paloalto NETWORKS | CORTEX

买家必备的端点安全指南

了解一下企业端点安全防护必须提供哪些最重要的功能

目录

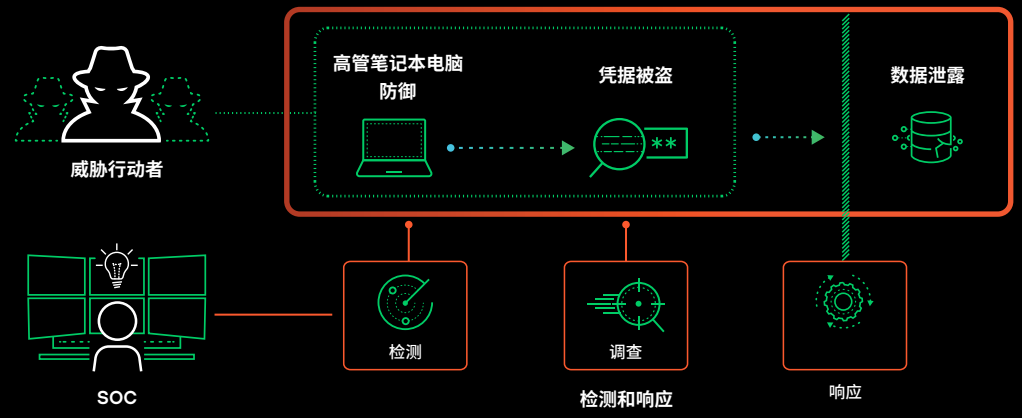
概述

高级持续性威胁、勒索软件即服务和 AI 助力的攻击正在重新定义安全格局，挑战着企业保持安全领先地位的能力。遗憾的是，当今各自为政的安全解决方案难以跟上这些不断演变的威胁，使企业容易受到攻击。这就意味着，攻击者入侵企业不是“有没有可能”的问题，而是“什么时候”的问题。

安全团队被海量警报、复杂调查和持续的攻击漏报风险压得喘不过气来。随着企业在云端和其他地方的数字足迹不断增加，需要分析的安全遥测数据的数量和种类也呈指数级增长，“淹没在数据中”已经不是夸张的说法。

端点安全是网络防御的基石，既是阻止攻击者或防止首次成功入侵的关键，也是追捕攻击者最有效的数据来源。它对整体安全态势和安全运营 (SecOps) 至关重要，因为这些都需要在入侵之前看到并阻止网络攻击。

归根结底，强大的**端点安全战略**对于保持安全领先地位至关重要。它应该提供跨传统端点、网络、云工作负载、移动设备、身份等的全面可视性和分析功能，以统一的方式实现快速检测和响应，从而支持日益重要的安全运营。



> 到 2028 年，30% 的企业将采用来自同一供应商的预防性端点安全、端点检测和响应以及身份威胁检测和响应解决方案，而 2024 年的这一比例只有 5%。
>
> - Gartner[1]

[1] Evgeny Mirolyubov 等人，端点保护平台魔力象限，Gartner，2024 年 9 月。

探索端点安全：
安全职责面临的主要挑战

安全职责面临的主要挑战

CISO

首席信息安全官 (CISO) 努力向董事会证明安全投资的合理性，同时展示对企业安全态势的切实改善。面临的挑战则是将技术指标转化成商业价值，在不断演变的威胁形势下管理风险，同时确保遵守各项法规。CISO 还必须在强大的安全措施需求与业务敏捷性和用户生产力之间取得平衡，同时在预算限制内运营并解决网络安全技能的差距。

SecOps 负责人

SecOps 即安全运营中心 (SOC) 负责人的使命是确保其团队拥有正确的知识、流程和工具，从而有效应对任何威胁。面临的挑战则包括了解对手的战术和技法、协调跨多个工具和平台的响应，以及管理团队内部的警报疲劳和倦怠。SecOps 负责人还必须不断调整其战略，从而应对新类型的威胁，优化资源分配，缩短平均检测时间 (MTTD) 和平均响应时间 (MTTR)。

安全架构师

安全架构师面临的挑战是设计和实施全面的端点安全战略，从而应对不断演变的威胁，同时与现有基础设施和安全运营无缝集成。安全架构师努力识别和消除安全控制中的潜在盲点，管理泛滥的安全工具，确保各种解决方案之间的互操作性。其主要关注点是不断改善企业的安全态势，同时平衡效率、成本与用户体验。

安全分析师

安全分析师处在威胁检测和响应的最前线，处理着源源不断的警报和潜在安全事故。安全分析师时刻与警报疲劳作斗争，经常陷入误报的泥潭中而浪费宝贵的时间。其主要挑战包括有效确定警报的优先级，减少调查时间，以及在日常任务与主动威胁狩猎和对关键事故的深入分析之间取得平衡。

评估端点安全提供商能力的十个重要问题

1. 解决方案如何处理对复杂攻击的检测?

端点检测和响应 (EDR) 功能

寻找提供最先进端点检测和响应功能的解决方案，能够持续监控端点是否存在恶意活动的迹象，从而快速检测和响应复杂威胁。

收集丰富的端点数据

有效的解决方案应该从端点收集大量遥测数据，从而发现潜在威胁。通过收集进程信息、文件活动、网络连接、注册表更改、用户活动等，解决方案可以检测到相对狭隘的工具可能遗漏的威胁。

机器学习 (ML) 和行为分析技术

寻找采用大量不断更新的机器学习模型进行自动威胁预防和检测的解决方案。这些解决方案应该借鉴网络安全专家的真实见解，自动整合最新的威胁情报。这种方法可以显著减少手动分析时间，加快威胁检测和响应的速度，使分析师能够专注于关键事故。

可定制的检测规则和预定义检测

虽然解决方案应该附带大量开箱即用的分析和检测规则，但也应该提供定制灵活性。安全团队应该能够创建和微调检测规则，从而顺应其企业的特定需求和威胁形势。预定义和可定制的检测相结合，可以确保全面覆盖各种高级攻击。

2. 解决方案提供哪些高级威胁防御功能?

多层次方法

实施纵深防御战略，将漏洞利用防御、AI 助力的恶意软件分析、基于云的文件检查、行为威胁检测和勒索软件防护集成在一起，确保即使攻击逃脱了一层，也会被另一层捕获，从而创建一个全面的安全网，防御从恶意软件到无文件攻击等复杂威胁。

基于行为的防护和漏洞利用防御

确保解决方案利用高级行为威胁防护来分析相互关联的进程行为并揭示主动攻击。这种全面的监控能够检测出在单独检查各个进程时可能遗漏的多阶段威胁，而强大的漏洞利用防护模块则为操作系统和应用程序漏洞提供了关键的防护措施。

基于 AI 和机器学习的防护

实施 AI 驱动的安全引擎，仔细检查所有传入的文件，同时不断学习如何应对新出现的攻击模式，从而能够检测和阻止传统基于特征的防御可能错过的复杂威胁。

3. 解决方案的调查和响应方法是什么？

自动将警报关联到事故

寻求一种利用机器学习自动将相关警报分组为统一事故的解决方案，从而大幅减少警报疲劳并使分析师能够将注意力集中在高优先级的安全问题上。

按风险优先级排序事故并评分

部署基于机器学习的系统，根据风险因素分析事故并评分，从而快速评估攻击范围和影响，确保安全资源的最佳分配。

根本原因分析和攻击链可视化

寻找能够自动揭示根本原因的功能，同时为每次事故提供声誉数据和可视化攻击链映射，使分析师能够快速了解威胁情境和范围。

自动和手动响应选项

实施灵活的响应框架，将对常规威胁的自动操作与对复杂场景的手动干预选项相结合，使安全团队能够根据威胁情境执行快速、自动的补救措施和精心定制的响应。

与 SOAR 平台集成

选择与 SOAR 平台无缝集成的解决方案，从而增强自动化工作流程并精简整个安全堆栈中的事故响应流程。

4. 解决方案如何应对警报疲劳和误报的挑战？

寻求一种使用 AI 驱动的警报分流和优先级划分进行智能警报分组和事故评分的解决方案

寻找一种 AI 助力的解决方案，可以智能地对警报进行分组和评分，自动关联相关事件，同时根据影响和威胁可能性评估风险。系统应该利用对资产关键性、用户行为和威胁情报的情境式分析，同时不断从分析师的反馈中学习，从而提高优先级划分的准确性并通过高级行为分析减少误报。

通过高级分析减少误报

理想的系统应该利用 AI 助力的分析以及来自端点、网络和云环境的跨数据关联，准确区分真正的威胁和无害的异常，通过情境式分析最大限度减少误报。

5. 解决方案如何从传统 EDR 扩展到 XDR 功能？

仅凭端点数据就可以奏效，但可以拓宽情境，实现更多检测和工作流程的整合

找到一种解决方案，以便仅使用端点数据就可以提供强大的保护，同时在条件允许时无缝整合网络、身份和云数据源，从而强化威胁检测情境并精简安全工作流程。

集成来自扩展数据源的数据

寻找无缝集成来自各种来源（例如网络、云环境和身份系统）的数据的能力，因为攻击者会在多个环境之间移动，而单一来源的可视性会留下危险的盲点。

跨数据分析和威胁关联

解决方案应该提供高级分析功能，可以关联不同数据源之间的威胁，从而提供对活跃安全事故的更全面的看法。

攻击的完整情境

理想的解决方案应该使用 MITRE ATT&CK 等通用框架，提供对整个攻击链的完整可视性，从初始进入到横向移动和数据泄露企图。

转型成统一的 SOC 平台

寻求一个将多种安全工具整合到单一界面和数据源中的平台，同时确保跨主流 SOC 技术（包括 SOAR、新一代 SIEM 和攻击面管理）的可扩展性。

6. 解决方案如何交付云检测和响应？

针对特定于云的架构调整运行时安全性（例如，容器、Kubernetes、VM）

解决方案应该针对云架构（包括容器、Kubernetes）进行优化，提供专门针对这些云原生架构调整的运行时安全性，确保跨各种云工作负载的全面防护。

将运行时遥测与无代理扫描和云服务提供商 (CSP) 日志数据相结合，全面了解云活动

寻找一种全面的云监控解决方案，将运行时遥测、无代理扫描和 CSP 日志数据与 CNAPP 安全洞察相结合，提供对云活动和工作负载行为的完整可视性。

基于机器学习的检测/响应和事故管理工作流程

选择在机器学习驱动的安全平台上运行的解决方案，在云和本地环境之间提供统一的检测和响应功能，支持混合架构和多云架构，同时为安全团队保持一致的工作流程。

7. 解决方案如何整合基于身份的安全性？

与身份提供商集成

确保解决方案与 Active Directory 和 Okta 等关键的身份提供商无缝集成，从而提取全面的用户活动数据，为企业范围的威胁检测和响应提供必要的情境信息。

身份数据与其他安全遥测数据的关联

找到一种将身份数据与更广泛的安全遥测关联起来的解决方案，从而提供全面的用户活动可视性，并结合风险评分和 UEBA 功能来快速识别可疑的行为模式。

基于机器学习自动检测和响应身份泄露

部署由机器学习助力的身份威胁检测和响应 (ITDR) 系统，自动识别异常用户和实体行为，从而发现泄露的凭据和内部威胁，同时实现快速自动响应，缓解基于身份的攻击。

8. 解决方案如何简化部署和管理？

单代理安装，部署后无需重新启动

这样可以最大限度减少对最终用户的干扰，允许在大型环境中快速部署和更新。

默认启用最佳实践安全策略

这样可以确保从第一天起就拥有强大的安全态势，同时仍允许进行定制来满足特定需求。

对安全内容更新的推出进行精细和分阶段的控制

允许分阶段测试和推出新的安全内容，确保稳定性并最大限度减少潜在的干扰。

统一的管理控制台

寻求一种通过单一、直观的控制台提供全面安全管理的解决方案 - 从端点策略管理到威胁检测、调查和响应 - 从而精简管理流程，同时呈现企业安全态势的一致视图。

对端点的性能影响

代理应该通过低 CPU 利用率和 I/O 对端点性能产生最小的影响，从而确保强大的安全性，而不会干扰用户的生产力或系统性能。

面向大型企业的可扩展性

应该可以轻松容纳不断增长的端点数量和不断增加的数据量，而无需进行重大的基础设施投资。

9. 哪些行业验证和独立测试结果支持了解决方案的效能？

在 MITRE Engenuity ATT&CK 评估中的表现

参考解决方案在最近的 MITRE Engenuity ATT&CK 评估中的表现。寻找高分的综合保护和检测，最好具有强大的开箱即用效果，无需更改配置。留意分析覆盖率和延迟检测的几率等指标。

来自 AV-Comparatives 和其他独立测试的结果

寻找端点防护和响应测试中的高分，这样可以验证解决方案在现实场景中的效果。

客户评价和分析师认可

参考行业特定的评价来考虑同行反馈，这些评价展示了实际性能，以及解决方案在 Forrester Wave™ 和 Gartner® 魔力象限™ 等分析师报告中的地位，因为这样可以验证市场地位和技术能力。

10. 解决方案是否支持从 EDR 演进到 XDR 并最终通过 AI 和自动化实现全面的 SOC 转型？

渐进式增长的基础

寻求一种将核心 EDR 功能（包括高级威胁预防、检测和响应）与必备的端点防护功能（如主机防火墙、磁盘加密支持和设备控制）相结合的解决方案，从而实现端点级别的全面安全。

向 XDR 功能演进

评估解决方案如何通过集成网络、云、身份和第三方数据扩展到 XDR，从而实现对所有安全遥测的统一可视性和自动关联。

实现 SOC 全面转型的途径

确保平台能够通过 SOAR 和新一代 SIEM 功能扩展到全面自动化，从而将攻击响应时间从几天缩短到几分钟。

面向未来的架构

解决方案应该提供统一的后端，支持贯穿所有三个阶段（从 EDR 到 XDR 再到真正的 SOC 平台），同时保持一致的工作流程并始终利用 AI 驱动的自动化。

考虑携手 CORTEX 制定面向未来的端点安全战略

在考虑了重塑端点安全战略的 10 个关键问题之后，很明显可以看出，在当今快速演变的威胁形势下，全面、智能的方法至关重要。

Cortex XDR® 作为解决这些关键问题的解决方案应运而生，提供了超越传统端点安全的高级威胁预防、检测和响应功能。

Cortex XDR 的 AI 驱动方法解决了本文中强调的挑战。它在威胁防御方面给出了业界最佳表现，在 2024 年 MITRE Engenuity ATT&CK 评估中实现了 100% 的检测率。Cortex XDR 显著减少了警报疲劳和误报，将来自多个来源的数据拼接起来从而获得整体视图，而且提供了自动和手动响应选项。这些功能与其云就绪的架构和身份安全集成相结合，使 Cortex XDR 成为现代安全团队掌握的强大工具。

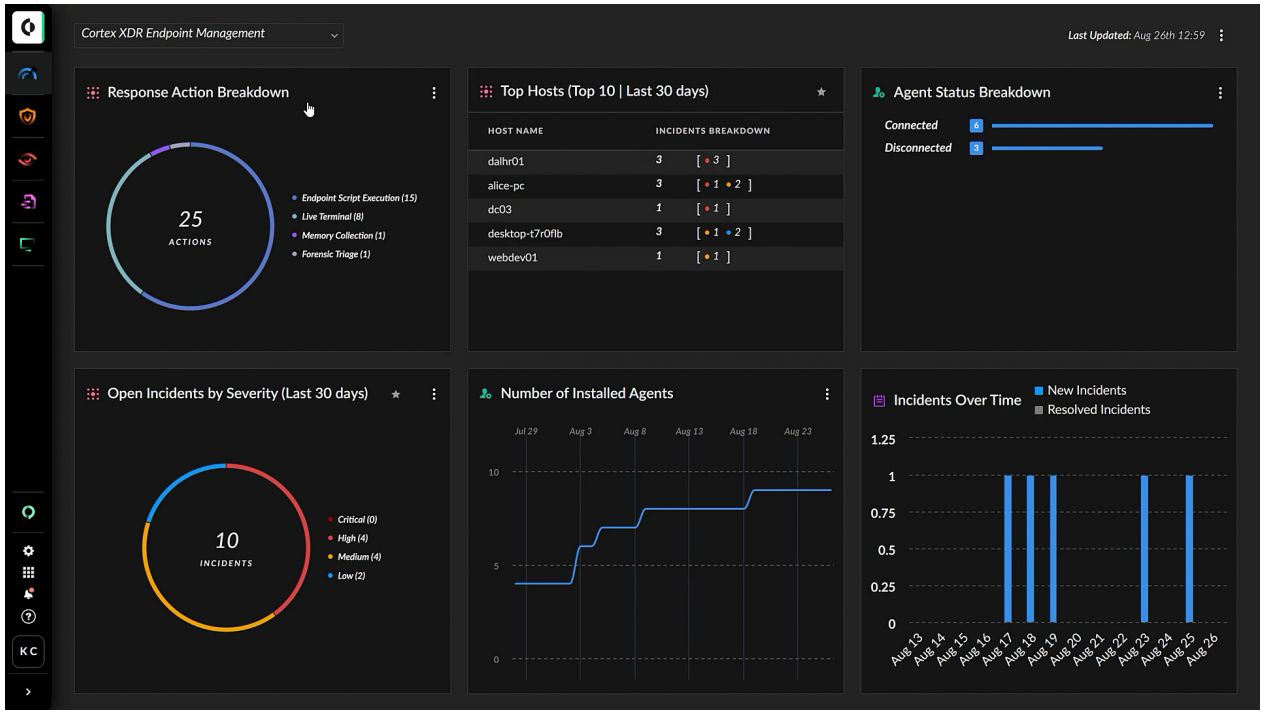


图 1： Cortex XDR 端点管理

对于寻求 SOC 转型的企业，Cortex XDR 提供了可扩展的基础。其架构允许安全团队从核心 EDR 功能开始，逐步扩展到完整的 XDR 功能，从而满足企业不断变化的需求。

作为这次安全旅程的下一步，Cortex XSIAM® 在 Cortex XDR 功能的基础上，通过 SOAR 扩展响应自动化，通过革命性的 AI 驱动方法将数据提取扩展到新一代 SIEM。XSIAM 平台通过 AI 和自动化重塑安全运营，在几分钟内（而不是几天或几周）阻止攻击。

选择 Palo Alto Networks Cortex® 解决方案，企业就相当于投资了一项不仅能满足当前需求，还能应对未来挑战的安全战略。Cortex XDR 和 XSIAM 致力于持续研发、适应新兴威胁，以及制定明确的路线图来满足未来的安全需求，为日益复杂的数字世界提供了一条通往更有韧性、更有效率、更有效能的安全态势之路。

参加 Cortex XDR 产品导览，亲身体验这些功能，探索平台的高级功能并了解如何重塑端点安全运营。

全面的 MDR

全天候专家级安全运营

我们的托管检测和响应 (MDR) 服务由 Cortex XDR 技术提供支持，通过将人类专业知识与先进的威胁检测和响应功能相结合，提供全面的 24/7 安全覆盖。我们通过警报管理、事故响应和主动威胁狩猎帮助各种规模的企业加强其安全态势。

我们灵活的、基于结果的方法包括根据企业的独特要求量身定制的规则和剧本，由基于时间的检测和响应 SLA 支持。与我们合作，可以立即完善自身的安全运营，让团队专注于战略议题，而我们则负责处理复杂的现代安全威胁。

携手面向 Cortex XDR 的 Unit 42 MDR 为未来保驾护航。

了解更多 →

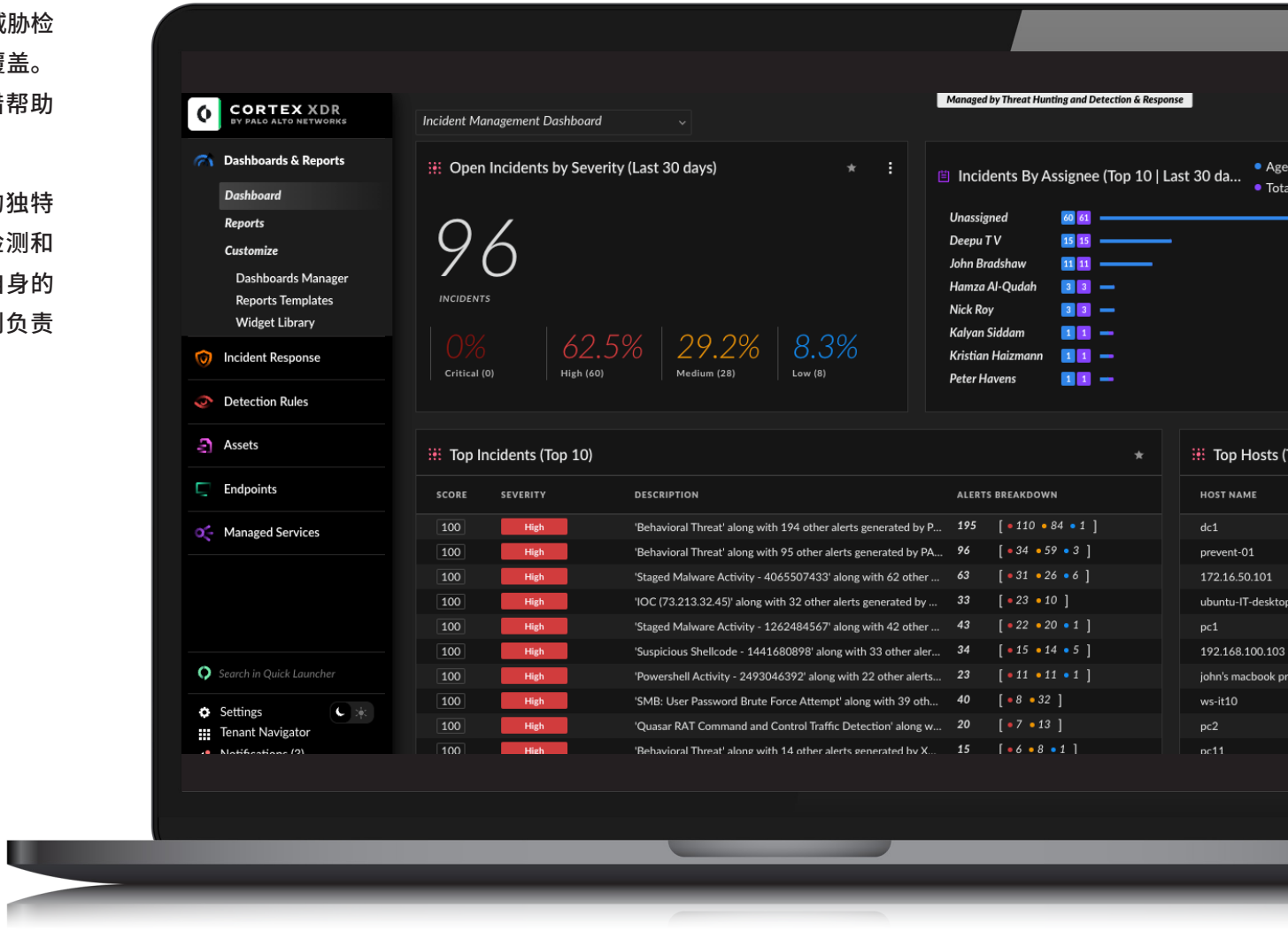


图 2： Cortex XDR 配备 Unit 42 托管检测和响应 (MDR) 仪表盘

您的端点安全必备评估清单

Advanced Threat Prevention

多层防护功能
- ☐ 新一代防病毒功能
- ☐ 勒索软件防护
- ☐ 无文件攻击预防
- ☐ 漏洞利用防御模块
- ☐ 基于行为的防护

基于 AI/机器学习的防护引擎
- ☐ 本地沙盒功能
- ☐ 持续更新的模型

附加安全功能
- ☐ 主机防火墙功能
- ☐ 磁盘加密支持
- ☐ 设备控制功能

检测功能

EDR 基础知识
- ☐ 实时监控
- ☐ 全面的端点遥测收集
- ☐ 跨源事件关联

机器学习和分析
- ☐ 行为分析能力
- ☐ 针对不同威胁类型的多种机器学习模型
- ☐ 定期模型更新

检测灵活性
- ☐ 预构建检测规则
- ☐ 自定义检测创建选项
- ☐ MITRE ATT&CK 框架对齐

调查和响应

警报管理
- ☐ 自动关联警报
- ☐ 基于风险的优先级划分
- ☐ 误报减少功能

调查工具
- ☐ 根本原因分析功能
- ☐ 攻击链可视化
- ☐ 详细事故情境

响应选项
- ☐ 自动响应功能
- ☐ 手动响应工具
- ☐ SOAR 平台集成

扩展的检测和响应

数据集成
- ☐ 网络数据采集
- ☐ 云安全集成
- ☐ 身份提供商集成

跨数据分析
- ☐ 多来源关联
- ☐ 统一事故视图
- ☐ 扩展调查情境

云安全

云工作负载防护
- ☐ 容器安全性
- ☐ Kubernetes 防护
- ☐ VM 安全性

云集成
- ☐ 云提供商日志集成
- ☐ CNAPP 集成
- ☐ 多云支持

部署和管理

实施
- ☐ 单代理架构
- ☐ 免重启部署
- ☐ 默认安全策略

管理
- ☐ 统一的管理控制台
- ☐ 基于角色的访问控制
- ☐ 策略管理工具

性能
- ☐ 低系统影响
- ☐ 面向企业的可扩展性
- ☐ 带宽优化

验证和测试

行业认可
- ☐ MITRE ATT&CK 评估结果
- ☐ 独立测试评分（AV-Comparatives 等）
- ☐ 分析师认可（Gartner、Forrester）

客户验证
- ☐ 所在行业的客户推荐
- ☐ 案例研究
- ☐ 生产环境测试结果

面向未来

供应商评估
- ☐ 研发投资
- ☐ 功能发布节奏
- ☐ 威胁研究能力

路线图评估
- ☐ 计划功能新增
- ☐ 技术合作伙伴关系
- ☐ 集成能力

平台演进
- ☐ 可扩展至完整的 SOC 平台
- ☐ AI/机器学习开发计划
- ☐ 自动化能力

成本和支持

定价结构
- ☐ 许可模式
- ☐ 额外模块成本
- ☐ 批量折扣

支持服务
- ☐ 24/7 技术支持
- ☐ 实施协助
- ☐ 培训资源

合规与报告

法规遵从
- ☐ 内置合规性报告
- ☐ 支持主要法规（GDPR、HIPAA、PCI DSS 等）
- ☐ 自定义合规性报告创建

审计支持
- ☐ 审计跟踪功能
- ☐ 历史数据保留选项
- ☐ 证据收集工具

集成功能

安全工具集成
- ☐ SIEM 集成
- ☐ 威胁情报平台集成
- ☐ 工单系统集成

API 可用性
- ☐ REST API 文档
- ☐ 自定义集成支持
- ☐ API 速率限制和配额

数据导出
- ☐ 自定义报告生成
- ☐ 原始数据导出功能
- ☐ 数据格式选项

供应商评估

公司稳定性
- ☐ 财务健康
- ☐ 市场地位
- ☐ 客户留存率

支持基础设施
- ☐ 全球支持覆盖
- ☐ 支持响应 SLA
- ☐ 知识库质量

社区资源
- ☐ 用户社区规模
- ☐ 社区论坛
- ☐ 第三方集成市场

运营要求

离线功能
- ☐ 离线保护功能
- ☐ 本地检测功能
- ☐ 数据缓存机制

备份和还原
- ☐ 代理备份选项
- ☐ 配置备份
- ☐ 灾难恢复支持

资源优化
- ☐ CPU 使用率控制
- ☐ 内存优化
- ☐ 网络带宽管理

使用这个检查清单作为选择全面端点安全解决方案的指南，让解决方案不仅能满足当前的需求，还能为安全运营转型奠定基础。正确的选择既能在当下保护企业，又能扩展到应对未来新出现的威胁。

立即开始使用

欢迎安排演示，了解 Cortex XDR 如何帮助您和企业简化运营、大规模阻止威胁并加速当下和未来的事故补救。

免费咨询热线：400 9911 194
网址：www.paloaltonetworks.cn
邮箱：contact_salesAPAC@paloaltonetworks.com

关注派拓网络
官方微信公众号