文件到磁盘驱动器
- 来自网络文件共享和 USB 传播受感染的文档和文件
- 系统或服务存在漏洞，被漏洞利用攻击
- 弱密码，被攻击者爆破

勒索软件如何防护?

全面的勒索软件防护需要同时在多个方面保持主动警惕，安全必须涵盖在每个方面。

抢先保护——创建勒索软件无法访问的用户文件的防篡改备份副本

阻止和预防——部署不依赖基于签名的检测技术，部署行业顶级的安全方案

监控和早期检测——观察可疑进程和网络活动，关联攻击指标

EDR 和事件响应——没有任何预防措施始终是 100% 有效的，你需要尽快在网络中部署 EDR 安全解决方案，EDR 可实时洞察早期的攻击活动，并主动采取响应

漏洞修补——主动和定期修复操作系统、第三方程序的漏洞，以预防高级攻击

风险配置管理——识别并纠正操作系统配置错误，防止被攻击者利用

用户行为风险监控——识别并纠正员工带来的网络安全风险，例如弱密码，密码重用、点击网络钓鱼邮件中的附件或链接、点击风险链接和下载，登录未加密的网站

应用程序和设备控制—— 监控使用情况，只允许运行所需的应用程序，只允许必要的 USB 连接系统。

击败勒索软件需要了解完整的网络攻击杀伤链，并将防护映射到每个攻击阶段。

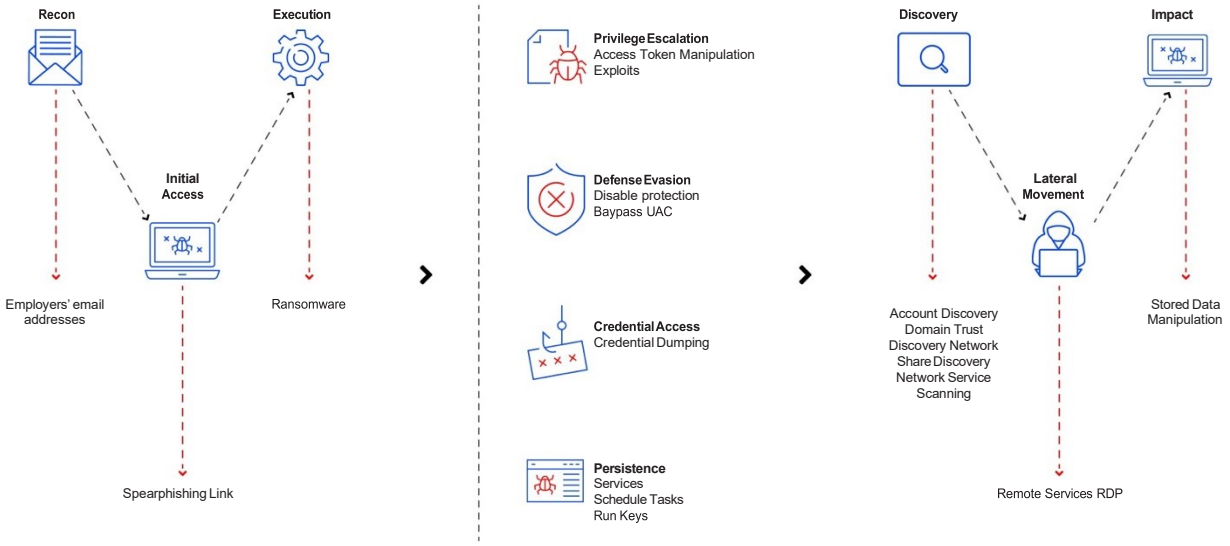


图 1：典型的勒索软件攻击策略和网络攻击杀伤链

Bitdefender 勒索软件防护技术简介

防篡改备份

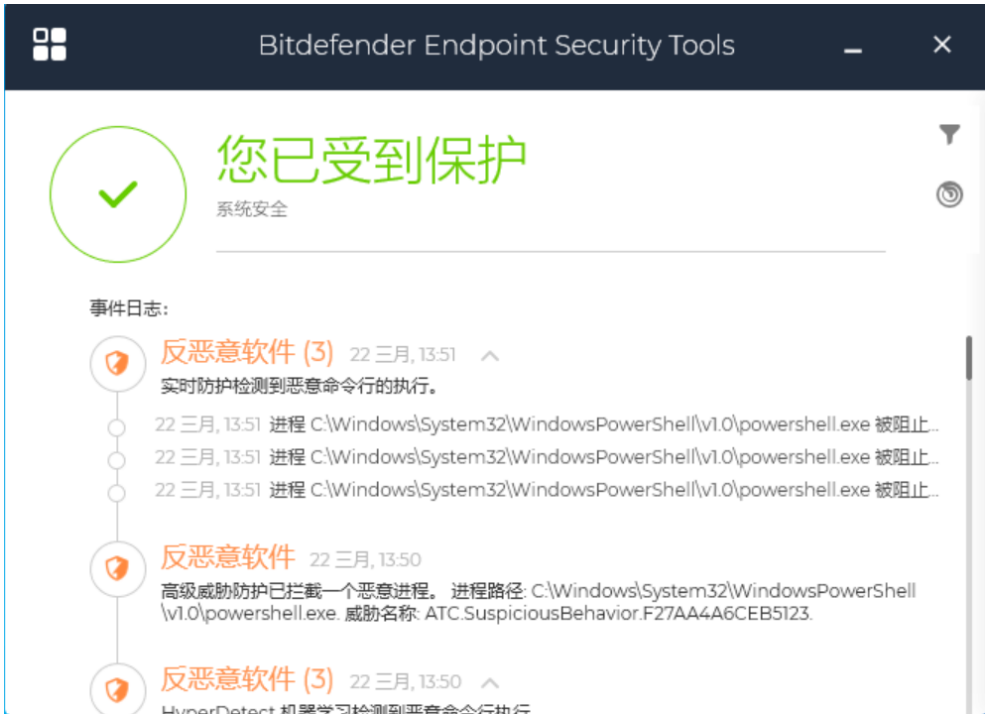
Bitdefender 创建用户文件的自动、最新的防篡改备份副本（非易受攻击的卷影备份），这是免提保护，用户无需做任何事情。 勒索软件无法访问受保护的备份文件。

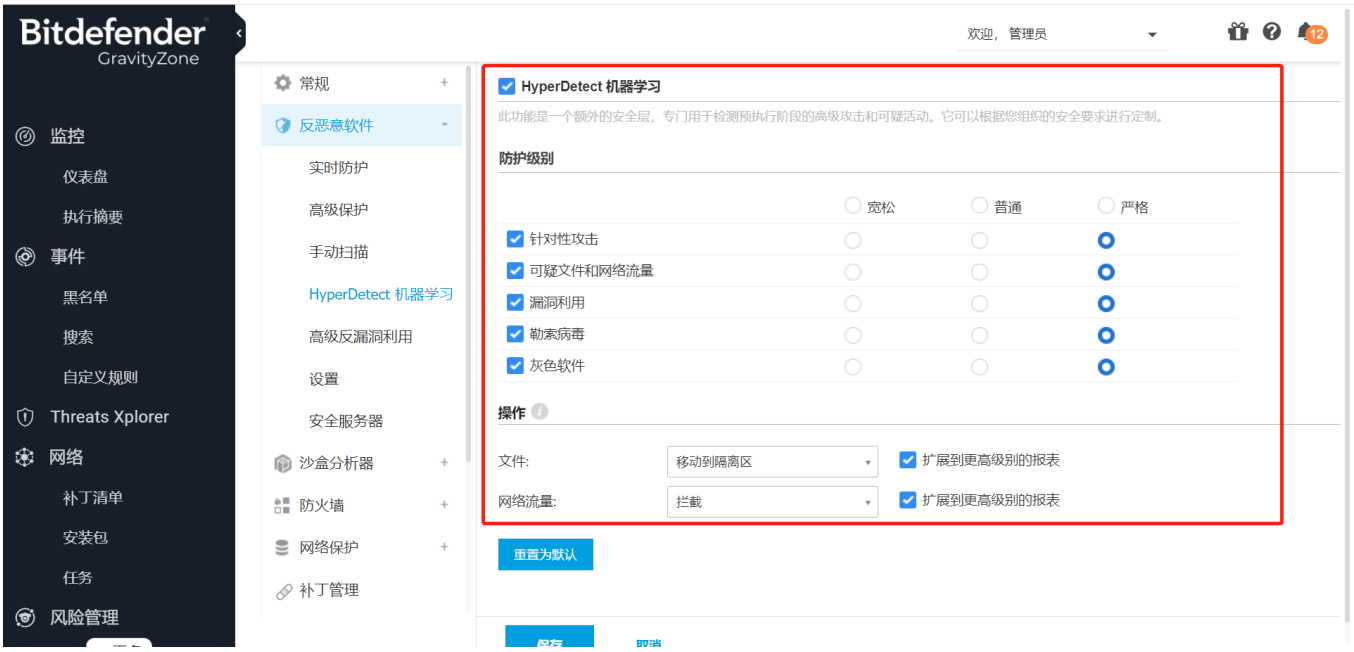
Bitdefender 勒索缓解基于机器学习技术，不依赖特征码，会识别任何未知勒索软件攻击，在加密早期阶段自动阻止攻击，并自动创建早期被加密文件的备份。 Bitdefender 会阻止参与攻击的所有进程并开始自动回滚恶意更改，并立即通知用户。

阻止和预防

无文件攻击防护和 HyperDetect

Bitdefender 会在预预执行阶段自动发现并阻止无文件攻击，防止文件加密并防止攻击者获得系统访问权限。 HyperDetect 使用高度优化的机器学习模型在执行前检测和阻止新的和未知的恶意软件，通过分析代码级别的行为，在网络攻击杀伤链的多个阶段阻止无文件勒索软件。





机器学习反恶意软件

Bitdefender 使用业界最大的样本存储库自动持续训练和改进其恶意软件识别能力，机器学习模型不断接受来自全球 5 亿个端点的 数万亿个样本的训练，这确保了 GravityZone 在恶意软件检测方面的全球领先性，提前预测攻击并应对网络犯罪的增长。

高级反漏洞利用

攻击者使用利用零日漏洞或未修补漏洞的漏洞利用工具包来获得系统立足点。 Bitdefender 高级反漏洞利用技术保护系统内存和易受攻击的应用程序，防止未经授权的进程提升权限和访问资源，保护 LSASS 进程免于泄露密码哈希和安全设置等。

网络攻击防护

网络攻击防护使用启发式行为分析，实时监测主机层的网络活动，在初始访问、凭证访问、发现和横向移动攻击阶段阻止恶意活动。例如，可阻止服务漏洞利用攻击，暴力破解，端口扫描，Samba 攻击，窃取密码，网络漏洞利用，SQL 注入攻击，目录遍历，僵尸网络攻击，恶意网址，远程 IoT 攻击，TOR/Onion 连接等等。

监控和早期攻击检测

高级威胁防护

高级威胁防护以零信任模式运行，持续监控操作系统中运行的所有进程、命令行、注册表修改、文件读/写、加密操作。 它可以自动采取适当的处理措施，包括终止进程和回滚恶意更改。 它在检测未知高级恶意软件（包括勒索病毒）方面非常有效。

EDR 端点检测与响应

并非所有攻击都可以被预防技术检测或阻止，并且某些攻击阶段会随着时间的推移缓慢显现。 EDR 将始终在检测隐蔽攻击，早期攻击方面发挥着重要作用。 GravityZone EDR 自动将多个攻击和危害指标 (IOA/IOC) 与在系统和网络上观察到的恶意活动关联起来，Bitdefender EDR 安全监控您的网络以及早发现可疑活动，并提供抵御网络攻击所需的工具。它将 EDR 分析和事件关联功能扩展到单个端点的边界之外, 使您能够更有效地处理涉及多个端点的复杂网络攻击，促进快速准确的事件响应，从而减少攻击者的停留时间，避免攻击者部署勒索软件到网络中。

用户和系统风险缓解

漏洞修补

黑客一直在寻攻击目标，并利用先进的攻击战术、技术利用操作系统和应用程序中的漏洞来实现他们的目标。GravityZone 的补丁管理模块可帮助公司保持 Windows、Linux 操作系统和第三方应用程序在最新状态。当软件供应商发布补丁来修复漏洞时，目录会自动更新为最新版本。

修复系统配置错误

配置不当的系统为勒索软件攻击敞开大门，包括浏览器安全设置、网络和凭据设置、操作系统安全设置（如开放端口）、启用非必要服务和管理脚本工具（例如 PowerShell）。 GravityZone 扫描系统配置错误，并可以远程自动修复配置错误的机器，主动减少攻击面。

应用程序漏洞

具有已知漏洞 (CVE) 的过时应用程序可能会被勒索软件攻击者利用，滥用程序功能或从 Internet 下载有害内容。风险程序可以更新到更新、更安全的版本，或者如果用户不需要此应用程序，可以从系统中删除。 GravityZone 扫描 CVE 并按严重程度对应用程序的漏洞进行排名，以便管理员可以迅速采取纠正措施。

危险的用户行为

用户每次打开钓鱼邮件、单击恶意链接或下载恶意文件时都会增加勒索软件感染的风险。

GravityZone 人为风险管理会分析用户的浏览网址、打开的文件、访问的文件位置、登录风险网站的方式和位置，并监控弱密码和重复使用密码，以便纠正风险行为。

为什么还需要 Bitdefender 勒索缓解技术

端点上的全面勒索软件保护至关重要，因为端点是通往高价值服务器和其他专有托管信息、客户数据、支付细节和其他高价值知识产权目标的重要跳板。

Bitdefender 勒索软件缓解技术带来的好处包括：

- 确保业务连续性，避免数据被勒索加密
- 提前预防未知勒索软件和勒索攻击技术
- 当备份出现问题时，Bitdefender 仍然能提供可靠的恢复保障
- 防止本地、共享文件夹被勒索加密

Bitdefender 勒索缓解技术用例

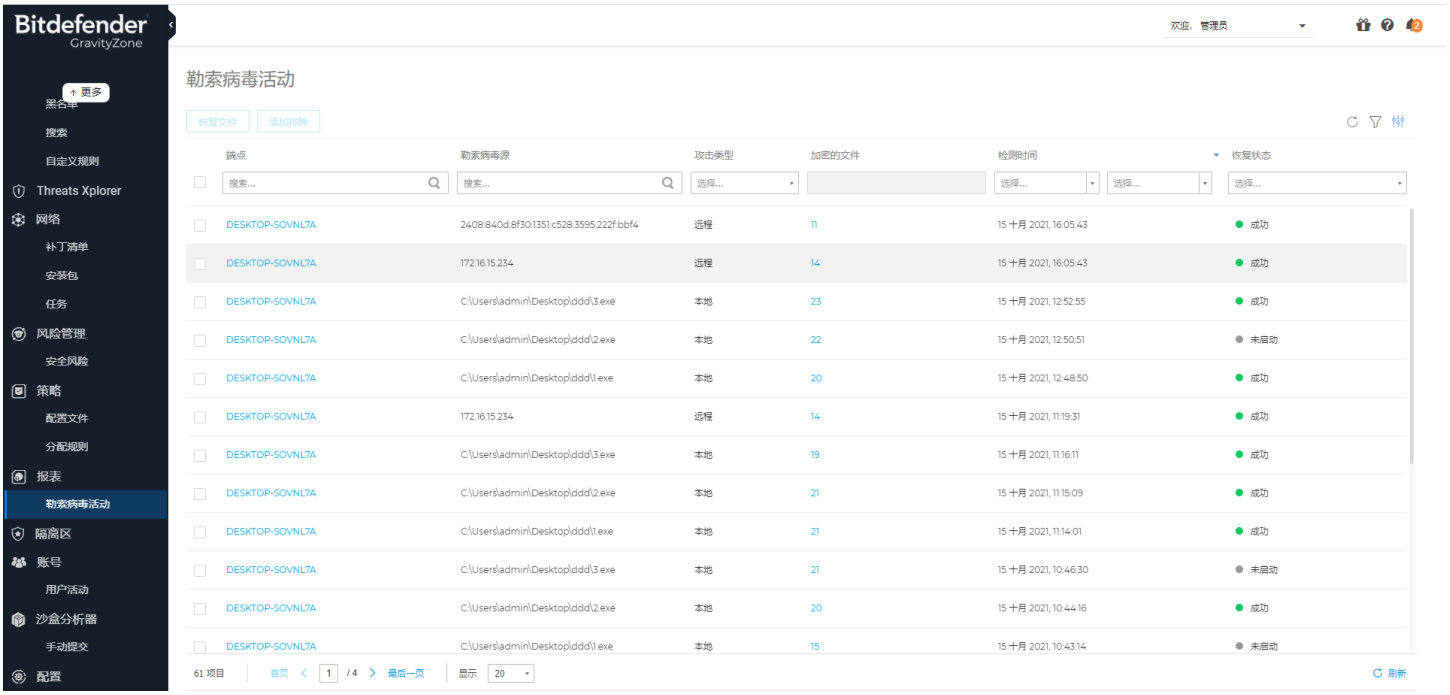
与市场上其它的安全解决方案相比，Bitdefender 涵盖了更多的勒索软件缓解用例，为用户和安全管理员提供了多个级别的工具，以阻止勒索软件攻击。

本地

对于本地勒索软件缓解，管理员可以配置 Bitdefender 安全策略来监控端点进程，自适应技术检测并阻止攻击时，万一勒索软件突破前面的防护层时，勒索缓解技术会立即阻断攻击，介入以自动或手动恢复这些文件。

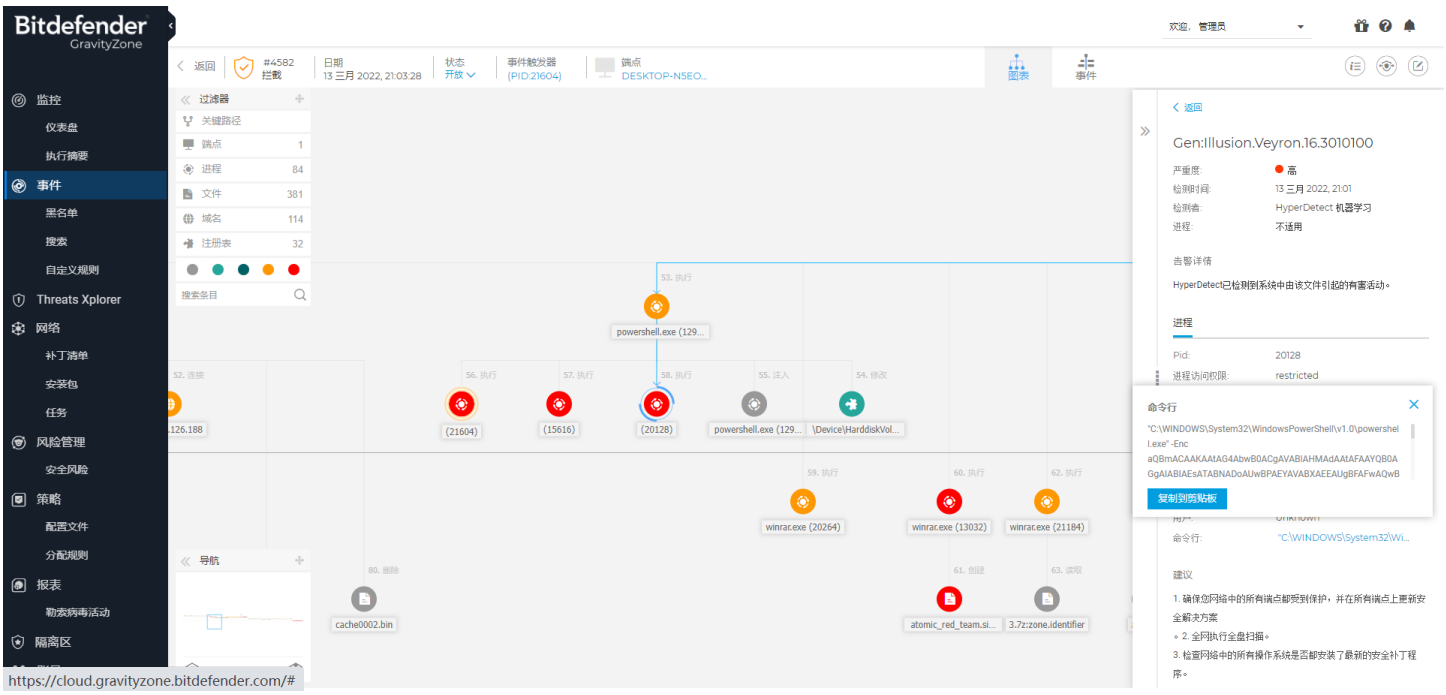
远程

对于远程勒索软件缓解，安全管理员可以启用该技术，监控网络共享文件夹并防止共享的文件被加密。Bitdefender 管理员可以快速运行审计报告，了解有关发起远程勒索软件攻击的 IP 地址，当攻击被阻止时，管理员还可以收到一封电子邮件通知，其中包含有关攻击者 IP 地址的信息。



安全事件管理

在 GravityZone 管理控制台，安全团队可以完全了解攻击杀伤链和受勒索软件攻击影响的文件。Bitdefender EDR 实时检测进程、网络、注册表、用户活动，洞察整个攻击阶段的所有活动。安全管理员可以杀死活动的可疑进程或隔离受感染的文件，还可以将攻击者的 IP 地址永久列入黑名单。



无与伦比的勒索软件防护技术组合

GravityZone 管理控制台和 Bitdefender 端点安全工具在多个级别内置了勒索软件预防和缓解，远远超过了行业中其它的安全解决方案。

GravityZone 无与伦比的勒索软件防护技术组合	
多个阻止层	端点和网络、预执行和访问、文件和无文件
多个检测层	零信任进程监控、注册表监控、代码和命令行检查、HyperDetect
多个恢复层	从本地机器、远程系统或 EDR 事件有效回滚
自适应防护	高级威胁防护、高级反漏洞利用、自适应启发式、可调节机器学习
风险缓解技术	自动漏洞修补、修复系统错误配置、应用程序控制、纠正用户风险行为
防篡改备份	不使用易受攻击的卷影副本，勒索软件无法删除备份
远程阻止勒索软件	阻止远程和网络勒索软件攻击并将攻击者 IP 列入黑名单
企业范围的清理	远程隔离主机，远程结束进程，沙盒分析全网联动判决，添加黑名单、检测规则轻松进行全局文件隔离和删除，全网 IOC 扫描和清理
早期攻击检测	EDR 安全监控您的网络以及早发现可疑活动，并提供抵御网络攻击所需的工具，将攻击者行动的全面实时可视化，提供丰富的上下文和威胁情报，突出关键的攻击路径，可帮助 IT 管理员快速识别、分析和响应安全事件，防止发生勒索。

行业顶级的安全技术

Bitdefender 在行业权威测试和评估中一直名列前茅：

- AV-Test 2019，2020 和 2021 年度最佳保护产品
- AV-Comparatives 2019，2020 和 2021 年度卓越产品
- Mitre ATT&CK 2021 年度 EDR 评估，检测率排名第一产品
- Gartner Peer Insights 2021 年度客户之选

联系 Bitdefendre 预约产品演示和免费试用

亲眼看看，了解 Bitdefender 抵御勒索软件的多种方式。

联系 Bitdefender 中国: 4000-132-568

申请免费试用：https://www.bitdefender-cn.com/business/free-trials.html

关于 Bitdefender

Bitdefender 是全球网络安全的领导者，为 150 多个国家的 5 亿用户提供尖端的端到端网络安全解决方案和先进的威胁防护。全球超过 38%的安全公司使用 Bitdefender 的技术。典型客户包括：奇虎 360，腾讯，百度，阿里巴巴，奇安信，绿盟科技，深信服，Microsoft，Cisco， IBM，软银，诺基亚，TeamViewer，FireEye，Cybereason 等等。Bitdefender 连续 10 年在国际权威测评机构 AV-Test 和 AV-Comparatives 的测试中排名第一。

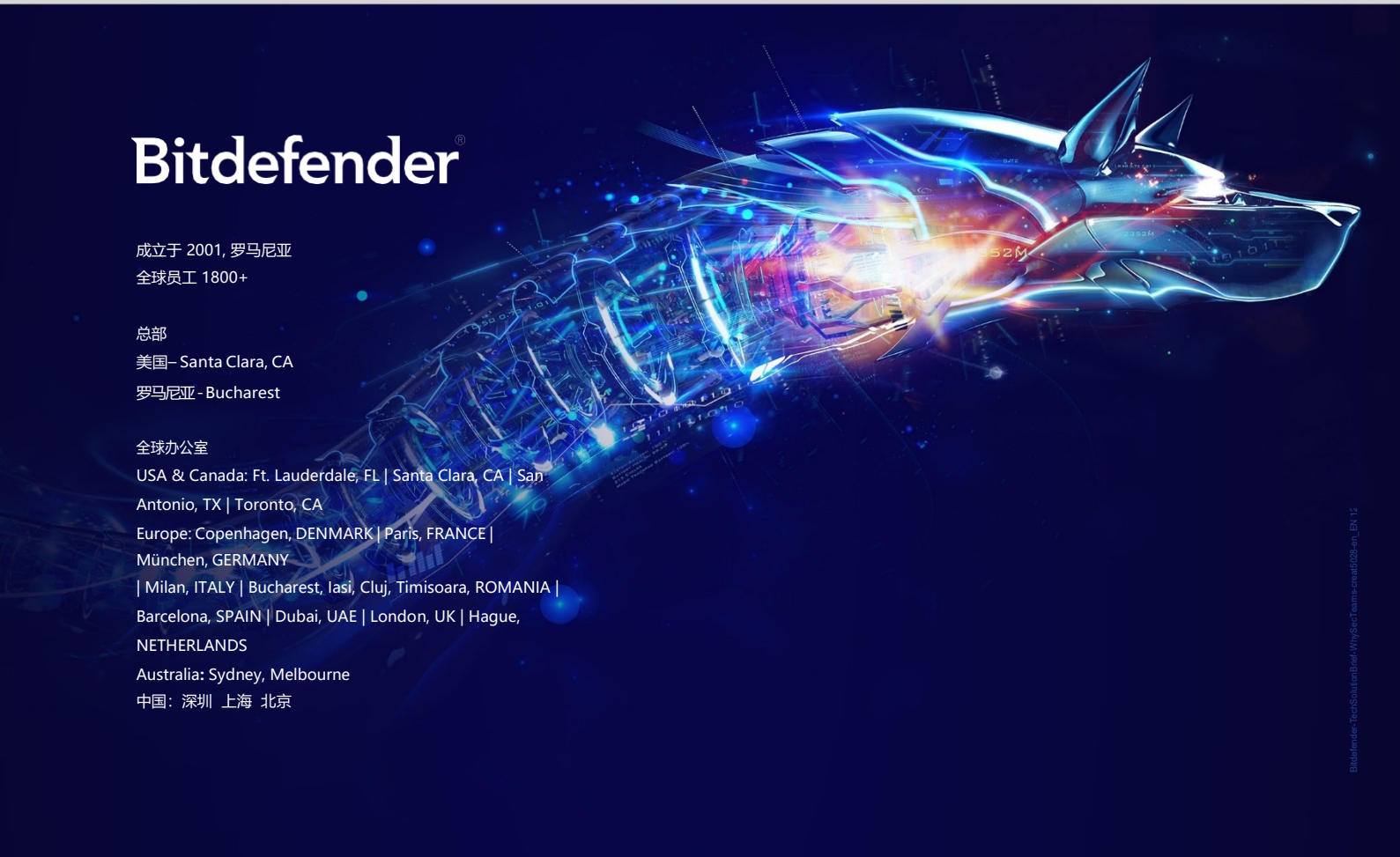
联系我们以获取更多信息和产品演示

请联系我们以安排独立 EDR，Ultra（端点保护+EDR），XDR， MDR 等产品的深入产品演示和讨论，索取产品白皮书和 PPT 等。

联系电话：4000-132-568

关注 Bitdefender 公众号

CRN AV-TEST AV Gartner 451 Research FORRESTER IDC GLOBAL Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX



Bitdefender®

成立于 2001, 罗马尼亚
全球员工 1800+

总部
美国– Santa Clara, CA
罗马尼亚 - Bucharest

全球办公室
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne
中国：深圳 上海 北京

Bitdefender-TechSolutionBrief-WhySecTeams-sreat5008-en_EN 12