

# Cisco Breach Protection Premier

保障运营可靠性和未来安全，加速实现价值

Cisco Breach Protection Suite 充分集成思科安全产品组合以及部分第三方工具，打造统一的威胁检测、调查、缓解和追踪解决方案，全面保护终端、邮件、网络和云。但是，有些组织并不具备部署和管理此类解决方案的能力或专业知识。对于这些组织，托管服务正好可以满足其需求。

Cisco Breach Protection Premier 利用组织目前已有的工具和遥测数据源，提供无可比拟的专业知识和指导，还可随着组织整体安全战略中多层安全措施与解决方案的扩展和增加而不断发展，无论您和您的团队当前处于什么状况，都能提供全面的保护。

## Cisco Breach Protection Premier 级许可证

订用 Cisco Breach Protection Premier 级许可证，可获得由思科安全专家精英团队全力支持的托管扩展检测和响应 (MXDR) 服务。该服务具体包括以下内容：对思科安全解决方案的集成支持、思科与部分第三方安全工具的精选集成、思科软件支持服务 (SWSS) 增强版、通过思科技术安全评估 (CTSA) 服务提供的安全评估、验证和增强功能，以及部分 Cisco Talos 事件响应 (Talos IR) 服务。

思科托管扩展检测和响应 (MXDR) 服务得到思科研究人员、调查人员和响应人员精英团队的大力支持，涵盖 Cisco XDR 解决方案、一体化工具集和其他思科安全技术，可用于监控潜在安全威胁和漏洞并及时做出响应。

### 由 Cisco XDR 提供支持的 MXDR 服务包含以下功能：

- 通过思科安全运营中心 (SOC) 全天候持续监控安全事件和警报。
- MXDR SOC 分析师负责根据既定策略分析平台数据，对所有事件进行关联分析，丰富事件情景信息，确定事件优先顺序并对其进行评估。
- 根据需要上报潜在安全事件。
- 引导式响应行动有助于遏制、缓解或消除威胁并采取补救措施。我们将根据预先批准的响应策略，代表您执行调查和响应行动。

- 季度威胁简报提供有关当前威胁模式、检测和热门事件的最新信息。
- 威胁公告有助于识别最新发现的威胁，通过实施缓解控制措施帮助主动预防事件。

**CTSA** 提供全套主动式服务，评估您的网络安全准备情况，并针对您面临的威胁、发生威胁的可能性以及对运营弹性的影响提供建议。服务包括（但不限于）：

- 威胁建模/缓解/模拟
- 渗透测试

- 红队/蓝队/紫队协作
- 安全架构评估
- 应用/SOC/DevOps 评估
- 构建/配置审核

**Talos IR** 提供全套主动式服务和紧急服务，可以帮助您针对网络安全事件进行准备、做出响应并从中恢复。

Talos IR 和 CTSA 服务时长会累计，具体取决于为覆盖用户 (CU) 购买的 Cisco Breach Premier 许可证数量。可以通过 Talos IR 和 CTSA 定制服务购买额外服务时长。

服务	最低小时数
按需情报服务	5
漏洞易感性研讨会	5
组织数字足迹评估	10
安全设计思维研讨会	20
紧急事件响应*	40
渗透测试	40
威胁建模	40
设备配置和构建审核	40
IR 计划	50
IR 策略	50
桌面练习	50
安全架构评估	80
IR 就绪性评估	80
感染评估	80
Cyber Range 网络防御环境模拟	80
主动威胁追踪	100
红队威胁模拟	160
紫队协作	160
安全运营评估	160

\* 所购服务时长为 20 至 39 小时的客户可享有限的紧急事件响应服务

借助思科提供的托管服务，保障运营可靠性和未来安全，加速实现价值。

详情请访问：[cisco.com/go/breach-protection](https://www.cisco.com/go/breach-protection)