Acronis

白皮书

多层网络安全保护：现代网络安全保护的组成部分

集成技术
实现更好的防御

数据是企业最重要的资产。随着全球数字化的不断深入，数据的数量和价值都在不断增长。事实上，数据是现代社会中最宝贵的资源，它的数量每年都会翻一番，而且增长率可能会进一步加快。这就带来了一个挑战：您是否安全存储数据？如何确保每一项数据操作都是安全的？现如今，丢失数据就意味着丢失一切：业务、身份、未来，在某些情况下甚至会失去生命。

在过去，许多企业通常会从两个不同的方面应对这一挑战。通过防病毒和防恶意软件解决方案来处理系统安全问题并提供一个安全的环境，同时通过备份解决方案来管理数据并确保数据副本始终可用。防恶意软件和备份代理程序通常安装在同一个终端上，但它们不会相互通信，因此无法保证在发生事件时快速恢复数据。

Acronis Cyber Protect 不仅解决了这一挑战，而且还为新建立的网络安全保护环境添加了其他基本功能。

为何要加强网络安全?

现代网络攻击、数据泄露和勒索软件的爆发都揭示了同一件事：对网络安全的防护失败了。导致这种失败的原因是技术薄弱以及由巧妙的社会工程造成的人为错误。在备份解决方案运行良好且未遭到破坏的情况下，通常需要数小时（甚至是数天）才能将系统（包含数据）恢复到正常运行状态。当网络安全保护解决方案失败时，备份是必不可少的；但与此同时，备份解决方案可能会遭到破坏、无法运转且耗时，从而导致企业因停机而招致巨大损失。

为了解决这些问题，Acronis 开发了 Acronis Cyber Protect：这是一种网络安全保护解决方案，它将防恶意软件和备份解决方案整合到一个在 Windows 操作系统下运行的代理程序中。这种集成可让您保持最佳性能、消除兼容性问题并确保快速恢复。如果漏掉了威胁或检测到威胁篡改了您的数据，那么将立即从备份中恢复数据 - 因为它有一个代理程序，能够自动知晓数据丢失并需要恢复。

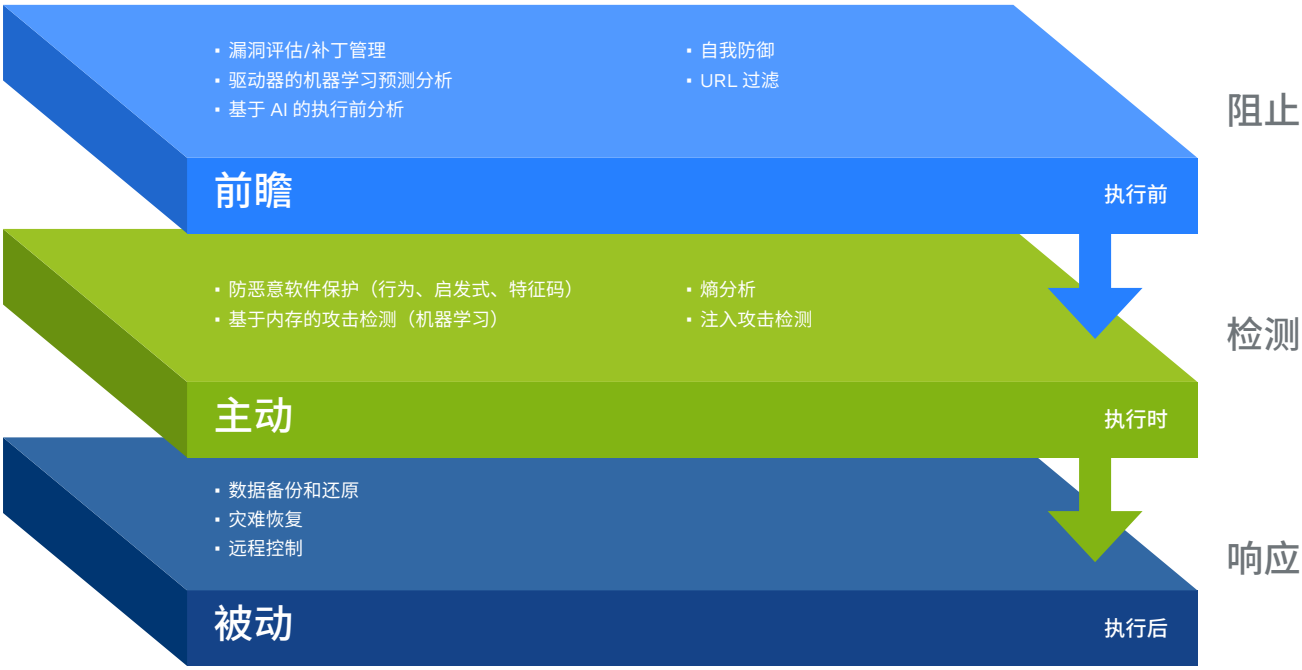
如果防恶意软件代理程序与拥有自己代理程序的备份产品各自为战，那么要做到这一点是不可能的。您的防恶意软件解决方案可能会阻止威胁，但某些数据或许已经丢失。备份代理程序并不会自动知晓这一情况，最多只会缓慢恢复数据（如果有）。

当然，Acronis Cyber Protect 会努力在您的环境被破坏之前检出并消除威胁，让数据恢复变得不再必要。它凭借增强的多层网络安全保护功能（本白皮书中将深入探讨该功能）做到了这一点。

应对新出现的威胁

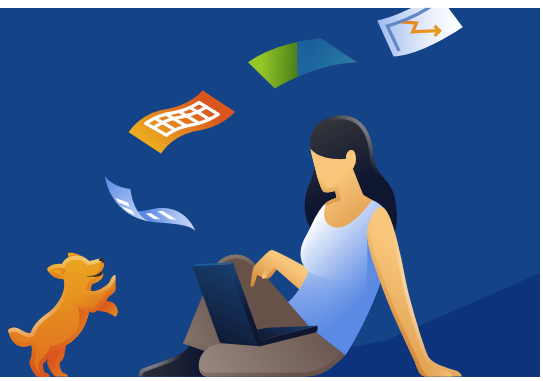
如今，理想的网络安全保护解决方案需要提供多层威胁防护功能。可通过一系列智能集成技术来提供该功能，其中每一项技术都应该在威胁防护的特定阶段发挥作用。例如，如果安全产品使用基于特征码的检测引擎，它将无法应对新的高危威胁，包括零日恶意软件威胁。

现代网络安全保护或防恶意软件解决方案应能够提供可靠的实时保护。这包括在当前的、新的或未知的威胁到达终端并试图破坏终端时检测到这些威胁的能力。在典型的终端安全解决方案中，可以由所谓的“访问时”或“执行时”检测方法来实现这一点，当然是在 Acronis Cyber Protect 中实现。此外，管理员还可以运行按需扫描：假设新软件出现在用户计算机上，则可以在执行前对其进行扫描。可通过多种技术来实现这些实时检测；在 Acronis Cyber Protect 中包括：



下面我们来专门介绍一下检测技术。请通过以下专用白皮书来熟悉这些主题：

- 漏洞评估和补丁管理
- Acronis Active Protection
- Acronis AnyData Engine
- 基于 AI 的 Acronis 驱动器运行状况分析
- 无文件攻击



ACRONIS CLOUD BRAIN

这项技术借助 Acronis 的全球数据中心提供云检测功能。当终端上的 Acronis Cyber Protect 代理程序检测到可疑内容时，它会将元数据发送到云端以进行进一步分析和研究，包括沙盒、已启用 AI 的处理等。此外，还可以在必要时由人类专家分析威胁。之后，将创建一个检测记录，并立即向连接到 Acronis Cloud 的所有其他终端提供此记录。比常规的代理程序特征码库和启发式规则更新（通常需要数小时才能提供保护）相比，这可以更快地提供更好的保护。

行为引擎（加上 ACRONIS ACTIVE PROTECTION）

静态检测方法（如特征码）很容易被绕过。网络罪犯只需打包并模糊处理恶意文件，特征码检测就会不起作用。这就是引入行为引擎的原因。这些行为引擎通常是一组行为规则，这些规则将对已知良好进程中的已知不良行为或异常行为做出反应。例如，试图恶意编辑注册表、删除文件、试图驻留在系统文件夹中或注入到其他进程的程序可能是恶意程序。

行为引擎将检测并停止表现出这些行为的进程。Acronis 行为引擎会分析可疑的内核级事件，以及源于 Windows 操作系统的事件。这些启发式规则可轻松进行更新，让 Acronis 安全专家能够快速响应新出现的威胁。此外，Acronis 行为引擎是一款非常强大的工具，可以检测无文件威胁，例如内存中或基于脚本的攻击。通过分析内存中的某些进程行为，Acronis 还可以确定它是否是威胁。例如，如果通过漏洞或者通过感染或创建恶意网站在 Web 浏览器的上下文中执行恶意代码。Acronis 行为检测引擎可以通过分析浏览器的线程行为来识别恶意代码并加以阻止，然后向管理员报告该恶意代码。

Acronis Active Protection 于 2017 年推出，它是由 AI 增强的、基于行为的独立引擎。它与新的通用 Acronis 行为引擎密切合作，后者可以检测任何类型的威胁，专门为 Acronis Cyber Protect 而开发。要查看 Acronis Active Protection 中实施的所有创新（如堆栈跟踪分析和合法进程注入攻击检测），您可以在本白皮书中了解更多信息。

机器学习与人工智能

Acronis 于 2018 年将机器学习技术纳入 Acronis Active Protection 防勒索软件技术中。借助机器学习模型和人工智能决策方法，我们分析了 Windows 可执行堆栈跟踪，为 Acronis Active Protection 行为启发式引擎添加了额外的置信层。

2019 年，Acronis 在 VirusTotal 上推出了基于 AI 的静态检测引擎。此引擎将处理 Windows 可执行文件和动态链接库（DLL）文件，以通过一组唯一参数来确定进程是否是恶意的。使用 Acronis Cloud Brain（已经处理了数千万个文件）中的恶意文件和干净文件，对机器学习模型进行训练，并记住数字证书的可用性和有效性等细节。持续分析 Acronis Cloud Brain 中的文件，同时还通过沙盒和其他安全工具对该模型进行训练。我们将有监督的训练方法和梯度提升技术与各种基于多种恶意行为情景或模式的决策树结合使用。

该模型由 Acronis 工程师不断优化，可以从云端轻松更新到每个终端。因此，训练中只包含相关参数，这有助于确保获得最佳结果。如果在检测后仍然无法确定某个进程的行为，那么将通过其他模型自动分析其行为，并且当我们稍后查看结果时，我们的检测模型会相应地进行调整。对于顶级恶意软件类型和系列，可以选择能提供最佳检测结果的单独模型。

从数量方面讲，好的机器学习模型并不需要太多数据。它需要的是高质量的相关数据。这就是训练模型来捕获常见威胁特征为何如此重要的原因。例如，勒索软件的关键特征是能够加密数据并连接到指挥控制中心。

目前，Acronis 静态检测模型的一次训练只需要 20 秒，我们每天有 10000 多个数据更新专门用于重新训练此模型。这意味着我们能够不断提高其抵御新兴威胁的有效性。目前，Acronis Cyber Protect 可以分析 Windows、macOS 和 Linux 操作系统。

白名单数据库

白名单是一个庞大的数据库，其中包含有关干净/非恶意应用程序的信息。它可以存储在云中，也可以存储在本地；本地版本有助于更快地作出反应，对于需要封闭边界、只想接收数据而不想与全球网络共享数据的企业而言，这是一个必备组件。政府和军队通常会使用白名单，鉴于其使用的数据性质，这种限制很有必要。

在云实现中，它也是 Acronis Cloud Brain 的一部分，位于 Acronis 数据中心。更有趣的是，Acronis 的网络安全保护产品还能够从备份填充白名单；如果您使用自定义软件，这是一项很有用的独特功能。假设使用的是开发人员在内部创建的应用程序。该应用程序允许某些系统访问，因此只有贵公司中的少数人可以使用该应用程序。如果传统的白名单系统遇到这样的应用程序，则会发出警报，并将其标记为可疑。清除该文件的唯一方法是下载并分析它，而这并不总是可行的。同时，管理员必须处理误报，这不仅会浪费时间，而且会降低工作效率。

现在，假设您在网络中注册一台使用此应用程序的新计算机。将对该计算机进行完整备份，如果使用 Acronis Cyber Protect，则各种防恶意软件引擎还会扫描该计算机。如果 Acronis Cyber Protect 在备份中发现了不在当前白名单中的新应用程序，则会立即对其进行分析，在需要时将其放入沙盒中，并在 24 小时或更长时间（具体取决于 Acronis 工程师设置的配置）内将其“清除”。之后，如果白名单在您注册的任何新计算机上遇到此应用程序，则白名单会作出正确的反应。

这种方法可最大限度地减少误报，让 Acronis 专家能够创建更准确、更积极的启发式检测规则，从而总体提高检测率并提供更好的保护。

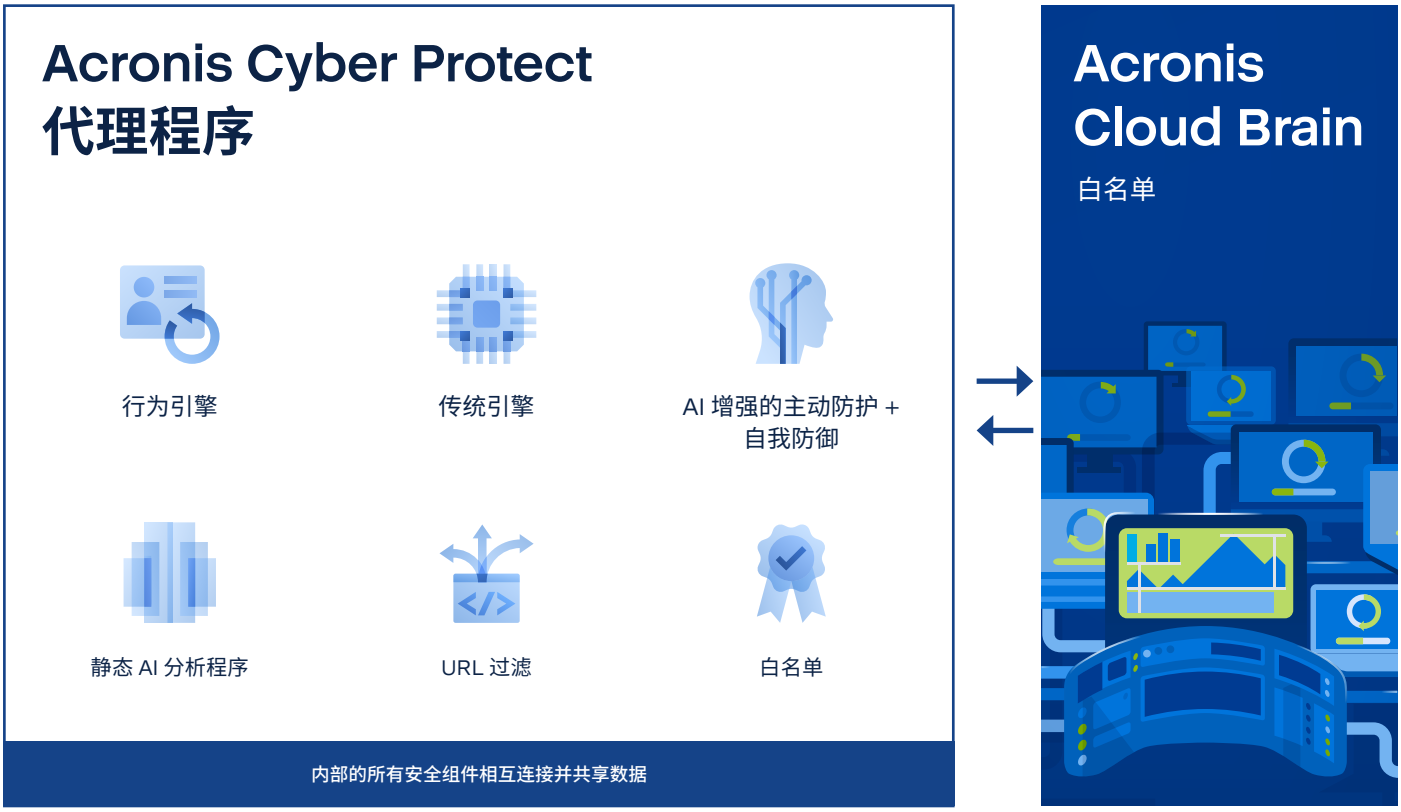
URL 过滤

过滤和识别网络钓鱼企图和恶意 URL 的能力，也是任何现代安全解决方案不可或缺的一部分。由于目前大多数威胁都来自互联网，因此务必要严格控制对已知不安全的特定网站的互联网访问。此外，合法网站也可能会遭到破坏，在被修复之前，它们还可能会被 URL 过滤或 Web 过滤阻止。

通常是通过云信誉库来提供 URL 过滤功能。Acronis Cloud Brain 使用以下方法来检测并阻止恶意 URL：

- **Acronis 的特征码**
- **基于 AI 的 Acronis 检测技术**
- **来自行业合作伙伴（包括反网络钓鱼工作组）的情报**

明智的做法是保留针对恶意和网络钓鱼 URL 的本地检测规则，以防发生互联网连接中断；我们所有的网络安全保护解决方案中都包含此功能。Acronis URL 过滤功能由通过分析链接和页面结构（标题、内容等）构建的机器学习模型进行了增强。

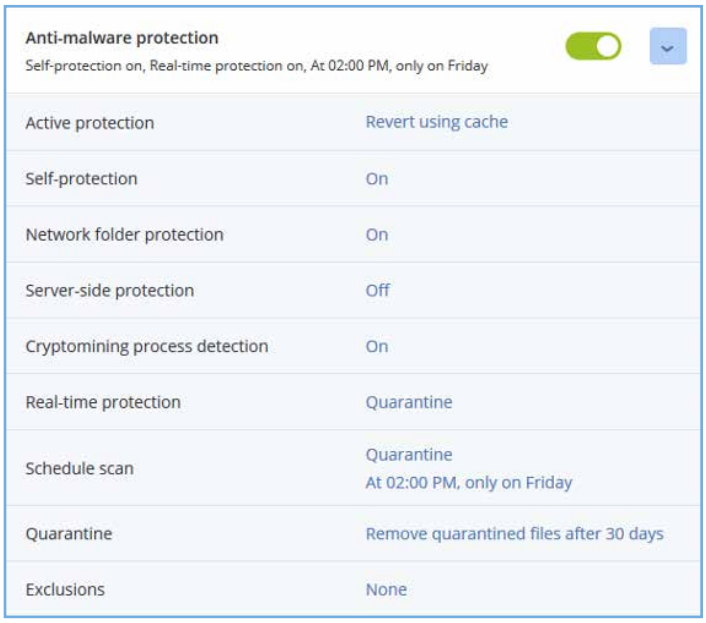


针对已知威胁的基于特征码的传统防恶意软件引擎

虽然专注于捕获零日威胁的前瞻技术非常重要，但是在安全解决方案中包含基于特征码的引擎很有必要，因为它的响应速度非常快。它将字节序列与终端代理程序上的本地数据库进行比较，这一过程要比向云发出请求的其他检测技术快得多。基于特征码的检测还可以为您提供额外的安全保障，并且能够抵御所有可能会出现的已知威胁。最终，大多数云检测方法、行为检测方法和由 AI 生成的检测方法也可以通过特征码来实现，从而加快检测过程。

然而，基于特征码的引擎的有效性可能各不相同。假设您有一些过时、不正确或损坏的记录。这可能会降低扫描引擎的性能。也可以假设以下情况：公司并不知道具体有哪些威胁，只创建了几个特征码，用于限制引擎可识别的内容。Acronis Cyber Protection 产品获得了市场上一个最佳经典引擎的授权，从而确保了出色的性能和覆盖范围。

此外，了解在这些引擎中如何更新防恶意软件记录也很重要。Acronis 实施了有效的分布式对等更新，它主要是依赖一台服务器（源服务器）将更新分发到网络中的数百台计算机，因此不会产生瓶颈。通过对等更新，只要一台计算机获得新库，另一台计算机也会获得，而无需等待更新服务器。



完全兼容 Microsoft Windows

作为 Microsoft 病毒计划的成员，Acronis 为 Windows 提供了一个经过认证的公认防恶意软件解决方案，此解决方案可以取代 Windows Defender。Acronis 遵循所有的 Microsoft 建议，并为其产品创建了完全兼容 ELAM 的驱动程序。Early Launch Anti-Malware（ELAM）是一项 Windows 8（及更新版本）安全技术，用于评估非 Microsoft Windows 启动时设备/应用程序驱动程序是否存在恶意代码。它是第一个在 Windows 操作模式下启动的系统内核驱动程序，排在任何第三方软件或驱动程序之前。在 Acronis Cyber Protect 中，Windows 安全中心集成完全受 Protected Process Light（PPL，一种基于 ELAM 的技术，可确保操作系统仅加载受信任的服务和进程）保护。Acronis Cyber Protect 还使用 PPL 来保护主要的防恶意软件服务。这使 Acronis 软件能够实现最高级别的自我防护，并覆盖了其他解决方案无法覆盖的核心防恶意软件模块。

在 Acronis Cyber Protect 管理中控台中，管理员可以：

- **在多个计算机上强制使用设置**
- **确保所有计算机上的防恶意软件库都是最新的**
- **查看所有 Windows Defender 检测事件**

确认网络安全保护功能正常运行

虽然许多安全公司都声称能够保护您的数据和环境，但他们不一定能够做到。在选择网络安全保护解决方案时，我们建议您从设置优先级开始。每个企业的最终目标都是盈利。任何业务中断或信誉损失都会招致巨大损失。

由于任何解决方案都无法保证 100% 的安全，因此您需要一个能够在事件发生后快速启动并运行的解决方案。多层网络安全保护解决方案应能够检测尽可能多的威胁，并让您能够评估其检测能力。通过检查 AV-Test 或 AV-Comparatives 等公司提供的各种独立测试，可以做到这一点。

如果您能够自行测试，最好自己测试一下。如果错过了威胁，您应该了解一下恢复已删除或损坏的数据或让用户计算机重新启动并运行的速度。因为与恶意数据丢失事件相关的成本可能比恶意软件本身造成的直接损失高得多。

扫描备份以发现恶意软件

防恶意软件扫描通常在终端或服务器上执行。但是，如果这些计算机正在进行完全备份（正在制作磁盘镜像），则在集中存储位置中扫描此完整磁盘镜像很有必要。在这种情况下，可以减少终端或服务器上的负载。这也是检查移动笔记本电脑和其他在公司网络上并非始终可用的计算机的一个好方法。

Acronis 可以扫描集中位置（云或本地）中的备份文件。但是，Acronis 可以做的不仅仅是扫描这些完整镜像。可以检查每个新切片是否存在恶意软件。您可以在本白皮书中了解操作方法。