McAfee Endpoint Security

专为运营调查和安全控制设计的安全产品

终端安全：您最关注什么？

在当今业务中，可能只有一个团队需要关注安全，也可能有多个团队需要关注安全。对于企业组织，安全则通常是一个职能部门，由多个团队（如 IT 管理和安全运营团队）共担职责。不管哪一种情况最符合您在业务中所扮演的角色，当涉及终端保护平台时，对您来说，最重要的事务自然会让您更关心的功能和结果集也有所不同。

您所依赖的终端解决方案的功能应与您最关注的事务的优先级保持一致。不管您的角色为何，McAfee® Endpoint Security 都能满足您的特定关键需求 — 从防范和追踪威胁到定制安全控制。凭借 McAfee Endpoint Security，您可以为用户确保系统正常运行时间，找到更多实现自动化的机会，并且简化复杂的工作流程。

确保正常运行时间和可见性

利用主动防御和补救工具，McAfee Endpoint Security 可让客户响应和管理威胁防御生命周期。自动回滚补救可将系统还原到健康状态，确保用户和管理员不中断工作，从而节省等待修复系统，执行恢复或重新映射受感染的机器所需要的时间。在终端与集成的 McAfee® MVISION EDR 之间共享全球威胁情报和实时本地事件情报，以便收集威胁事件详细信息，检测和阻止尝试规避检测的威胁，并将其映射到 MITRE ATT&CK 框架以供将来进行调查。通过可选择的本地、SaaS 或虚拟环境部署的集中式管理控制台，管理工作变得简单易行。

McAfee Endpoint Security 从使用单一软件代理的多个接触层收集威胁见解，从而消除多点产品产生的冗余性。其结果是采用一种集成的安全方法，消除了人工威胁关联，并且能够自动向事件响应者提升需要进一步调查的详细信息。通过 Story Graph 以简明易读的格式呈现威胁事件数据，从而可视化威胁详细信息，并支持管理员轻松深入研究和调查恶意攻击者的来源。

联系我们

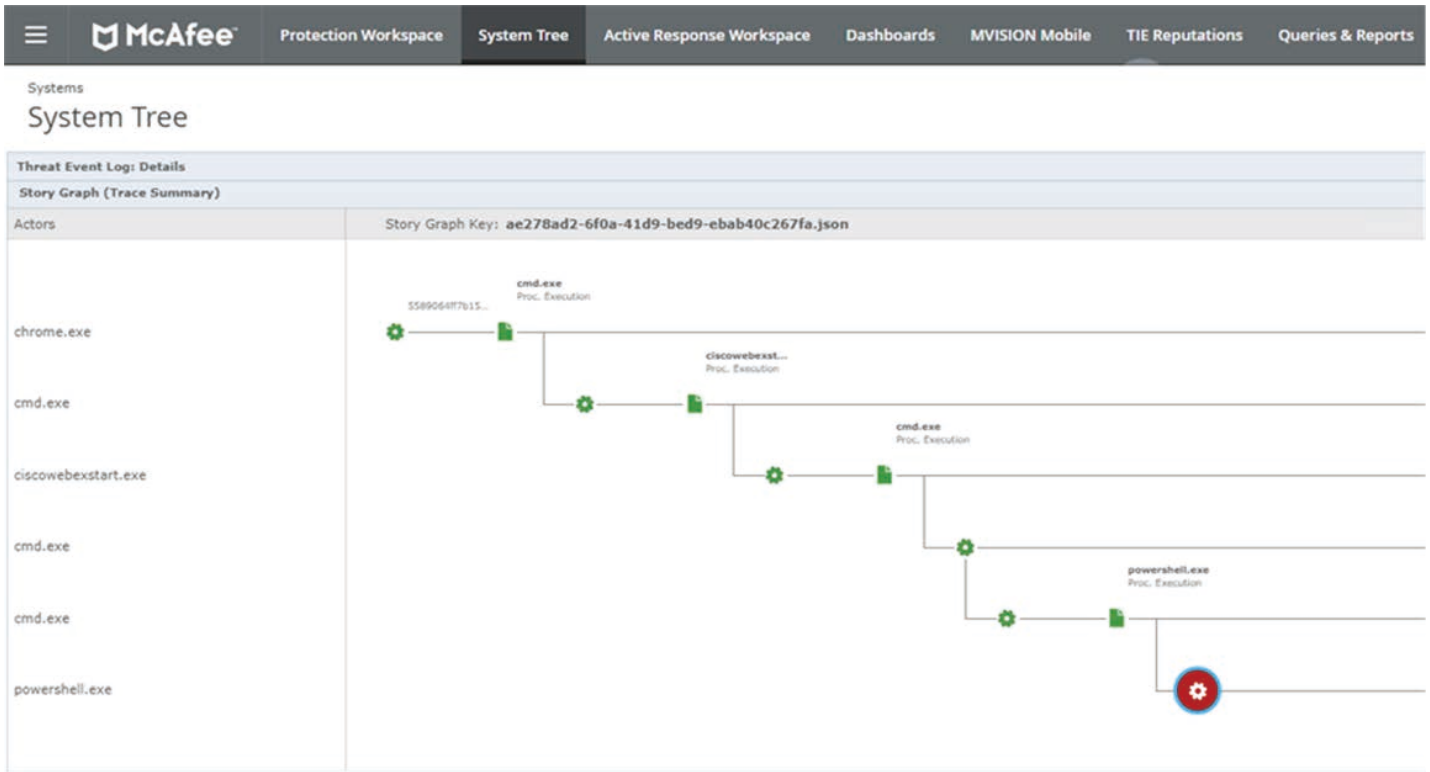

图 1. Story Graph。

集成的高级威胁防御实现自动化响应并将响应速度提高数倍

其他高级威胁防御（如动态应用程序遏制 (DAC)）也作为集成的 McAfee Endpoint Security 框架的一部分提供，可帮助组织防范最新的高级威胁。[1] 例如，DAC 对灰色软件和其他新兴恶意软件进行分析，并采取相应的措施遏制它们，防止感染。

针对高级威胁的另一种技术是 Real Protect。该技术使用机器学习行为分类来检测零日恶意软件并改善检测效果。无签名分类在云中执行，不仅可以提供近实时的检测，而且占用的客户端空间也非常小。还提供了切实可行的见解，您可以使用这些见解来创建攻击指标和攻陷指标。这对横向移动检测、第一传染源发现、威胁攻击者属性、取证调查和补救非常有用。

Real Protect 还可以通过自动进化行为分类来提高未来分析的速度，从而使用静态和运行时功能识别行为并添加规则，以识别类似的未来攻击。

最后，为了立即阻止感染和减少 IT 安全管理员所需要的时间，客户端根据最后一次确定的良好状态修复终端。

智能化终端保护让您对攻击者的所作所为了如指掌

智能化程度越高，结果越优秀。McAfee Endpoint Security 与连接到其框架的多种终端防御技术实时共享其观察结果，从而进行协作并加快识别可疑行为的速度，促进更好的防御协调，并对针对性攻击和零日威胁提供更好的保护。跟踪文件哈希、来源 URL、AMSI 和 PowerShell 事件等见解，不仅可以与其他防御技术共享这些信息，还可以与客户端和管理界面共享，从而帮助用户理解攻击，为管理员提供切实可行的威胁取证。

此外，凭借 McAfee® Threat Intelligence Exchange 技术，自适应防御技术可以与其他 McAfee 解决方案（包括网关、沙盒）和我们的安全信息和事件管理 (SIEM) 解决方案协作。收集和分发本地、社区和全球安全情报，从而将攻击、发现与遏制之间的时间从数周或数月缩短至毫秒级。

通过与 McAfee® Global Threat Intelligence (McAfee GTI) 相结合，McAfee Endpoint Security 框架利用云跨所有媒介（文件、Web、消息和网络）实时监控和响应全范围的新威胁和新兴威胁。利用本地和全球威胁情报，现有终端占用空间和管理系统得到了增强，从而即时抵御未知和针对性恶意软件。针对可疑应用程序和进程的自动操作可快速升级响应，从而防范新威胁和新兴形式的攻击，同时通知其他防御技术和全球社区。

使用 DAC 和 Real Protect 的客户可以获得更多高级威胁及其所展现的行为的见解。例如，DAC 可提供关于遏制的应用程序及其尝试获取的访问权限类型（如注册表或内存）的信息。

对于有兴趣收集终端进程威胁见解以追踪恶意软件和装备事件响应程序的组织来说，Real Protect 是不二之选，它可以提供对已被视为具有恶意的行为的见解，还可以对威胁分类。这些见解对于揭示基于文件的恶意软件如何尝试通过打包、加密或滥用合法应用程序等技术来规避检测尤其有帮助。

强大高效的性能，助您及时作出响应

如果智能防御扫描速度缓慢，安装时间过长或管理操作复杂，则会对用户造成消极影响，其价值也必将大打折扣。McAfee Endpoint Security 利用公共服务层和我们新的防恶意软件核心引擎来保护用户的生产力，有助于减少用户系统所需的资源和能源。终端扫描仅在设备处于空闲状态时才会执行，并且可以在重启或关机后无缝恢复，因此不会影响用户的生产力。

通过了解哪些进程和来源可信，以便将资源集中在可疑或来自未知来源的进程和源上，自适应进程扫描还有助于降低 CPU 需求。McAfee Endpoint Security 具有集成的防火墙，利用 McAfee GTI 来保护终端，防范僵尸网络、分布式拒绝服务 (DDoS) 攻击，高级持久性威胁和危险的 Web 连接。

降低复杂性，提高可持续性，减轻压力

安全产品的数量与日俱增，不同的产品使用不同的管理控制台，但同时又具有相同或类似的功能，这使得很多组织难以清晰了解潜在的攻击威胁。凭借开放式和可扩展的框架，将其作为集中当前和未来终端解决方案管理的基础，McAfee Endpoint Security 可提供强大而持续的保护。该框架利用 Data Exchange Layer 来实现与其他现有安全投资的跨技术协作。该集成基础架构与 McAfee 的其他产品无缝集成，进一步减少了安全差距、孤立的技术和冗余性，同时通过降低运营成本和管理复杂性来提高生产率。

通过提供单一管理控制台来监控、部署和管理终端，McAfee® ePolicy Orchestrator® (McAfee ePO™) 软件可以进一步降低复杂性。可定制的视图和可操作的工作流采用易于理解的语言，提供了快速评估安全状况和定位感染的工具，并通过隔离系统、拦截恶意进程和阻止数据泄露来减轻威胁影响。它还提供了一个单独的位置来管理每个终端、其他 McAfee 功能和 130 多个第三方安全解决方案。

功能	需要的理由
Real Protect	▪ 机器学习行为分类可近乎实时地检测零日威胁，并生成切实可行的威胁情报。 ▪ 自动进化行为分类以识别行为和添加规则，从而识别未来的攻击。
防范针对性攻击的终端保护	▪ 将遭遇攻击到遏制攻击的响应时间从数天缩短到毫秒级。 ▪ McAfee Threat Intelligence Exchange 从多个来源收集情报，使安全组件能够即时相互通信，从而了解新兴的和多阶段的高级攻击。 ▪ AMSI 和 PowerShell 事件日志记录可揭示和帮助防范无文件以及基于脚本的攻击。
智能化自适应扫描	▪ 通过绕过受信任进程的扫描并优先扫描可疑进程和应用程序，从而提高性能和生产率。 ▪ 自适应行为扫描监控并锁定威胁，同时根据可疑活动升级响应。
回滚补救	▪ 自动恢复恶意软件执行的更改，并将系统还原至其最后已知的健康状态，同时保持用户的生产力。
前瞻性 Web 安全措施	▪ 对终端使用 Web 保护和过滤，确保安全浏览。
动态应用程序遏制	▪ 防范勒索软件和灰色软件并阻止“第一传染源”。[2]
阻止恶意网络攻击	▪ 集成式防火墙使用基于 McAfee GTI 的信誉评分来保护端点免受僵尸网络、DDoS、高级持久性威胁和可疑 Web 连接的攻击。 ▪ 防火墙保护在系统启动时仅允许出站流量，从而保护不在公司网络中的终端。
Story Graph	▪ 管理员可以快速查看受感染位置、受感染原因，以及受感染的时长，进而更加快速地了解威胁并做出反应。
可选择多种部署方式的集中式管理（McAfee ePO 平台）	▪ 真正的集中式管理可提高信息透明度，简化操作，提升 IT 部门工作效率，统一安全防护并降低成本。
开放式可扩展终端安全框架	▪ 集成式基础架构可让终端防御进行协作和通信，进而实现更坚固的防御。 ▪ 通过消除冗余和优化流程，降低运营成本。 ▪ 通过与其他 McAfee 和第三方产品无缝集成，从而缩小保护差距。

表 1. 关键功能以及需要这些功能的原因。

获得防范网络威胁的优势

McAfee Endpoint Security 为当今安全从业人员提供了战胜攻击者优势的必需功能：智能化的协作防御和可简化复杂环境的框架。凭借第三方测试已经证明的强大而有效的性能和威胁检测有效性，组织可以保护他们的用户，提高生产力并解除后顾之忧。

作为终端安全防护行业的领导者，McAfee 提供了一整套解决方案，通过将强大的保护与高效的管理相结合，提供深度威胁防御。该产品可提高安全防护工作的效率和效果，并提高管理工作的效率和效果，因此可帮助安全团队在较短的时间内使用更少的资源解决更多威胁。

轻松实现迁移

对于部署了 McAfee ePO 软件、McAfee VirusScan® Enterprise 和 McAfee Agent 最新版本的环境，利用我们的自动迁移工具，只需不到 20 分钟即可将现有策略迁移到 McAfee Endpoint Security。[3]

McAfee Endpoint Security 还提供了以下优势：

- 对用户毫无影响的扫描，从而提高用户工作效率。
- 映射到 Story Graph 中的更强大的取证数据，提供了一目了然的见解，并简化了调查流程，从而帮助您加强策略。
- 通过回滚补救自动恢复恶意软件更改和保持系统健康。
- 要管理的代理数量更少，忽略无需扫描的对象，从而减少人工干预。
- 通过共同作用的协作防御来应对高级威胁。
- 可将下一代框架直接嵌入我们的其他高级威胁以及终端检测和响应 (EDR) 解决方案。

了解更多信息

要了解 McAfee Endpoint Security 的更多信息，请访问此处。

要了解有关 McAfee Endpoint Security 如何补充 McAfee 产品组合的更多信息，请访问：

- MVISION Endpoint
- MVISION 产品系列
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator

1. 大部分 McAfee 终端套件中有提供。有关详细信息，请咨询销售代表。
2. 同上。
3. 迁移时间取决于您的现有策略和环境。

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn

2019 年 11 月