Cisco Advanced Malware Protection для оконечных устройств

Cisco Advanced Malware Protection (AMP) для оконечных устройств предлагает единственную систему усовершенствованной защиты от вредоносного ПО, охватывающую весь период атаки: до ее начала, во время ее проведения и после завершения. Система обеспечивает непрерывный анализ и расширенную аналитику, поддерживающие возможности ретроспективной безопасности Cisco. Ретроспективная безопасность – это возможность заглянуть в прошлое и отследить процессы, активность файлов и связи, чтобы понять весь объем заражения, выявить исходную причину и произвести восстановление. Потребность в ретроспективном анализе возникает в случае каких-либо признаков нарушения, например срабатывания триггера события, изменения в расположении файла или срабатывания триггера признака нарушения (интегрированный центр управления). Ретроспективная безопасность дает администраторам возможность вернуться в прошлое для изучения угроз в системах. Такие инструменты как ретроспекция, взаимосвязь элементов цепочки атаки, поведенческие интегрированные центры управления, траектория и поиск нарушений помогают специалистам по безопасности определить масштабы, установить контроль в случае нарушения. Эта возможность позволяет команде по обеспечению безопасности быстро и эффективно устранять все угрозы в среде, прежде чем станет слишком поздно.

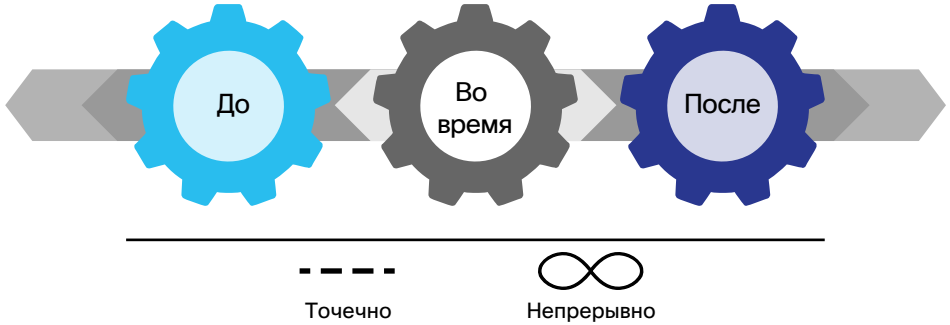
Помимо ретроспективной безопасности ключевыми функциями Cisco AMP для оконечных устройств являются следующие.

- **Непрерывный анализ:** AMP для оконечных устройств использует облачную аналитику больших объемов данных для выхода за пределы точечной защиты, постоянно заново оценивая новые и исторические данные, собираемые с течением времени, в целях выявления скрытых атак.
- **Контроль эпидемий:** AMP для оконечных устройств дает возможность обнаруживать и контролировать подозрительные файлы на оконечных устройствах как для будущих, так и для прошедших случаев угроз. Контроль «эпидемий» является одной из ключевых функций, позволяющей быстро остановить распространение вредоносного ПО в среде.
- **Интегрированный центр управления:** AMP для оконечных устройств автоматически сопоставляет данные о событиях в системе безопасности из разных источников, например события о вторжении или данные о вредоносном ПО, чтобы помочь командам по обеспечению безопасности связать события с более крупными, скоординированными атаками.

Недостатки средств точечной защиты

Одни лишь точечные проверки никогда не будут эффективными на 100 процентов. Чтобы преодолеть защиту и нарушить вашу среду, достаточно лишь одной угрозы. Используя адресное, вредоносное ПО с учетом контекста, опытные злоумышленники имеют достаточно ресурсов, опыта и настойчивости, чтобы обойти средства точечной защиты и в любой момент создать угрозу для любой организации. Кроме того, средства точечной защиты совершенно неспособны определить масштабы и глубину нарушения после того, как оно возникло.

Рис. 1. Точечная защита в сравнении с непрерывной защитой



Дополнительные функции AMP для оконечных устройств

Кроме того, AMP для оконечных устройств предлагает следующие возможности.

- **Репутация файла:** использует расширенную аналитику и результаты коллективной интеллектуальной работы для определения, является ли файл безопасным или вредоносным, что повышает точность обнаружения.
- **Анализ файлов и изолированная среда:** использует безопасную среду для выполнения, анализа и тестирования поведения вредоносного ПО, помогая обнаруживать ранее неизвестные угрозы нулевого дня.
- **Траектория файла:** отслеживает продвижение файлов в среде с течением времени, чтобы снизить до минимума количество времени, необходимое для определения масштабов распространения вредоносного ПО.

- **Траектория устройства:** отслеживает активность и связи с течением времени на уровне системы, что позволяет быстро выявлять исходную проблему и историю событий до и после нарушения.
- **Гибкий поиск:** обеспечивает простой, неограниченный поиск по файлам, телеметрическим данным и коллективным данным информационной безопасности, помогая связать контекст и масштабы нарушения с интегрированным центром управления или вредоносным приложением.

Преимущества

Благодаря Cisco AMP для оконечных устройств вы получите следующее.

- **Точечная защита:** AMP для оконечных устройств применяет подход ретроспективной безопасности к традиционному обнаружению, помогая улучшить возможности точечных средств защиты и повышая их эффективность, производительность и широту охвата.
- **Контроль цепочки атаки:** AMP для оконечных устройств не ограничивается ретроспекцией. Эта система вводит новый уровень аналитики, связывающей и сопоставляющей различные формы ретроспекции в ряд действий, доступных для анализа в режиме реального времени. Затем она ищет шаблоны вредоносного поведения на отдельном оконечном устройстве или для всех оконечных устройств в среде.
- **Расширенный анализ:** AMP для оконечных устройств предоставляет автоматизированные, расширенные возможности обнаружения поведения, обеспечивающие распределенное по приоритету и сопоставленное представление главных областей нарушения и риска.
- **Исследование, превращающее жертву в охотника:** AMP для оконечных устройств выводит исследовательские действия за пределы простого поиска фактов и ориентирует на целенаправленный поиск нарушений на основании реальных событий, например обнаружений вредоносного ПО и поведенческих интегрированных центров управления.
- **Упрощенное сдерживание:** AMP для оконечных устройств обеспечивает наглядность цепочек событий и контекста, дополняющую инструментальные панели и представления траектории. AMP для оконечных устройств позволяет определять в качестве цели конкретные приложения, файлы, вредоносное ПО и другие основные причины, давая возможность быстро и просто разбивать цепочку атак.
- **Контекстуальные инструментальные панели, позволяющие действовать:** отчеты не ограничены сбором и подсчетом событий. Отчетность в AMP для оконечных устройств включает дающие возможность действовать панели мониторинга и определение тенденций, которое показывает уместность с точки зрения бизнеса и воздействие с точки зрения риска.
- **Хорошо интегрированные платформы:** AMP можно активировать в решениях Email и Web Security Cisco всего лишь одним нажатием. Чтобы улучшить контроль, AMP можно развернуть во встроенном режиме в качестве специального сетевого устройства, а также на оконечном устройстве в качестве небольшого коннектора.

Collective Security Intelligence

Решение Collective Security Intelligence от аналитического центра Cisco в сфере информационной безопасности и группы исследования уязвимостей (VRT) Sourcefire – это интеллектуальные средства мониторинга угроз, которые собирают аналитическую информацию со всего мира в режиме реального времени. (Sourcefire теперь является частью корпорации Cisco.) Для сбора информации используется 1,6 млн датчиков по всему миру. Ежедневно мы получаем 100 ТБ данных и свыше 180 тыс. образцов файлов, а также имеем возможность отслеживать 35 процентов мирового трафика электронной почты. Над анализом этой информации, а также над публичной и частной передачей данных об угрозах работает свыше 600 инженеров, технических специалистов и исследователей, говорящих на 40 языках. Работа ведется круглосуточно, без перерывов и выходных. Постоянное взаимодействие с сообществами FireAMP™, Snort и ClamAV, а также участие в программе Sourcefire Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) позволяет нам делиться передовыми методами анализа угроз и восстановления. Благодаря этому мы лучше подготовлены к защите от будущих атак.

Преимущества решений Cisco

Cisco предлагает самый обширный портфель интегрированных решений улучшенной защиты от вредоносных программ, которые позволяют заказчику непрерывно отслеживать и контролировать вредоносное ПО в расширенной сети на протяжении всего периода атаки, т. е. до ее начала, во время ее проведения и после завершения. Система AMP, которая доступна как интегрированная функция, расширяющая возможности решений Email и Web Security Cisco, устройств сетевой защиты FirePOWER®, мобильных и виртуальных систем, а также решений для защиты ПК, обеспечивает гибкие варианты развертывания и защиту от атак с любых направлений.

Дальнейшие шаги

Дополнительные сведения см. на домашней странице Cisco AMP. Чтобы узнать, чем продукты Cisco будут полезны для вас, обратитесь к торговому представителю, торговому партнеру или системному инженеру Cisco.

C45-731874-00 05/14