执行摘要

本次 85 条测试用例覆盖恶意软件、进程执行、内存注入、提权后利用、远控外联、数据访问、勒索破坏以及内核安全。按原始表格，VEILGUARD 检测与预警各 81 条，阻止 85 条；360 EDR 分别为 10、9、9 条；火绒 EDR 均为 6 条；奇安信 EDR 分别为 5、4、4 条。VEILGUARD 在三个统计维度均明显领先。

核心指标	VEILGUARD	360	火绒	奇安信
检测阳性	81/85 95.29%	10/85 11.76%	6/85 7.06%	5/85 5.88%
预警阳性	81/85 95.29%	9/85 10.59%	6/85 7.06%	4/85 4.71%
阻止阳性	85/85 100.00%	9/85 10.59%	6/85 7.06%	4/85 4.71%
三项同时阳性	81/85 95.29%	9/85 10.59%	6/85 7.06%	4/85 4.71%
有阻止记录的类别	8/8	3/8	1/8	1/8

优势主要体现在 A11 至 A19 未知与脚本执行、C 类内存操作、D02 至 D05 失陷后动作以及 E、F、G 类主机行为约束。360 EDR 在三款 EDR 中总体记录最高，除传统样本外还覆盖部分提权与内核模块用例；火绒与奇安信在 A 类各有独立样本覆盖。

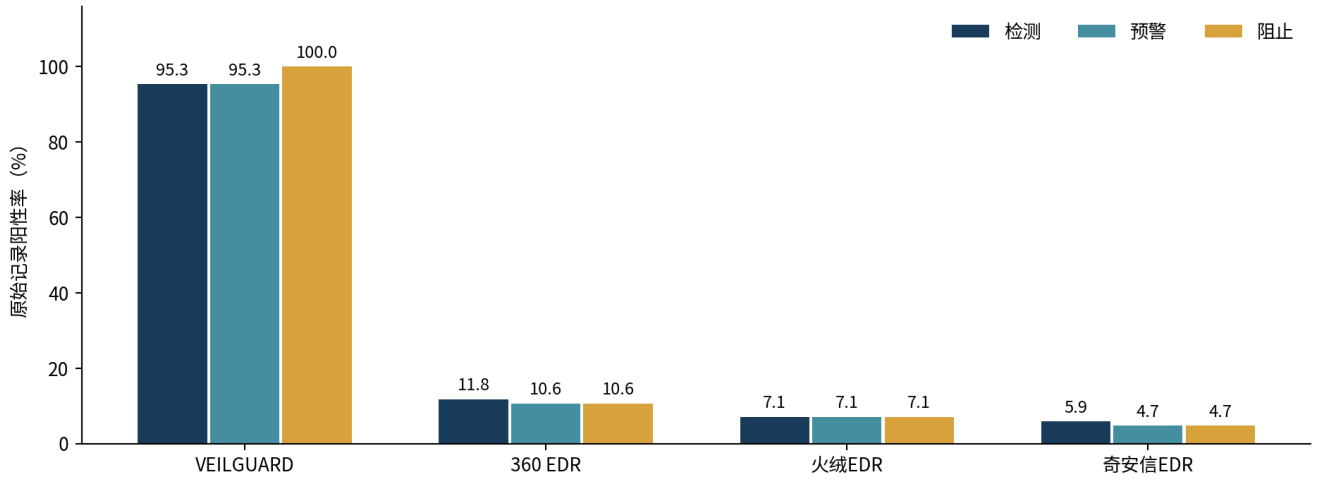


图 1 四产品检测 预警和阻止原始记录对比

执行摘要 攻击类别与防御能力比较

下表汇总八类攻击与安全场景的阻止记录，以便直接比较各产品在关键操作边界的覆盖。每格为阻止阳性数量 / 该类数量及百分比；检测和预警的总体比较见前页，分类明细见第 6 章。

攻击类别	VEILGUARD	360 EDR	火绒 EDR	奇安信 EDR
A 传统威胁	19/19 100.00%	6/19 31.58%	6/19 31.58%	4/19 21.05%
B 进程执行	13/13 100.00%	0/13 0.00%	0/13 0.00%	0/13 0.00%
C 内存注入	11/11 100.00%	0/11 0.00%	0/11 0.00%	0/11 0.00%
D 提权后利用	5/5 100.00%	1/5 20.00%	0/5 0.00%	0/5 0.00%
E 远控外联	11/11 100.00%	0/11 0.00%	0/11 0.00%	0/11 0.00%
F 数据保护	9/9 100.00%	0/9 0.00%	0/9 0.00%	0/9 0.00%
G 勒索破坏	12/12 100.00%	0/12 0.00%	0/12 0.00%	0/12 0.00%
H 内核安全	5/5 100.00%	2/5 40.00%	0/5 0.00%	0/5 0.00%

分类比较结论

VEILGUARD 在八类中均为 100%阻止阳性记录，优势分布覆盖主机执行、内存、网络、数据及内核边界。360 EDR 在传统威胁、提权后利用和内核安全三类分别为 31.58%、20.00%和 40.00%；火绒 EDR 与奇安信 EDR 的阻止记录均集中在传统威胁类，分别为 31.58%和 21.05%。

B、C、E、F、G 五类中，VEILGUARD 均有完整阻止记录，三款 EDR 均未记录阻止；D 和 H 类中 360 存在部分覆盖。三款 EDR 在部分传统样本的具体命中对象不同，因此相同数量不表示覆盖完全相同。

上述比较反映本次配置与用例集合。A、B、E、F、G 含正常或混合方向争议项目；100%阻止阳性不等于 100%正确防御。未记录阻止也不能直接推定真实危害已发生。

执行摘要 综合防御能力雷达比较

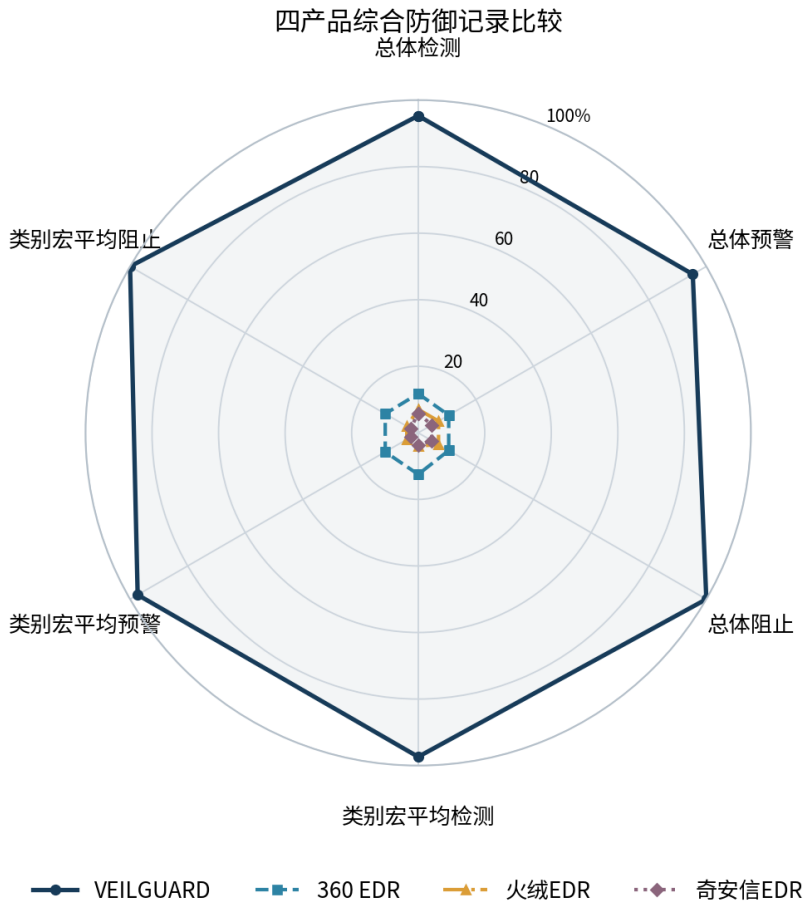


图 2 六项可计算指标的综合雷达图 各轴 0 至 100%

产品	总体检 / 预 / 阻 %	宏平均检 / 预 / 阻 %
VEILGUARD	95.29 / 95.29 / 100.00	97.37 / 97.37 / 100.00
360 EDR	11.76 / 10.59 / 10.59	12.49 / 11.45 / 11.45
火绒 EDR	7.06 / 7.06 / 7.06	3.95 / 3.95 / 3.95
奇安信 EDR	5.88 / 4.71 / 4.71	3.67 / 2.63 / 2.63

六个维度的排序一致，均为 VEILGUARD、360 EDR、火绒 EDR、奇安信 EDR。VEILGUARD 的总体检测与预警均 95.29%，对应类别宏平均均 97.37%；总体与宏平均阻止均 100%，表明其领先并非仅由单一大类驱动。

总体率按 85 条用例等权，宏平均按 8 类等权。六轴存在相关性，雷达图用于展示能力记录轮廓，不对多边形面积评分，也不把六轴再次平均成综合分。真实危害避免、误报、性能和 AI 语义防护尚未纳入。