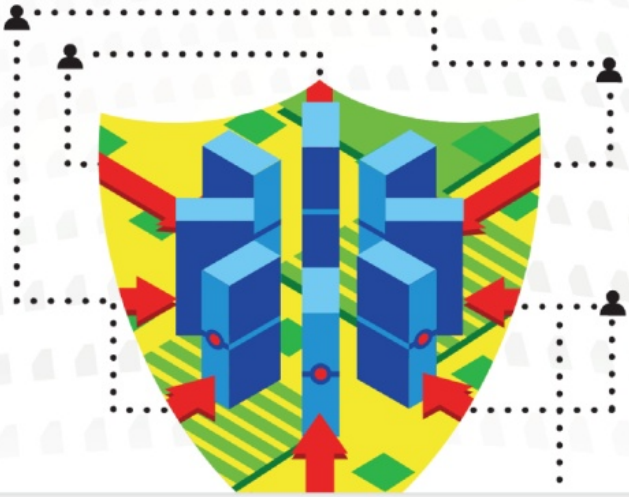
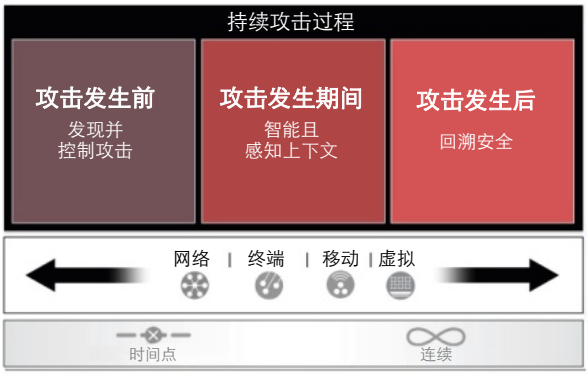
高级恶意软件防护买家判断标准



简介

众所周知，当今技术高明的攻击者拥有丰富资源、专业知识与不懈耐心，随时危害各种机构的安全。传统的防御措施，包括防火墙和终端保护等，已不再能够有效抵御这些攻击，也就是说，应对恶意软件的流程必须快速发展，才能与时俱进，提供完美保护。这其中首先须有以下认识：检测到恶意软件以及它们所带来的、持久且有针对性的攻击，非常重要，绝非单一时间点控制措施或产品能够单独完成的。高级恶意软件防护需要一套集成控制措施和一个持续流程，来检测、确认、跟踪、分析和修复这些威胁 – 涵盖攻击发生前、发生期间和发生后的所有阶段。

现在的形势日益严峻。随着多态恶意软件的出现，机构每小时都要面对数万新恶意软件的攻击，而且攻击者可以使用相当简单的恶意软件工具来成功入侵设备。将文件与已知恶意软件签名相匹配的黑名单方法，其扩展速度已无法满足实际需求，而沙箱等较新检测技术则非100%有效。在本《高级恶意软件防护买家判断标准》中，我们将提供一些在您购买高级恶意软件防护时，应向厂商提出的关键问题，此外，



回溯安全是Sourcefire所特有的技术，也是应对高级恶意软件的基础。它具备持续功能，能够利用大数据分析来汇总扩展网络上的数据和事件，进行长期文件跟踪与分析，对于过去认为安全而现在确定恶意的文件提供报警并修复。

我们还将介绍 Sourcefire 是如何将大数据分析，集体安全智能信息，跨网络、终端、虚拟系统和移动设备的全方位防护，以及独特的回溯安全（Retrospective Security）相结合，游刃有余地应对当前爆炸式恶意软件攻击的。

向高级恶意软件防护厂商提出的关键问题

1. 您如何利用大数据来持续判别恶意软件?
2. 如何分析恶意软件，以精确确定它的行为?
3. 您的恶意软件分析如何为所有控制点乃至所有客户自动更新检测功能?
4. 您如何收集有关新兴恶意软件威胁的智能信息?
5. 您如何执行持续分析，以便回溯检测恶意软件?

应用大数据分析和集体安全智能来解决恶意软件问题

随着已知恶意软件呈指数增长，为尝试更好地服务于客户，传统终端保护厂商推出了"云辅助防病毒"功能，将签名数据库迁移到了云中。这解决了每隔五分钟就需要向每个终端分发数十亿病毒签名的问题，但并不能有效应对日前正蓬勃发展的、专为逃避签名检测而设计的高级恶意软件。

云辅助防病毒模式的另一限制是，攻击者很有耐心，会花费大量时间来达到其目的。大多数防恶意软件技术的缺点都在于缺乏持续性和上下文感知能力，重点主要是在初次发现某一文件时检测其是否为恶意（时间点）。但是，现在看起来不是恶意软件的文件，在将来（甚或明天）就可能很容易地变为恶意软件。所以我们需要的是持续分析能力，能够长期监控，并根据最新威胁智能，将文件状态从最初的无害改为恶意。

高级恶意软件编写者创造并使用各种技术，来掩盖恶意软件的意图，使其更难被发现。这其中包括旨在欺骗签名引擎的多态文件变换，从命令和控制（CnC）网络上按需获得恶意软件的高级下载器，以及能够删除自己的组件，使得检验员很难发现并分析恶意软件的可擦除木马等等，各种技术层出不穷。鉴于恶意软件不再能够根据"表象"识别，我们需要新技术，在恶意软件的生命周期中捕获它们并加以分析，了解它们的行为、它们的目标，以及在初始检测期之后发现时间点检测技术所无法识别的恶意操作和感染指标。

Sourcefire已采取更加面面俱到的新方式来迎接上述检测恶意软件的挑战。在全球数千企业客户和数百万在用终端恶意软件防护代理的支持下，Sourcefire每月收集的恶意软件样本超过百万之多。在Sourcefire的Collective Security Intelligence Cloud中，分析数万软件特性，以便将恶意软件与正常软件区分开来。此外，也会分析网络流量特征，以检测出恶意软件对于CnC网络的搜索。Sourcefire还利用其庞大的部署产品群，来确定从全球角度以及从每个特定客户机构角度来说，哪些属于正常文件和网络行为的范畴，以便比较。

为了检测出专为逃避传统检测方法而设计的恶意软件，需要更加先进的手段。Sourcefire采用特别定制模型，根据恶意软件的行为而非表象来进行识别，能够检测出新型攻击，甚至零日攻击。为保证与恶意软件变化速度同步，这些模型会根据Sourcefire VRT®（漏洞研究团队）所发现的新攻击途径，而自动实时更新。

Sourcefire的集体安全智能（Collective Security Intelligence）的优势还远不仅此，当文件通过任意检测点时，Sourcefire的云分析功能将在超长时间内，根据最新威胁智能信息，持续评估此文件，使得Sourcefire的高级恶意软件防护（Advanced Malware Protection）解决方案（Sourcefire AMP）能够在文件初始分析后很长一段时间内，如果出现问题，依然可以报警。

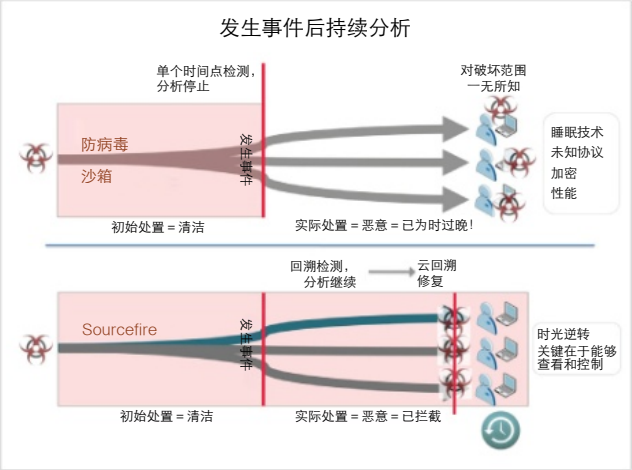
最后，这些优势将使整个Sourcefire AMP社区受益，每当对于某个文件的处置方式发生变化，都会通知整个社区。藉此，所有利用Collective Security Intelligence Cloud的机构都能立即了解恶意文件，借助云的力量，实现"集体免疫"。

__回溯安全：__采用持续分析功能，对于初始判断为正常或未知、而之后确定为恶意的文件报警。回溯安全能够确定攻击爆发的范围、遏制攻击，并最终逆转时光，自动进行恶意软件修复。

回溯安全逆转时光，使攻击者无处遁形

攻击者并非静止不动。他们不断评估当前安全技术，变换其战术方法，力争领先于防御措施。实际上，大多数攻击者在发起攻击前，会针对领先防恶意软件产品来测试其恶意软件，以确保攻击成功。随着黑名单方式效果的减弱，越来越多的安全产品公司依靠虚拟机（VM）动态分析，来研究和应对恶意软件。而同时，攻击者也调整了战略战术，他们假设如果评估期文件不进行任何恶意行为，则文件会被判别为安全，所以，在VM中运行时，他们或者不作为，或者延迟几小时（或几天）后再攻击。当然，一旦等待期过去，受害者的设备就会被损坏。不幸的是，目前，各种单个时间点的技术都无法再次对这些文件进行分析。如果一个文件被判定为安全，则无论是检测技术进行了改进，还是文件表现出恶意行为，它的状态依然是安全。更糟的是，当恶意软件避开了检测，控制措施就无法跟踪其在环境中的传播、了解其根本原因，或发现恶意软件潜在入侵通道（系统会被恶意软件重复感染，或作为发射台，传播更广泛感染）。

尽管这只是恶意软件编写者如何处心积虑，领先于安全产品公司一步，利用现有防恶意软件控制措施的限制的一个案例，但我们最好是以没有一种检测 – 防御机制会100%有效为前提。如果认为只是依靠检测就能实现全面保护，不仅过高估计了您为关键资产提供防御的能力，而且也小看了您的对手发动攻击的能力。因此，机构需要为攻击者避开了防线的情况而制订一个计划，确保能够了解入侵范围和内容，快速遏制破坏，消除威胁，解决根本原因，消除恶意软件入侵通道，这就需要“回溯安全”。



向防恶意软件厂商提出的关键问题

1. 您采取什么方法判断恶意软件在网络中的扩散程度和对受感染设备造成的破坏程度?
2. 如果在数小时甚至数天后才检测到恶意软件，您如何确定哪些设备已被恶意软件感染?
3. 您如何处理成功规避了措施检测或在网络中未被拦截的恶意软件?
4. 您如何能够快速为可疑行为执行根本原因分析?
5. 您采取什么形式的控制措施来终止入侵和消除根本原因?

回溯安全使得机构实际上可以实现时光逆转，无论文件是否判定为恶意软件，都能确定哪些设备暴露在恶意软件的攻击之下。这需要跟踪每个穿越受保护网络的文件，以及全方位了解每个受保护设备上发生的每个行为，对应查看文件通过机构的方式与文件在系统上执行的操作。

使用传统防恶意软件防护时，如果在未来某个时刻，文件被判定为恶意软件，您可采取的措施通常十分有限，因为您无法进入时光机，在文件进入系统时将其拦截 – 它实际上已在您的环境中横行肆虐。这正是大多数防恶意软件控制措施无能为力之处，让您无法了解问题的全部，从而对“现在该怎么办”这个棘手问题一筹莫展。

而这也正是Sourcefire AMP的基础 – 大数据分析大显神威之处。通过名为“轨迹跟踪”的功能，它能够快速判断文件如何穿行机构，从而跟踪恶意软件，立即（在一些情况下自动）清理受感染设备。更重要的是，因为Sourcefire AMP跟踪每个文件的每一次使用，机构能够发现“第一感染源”（第一个遭受恶意软件攻击的设备）以及其它每个受感染设备，确保完全根除感染。因为，众所周知，如果清理后即使只有一个恶意软件实例存活，再次感染的可能性也非常大。

此外，轨迹分析不仅能够分析与文件活动相关的信息，而且能够跟踪文件世系、使用情况、相关性、通信、协议以及哪些文件安装了恶意软件等信息，对所检测到的恶意软件或可疑行为快速执行根本原因分析。这使安全团队能够在遭遇攻击时，即刻从检测切换到控制操作，迅速了解攻击范围和根本原因，有效终止进一步感染。

当面对大量检测事件，特别是恶意软件时，另一个挑战在于，确定哪些事件真正需要优先重视并作出响应。单一事件，甚至在某个终端拦截了一个感染恶意软件的文件，并不一定意味着发生安全问题。但是，当多个事件，哪怕是多个看起来正常的活动，互相关联起来时，其结果可能大大提高了系统遭受破坏的风险，表明安全违背即将或正在发生。

Indications of Compromise（感染指标）是Sourcefire AMP的另一功能，执行更深层次的分析，来发现系统遭受入侵的迹象。此功能是时间点检测技术所无法企及的，能够在初始分析后，继续捕获、分析和关联恶意软件相关活动，为安全人员提供自动分析和风险排序。

最后，一旦恶意软件在企业中扎根，它通常会尝试与CnC服务器通信，或者如果它直接被攻击者所控制，会开始侦查活动，逐步移向既定目标。

Sourcefire AMP监控受保护终端上的通信活动，并根据Sourcefire集体安全智能（Collective Security Intelligence）进行关联，判断是否发生入侵，拦截终端上恶意软件的通信与分发。藉此，安全人员能够获得独特优势，对于并未处于公司网络保护范围内的终端，如远程或移动员工所使用的系统等，能够控制这些终端上恶意软件的扩散。此外，轨迹跟踪和感染指数还能利用所捕获的网络活动，加速调查和感染的优先级划分。

多管齐下：在网络、物理和虚拟终端及移动设备上同时实施

独木不成林，单一安全控制措施并不能解决全部问题。为了防御高级恶意软件的入侵，必须在网络防御、终端保护和跟踪威胁及修复活动的管理控制台之间实现出色协作。Sourcefire提供了一个集成系统，利用基于云的集体安全智能（Collective Security Intelligence）、出色网络分析以及多点部署，来确保高级恶意软件不会乘隙入侵您的机构。

Sourcefire广泛的AMP功能从恶意软件一进入网络开始，就检测/拦截它们。当每个文件进入（或离开）网络时，Sourcefire AMP生成一个文件指纹，然后咨询Sourcefire的FireSIGHT®中央管理控制台，来判断该文件是否已被识别为恶意。

如果FireSIGHT从未看到过此文件，它在Sourcefire集体安全智能（Collective Security Intelligence ）Cloud中查找，快速判断该文件是否曾在Sourcefire的Collective Security Intelligence网络中出现。与对网络上每个文件进行沙箱操作相比，这一查询可扩展性更好，且对延迟无影响。对于已识别为恶意的文件，FireSIGHT提供文件跟踪功能，了解感染的程度和上下文环境。

Sourcefire的轻量级终端恶意软件防护代理（FireAMP™连接器）也可部署于每个受保护设备之上，从而根据集体安全智能（Collective Security Intelligence）Cloud检查所有文件活动，发现已知恶意文件。而且，FireAMP并不只是查找恶意文件，而是即使以前从未发现过此文件，也能有效检测和拦截设备上恶意软件的行为特征，保护终端免遭零日攻击。FireAMP连接器还利用回溯检测和上述文件跟踪功能，确定感染程度和需要立即修复的设备。

如果文件已被判断为可疑，则Sourcefire AMP将执行更深层次的文件分析。如上所述，Sourcefire基于云的分析功能可以精确确定文件的行为，如果判断文件为恶意，则将记录攻击简况，生成感染指标和其它能够使用强大的大数据分析功能搜索的特性。

利用这些恶意软件简况，Sourcefire AMP 使得机构能够占据主动，防御恶意软件攻击。如果在另一环境中（通过回溯安全）用事实证明某个文件为恶意，集体安全智能（Collective Security Intelligence）Cloud 能够将此判断发送到您机构的 FireSIGHT 控制台，帮助您在网络或终端拦截恶意软件，确保 Sourcefire AMP 社区的其他成员都实现集体免疫。此外，如果本地管理员发现了一个本地攻击，需要立即采取行动，机构能够设置定制规则来拦截特定文件和 IP 地址。

向AMP厂商提出的关键问题

1. 您能否在网络、物理和虚拟终端，以及移动设备上，拦截、跟踪、分析并修复恶意软件及根本原因?
2. 您如何为在受保护网络范围外漫游的设备提供保护?
3. 您如何确定哪些设备正在遭受攻击?
4. 您如何确认某个系统是否正被入侵，并执行修复措施?
5. 是否支持定制恶意软件检测规则，以修复独特攻击？如何提供此支持?

FireAMP™ Mobile连接器也是依靠集体安全智能（Collective Security Intelligence）Cloud快速分析安卓应用，实时发现可能的威胁。通过将可视性扩展到移动设备，您能快速了解哪些设备被感染，哪些应用为系统注入了恶意软件等等。当您希望针对攻击进行修复时，FireAMP Mobile提供强大控制措施，拦截特定应用（并将其置于黑名单），以便您能控制移动设备可使用哪些应用访问公司资源。FireAMP™ Virtual连接器则将相同功能和高级恶意软件防护措施扩展到了VMware虚拟机。

正如我们所述，恶意软件能够通过网络、直接通过终端、通过移动设备甚至虚拟系统，进入机构。重要的是，应能够全面查看整个机构中的活动。通过利用一个全球安全智能网络，并能在网络、终端、移动设备和虚拟系统上，检测、拦截、跟踪、调查和修复安全入侵，机构完全可以消除盲点，而这些盲点是其它缺乏广泛检测能力的安全控制技术所不可避免的。

采用回溯安全的
Sourcefire Advanced Malware Protection

Advanced Malware Protection的出色作用

如需了解集成高级恶意软件防护的功能，最佳方式是观察它如何在一个Java零日攻击公开发布前两天，就能检测出该攻击。在此例中，一位客户使用FireAMP Console（终端、移动和虚拟连接器管理控制台），检测到几个设备上有一些奇怪活动，看起来像是恶意软件的行为模式。客户利用集体安全智能（Collective Security Intelligence ）Cloud分析这些文件，得出其为恶意软件的清晰判断。

下一步是确定攻击范围并尽可能快速清除。客户随后使用FireAMP的轨迹跟踪功能，发现哪些设备被这些文件感染和/或显示出遭受攻击的行为模式。一旦受感染设备被清理，客户设置定制规则来拦截这些文件，并定义恶意软件的感染指标。

这些定制规则只须存在一段较短的时间，因为当这些文件和指标添加到大数据分析引擎后，每个Sourcefire AMP 客户都会受益于集体免疫。如果在客户环境中发现此攻击，就会向客户报警。藉此，在零日攻击公开发布前，整个 Sourcefire AMP 客户群就都已获得了必要保护。

总结

尽管业界已承认，需要采用创新解决方案来检测和修复高级恶意软件攻击，但仍然有太多机构还是将其全部重心放在检测方面，无论他们使用传统终端保护套件，还是全新“高级”防御，都是如此，毫无疑问这将遭致失败，业界不断出现的重要数据丢失和安全违背案例已经证明了这一点。

为了高效防御高级的零日攻击，解决方案必须采用大数据分析功能，跟踪网络、物理和虚拟环境，以及受保护终端及移动设备上的文件交互和活动。考虑到许多攻击在传统检测期处于潜伏状态，能够“逆转时光”，回溯将其更改为恶意软件，跟踪这些文件通过机构的轨迹与指标，将使客户可以更有效的遏制这些高级攻击造成的破坏并修复。

最后，不仅要对受保护终端设备，而且要为网络、移动设备和虚拟系统实施高级恶意软件防护，才能确保获得一致、出色的保护，因为下一波攻击的目标无法预测，所以只有如此，才能高枕无忧。

Sourcefire的Advanced Malware Protection提供：

- 能够灵活地在终端、网络、移动设备和虚拟系统上部署，且采用统一策略；
- 利用集体安全智能（Collective Security Intelligence）Cloud的优势，甚至能在业界发现新兴攻击前，就予以识别并进行分析；
- 能够回溯识别恶意软件，并经由文件跟踪功能，在其开始传播前，就发现机构中的所有恶意软件实例；
- 参加Sourcefire AMP社区，利用集体免疫，访问来自Sourcefire VRT的领先研究成果，以及全球数千客户所部署的上百万终端恶意软件防护代理发现的恶意文件样本。

如果您正在评估，将Sourcefire AMP解决方案作为部署高级恶意软件防护的选项之一，请联系我们：info@sourcefire.com。

5.13 I REV1B