Microsoft Security

转为采用集成式威胁防护的 3 个原因

目录

引言

现在，普通企业都会使用超过 30 种不同的安全工具，这些工具通常互不关联并作为“追加项”存在。

安全问题迎来变革的转折点。网络攻击正变得越来越复杂，组织需要持续应对各种挑战，包括人才短缺、成本平衡，以及化解混合工作带来的压力。

与此同时，如今的安全市场比以往更为分散和复杂。现在，普通企业都会使用超过 30 种不同的安全工具，这些工具通常互不关联并作为“追加项”存在，无法为安全运营中心 (SOC) 提供足够深入的信息及见解。

安全和合规性领导者需要更全面地认识最新的风险和威胁，还需要了解哪些安全工具有用、哪些工具无用，以及他们在哪方面存在不足。

虽然当今面临的安全挑战看起来形势严峻，但对于希望提高安全运营效率和效力的首席信息安全官 (CISO) 来说，仍然有理由保持乐观。挑战的解决之道就在于集成式端到端网络威胁防护方法，这种方法可以帮助组织：

原因 1：实现事半功倍的效果

整合单点解决方案并降低安全运营 (SecOps) 开销。

原因 2：助力 SecOps 专注于高价值任务

使用工具以提高效率，甚至相比以往提升初级分析师的能力。

原因 3：提高员工工作效率

保护你的组织，让员工安心进行创造和创新。

集成式端到端威胁防护方法之所以能够实现，得益于扩展检测和响应 (XDR) 解决方案与使用人工智能 (AI) 和自动化功能的云原生安全信息和事件管理 (SIEM) 系统的集成。此集成式解决方案可提升你的 SOC 在应对整个企业范围的攻击时提前预测、主动响应、积极预防的能力。

原因 1

实现事半功倍的效果

通过将工具与 Microsoft 的集成解决方案相整合，你还能节省成本，只需为自己使用的内容付费。

许多组织已采用以出色的单点解决方案为核心的安全工具。遗憾的是，实际上这种方法会使安全专业人员更难以快速识别和应对威胁。此外，还可能会对 IT 支出和最终用户工作效率产生负面影响。

如果组织期望实现事半功倍的效果，Microsoft SIEM 和 XDR 等集成式方法可以提供帮助。这种方法通过整合各个工具来降低复杂度，并且由于云原生的特性，集成式解决方案还可以提高性能和扩大规模。

通过将工具与 Microsoft 的集成解决方案相整合，你还能节省成本，只需为自己使用的内容付费。你还可以通过提高自动化和集成水平，降低管理解决方案所需的 SecOps 开销。

> 开始采用全新的安全工具很容易，因为如你所料，可能存在很大的安全差距。此后，你很快就会意识到，来自不同供应商的工具可能在任务上存在重叠。这样的重叠对于检查和平衡可能是必要的，**但也可能需要付出巨大的财务成本。**”
>
> **Jonathan Cassar**
> MITA 首席技术官

160 万美元

由于供应商整合每年实现的成本节省

Microsoft 委托 Forrester Consulting 进行了 Total Economic Impact ™ (TEI) 研究，揭示了企业通过部署 Microsoft SIEM 和 XDR 可能实现的潜在投资回报率 (ROI)。该研究通过调查一个假设的拥有共 8,000 名员工和 10 名安全专业人员的复合型组织，得出了以下重要发现：

- **供应商整合每年实现近 160 万美元的成本节省。**该复合型组织通过进行 Microsoft SIEM 和 XDR 投资，降低了其之前的 SIEM 成本（560,000 美元）、相关的本地基础结构成本（超过 360,000 美元）、三个 XDR 单点解决方案成本（192,000 美元）以及管理这些方面所需的持续人工成本（480,000 美元）。
- **将发生重大数据泄露的风险降低 60%。**借助更高效的安全调查和响应工作流，改进的安全响应自动化功能，以及增强的保护所有计算环境的能力（包括多云保护），该复合型组织降低了数据泄露风险，每年节省成本近 160 万美元。
- **实现 207% 的投资回报率。**代表采访和财务分析发现，该复合型组织在三年内获得了 1,768 万美元的收益，而成本仅为 576 万美元，净现值 (NPV) 增加了 1,192 万美元。

原因 2

助力 SecOps 专注于高价值任务

有必要集成 SIEM 和 XDR 以关联警报、确定最大威胁的优先级以及协调整个企业的行动。

SecOps 团队由于需要分析大量的信号而不堪重负，这些信号中包括许多低保真信号，难以（即使不是不可能）手动检测和减少。随着威胁的增加，超负荷运转的 SOC 很难应对这么大的工作量，特别是在尝试分析来自多个单点解决方案的数据时。分配更多的资源来填补缺口并不能真正解决问题，因为熟练安全专业人员数量不足这个问题始终摆在面前。

因此，有必要集成 SIEM 和 XDR 以关联警报、确定最大威胁的优先级以及协调整个企业的行动，同时借助高级 AI 和自动化功能来主动检测和修复威胁。

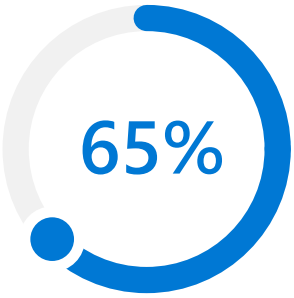
例如，单个的低水平信号可能不会获得传统 SIEM 的太多关注。但使用 AI 后，云原生 SIEM 可以自动将信号与来自整个组织的其他来源的信号进行比较，跨多个数据集进行关联，以发现多阶段攻击。

集成式 SIEM 和 XDR 可释放 SecOps 资源，同时还能增强初级分析师的能力和信心。

然后，系统可以对数据进行规范化处理，并分析和关联数据，同时提供有关网络攻击如何进入基础结构的背景信息以及其传播情况的时间线。这样，SOC 团队就可以从单个控制台中直观地看到漏洞并有效地解决漏洞。

> 许多 CISO 并没有意识到 **20 种不同的‘单一界面’**或单点解决方案**给其团队带来的工作量**以及相关的年度成本 ... 通过与单一供应商合作，我们无需再疲于应对各种工具。”
>
> **Terence Jackson**
> Thycotic 首席信息安全和隐私官

组织不需要掌握深入的专业知识就能发挥安全解决方案的价值。集成式 SIEM 和 XDR 可释放 SecOps 资源，同时还能增强初级分析师的能力和信心。



Microsoft SIEM 和 XDR 的集成式方法将用于调查威胁的时间缩短了 65%。

Microsoft 委托进行的 Forrester Total Economic Impact™ (TEI) 研究表明，实现这种 SecOps 效率的复合型组织能够：

- **将用于调查威胁的时间缩短 65%，将用于响应威胁的时间缩短 88%。**通过 Microsoft SIEM 和 XDR 的集成式安全威胁调查和响应方法，复合型组织的安全专业人员能够更高效地执行这些工作流。他们不再需要在多个工具之间快速切换来识别威胁，而且安全自动化功能也能够进一步改进响应工作流。

- **将用于创建新工作簿的时间缩短 90%，将用于对新入职的安全专业人员进行培训的时间缩短 91%。**Microsoft SIEM 和 XDR 的集成式方法还有助于提升其他安全专业人员工作流的效率。由于 SIEM 日志集成在整个解决方案套件中，因此创建工作簿几乎可以自动完成，而借助单一登录，新的安全专业人员能够提前近 16 周完成入职培训。

原因 3

提高员工工作效率

集成式 SIEM 和 XDR 解决方案可以帮助你的组织提高最终用户的工作效率。

集成式 SIEM 和 XDR 解决方案除了可以实现事半功倍的效果和提高 SecOps 效率，还可以帮助你的组织提高最终用户的工作效率。

正如 SecOps 团队所知，如果做好妥善的安全防护，人们就可以在安全的环境中工作。因此，如果最终用户体验没有帮助提高员工工作效率，反而是造成了阻碍，则组织可能会因此面临更多的安全风险和更高的成本。密码薄弱或丢失、通过个人设备进行不安全访问或敏感数据自由共享只是一部分挑战。

> [过去] 我们没有利刃来解决人们遇到的问题，而只能关闭一切并禁止访问，这对我们的业务产生了负面影响。所有人都很清楚这一点，因为一切都会暂时停止运转。Microsoft Sentinel 为我们提供了一种工具，使我们能够像用手术刀做手术一样应对所发生的情况。**当我们正在应对威胁时，整个企业甚至都察觉不到**，这是衡量我们成功与否的重要标准。”
>
> **Rick Gehringer**
> Wedgewood 首席信息官

接近
68,000
Microsoft SIEM 和 XDR 提高了其他员工的工作效率，每年节省接近 68,000 工时。

集成式 SIEM 和 XDR 方法可帮助你提供无缝的用户体验，让员工在其日常体验的各个方面都能保持高效和安全。该方法可以降低对工作效率的负面影响，例如必须关闭服务或进行隔离，然后对机器重置映像。除此之外，集成式 SIEM 和 XDR 还可以为提高最终用户的工作效率创造新的机会，例如提供更多的自助式安全支持、更出色的仪表板和报告，以及通过减少问题经过的安全代理数量来加快响应速度和缩短启动时间。

在 Microsoft 委托进行的 Forrester Total Economic Impact ™ (TEI) 研究中，一个假设的拥有共 8,000 名员工的复合型组织表明，通过部署 Microsoft SIEM 和 XDR 可以提高员工的工作效率：

- **提高了其他员工的工作效率，每年节省接近 68,000 工时。** Microsoft SIEM 和 XDR 可防止低效的安全流程对其他员工产生负面影响。例如，由于 IT 专业人员学会了如何自助处理相关安全更新和建议，该复合型组织每年可节省 4,000 工时。此外，该组织还能够对员工计算机进行基于远程安全性的故障排除，减少了进行故障排除的安全代理数量，这提高了最终用户的工作效率，每年节省接近 64,000 工时。

安全性已成为实现技术成功的重要推动因素。正因为此，组织需要采取安全措施，尽量提高针对现代攻击的复原能力，从而保护和提升工作效率和创新能力，以实现增长。

借助 SIEM 和 XDR 实现集成式网络威胁防护

此方法集成了行业领先的产品，通过一个全面的解决方案提供网络威胁防护、检测和响应。

Microsoft 提供业内首个也是唯一的集成式 SIEM 和 XDR 解决方案，可在所有云和平台中实现端到端可见性。此方法集成了行业领先的产品，通过一个全面的解决方案提供网络威胁防护、检测和响应。

Microsoft SIEM 和 XDR 利用强大的 AI 和自动化功能，以及在网络威胁检测和分析方面的深度持续投资，每天提供对 43 万亿个信号的专家见解和深入信息。借助这些产品的集成，SOC 团队将能够相比以往获得更多的背景信息，从而更快地发现和解决关键网络威胁：

Microsoft Sentinel

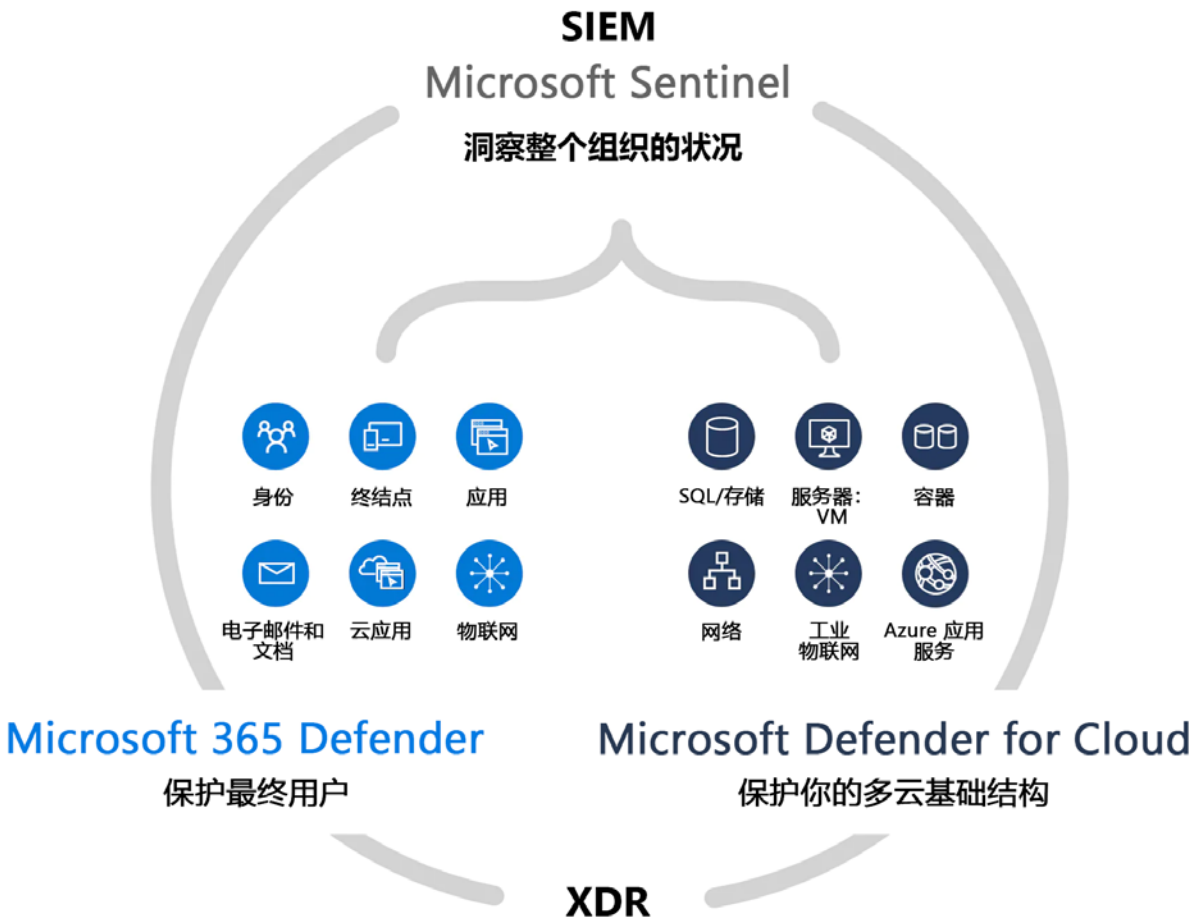
借助 Microsoft 的云原生 SIEM 了解企业的整体概况。通过内置的编排和自动化功能，聚合几乎任何来源的安全数据，应用 AI 以将噪音信号与合法事件分开，跨复杂网络攻击链关联警报，以及加快网络威胁响应。

Microsoft Defender XDR

借助XDR功能防止和检测跨身份、终结点、应用、电子邮件、数据和云应用的网络攻击。利用现成的卓越保护功能调查和应对网络攻击。通过单一仪表板发现威胁并轻松地协调你的响应。

Microsoft Defender for Cloud

通过内置的 XDR 功能保护你的多云和混合云工作负载。保护你的服务器、存储、数据库、容器等。通过区分优先级的警报专注于最重要的事情。



安全保护不应追加，而应内置。

让合适的人员掌控合适的工具和情报。借助端到端的云原生集成解决方案防御现代攻击。

详细了解 Microsoft 的 SIEM 和 XDR 解决方案如何提供集成式网络威胁防护 >

Microsoft Security