XDR 选购指南

像专业人士一样从容驾驭 “扩展检测和响应” 市场

了解扩展检测和响应 (XDR)

为什么当今世界需要一种截然不同的安全方法？

在当今多供应商、多媒介的混合环境中，复杂性已成为企业面临的最大挑战。安全团队必须保护不断扩展的生态系统，利用数十种集成度不一的工具开展运维工作。随着物联网和混合办公模式的兴起，企业的受攻击面不断扩大。网络钓鱼、恶意软件和勒索软件攻击正以每年两倍甚至三倍的速度增长。与此同时，各企业之间形成了前所未有的高度互联。一家公司的安全漏洞可能会影响其供应商、合作伙伴、客户，甚至相关的各个行业。

在这种新常态下，构筑安全弹性势在必行。安全弹性是指保护企业各方面完整性的能力，让企业能够抵御不可预测的威胁或变化，不断增强安全水平。过去的方法已无法满足安全弹性的需求。

如何应对威胁？

随着安全威胁形势日益复杂，基于独立单点安全解决方案构建的传统检测和响应模式已经无法充分满足需求。因此，扩展检测和响应 (XDR) 应运而生。XDR 是一种统一的安全事件检测和响应工具。XDR 解决方案会自动收集多种安全工具的遥测数据并进行关联分析，应用分析功能来检测恶意活动，然后对威胁做出响应并采取补救措施。作为一种有效的全方位解决方案，XDR 可对电子邮件、终端、服务器、云工作负载和网络等所有媒介中的数据进行关联分析，提供对整个环境的可视性，实现情景感知，让最高级的威胁也无所遁形。

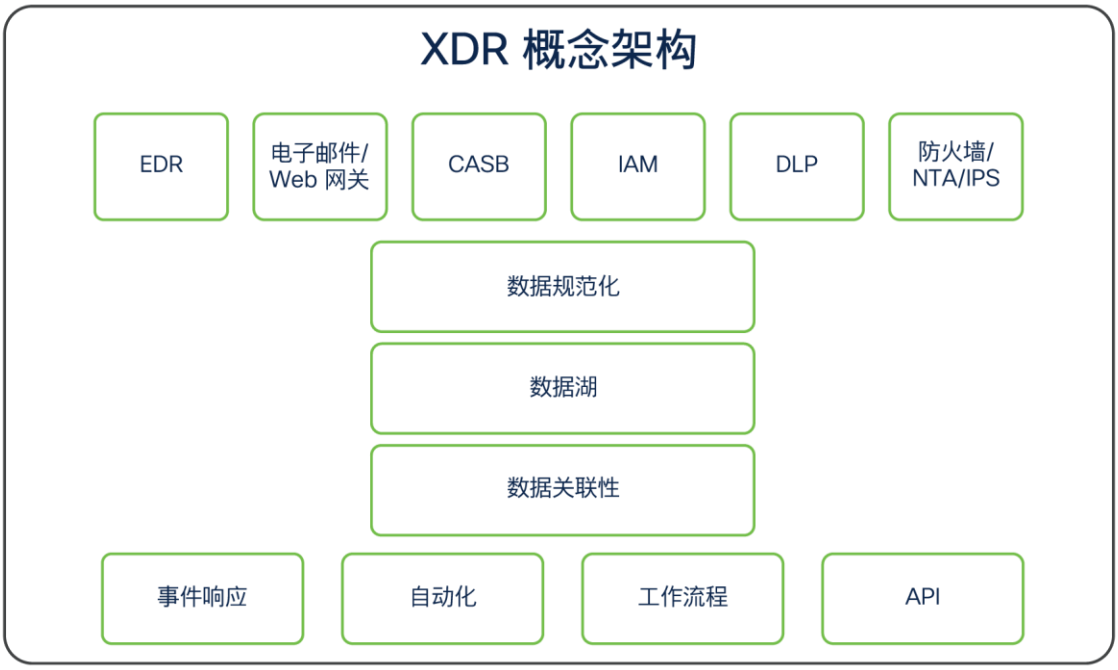
为什么选择 XDR？

首先，借助 XDR 的事件关联和多供应商检测功能，团队可检测出网络、云、终端、电子邮件等媒介中极其复杂的威胁。

其次，利用 XDR，团队能够根据威胁的影响确定其优先级，进而减少警报疲劳。

第三，XDR 可自动执行任务，提高团队工作效率，让团队更有效地利用 SOC 资源。

第四，依托 XDR，组织能够弥合安全漏洞并通过切实可行的情报预测未来趋势，构筑安全弹性。



正确实施 XDR 的五大要素

1.提供按优先级排序且切实可行的遥测数据，随时随地为您所用

您能否高效筛选海量警报，对威胁进行分类？

广泛的可视性和深度洞察是 XDR 的基础。许多复杂的威胁活动不仅仅攻击终端或网络，还会攻击其他多种媒介，比如电子邮件、身份管理、沙盒和防火墙。因此，您需要一种能提供广泛遥测技术和高质量数据的 XDR 解决方案。这些数据不仅可为 XDR 的有效运行提供信息支持，而且还将帮助您全面了解整个环境中的状况。除了收集洞察以外，事件管理也同样重要。要让 XDR 实现预期成效，对这些洞察进行优先级排序是一项必不可少的措施。XDR 解决方案可提供基于风险的优先级排序（即按风险的重大程度确定事件的优先级），助您把握重点，快速行动。此类解决方案还可提供后续措施建议，助您做出明智决策，采取最佳行动。

关键功能和能力	相关产品领域
• 确保效力和准确性，尽可能减少误报带来的干扰 • 汇聚整个环境中的警报，进行关联分析	终端检测和响应 (EDR)
• 持续实时监控网络	网络检测和响应 (NDR)
• 高级分析功能，在检测到未知恶意软件和其他复杂网络攻击时，根据情景按优先级生成警报	扩展检测和响应 (XDR)
• 持续实时监控电子邮件威胁，自动确定补救措施的优先级	电子邮件安全

针对供应商的问题

- 您的解决方案如何为我提供涵盖所有环境（终端、设备、网络）的可视性？
- 您的解决方案如何提供洞察？您的解决方案是否提供按优先级排序的遥测数据？
- 您的解决方案如何根据业务影响和风险确定威胁的优先级？
- 哪些类型的威胁情报可为您的检测提供依据？这些情报从何而来？
- 您如何验证解决方案所使用的数据源？
- 该产品如何处理 Wannacry、NotPetya 和 Turla 等复杂威胁？

2.支持统一检测，不受媒介和供应商的影响

您的 XDR 解决方案能否确保您购买的安全产品作为统一整体协同运行？

随着威胁形势日益复杂，攻击媒介的类型也越来越多样化，确保在整个环境中实现一致的检测变得前所未有的重要。如今，安全团队在其安全环境以及由全球供应链、攻击者和防御者组成的生态系统中，都面临着前所未有的复杂局面。XDR 解决方案可以根据威胁的严重程度及其影响汇聚各种检测措施、进行关联分析并确定优先级，助您从容应对复杂局势。要做到这一点，您的安全体系需要协同运行。选择开放、可扩展且云优先的 XDR 解决方案，即可在整个环境中实现统一检测和事件关联，而不会额外增加复杂性。安全体系中的每个组件都具备独特的检测元素，如网络、电子邮件、防火墙等；当这些元素组合在一起时，威力倍增。需要注意的是，为便于您全面了解潜在威胁，XDR 应涵盖所有六个遥测源，即终端、网络、防火墙、电子邮件、身份和 DNS。您的 XDR 解决方案应能通过本机后端到前端集成轻松与整个安全体系集成，因此即使供应商更改产品组合或更换供应商，覆盖范围也能保持一致。最后，要优化安全体系的威胁检测功能，不妨试试 XDR 解决方案，不仅可以提供宝贵的本地情景信息，还能提供值得信赖的准确威胁情报判定。

关键功能和能力	相关产品领域
• 检测并阻止终端运行程序的异常行为，包括基于漏洞实施的内存注入攻击 • 通过 MITRE ATT&CK 映射确定感染指标 (IoC) • 监控文件信誉，在入口点检测并隔离威胁 • 确定环境中的操作系统漏洞，确保管理员能够根据风险确定补救措施的优先级，缩小受攻击面	终端检测和响应 (EDR)、漏洞管理
• 利用高级分析功能，快速检测未知恶意软件、内部威胁（如数据渗漏和策略违规）以及其他复杂攻击 • 通过精准的警报实时检测网络攻击	扩展检测和响应 (XDR)、网络检测和响应 (NDR)
• 通过信誉过滤检测并阻止不受欢迎的电子邮件 • 识别并防御基于欺骗的电子邮件攻击，例如社交工程、冒充者	电子邮件安全

针对供应商的问题

- 我的现有投资可以在多大程度上通过您的 XDR 平台发挥价值？
- 无论我使用哪一家供应商的解决方案，是否都能与您的 XDR 平台兼容？
- 您的解决方案彼此之间是否已进行集成，支持开箱即用？

- 与市面上其他检测技术相比，您的检测技术有何优势？
- 您的解决方案可以检测出哪些威胁？是否可将警报映射到 MITRE ATT&CK 框架？

3.快速、准确应对威胁

识别威胁后，您能以多快的速度有效应对威胁？

统一来自网络、终端和电子邮件等媒介的洞察，可以更准确地了解发生的威胁、威胁的发展动态 ，进而确定需要采取的补救措施以消除威胁。理想情况下，您应该能够一站式查看威胁的影响和范围，只需点击一两下即可采取行动。有效的 XDR 需要具备原生响应和补救能力，例如隔离主机或删除所有收件箱中的恶意电子邮件。XDR 还应该能够简化创建自定义响应的操作，提供自动化机会，以便团队能够不断改进其安全措施。

关键功能和能力	相关产品领域
• 终端受到攻击后快速响应威胁	终端检测和响应 (EDR)
• 只需几秒钟即可隔离网络问题或事件，确定其根本原因	扩展检测和响应 (XDR)、网络检测和响应 (NDR)
• 通过实时点击时间分析，快速阻止恶意网站	电子邮件安全

针对供应商的问题

- 您的产品可提供哪些响应措施？
- 是否可以一站式使用 XDR 解决方案在终端上执行补救措施，然后将其扩展到其他位置？
- 您的产品如何与支持响应的现有安全工具集成？
- 您的解决方案如何加速实施补救措施？
- 从威胁警报到补救，响应时间有多长（例如，就网络钓鱼攻击而言）？

4.提供统一调查视角，简化用户体验

威胁检测、响应和补救是否可通过统一界面进行管理？

评估 XDR 解决方案时，必须考虑安全分析师的经验。SecOps 团队已然有大量任务需要管理，没有必要使用数十种工具和众多控制台来降低工作效率。因此，我们推荐使用 XDR 解决方案，该解决方案旨在针对多种安全工具和数据源提供统一的安全数据视图，帮助分析师更快速、更有效地检测和应对威胁。这有助于简化工作流程，减少调查安全事件和采取补救措施所需的时间和精力。XDR 解决方案可提供完整生命周期控制面板，涵盖各种威胁媒介和无线接入点。该解决方案可通过 MITRE ATT&CK 等模型方便进行威胁追踪，即使刚开始接触此过程的用户也能基于假设追踪威胁，轻松预测未来动向。另一个需要考虑的因素是设计对分析师体验的影响。XDR 解决方案可通过渐进式披露功能为警报提供更完善的情景信息，快速确定潜在威胁的范围和严重程度，从而提高工作效率，缩短与检测、调查和响应等关键功能相关的决策时间，助力初级和中级分析师执行安全运维中的高级任务。

关键功能和能力	相关产品领域
• 提供完整生命周期控制面板，涵盖各种威胁媒介和无线接入点 • 提供可扩展到 ITOps、SecOps 和 NetOps 的统一工具集	扩展检测和响应 (XDR)

关键功能和能力	相关产品领域
• 一站式访问和管理数据、进行分析、实现自动化	

针对供应商的问题

- 您的解决方案如何帮助我的团队追踪威胁？
- 该解决方案如何与现有安全技术（例如 SOAR 和 SIEM 解决方案）集成？
- 我能否使用您的 XDR 来了解威胁的影响和漏洞的范围，通过统一界面执行一键式操作？
- 您的解决方案是否支持基于角色的安全性，通过限制系统/子系统的全部或部分访问权限，仅允许授权用户组和个人用户进行访问？
- 借助您的解决方案，我能否集中管理和分析全部现有安全技术的遥测数据？
- 您的解决方案可否简化事件响应工作流程，缩短整体调查时间？

5.提供机会，提高工作效率，加强安全态势

您的 XDR 解决方案能否以更少的开销提高威胁检测和响应效率？

要为公司打造安全弹性，其中一个重要因素就是自动化和协调。安全人员承担重要任务。面对安全威胁时，无需耗费时间执行复杂的手动操作和重复的工作流程。XDR 解决方案可自动执行关键工作流程（例如发现警报、对警报进行关联分析、确定警报的优先级，然后快速采取响应措施），提高团队的工作效率，在整个生命周期中让团队可以腾出精力专注于更重要的工作。有效的 XDR 解决方案可提供清晰的决策和措施，推进调查进程，确保分析师能够根据其策略和程序以一致的自动化方式做出响应，从而缩短响应时间。这意味着 SecOps 团队可以将时间和精力投入到更具战略性和前瞻性的安全任务上，从而进一步加强公司的安全态势。

关键功能和能力	相关产品领域
• 自动追踪终端威胁，包括低危险威胁 • 确保管理员能够写入和扫描自定义感染指标 (IoC)	终端检测和响应 (EDR)
• 通过基于行为分析的洞察，预测网络威胁并采取补救措施	扩展检测和响应 (XDR)、网络检测和响应 (NDR)
• 自动确定电子邮件威胁补救措施的优先级	电子邮件安全

针对供应商的问题

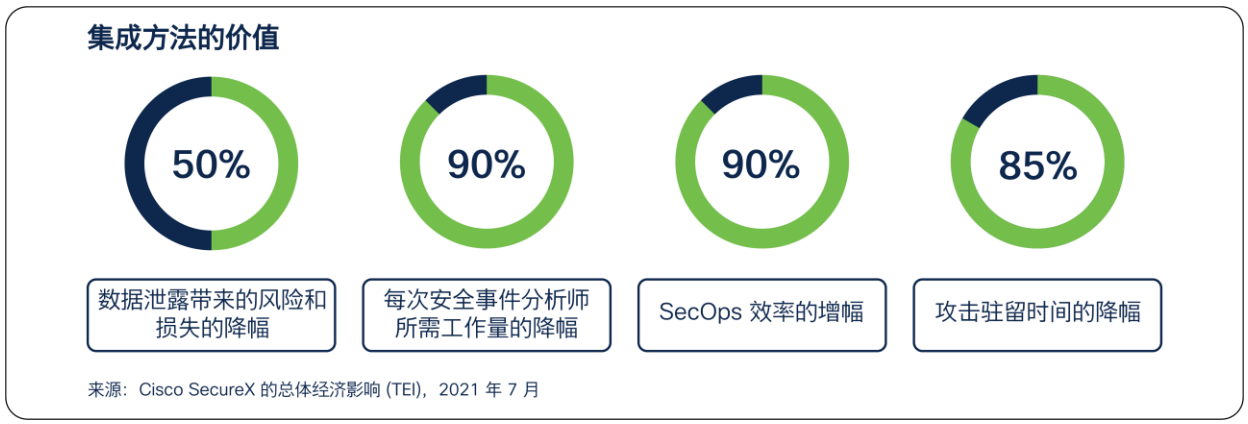
- 如果您使用的第三方集成的 API 发生了变化，是否会导致您的自动化脚本无法正常运行？
- 您的解决方案如何监控云工作负载的流量进出情况？
- 使用 XDR 解决方案时，我是否需要改变环境或部署新技术？
- 您的 XDR 解决方案是否提供与第三方安全技术的集成（预构建集成或开箱即用的集成）？
- XDR 解决方案是否可帮助分析师更快地调查和解决事件？
- 您的 XDR 解决方案是否支持策略管理，助力构筑弹性？

Cisco XDR

XDR 是安全弹性的重要组成部分

当今之世，不确定性乃是必然。为应对不确定性，公司大力投资从财务到供应链的各个领域，以期提升业务弹性。如果不对安全弹性（即保护企业免受威胁和干扰，从容应对变化，进而不断增强安全水平的能力）进行投资，所有努力都将功亏一篑。

要为企业打造安全弹性，XDR 不可或缺。正确实施 XDR 可让安全团队按影响确定威胁的优先级，更快检测到威胁并加快响应速度，从而增强安全态势。自动化和协调功能简化了这一过程，让安全团队能够腾出精力专注于最重要的工作。



利用 Cisco XDR 简化安全运维

思科拥有市面上高度全面的安全产品组合，在 XDR 领域处于领先地位。思科积极投资，力求开发高度全面的安全产品组合，预测未来的安全需求，并集成各种组件，确保所有团队都可以轻松、方便地采取有效的安全措施，而不受供应商或媒介的限制。我们深知，构建 XDR 方法需要一个过程。如今，行业中充斥着各种单点解决方案，我们希望您的团队能够摆脱保护措施孤立分散的恶性循环。Cisco XDR 的目标是探索从检测到响应的最短路径，同时尽可能保证整个流程的无缝运行。

Cisco XDR 由 SOC 专家精心设计，旨在简化安全运维，帮助安全分析师积极主动地灵活应对复杂威胁。我们的解决方案具有开放性、可扩展性和云优先等特点，因此您可以利用现有安全投资，在整个环境中实现统一的安全检测。

对客户而言，我们也是其客户，因此我们将恪尽职责，竭力保护客户资产。Cisco Security Cloud 是一个开放安全平台，可帮助您保护整个生态系统。无论未来发生什么，我们都希望能与您携手合作，共同打造安全弹性之旅。与我们携手共建全面安全的强大优势。

是否已做好准备，构建面向未来的安全运维？

探索 Cisco XDR

关键 XDR 要素和功能

在与 XDR 供应商交流过程中，请使用此表（第 9-10 页）作为快速参考。

关键要素	主要功能	符合要求的思科产品
提供按优先级排序且切实可行的遥测数据，随时随地为您所用	• 内置终端检测和响应 (EDR)，可完全托管，主动追踪威胁 • 基于风险的集成漏洞管理，助力快速识别漏洞、进行风险评分、确定优先级并采取补救措施	Secure Endpoint
	• 持续的云活动分析 • 高级分析，包括行为建模和机器学习算法 • 涵盖各种安全基础设施的统一视图，可提供统一的可视性和切实可行的汇总情报	Cisco XDR
	• 具有实时点击时间分析功能的高级病毒爆发过滤器	Secure Email
支持统一检测，不受媒介和供应商的影响	• 运行时检测，阻止运行程序的异常行为 • 支持在终端上实时进行高级操作系统查询 • 映射到 MITRE ATT&CK 框架的内置威胁追踪	Secure Endpoint
	• 实时检测整个云端的攻击，并提供精准的警报及丰富的相关情景信息（包括用户、设备、位置、时间戳和应用） • 确认检测结果后，隔离威胁 • 利用 NDR 检测恶意实体并自动隔离终端 • 检测与外部主机通信的内部主机 • 提供所有云事务的完整变更记录，提高调查分析的成效 • 内置与产品组合中的其他 XDR 解决方案的集成 • 通过内置、预打包或自定义集成与第三方解决方案集成，以实现互联后端架构和一致的前端体验 • 内置其他技术集成，涵盖云、终端、网络和应用（包括其他第三方技术）	Secure Network Analytics 和 Cisco XDR
	• 反垃圾电子邮件、URL 相关保护和控制、高性能病毒扫描、病毒爆发过滤器以及针对域功能的信誉扫描 • 伪造电子邮件检测，可防御针对高管的 BEC 攻击 • 自动执行恶意软件分析和沙盒	Secure Email
快速、准确应对威胁	• 利用全球特设安全运维中心 (SOC) 汇集的威胁情报和洞察，为广大客户群提供无间断的保护	所有 Cisco Secure 产品
	• 持续监控所有终端活动，提供运行时检测并阻止异常行为	Secure Endpoint
	• 在不影响隐私和数据完整性的情况下识别并隔离加密流量中的威胁 • 一站式触发 “响应” 工作流程 • 威胁响应，通过 API 汇聚来自安全产品数据源的情景感知信息以及来自 Talos® 和第三方来源的全球威胁情报 • 创建事件调查案例手册	Cisco XDR
	• 通过对潜在恶意链接的实时分析，针对基于 URL 的威胁提供持久防御 • 持续利用实时 Talos® 监控、分析和威胁情报来识别以前未知的威胁或突发变化	Secure Email

关键要素	主要功能	符合要求的思科产品
提供统一调查视角，简化用户体验	• 利用统一视图收集全球情报，展开关联分析，从而加快威胁调查 • 创建自定义响应操作，缩短响应时间 • 自动从多个数据源提取信息，并结合威胁情报进行综合分析	Cisco XDR
提供机会，提高工作效率，加强安全态势	• 自动识别低危险可执行文件并进行威胁分析 • 能够编写自定义 IoC，扫描整个终端部署中的感染后指标。	Secure Endpoint
	• 行为建模、多层机器学习和全球威胁情报 • 在新设备角色添加到网络时自动对其进行分类 • 与 XDR 解决方案集成，实现跨所有威胁媒介和无线接入点的自动化	Secure Network Analytics 和 Cisco XDR
	• 自动触发动态信誉分析，帮助了解电子邮件中恶意软件的来源、受影响的系统以及恶意软件的行为 • 根据获得的补救措施洞察，对入站和出站电子邮件采取行动	Secure Email
	• 预先建立与常见使用案例一致的工作流程，实现常规任务自动化 • 在 SecOps 团队之间共享行动指南 • 自动对来自其他安全产品组合解决方案的警报进行分类并确定其优先级	Cisco XDR

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。

美国印刷 C07-3236254-03 04/23