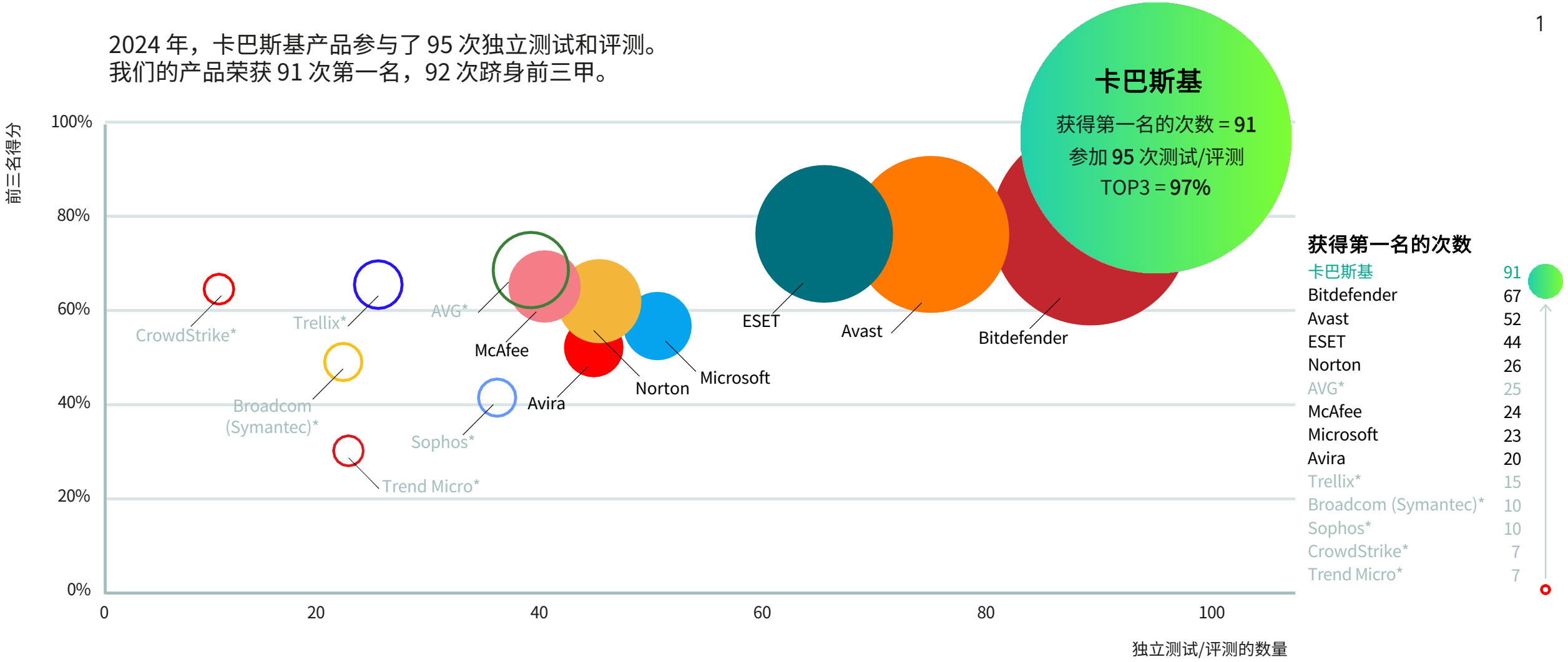
卡巴斯基保护：久经考验，屡获殊荣*

2024 年，卡巴斯基产品参与了 95 次独立测试和评测。
我们的产品荣获 91 次第一名，92 次跻身前三甲。



MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION
*kaspersky.com/top3

* 备注：
- 根据 2024 年针对企业、消费者和移动产品的独立测试结果综述。
- 汇总结果包括以下机构进行的独立测试：AV-Comparatives、AV-TEST、MRG Effitas、SE Labs、Testing Ground Labs、Virus Bulletin。
- 这些程序中执行的测试会评估针对已知、未知和高级威胁的所有防护技术。
- 气泡的大小反映了获得的第一名的次数。
- 标有 * 的供应商参与测试的次数不到测试总数的 35%，因此它们作为补充添加到图表中。

2024 年 TOP3 指标说明

TOP3 指标反映了一家供应商在一个日历年内参与独立比较测试的成功程度。

成功的主要特征是 TOP3 分数，它显示了一家供应商及其产品在报告期内参与的独立测试中获得第一、第二或第三名的次数。TOP3 分数的计算方式是将供应商的 TOP3 计数除以该供应商的参与计数。

每个参与的供应商的 TOP3 分数 都是分别独立计算的，然后相互比较。

1. 根据测试的不同，最终测试结果可能会有所不同，有的测试为所有参与的供应商授予奖项，有的测试只要求提供检测率和误报列表。
   供应商每在一次测试中赢得奖项或排名前三，其 TOP3 计数就会加一。该计数不能因同时获奖并排名前三而增加两次。
   多家供应商可能在检测率或汇总结果上取得相同的结果，或者赢得相同等级的奖项。在这种情况下，这些供应商在同一测试中共享同一排名。
   对于检测率或汇总结果，结果较低的供应商的排名计算为“较高排名的供应商数量 + 1”。例如，排名顺序“1,1,2,3”是不可能出现的，而**“1,1,3,4”**或**“1,2,2,4”**或**“1,1,1,1,1,6”**是可能的。在最新的排名顺序中，只有加粗的供应商的 TOP3 计数会递增。
   关于奖项，请参阅以下测试说明中列出的规则说明。

2. 供应商的一个产品每参与一项测试/评测/综述，该供应商的参与计数就会加一。
   在某些测试中，一个供应商的多个产品可能参加同一测试。在这种情况下，由于所有产品都会增加该供应商的参与计数，因此参与计数可能高于测试总数。

只有参与 35% 或更多测试的供应商的结果会在图表中展示。

提交 2024 年所获分数的截止日期为 2025 年 3 月 8 日，此日期之后不能再增加任何测试/评测。

参与 TOP3 测评的安全供应商包括：AhnLab、Avast、AVG、Avira、Bitdefender、Broadcom (Symantec)、CrowdStrike、ESET、F-Secure、卡巴斯基、McAfee、Microsoft、Norton、Trellix、Trend Micro、WithSecure。本文档的末尾提供了参与者的完整列表。

	参与的测试次数	获得前三名的次数	TOP3 分数 (%)	获得第一名的次数
卡巴斯基	95	92	97%	91
Bitdefender	89	69	78%	67
Avast	75	57	76%	52
ESET	66	50	76%	44
AVG*	38	26	68%	25
Trellix*	26	17	65%	15
McAfee	40	26	65%	24
CrowdStrike*	11	7	64%	7
Norton	45	28	62%	26
Microsoft	51	29	57%	23
Avira	44	23	52%	20
Broadcom (Symantec)*	23	11	48%	10
Sophos*	36	15	42%	10
Trend Micro*	23	7	30%	7

*虽然 AVG、Broadcom (Symantec)、CrowdStrike、Sophos、Trellix 和 Trend Micro 只参与了测试总数的 34%、21%、10%、32%、23% 和 21%，但我们认为在图表中显示这些供应商的结果还是有价值的。

2024 年 TOP3 指标说明

这些测试针对各种类型的恶意软件进行，
包括高级威胁以及误报。

具体威胁

APT

- AV-Comparatives。高级威胁防护测试：消费级和企业级
- AV-Comparatives。端点防御与响应 (EPR) 测试
- AV-TEST。高级 EDR 测试
- AV-TEST。高级威胁防护 (ATP) 测试：消费级和企业级
- SE Labs。企业高级安全 (EDR) – 检测

勒索软件

- AV-Comparatives。高级威胁防护测试：消费级和企业级
- AV-Comparatives。端点防御与响应 (EPR) 测试
- AV-Comparatives。企业安全测试
- AV-Comparatives。恶意软件保护测试
- AV-Comparatives。真实世界防护测试
- AV-TEST。高级威胁防护 (ATP) 测试：消费级和企业级
- AV-TEST。双月认证：个人版和企业版产品
- MRG Effitas。360 度评估和认证
- SE Labs。企业高级安全 (EDR) - 检测
- SE Labs。端点安全 (EPS)：企业测试
- SE Labs。端点安全 (EPS)：家庭测试
- SE Labs。端点安全 (EPS)：中小企业测试

钓鱼

- AV-Comparatives。反钓鱼测试
- SELabs：电子邮件安全服务

无文件

- AV-Comparatives。高级威胁防护测试：消费级和企业级
- AV-Comparatives。端点防御与响应 (EPR) 测试
- AV-TEST。高级 EDR 测试
- AV-TEST。高级威胁防护 (ATP) 测试：消费级和企业级
- MRG Effitas。360 度评估和认证
- SE Labs。端点安全 (EPS)：企业测试
- SE Labs。端点安全 (EPS)：家庭测试
- SE Labs。端点安全 (EPS)：中小企业测试

漏洞利用

- AV-Comparatives。高级威胁防护测试：消费级和企业级
- MRG Effitas。360 度评估和认证
- SE Labs。企业高级安全：EDR 检测
- SE Labs。端点安全 (EPS)：企业测试
- SE Labs。端点安全 (EPS)：家庭测试
- SE Labs。端点安全 (EPS)：中小企业测试

真实世界测试

- AV-Comparatives。高级威胁防护测试：消费级和企业级
- AV-Comparatives。企业安全测试
- AV-Comparatives。真实世界防护测试
- AV-TEST。高级威胁防护 (ATP) 测试：消费级和企业级
- AV-TEST。半月认证一次的客户和企业
- MRG Effitas。360 度评估和认证
- SE Labs。端点安全 (EPS)：企业测试
- SE Labs。端点安全 (EPS)：家庭测试
- SE Labs。端点安全 (EPS)：中小企业测试

ANDROID 测试

- AV-Comparatives。移动安全评测
- AV-TEST。Android 移动安全产品测试：消费级
- MRG Effitas。Android 360 度评估计划
- Testing Ground Labs。Android 恶意软件检测测试：消费级和企业级

MAC 测试

- AV-Comparatives。Mac 安全测试与评估
- AV-TEST。Mac 检测和性能测试：消费级和企业级

专门测试

- AV-Comparatives。LSASS 凭证转储认证测试
- AV-Comparatives。进程注入认证测试
- AV-Comparatives。VPN 测试
- AV-Comparatives。家长控制认证
- AV-TEST。家长控制认证测试
- AV-TEST。VPN 附加安全功能评估

误报 (FP)

- 上述所有测试均包括误报测量

2024 年 TOP3 指标说明

以下测试于 2024 年进行，用于计算指标。
测试实验室按字母顺序列出。

AV-Comparatives

- **年度产品**

  此年度奖项在年底颁发给在整年测试周期中获得最高奖项的消费级相关产品，涉及以下测试：两项恶意软件防护测试 (MPT) + 两项真实世界防护测试 (RWPT) + 两项性能测试 + 高级威胁防护测试（ATP，以前称为增强版真实世界测试）。根据 AV-Comparatives 的规则，如果两个或更多产品获得相同的最高分，该奖项将授予单项分数最高且上一年未获得该奖项的产品。该印章在 TOP3 指标中被视为第一名。

  被提名但没有获得“年度产品”奖的产品将代表其供应商获得“杰出产品”评级，这在 TOP3 指标中被视为第二名。

  在整个测试周期中获得至少 90 分的产品将代表其供应商获得“顶级排名”评级，这在 TOP3 指标中被视为第三名。其余产品的 TOP3 计数不会增加。

  在年底，还将为具体测试（MPT、RWPT、性能、ATP）中取得最佳结果的产品颁发奖牌（“金牌”、“银牌”、“铜牌”）。由于这些测试结果已经计入整体 TOP3 指标，因此自 2015 年起，奖牌本身不再计入其中。

  在 AV-Comparatives 测试中，只有奖项才能增加 TOP3 计数。

- **恶意软件保护测试**

  该测试的前身为文件检测测试，包括执行测试文件。该测试每年进行两次，相应地也计入指标两次。测试由两部分组成：检测率和误报。

  产品将获得以下奖项：“高级+”、“高级”、“标准”或“通过测试”。只有获得“高级+”的产品才能让其供应商的 TOP3 计数加一。

- **真实世界防护测试**

  该测试持续四个月，主要使用当前可见和相关的恶意网站/恶意软件进行测试，并在半年报告中确定结果。该测试每年进行两次，相应地也计入指标两次。由于所有产品组件在整体保护中都发挥着重要作用，因此在该类别取得的结果可以很好地反映反恶意软件产品在真实世界场景中的效率。

  产品将获得以下奖项：“高级+”、“高级”、“标准”或“通过测试”。只有获得“高级+”的产品才能让其供应商的 TOP3 计数加一。

- **高级威胁防护测试：消费级和企业级**

  该测试使用黑客和渗透技术，允许攻击者以特定的外部计算机系统为目标，并评估安全产品抵御此类攻击的效果。该测试可检查对定向高级威胁（例如漏洞利用和无文件攻击）的防护。

  虽然默认情况下预期对消费级主测试系列的所有产品都进行测试，但供应商有机会在测试开始前选择退出此测试，这就是并非所有供应商都包含在此测试中的原因。该测试每年执行并计入指标一次。消费级和企业级相关产品分别进行评估。

  消费级产品获得以下奖项：“高级+”、“高级”、“标准”或“通过测试”。只有获得“高级+”的产品才能让其供应商的 TOP3 计数加一。

  企业级产品如在测试中阻止 15 种攻击中的至少 8 种，并且未阻止非恶意操作，将获得测试实验室的认证，并让其供应商的 TOP3 计数加一。

- **端点防御与响应 (EPR) 测试**

  该测试每年执行并计数一次，可评估安全解决方案对定向攻击的响应能力（主动响应、被动响应），以及采取补救措施、调查攻击性质、以易于访问的形式收集和显示有关入侵指标的信息的能力。Enterprise EPR CyberRisk Quadrant 会将每种产品防止泄露的有效性、由此计算出的节省成本、产品购买成本以及产品的准确性成本等因素纳入考量。

  产品将获得以下三个认证级别之一：“战略领导者”、“网络风险预见者”和“强大挑战者”，或者不获得认证。只有获得“战略领导者”认证的产品才能让其供应商的 TOP3 计数加一。

2024 年 TOP3 指标说明

以下测试于 2024 年进行，用于计算指标。
测试实验室按字母顺序列出。

- **进程注入认证测试**

  该测试每年执行并计入指标一次。它侧重于评估 AV/EPP/EDR 产品在初始访问场景范围内对进程注入和 shellcode 执行的预防和检测能力。

  只有获得认证的产品才能让其供应商的 TOP3 计数加一。

- **LSASS 凭证转储认证测试**

  该测试每年执行并计入指标一次。它评估企业安全产品在多大程度上确定其强化措施能够防御对 Windows 本地安全授权子系统服务 (LSASS) 的攻击。

  只有获得认证的产品才能让其供应商的 TOP3 计数加一。

- **企业安全测试**

  该测试每年发布两次。相应地，计入指标两次。报告包括对各种企业级安全产品的评测，并评估各类别下的防护效率，例如对不同恶意软件集、网站和漏洞的防护率、误报水平以及对系统性能的影响。

  如果产品在恶意软件防护测试中达到至少 90% 的防护率，对常见的企业软件没有误报，并且在整体真实世界保护测试中达到至少 90% 的防护率，对任何干净软件/网站的误报少于 100 次，且没有重大性能问题，将获得测试实验室的认证，并让其供应商的 TOP3 计数加一。

- **反钓鱼测试**

  该测试每年执行并计入指标一次，模拟一种常见情况：用户在浏览网页时依赖其安全产品提供的反网络钓鱼保护。测试由两部分组成：检测率和误报。

  如果所有产品均实现零误报，则防护率排名前三的产品的供应商 TOP3 计数将加一。

  如果所有产品均出现误报，则只有通过认证的产品才能让其供应商的 TOP3 计数加一。

- **移动安全评测**

  该评测每年执行并计入指标一次，包括恶意软件防护测试以及附加功能（防盗、电池消耗等）概述。

  如果所有产品均实现零误报，则防护率排名前三的产品的供应商 TOP3 计数将加一。

  如果所有产品均出现误报，则只有通过认证的产品才能让其供应商的 TOP3 计数加一。

- **Mac 安全测试与评估**

  该评测每年执行并计入指标一次，根据产品功能列表对各种 Mac 保护产品进行评估，并测量各类别的保护级别，例如对单独的 Mac 和 Windows 相关恶意软件集的检测率以及误报水平。

  如果所有产品均实现零误报，则防护率排名前三的产品的供应商 TOP3 计数将加一。

  如果所有产品均出现误报，则只有通过认证的产品才能让其供应商的 TOP3 计数加一。

- **家长控制认证**

  该测试每年执行并计入指标一次，评估安全产品阻止儿童访问有害网站的效率。

  只有阻止了至少 98% 的色情网站，对儿童友好网站零误报，并且在评测过程中没有严重的未解决错误（或设计缺陷）的产品才能获得认证，并让其供应商的 TOP3 计数加一。

- **VPN 认证测试**

  该测试每年执行并计入指标一次，评估 VPN 产品在安全、隐私、下载速度、上传速度和延迟等关键方面的性能表现。

  只有获得认证的产品才能让其供应商的 TOP3 计数加一。

2024 年 TOP3 指标说明

以下测试于 2024 年进行，用于计算指标。
测试实验室按字母顺序列出。

AV-TEST

- **最佳保护奖：消费级和企业级**

  该年度奖项每年颁发一次，获得全年“保护”类别最佳成绩（每两个月进行一次认证）的产品将被授予此奖项。消费级和企业级相关产品分别进行评估。

  只有获得此奖项的产品才能让其供应商的 TOP3 计数加一。

- **最佳可用性奖：消费级和企业级**

  该年度奖项每年颁发一次，获得全年“可用性”类别（指防误报）最佳成绩（每两个月进行一次认证）的产品将被授予此奖项。消费级和企业级相关产品分别进行评估。

  只有获得此奖项的产品才能让其供应商的 TOP3 计数加一。

- **最佳 Android 安全奖：消费级**

  该年度奖项每年颁发一次，获得全年 Android 安全测试最佳成绩的产品将被授予此奖项。

  只有获得此奖项的产品才能让其供应商的 TOP3 计数加一。

- **最佳 Mac 安全奖：消费级和企业级**

  该年度奖项每年颁发一次，获得全年 Mac 安全测试最佳成绩的产品将被授予此奖项。消费级和企业级相关产品分别进行评估。

  只有获得此奖项的产品才能让其供应商的 TOP3 计数加一。

- **最佳高级威胁防护奖：消费级和企业级**

  该年度奖项每年颁发一次，获得整个日历年期间高级威胁防护测试最佳成绩的产品将被授予此奖项。消费级和企业级相关产品分别进行评估。

  只有获得此奖项的产品才能让其供应商的 TOP3 计数加一。

- **双月认证：消费级和企业级**

  这个一年之久的认证系列由消费级和企业级两部分组成，每个部分又分为六个单独的、为期两个月的测试，测试结果在每个偶数月发布，即，该测试计入指标 6 次。消费级和企业级相关产品分别进行评估。所有参与产品均接受评估，并获得“保护”、“性能”和“可用性”类别的分数。各个类别所获分数的总和即为总分；排名前三的产品可以让其 TOP3 计数加一。

- **高级威胁防护测试：消费级和企业级**

  该测试计入指标七次（十二月、二月、四月、六月、八月、十月、十二月）。消费级和企业级相关产品分别进行评估。该测试评估端点解决方案对部署勒索软件和数据窃取程序的 APT 攻击的检测和威胁防御，且不对正常操作产生误报的能力。执行的攻击链分成不同阶段，分别归因于 MITRE ATT&CK 的不同 TTP。各个阶段所获分数的总和即为总分；排名前三的产品可以让其 TOP3 计数加一。

2024 年 TOP3 指标说明

以下测试于 2024 年进行，用于计算指标。
测试实验室按字母顺序列出。

- **高级 EDR 测试**

  该测试每年执行并计入指标一次，衡量安全解决方案识别和阻止通常与高级持续性威胁 (APT) 相关的恶意活动的有效性。该研究包括在两种不同的检测场景中模拟一系列红队攻击，每种场景都包含攻击者可能采用的各种战术和技术。

  只有获得认证的产品才能让其供应商的 TOP3 计数加一。

- **Android 移动安全产品测试：消费级**

  这个一年之久的认证系列评估各种适用于 Android 的安全保护产品，仅包含消费级部分，分为六个单独的测试。测试结果在每个奇数月发布，即，该测试计入指标 6 次。所有参与产品均接受评估，并获得“保护”、“性能”和“可用性”类别的分数。各个类别所获分数的总和即为总分；排名前三的产品可以让其 TOP3 计数加一。

- **Mac 检测和性能测试：消费级和企业级**

  该测试评估各种适用于 Mac OS X 的安全保护产品，包含消费级和企业级两部分，测试结果每年发布并计入指标四次。消费级和企业级相关产品分别进行评估。所有参与产品均获得“保护”、“性能”和“可用性”类别的分数。各个类别所获分数的总和即为总分；排名前三的产品可以让其 TOP3 计数加一。

- **家长控制认证测试**

  这项供应商委托的测试每年执行并计入指标一次，评估安全产品在 Windows、Android 和 iOS 平台上防止儿童访问有害网站的效率。

  只有获得认证的产品才能让其供应商的 TOP3 计数加一。

- **VPN 附加安全功能评估**

  这项供应商委托的测试每年执行并计入指标一次。它评估并比较 VPN 解决方案，重点关注它们阻止恶意 URL 和网络钓鱼网站以及避免误报的附加功能。

  每个通过认证的产品都会让其供应商的 TOP3 计数加一。

MRG Effitas

- **360 度评估和认证**

  该测试每年进行并发布四次，评估阻止初始感染的能力以及在被入侵的系统上检测并消除恶意软件所需的时间。该测试取代了此前的“检测和补救时间评估”测试，并且自 2020 年第二季度以来包含网上银行部分，用于评估产品防范金融恶意软件的效率。只有获得认证的产品才能让其供应商的 TOP3 计数加一。

- **Android 360 度评估计划**

  该测试每年进行并发布四次，评估将初始感染复制到设备时（所谓的早期检测）和运行时（安装阶段）阻止感染的能力。该测试还包括误报子测试。

  如果所有参与产品均获得认证，则两个阶段检测率综合排名前三的产品可以让其供应商的 TOP3 计数加一。

  如果任何一个参与产品未通过认证，则只有通过认证的产品才能让其供应商的 TOP3 计数加一。

2024 年 TOP3 指标说明

以下测试于 2024 年进行，用于计算指标。
测试实验室按字母顺序列出。

SE Labs（前身为 Dennis Technology Labs）

- **端点安全 (EPS)：企业测试**
- **端点安全 (EPS)：中小企业测试**
- **端点安全 (EPS)：家庭测试**

  这些为期一个季度的测试以前称为“企业端点”、“小型企业端点”和“家庭反恶意软件保护”测试，每年发布并计入指标四次。这些测试旨在比较知名安全公司提供的反恶意软件产品的有效性。企业、家庭和小型企业产品分别进行评估。在测试期间，这些产品将直面实时互联网威胁。这种对决以非常真实的方式进行，紧密反映了客户体验。结果反映了产品在真实的客户用例场景下的表现，即用户访问受感染网站时发生的情况。这些测试包括检测子测试和误报子测试。

  总准确率评分（根据两个子测试的得分组合计算）最高的三种产品可以让其供应商的 TOP3 计数加一。

- **企业高级安全 (EDR) 测试 - 检测**

  该测试在这一年发布并计入指标一次。也称为入侵响应测试，评估受测产品防范一系列旨在入侵系统和渗透目标网络的黑客攻击的有效性，这些黑客攻击的行为方式与犯罪分子和其他攻击者入侵系统和网络的方式相同。这些测试包括检测子测试和误报子测试。

  总准确率评分（根据两个子测试的得分组合计算）最高的三种产品可以让其供应商的 TOP3 计数加一。

- **电子邮件安全服务 (ESS)：大型企业和小型企业**

  该测试每年执行并计入指标一次，评估电子邮件托管保护服务在实时检测和/或防御威胁方面的有效性，威胁包括 BEC（商业电子邮件入侵）、社会工程和真实世界的垃圾邮件。该测试包括检测子测试和误报子测试。

  每个通过认证的产品都会让其供应商的 TOP3 计数加一。

Testing Ground Labs

- **Android 恶意软件检测测试：消费级和企业级**

  该测试评估移动产品保护用户的 Android 设备免受威胁的有效性。包括检测子测试和误报子测试。消费级和企业级相关产品分别进行评估，在这一年相应发布六次和三次。

  总分数（根据两个子测试结果的组合计算）最高的三种产品可以让其供应商的 TOP3 计数加一。

VirusBulletin

- **VB100 认证**

  这些测试每个月进行一次，旨在评估不同类型的产品（之前，这些测试在每个偶数月进行一次）；这一年已发布十二次报告。

  每个通过认证的产品都会让其供应商的 TOP3 计数加一。

2024 年 TOP3 指标说明

TOP3-2024 中注册的测试参与者完整列表。

- 1E
- Acronis
- AhnLab
- Antiy Labs
- ArcaBit
- Avast
- AVG
- Avira
- Bitdefender
- Bkav
- Broadcom (Symantec)
- Check Point
- CHOMAR
- Cisco
- ClamXAV
- Clario
- CMC Cyber Security
- Combo
- Coronet Cyber Security
- CrowdStrike
- Cybereason
- Cynet
- CyRadar
- Defenx
- Delta
- Dr.Web
- Elastic
- Elpha Secure
- EmsiSoft
- Enigma Software Group
- ESET
- ESTsecurity
- Exosphere
- ExpressVPN
- Faronics
- Fortect
- Fortinet
- F-Secure
- G DATA
- Google
- Hammock
- Hauri
- HP
- Ikarus
- Intego
- IPVanish VPN
- K7
- 卡巴斯基
- Mailcow
- Malwarebytes
- McAfee
- Microsoft
- MicroWorld
- Mullvad VPN
- NAVER Cloud
- Net Protector
- NetSecurity
- NordVPN
- Norton
- Open EDR
- Palo Alto
- Panda
- PC Matic (PC Pitstop)
- Priil
- Private Internet Access Inc.
- Protectstar
- Proton Technologies
- Qi-ANXIN
- Qualys
- Quick Heal
- Rapid7
- ReasonLabs
- Rising
- securiON
- SenseOn
- SentinelOne
- Seqrite
- SGA EPS
- Shield Antivirus
- SOMANSA
- Sophos
- Surfshark
- TGSoft
- ThreatBook
- Total Defense
- TotalAV
- Trellix
- Trend Micro
- Tweaking Technologies
- Vendor A (AVC-EPR)
- Vendor A (AVC-PC)
- Vendor B (AVC-EPR)
- Vendor B (AVC-PC)
- Vendor C (AVC-EPR)
- Vendor C (AVC-PC)
- Vendor D (AVC-EPR)
- Vendor D (AVC-PC)
- Vendor E (AVC-EPR)
- Vietnam Posts and Telecommunications Group
- Viettel Security
- VIPRE
- VMware (Carbon Black)
- Webroot
- WithSecure
- Xcitium (Comodo)
- Zoner