Непрерывное обнаружение и отражение угроз для конечных устройств — в мире решений, обеспечивающих защиту только в определенный момент времени

Обзор

Единственный способ нейтрализовать современные угрозы безопасности — применять комплексный подход, охватывающий весь жизненный цикл атаки: до, во время и после. Основу этой модели составляет предлагаемая Cisco методика непрерывного анализа конечных устройств в сочетании с архитектурой для больших данных. Наши инновации в области защиты от усовершенствованного вредоносного ПО включают:

- непрерывный анализ;
- ретроспективный анализ;
- поведенческие индикаторы компрометации;
- траектории устройств и файлов;
- контроль эпидемии;
- функция контроля частоты распространения.

Сочетание этих возможностей в интегрированном рабочем процессе оказывает реальное и заметное влияние на обнаружение, мониторинг, анализ, расследование и сдерживание угроз.

Новая модель защиты конечных устройств

Корпорация Cisco обладает немалым опытом в области безопасности. И мы не сидели сложа руки, пока злоумышленники продолжали совершенствовать свои приемы. Еще в 2003 году мы (ранее — Sourcefire) имели представление о том, что требуется для противостояния изощренным угрозам. Мы первыми разработали концепцию непрерывного сетевого обнаружения, которая стала основой для следующего поколения систем предотвращения вторжений (NGIPS). Сегодня целенаправленное вредоносное ПО и изощренные атаки используют новые скрытые приемы компрометации. И Cisco меняет подход к обеспечению безопасности. Мы используем наши средства непрерывной защиты и представляем новую модель для отражения атак.

Непрерывная защита в непрерывно меняющемся мире

Когда более 10 лет назад компания Sourcefire (теперь часть Cisco) представила технологию получения информации о состоянии сети в реальном времени, для мониторинга сети стандартно использовались средства сканирования, действующие в определенный момент времени и нарушающие рабочий процесс. Полное сканирование с помощью этих средств занимало много времени и нарушало работу проверяемых систем и самой сети. Из-за динамической природы сетей данные быстро устаревали, поэтому приходилось снова и снова повторять весь процесс. Наконец, в данных было много «белых пятен», и их было трудно связать с данными по угрозам реального времени.

В Cisco поняли: основная проблема, с которой сталкиваются многие специалисты по защите, заключается не в обеспечении безопасности среды, а в том, чтобы определить, каковы объекты защиты и как они организованы. Поняв это, можно начать непрерывный процесс защиты. Благодаря постоянной осведомленности о состоянии сети в реальном времени контроль можно было бы впервые тесно интегрировать с обнаружением угроз, навсегда изменив подход к защите от сетевых угроз. По определению Gartner, осведомленность о состоянии сети в реальном времени стала основным требованием для систем NGIPS и была реализована в нашей технологии Cisco FireSIGHT™.

В 2013 году мы ввели еще одну революционную модель обеспечения безопасности для решения острой проблемы борьбы с современными сложными угрозами. Эта новая модель, учитывающая динамичность и стремительное расширение спектра современных угроз и ИТ-среды, охватывает весь жизненный цикл атаки: до, во время и после ее проведения.

Осведомленность о состоянии сети в реальном времени дает возможность перейти от традиционной методологии защиты в определенный момент времени к непрерывному походу. Эта модель:

- способствует внедрению уникальных инноваций в борьбе с современными изощренными угрозами;
- обеспечивает беспрецедентный контроль случаев компрометации и атак;
- позволяет службам безопасности быстро и оперативно сдерживать и устранять заражение, не нарушая работу конечных пользователей и персонала;
- дает возможность службам безопасности стать охотниками, а не жертвами.

Ожидание других результатов

Рынок решений по обнаружению и отражению угроз для конечных устройств переполнен крупными поставщиками, предлагающими одни и те же возможности. Каждый претендует на лидерство в следующем перевороте в области обнаружения вредоносного ПО. Как некогда поставщики средств сканирования сети, каждый участник рынка заявляет, что его решение обеспечивает лучшую непрерывную защиту в реальном времени. Но на самом деле речь идет лишь о нескольких усовершенствованиях одного и того же инструмента с сохранением всех основных ограничений.

> «Безумие — делать одно и то же снова и снова и ждать при этом разных результатов».
>
> Альберт Эйнштейн

Последние усовершенствования в обнаружении угроз включают выполнение файлов в изолированной среде для обнаружения и анализа угроз, использование виртуальных уровней эмуляции, затрудняющих анализ вредоносного ПО для пользователей и операционных систем, и составление «белого» списка приложений на основе репутации для отделения допустимых приложений от вредоносных. Недавно появилось моделирование последовательности атаки и аналитическое обнаружение. Но злоумышленники понимают статическую природу этих технологий безопасности и, естественно, учитывают их недостатки, совершенствуя приемы обхода средств защиты сети и конечных устройств.

К сожалению, конечному пользователю предлагаются не особо революционные усовершенствования, по сравнению с прошлогодней «ультрасовременной» технологией обнаружения угроз, и этот цикл повторяется снова и снова, без устранения основных ограничений. Сегодняшняя технология обнаружения привязана ко времени, точнее, она действует лишь в определенный момент.

Вредоносное ПО является динамическим и трехмерным. Оно существует не в двумерном пространстве X-Y, где X — время, а Y — механизм обнаружения, который применяется в фиксированный момент времени. Вредоносное ПО — это взаимосвязанная экосистема, которая постоянно меняется. Чтобы средства защиты от вредоносного кода можно было эффективно применять даже удаленно, они должны быть многомерными и столь же динамичными, как и само вредоносное ПО, учитывая взаимосвязи между различными его компонентами. Не нужно рассчитывать на то, что технология über-обнаружения решит проблему.

Необходимо кардинальное изменение подхода к обнаружению изощренных угроз и нарушений безопасности. Нужна непрерывная защита и прозрачный контроль на всех этапах — от момента вторжения до распространения и устранения последствий заражения.

Модель непрерывной защиты отвечает на самые важные вопросы

- Каковы метод атаки и точка вторжения?
- Какие системы были затронуты?
- Что сделала угроза?
- Можно ли остановить угрозу и ее первопричину?
- Как восстановить систему?
- Как предотвратить угрозы в дальнейшем?
- Можно ли быстро обнаруживать индикаторы компрометации, прежде чем они повлияют на работу организации?

Изменение парадигмы защиты на определенный момент времени

Современное вредоносное ПО характеризуется множеством направлений атак, принимает бесконечно разнообразные формы, запускает атаки с течением времени и может затруднять обнаружение утечки данных. По мере развертывания вредоносный код оставляет после себя огромные массивы информации, которые можно собирать, хранить, анализировать и подвергать различным действиям, чтобы понять принципы этих атак и способы их отражения. Основанное на модели защиты до, во время и после атаки решение Cisco® Advanced Malware Protection (AMP) для конечных устройств объединяет непрерывный подход с архитектурой для больших данных, устраняя ограничения традиционных технологий обнаружения и нейтрализации угроз в определенный момент времени.

В этой модели выполняется непрерывный сбор данных телеметрии на уровне процессов со всех источников в реальном времени, и эти данные всегда актуальны. Анализ можно встроить в процесс для исключения воздействия на контрольные точки и обеспечения эффективного обнаружения угроз на протяжении длительного периода времени. Анализ не ограничивается перечислением и корреляцией событий; он также подразумевает связывание данных телеметрии для создания более точной картины среды. Получая информацию от более широкого сообщества пользователей, система Cisco Collective Security Intelligence постоянно обновляется в глобальном масштабе, и ее данные распространяются мгновенно. Эта глобальная аналитическая информация сопоставляется с локальными данными для принятия более обоснованных решений.

В такой модели обнаружение и реагирование являются не отдельными дисциплинами или процессами, а продолжением одной и той же цели — нейтрализации изощренных угроз, прежде чем они нарушат вашу работу. Интегрированные средства обнаружения и реагирования действуют непрерывно и выходят за рамки традиционных методологий защиты на определенный момент времени.

Преимущества непрерывного анализа

- Меньше внимания уделяется обнаружению данных.
- Автоматизация расширенных аналитических функций.
- Улучшенное распределение угроз по приоритетам.
- Ускорение восстановления.

Обнаружение

Ни один метод обнаружения не является стопроцентно эффективным, поскольку злоумышленники постоянно совершенствуют свои приемы, чтобы обойти средства защиты на переднем крае. Но, несмотря на ограничения обнаружения в определенный момент времени, оно по-прежнему играет важную роль в устранении подавляющего большинства потенциальных угроз. Более того, применяя непрерывный подход к традиционному обнаружению, специалисты по защите могут улучшить технологии, действующие в определенный момент времени, повысив их эффективность и увеличив охват.

Но это только начало преобразования защиты от вредоносного ПО с помощью непрерывного подхода Cisco. Важнее то, что этот подход позволяет нам внедрить ряд других инноваций, которые улучшают весь процесс защиты — от обнаружения вредоносного ПО до принятия ответных мер.

Непрерывные возможности способствуют внедрению инноваций

Единственный способ нейтрализовать изощренные угрозы — применять комплексный подход, охватывающий весь жизненный цикл атаки: до, во время и после ее возникновения. Основу этой модели составляет наш непрерывный подход в сочетании с архитектурой для больших данных. Этот подход способствует внедрению ряда дополнительных инноваций в области защиты от вредоносного ПО, включая следующие возможности.

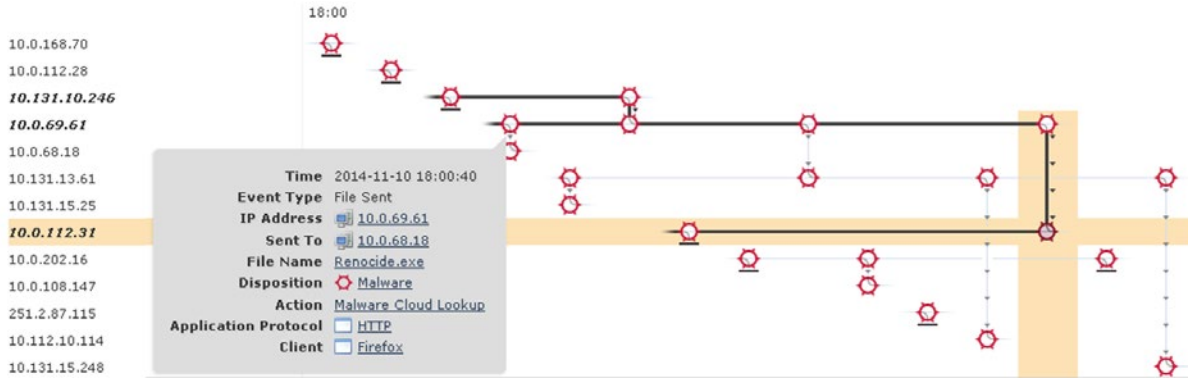
- **Ретроспективный анализ.** Возможность проводить анализ в начальный момент времени, и на протяжении длительного периода не ограничивается файлами. Этот анализ также охватывает процессы, каналы связи и другие данные телеметрии, которые просто невозможно обработать при помощи традиционных моделей защиты на определенный момент времени.
- **Восстановление последовательности атаки**. Метод связывания данных ретроспективного анализа файлов, процессов и каналов информационного обмена с течением времени для определения их корреляции отсутствует в двумерных технологиях защиты на определенный момент времени.
- **Поведенческие индикаторы компрометации.** Это не просто статические артефакты, а сложные поведенческие признаки, которые средства восстановления последовательности атаки собирают в реальном времени и обнаруживают по мере возникновения.
- **Траектория.** Траектория — это не просто маркетинговый эквивалент термина «отслеживание». В результате отслеживания создается перечень событий, возникших в том или ином месте в определенные моменты времени. Траектория — это непрерывный путь, по которому перемещается объект (в данном случае вредоносное ПО), как функция времени. Она гораздо эффективнее демонстрирует масштаб и первопричины атаки в контексте места ее возникновения и действий вредоносного кода.

- **Поиск угроз.** Учитывая динамический характер вредоносного ПО, обнаруживаемого со временем, и обширность этих всегда актуальных данных, прицельно отследить трудноуловимые индикаторы компрометации так же легко, как найти в поисковике любимый ресторан готовой еды.

Каждая из перечисленных инновационных технологий в отдельности нейтрализует вредоносное ПО и изощренные угрозы, связанные с ним. Но объединение этих возможностей в интегрированном рабочем процессе оказывает реальное и заметное влияние на обнаружение, мониторинг, анализ, расследование и сдерживание угроз.

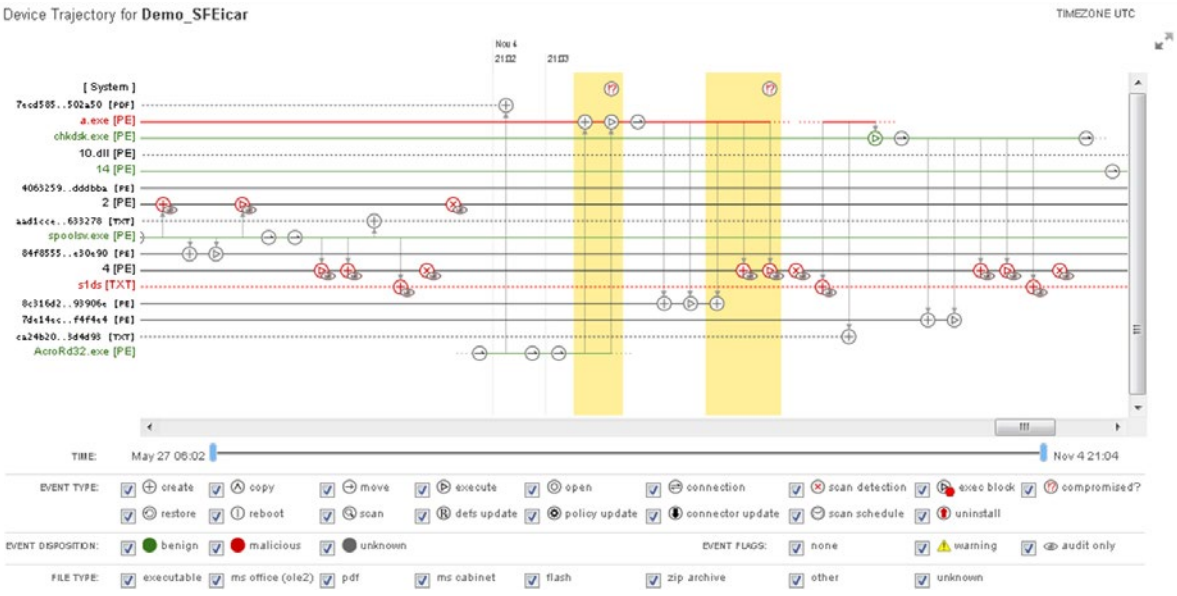
На рисунке 1 показано распространение вредоносного ПО с информацией о точке вторжения, действиях вредоносного кода и затронутых конечных устройствах.

Рисунок 1. Экран с траекторией сетевого файла, полученной при помощи Cisco AMP



На рисунке 2 показан экран с траекторией распространения вредоносного ПО для устройства с информацией о точке вторжения, действиях вредоносного кода, двоичных и исполняемых файлах, затрагивающих конкретное конечное устройство. Эта информация коррелируется и распространяется между конечными устройствами во всей сети и интегрируется с представлением сети на рисунке 1.

Рисунок 2. Экран с траекторией устройства, полученной при помощи Cisco AMP для конечных устройств



Мониторинг

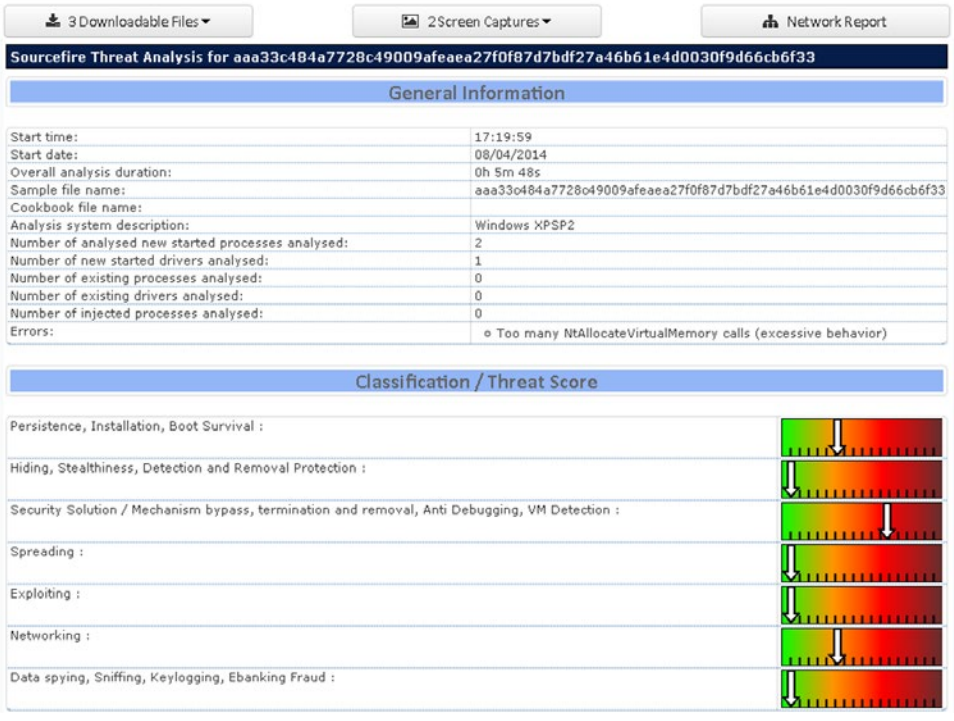
Возможность собирать данные телеметрии с конечного устройства и анализировать их на предмет проявлений угроз (как в момент их возникновения, так и за продолжительный период времени) называется ретроспективным анализом. Компания Cisco первой реализовала эту инновационную технологию. Ретроспективный анализ — это большой шаг вперед по сравнению со сбором данных, управляемым событиями, и запланированными проверками новых данных. Он фиксирует атаки в момент их возникновения, действуя подобно системе видеонаблюдения.

Автоматизированная расширенная аналитика

Чтобы обнаруживать современные атаки по мере их скрытого распространения по сети и конечным устройствам, специалистам по защите требуются технологии, которые будут вести автоматический поиск индикаторов компрометации, оставляемых вредоносным ПО и эксплойтами, а также более сложных признаков компрометации, проявляющихся со временем. Непрерывный подход Cisco обеспечивает такой уровень автоматизации благодаря расширенным возможностям поведенческого обнаружения, которые нацелены не на предоставление очередного перечня оповещений для расследования, а на формирование обобщенной картины основных областей компрометации и нарушений безопасности с распределением по приоритетам. Использование анализа больших данных и непрерывно действующих возможностей позволяет обнаруживать тенденции и индикаторы компрометации в момент их возникновения. Это позволяет службам безопасности сосредоточиться на наиболее опасных угрозах.

На рисунке 3 приведена подробная информация о поведении файлов, включая уровень серьезности действий, исходное имя файла, снимки экрана выполняющегося вредоносного ПО и собранные образцы пакетов. Эти сведения помогут лучше понять, что нужно для сдерживания эпидемии и блокирования будущих атак.

Рисунок 3. Экран анализа файлов при помощи Cisco AMP для конечных устройств



Поиск угроз или расследование

Без контекста и возможностей непрерывного подхода слово «расследование» может вызвать несколько нервную реакцию со стороны служб безопасности, которым хорошо знаком трудоемкий процесс выявления нарушения при недостаточных контекстных доказательствах. Часто самый сложный вопрос, на который приходится отвечать, — с чего начать. При использовании непрерывного подхода расследования становятся более целенаправленными, эффективными и быстрыми.

Непрерывный подход позволяет перейти от поиска трудноуловимых признаков и фактов к прицельному поиску нарушений безопасности на основе реальных событий, таких как обнаружение вредоносного ПО и статические или поведенческие индикаторы компрометации. Благодаря непрерывно действующим средствам и архитектуре для больших данных можно легко вести поиск любой информации в любое время. В непрерывной модели, которая использует ранее описанные возможности (включая поведенческое обнаружение и обнаружение на определенный момент времени, а также ретроспективный анализ), отслеживать вредоносное ПО можно быстро и эффективно. Расследование или поиск угроз включают наглядное представление точки вторжения, масштаба и первопричин заражения. Сюда также входит возможность определить временной интервал для поиска, увеличить или уменьшить этот интервал и сделать поиск более прицельным при помощи фильтров. Эта возможность становится важным инструментом и фактором повышения эффективности по мере того, как службы безопасности вместо непродуманного реагирования на оповещения и инциденты могут быстро отследить вредоносное ПО, пока область атаки не увеличилась.

Контроль или сдерживание эпидемий

Расследование может показаться невероятно сложной задачей, если оно ограничено обнаружением на определенный момент времени и средствами технической экспертизы. То же самое можно сказать и об идее сдерживания вредоносного или подозрительного ПО без восстановления заводских настроек всех устройств. Технологии, действующие в определенный момент времени, не способны восстановить последовательность событий и анализировать связанную с ней контекстную информацию, поэтому радикальное сдерживание вредоносного ПО находится за гранью возможного.

Благодаря прозрачности, которую обеспечивает непрерывный подход, в сочетании с возможностью сосредоточиться на конкретных первопричинах можно не только быстро, но и легко разрушить цепочку атаки. Более того, даже если стандартной процедурой является восстановление заводских настроек устройства, подвергнувшегося серьезной компрометации, все данные обнаружения и телеметрии сохраняются и сдерживающие мероприятия все равно можно провести, чтобы помешать злоумышленникам совершать атаки в будущем с использованием той же точки доступа.

Наконец, традиционные технологии защиты на определенный момент времени иногда не способны даже обнаружить нарушение, и организация может оказаться в эпицентре развернутой атаки. Обычно множество конечных устройств заражалось на протяжении длительного периода времени, и для расследования и исправления ситуации привлекалась группа реагирования на инциденты. Как и в случае обнаружения, время здесь крайне важно, и приходится задавать те же основные вопросы: «С чего начать и насколько серьезно положение?» Однако для отражения и сдерживания атаки при таком сценарии эпидемии часто требуется очень быстро понять масштаб и первопричины, не раскрывая свою осведомленность злоумышленникам. Важно быстро завершить работу всех скомпрометированных устройств и одновременно закрыть точки доступа, через которые распространяется заражение, чтобы предотвратить обходные маневры злоумышленников.

С момента развертывания непрерывного подхода начинается сбор важнейших данных обнаружения и телеметрии, которые помогают группам реагирования понять серьезность эпидемии, расположение «горячих» точек и, самое главное, создать профиль сдерживания, который можно немедленно ввести в действие. Сразу включаются расширенные средства поведенческого обнаружения, отслеживания и визуализации, но, в отличие от процессов в сценарии обнаружения и защиты, они все работают в режиме аудита. Эти средства выполняют обнаружение и оповещение, но вместо того, чтобы активно блокировать вредоносное ПО, они собирают «улики», подобно детективам на месте происшествия, собирающим информацию, на основании которой оперативная группа проводит захват преступника.

Принципиальное различие между непрерывным реагированием и реагированием в определенный момент времени заключается в том, что в первом случае обеспечивается надежный контроль эпидемии, включая оперативное сдерживание, тогда как второй подход предоставляет лишь перечни фактов и свидетельств. Хотя службы безопасности могут использовать эти перечни, их сложно применить на практике для сдерживания атаки.

Интеграция и отчетность

Решение Cisco AMP для конечных устройств с самого начала было ориентировано на непрерывный подход и архитектуру для больших данных. Оно использует облачную модель для поддержки упрощенного коннектора вместо громоздкой архитектуры агентов на конечном устройстве. Коннектор подобен средству сбора данных файлов и телеметрии, в отличие от агента обнаружения, ограниченного по охвату и эффективности из-за потребления вычислительных ресурсов и памяти на пользовательских конечных устройствах. Эта модель освобождает ресурсы, благодаря чему коннектор может непрерывно вести мониторинг, сбор и эффективную передачу данных телеметрии в облако для анализа больших данных.

Модель упрощенного коннектора поддерживается на различных платформах конечных устройств, таких как Windows, Mac, Android, и в виртуальных средах, предоставляя равноценные функциональные возможности. Это обеспечивает обнаружение вредоносного ПО и защиту от него на других контрольных точках, таких как шлюзы электронной почты и веб-шлюзы, новое поколение систем предотвращения вторжений и межсетевых экранов, облачные службы с большим объемом файловых операций.

Повсеместный сбор и расширенный анализ данных файлов и телеметрии на контрольных точках повышают уровень коллективной аналитики, которая может распространяться локально в пределах среды и глобально среди заказчиков посредством облака Cisco Collective Intelligence Cloud. Обмен аналитической информацией в реальном времени помогает службам безопасности предупреждать обширные атаки, использующие такие приемы, как фишинг, когда множество пользователей заражаются через одни и те же начальные полезные данные, а затем получают разные загружаемые компоненты или команды. Помимо анализа файловых данных можно проводить анализ других данных телеметрии по всем контрольным точкам, чтобы точнее определить масштаб эпидемии.

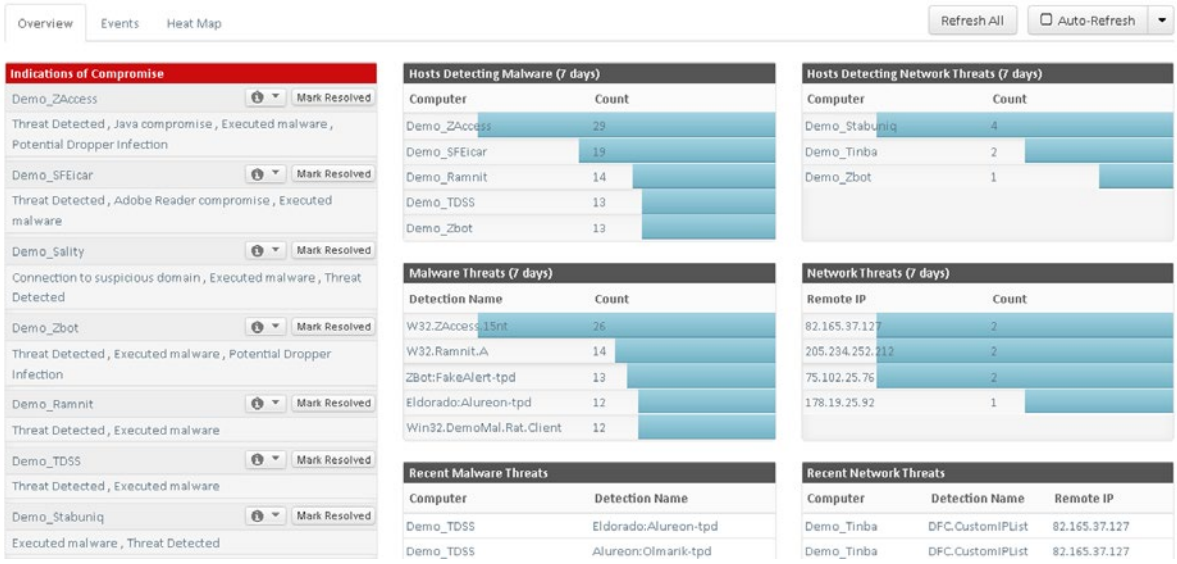
Благодаря облаку собранные данные телеметрии можно распространять среди всех контрольных точек, обеспечивая равный доступ к контекстной информации даже на тех устройствах, где собрать данные такого уровня невозможно. Например, службы сетевой безопасности могут использовать данные телеметрии и поведенческого обнаружения, собранные с конечного устройства, чтобы оценить степень уязвимости для определенного вредоносного ПО. Информация о том, был ли файл загружен, открыт или даже перемещен, может дать специалистам по безопасности более полную картину, чем общие оповещения. Конечные устройства, активировавшие вредоносное ПО, получают более высокий приоритет, чем те, что просто загрузили его. Обширная контекстная информация с конечного устройства, передаваемая в реальном времени на другие контрольные точки для более эффективного выявления угроз и принятия решений, резко контрастирует с обычным перечнем событий, которые с равной долей вероятности могут представлять реальную угрозу или быть безвредными.

Непрерывный подход также распространяется на возможности отчетности. Отчеты больше не ограничиваются перечислением и составлением сводки событий. Они могут включать информативные инструментальные панели и данные о тенденциях, акцентируя внимание на актуальности для бизнеса и потенциальных рисках. Технологии защиты на определенный момент времени также могут предоставлять инструментальные панели и сведения об актуальности рисков. Но для обработки и установления корреляции огромных объемов данных о событиях здесь требуется сложная интеграция системы управления информацией о безопасности и событиями (SIEM).

Архитектура для больших объемов данных помогает справиться со стремительно растущим объемом информации, важной для эффективного обнаружения и анализа вредоносного ПО. Используя эти данные, непрерывный подход предоставляет контекст и, самое главное, распределяет угрозы по приоритетам (в нужное время и в нужном месте).

На рисунке 4 показаны информативные инструментальные панели Cisco AMP для конечных устройств и результаты анализа тенденций, которые акцентируют внимание на актуальности для бизнеса и влиянии на него с точки зрения рисков. Отчеты не ограничиваются перечислением и составлением сводки событий. В этом представлении, помимо прочего, показано распределение индикаторов компрометации по приоритетам, узлы, на которых обнаружено вредоносное ПО, и сетевые угрозы.

Рисунок 4. Инструментальные панели Cisco AMP для конечных устройств



Заключение: на самом деле, 1 + 1 не равно 3. Иногда эта сумма равна 6.

Непрерывный подход в сочетании с архитектурой для больших наборов данных поддерживает шесть основных направлений преобразования борьбы против изощренных угроз, направленных на конечные устройства.

1. **Обнаружение, выходящее за рамки определенного момента времени.** Благодаря непрерывному подходу обнаружение становится более эффективным и повсеместным. Методы поведенческого обнаружения, такие как анализ в изолированной среде, оптимизированы; сведения о вредоносных действиях собираются по мере их развертывания, а аналитическая информация распространяется среди подсистем обнаружения и контрольных точек.

2. **Мониторинг, позволяющий восстановить последовательность атаки.** Ретроспективный анализ — непрерывный мониторинг файлов, процессов и каналов информационного обмена и связывание этих данных для восстановления последовательности событий — обеспечивает беспрецедентную глубину знаний об атаке, получаемых по мере ее развертывания.
3. **Автоматизированный расширенный анализ поведения с течением времени.** Сочетание анализа больших наборов данных и непрерывно действующих возможностей для выявления тенденций и индикаторов компрометации по мере их возникновения помогает службам безопасности сосредоточить свои усилия на наиболее серьезных угрозах.
4. **Расследование, которое превращает жертву в охотника.** Благодаря преобразованию расследования в целенаправленный поиск угроз на основе реальных событий и индикаторов компрометации службы безопасности могут быстро и эффективно понять суть атаки и оценить ее масштаб.
5. **Простое сдерживание атаки.** Прозрачность, которую обеспечивает непрерывный подход, в сочетании с возможностью сосредоточиться на конкретных первопричинах позволяет быстро и эффективно разрушить цепочку атаки.
6. **Информативные инструментальные панели, учитывающие контекст.** Отчеты, которые составляются по результатам повсеместного сбора и расширенного анализа данных файлов и телеметрии на контрольных точках и затем дополняются контекстной информацией, акцентируют внимание на тенденциях, актуальности для бизнеса и влиянии риска.

Используя инновационные средства непрерывной защиты в сочетании с архитектурой для обработки больших данных, Cisco предоставляет новую модель для отражения современных сложных атак. В такой модели обнаружение и реагирование являются не отдельными дисциплинами или процессами, а продолжением одной и той же цели — нейтрализации изощренных угроз, прежде чем они нарушат вашу работу. Выходя за рамки традиционных методологий защиты в определенный момент времени, интегрированные средства обнаружения и реагирования действуют непрерывно. Именно это требуется для обнаружения и отражения угроз, направленных на конечные устройства, в реальном мире.

Сравнение непрерывного подхода с моделью защиты в определенный момент времени

Далее приведено подробное сравнение возможностей, отличающих непрерывный подход от модели защиты в определенный момент времени. Также описаны усовершенствования в обнаружении и инновации в сфере защиты от вредоносного ПО.

Таблица 1. Обнаружение

Непрерывный подход	Модель защиты в определенный момент времени
• Интегрированная сеть подсистем работает согласованно, обмениваясь контекстной информацией для улучшения процессов обнаружения. • Поведенческие методы обнаружения, такие как анализ в изолированной среде, оптимизированы за счет уменьшения рабочих нагрузок и задержки и исключения необходимости изолировать каждый новый файл. • Обнаружение выполняется на протяжении длительного периода времени, в точности соответствуя характеру развертывания атаки. • Режим аудита преобразован из простой настройки для снижения числа ложных срабатываний в средство сбора данных для реагирования на инциденты. Он позволяет фиксировать нарушения безопасности в реальном времени втайне от злоумышленников. • Аналитическая информация по обнаружению мгновенно распространяется среди множества контрольных точек.	• Несколько подсистем работают как стек (последовательно и независимо), что снижает эффективность и производительность на уровне конечного устройства. • Требуются обновления от поставщика, что занимает время и создает дополнительные бреши в системе безопасности.

Таблица 2. Мониторинг

Непрерывный подход	Модель защиты в определенный момент времени
• Ретроспективный анализ файлов. После первоначального анализа данных по обнаружению детальное исследование файла продолжается на протяжении длительного времени с использованием новейших средств обнаружения и коллективной аналитики по угрозам. После этого можно визуализировать обновленную диспозицию и провести дальнейший анализ за пределами момента, когда файл был впервые обнаружен. • Ретроспективный анализ процессов. Аналогично ретроспективному анализу файлов ретроспективный анализ процессов — это возможность непрерывно собирать и анализировать данные ввода-вывода системных процессов на протяжении длительного периода времени для проведения анализа последовательности атаки и обнаружения поведенческих индикаторов компрометации. • Ретроспективный анализ каналов связи. Информационные потоки, передающиеся на конечное устройство и от него, постоянно фиксируются вместе со связанными приложениями и процессами, инициирующими этот обмен или получающими данные. Эта информация предоставляет дополнительные контекстные данные в ходе анализа последовательности атаки и обнаружения поведенческих индикаторов компрометации. • Восстановление последовательности атаки. Возможности решения Cisco AMP для конечных устройств не ограничиваются ретроспективным анализом. Оно выводит аналитику на новый уровень, объединяя различные формы ретроспективных данных для восстановления последовательности событий, которую можно проанализировать в реальном времени. В частности, связывание различных типов ретроспективных данных в ходе анализа позволяет выявлять тенденции в поведении на уровне отдельного конечного устройства или их группы.	• Отсутствие ретроспективного анализа. Модель не способна выявлять связанные действия на уровне конечного устройства за рамками обнаружения. • Модель также не может выявлять события в сети, произошедшие после того, как вредоносное ПО миновало контрольную точку.

Таблица 3. Автоматизированная расширенная аналитика

Непрерывный подход	Модель защиты в определенный момент времени
• Реагирование в реальном времени. Данные телеметрии, которые непрерывно собираются с конечных устройств и добавляются в хранилище, могут автоматически сопоставляться со статическими и поведенческими индикаторами компрометации. Таким образом, время обнаружения статического или поведенческого индикатора компрометации можно существенно уменьшить. • Поведенческие индикаторы компрометации. Используя восстановление последовательности атаки, поведенческие индикаторы компрометации позволяют выявить сложные тенденции среди различных событий обнаружения, статических индикаторов и данных телеметрии, которые свидетельствуют о возможном нарушении безопасности. Классический пример — вирус-сбрасыватель, ускользнувший от средств первоначального обнаружения. • Восстановление последовательности атаки. Средства восстановления последовательности атаки также фиксируют события, которые произошли до и после появления поведенческих индикаторов компрометации. Основываясь на информативном оповещении, служба безопасности быстро может оценить масштаб эпидемии и локализовать проблему. • Открытые индикаторы компрометации. Благодаря открытым индикаторам компрометации заказчики могут использовать собственные перечни статических индикаторов для обнаружения. • Индикаторы компрометации, основанные на аналитике. Более чем статические аналитические данные, черные списки или сценарии обнаружения, эти индикаторы компрометации основаны на поведенческих алгоритмах, нацеленных на поиск определенных вредоносных действий и связанных с ними событий с течением времени. Индикаторы компрометации, основанные на аналитике, разрабатываются и полностью поддерживаются подразделением Cisco Talos Security Intelligence and Research Group. • Функция контроля частоты распространения. Аналитическая подсистема определяет частоту распространения обнаруженного вредоносного ПО в масштабах организации и более обширного глобального сообщества. Нередко вредоносное ПО с низким уровнем распространения является признаком целенаправленной атаки и попытки взлома. Службы безопасности обычно упускают такие файлы. Анализ распространеня помогает выявить атаки этого типа, особенно при использовании в корреляции с другими статическими или поведенческими индикаторами компрометации.	• Некоторые технологии защиты на определенный момент времени могут искать статические индикаторы компрометации, но не в режиме реального времени. Кроме того, для подобных технологий часто требуется длительный сбор данных, прежде чем можно будет запустить анализ индикаторов компрометации. • Такая модель может показать, сколько раз или где было обнаружено вредоносное ПО, но информация о связях с первопричинами отсутствует. • Невозможно понять значимость или уровень распространенности угрозы. • Если средства оценки распространенности все же существуют, они не могут ни работать в реальном времени, ни продолжать отслеживание конкретных файлов, процессов и каналов связи. • Невозможно выявить поведенческие индикаторы компрометации.

Таблица 4. Поиск угроз или расследование

Непрерывный подход	Модель защиты в определенный момент времени
• Траектория файлов. Степень уязвимости для вредоносных или подозрительных файлов можно быстро оценить вместе со временем, методом атаки и точкой вторжения, затронутыми системами и распространенностью — и все это без сканирования и создания снимков конечных устройств. • Траектория устройств. Основываясь на данных о масштабе, полученных из траектории файлов, траектория устройств обеспечивает расширенный анализ системных процессов в определенном интервале времени для получения статистики первопричин и восстановления последовательности событий. Можно увеличить или уменьшить интервал и применить фильтр, чтобы быстро определить точную причину компрометации. • Гибкий поиск. Гибкий поиск помогает легко и быстро получить ответ на вопрос «Где еще этот индикатор был обнаружен?» без типичных ограничений запросов к реляционной базе данных. Можно выполнять поиск любых элементов: имени узла, имени файла, URL-адреса, IP-адреса, текстовых строк — по всему набору данных и в глобальной экосистеме коллективной аналитики. Учитывая миллионы файлов, анализ которых проводится регулярно, такой поиск становится мощным средством для быстрого и своевременного обнаружения изощренных угроз. • Анализ файлов. Во-первых, модель предоставляет безопасный механизм для запуска файла в изолированной среде, чтобы полностью проанализировать поведение и оценить уровень угрозы этого поведения. Во-вторых, результаты этого анализа можно вывести в подробном отчете. В-третьих, все результаты анализа добавляются в коллективную аналитическую базу. И в-четвертых, ко всем результатам анализа можно применять гибкий поиск. Опять же, службы безопасности могут по индикатору в отчете об анализе файла быстро понять, где еще был обнаружен этот индикатор в организации. Это особенно важно, когда атака является целенаправленной, но использует общий способ заражения.	• Традиционные технологии обнаружения на определенный момент времени лишены таких возможностей. Они не предоставляют данные мониторинга после обнаружения и контекстную информацию. ◦ Средства обнаружения часто фиксируют независимые события, которые добавляются в перечень. Этот перечень постоянно обновляется, но без учета контекстных ретроспективных данных. ◦ Невозможно узнать, какие события произошли до и после обнаружения. ◦ Невозможно полностью проанализировать поведение файлов и затем быстро искать уникальные индикаторы компрометации по всем конечным устройствам. • Некоторые технологии могут предоставлять ограниченные возможности (например, позволяющие определить, когда и где было обнаружено вредоносное ПО, по данным из перечня событий). Но они не способны установить события, произошедшие до и после компрометации в определенном временном интервале. • Традиционные средства технической экспертизы и расследования, действующие на определенный момент времени, не намного лучше средств обнаружения, даже если поставщик заявляет, что они работают непрерывно. ◦ Эти средства лишены расширенных возможностей обнаружения угроз. Обнаружение в сочетании с непрерывным получением контекстной информации может стать важной отправной точкой, но средства технической экспертизы предназначены для поиска артефактов и признаков, а не для установления взаимосвязей. ◦ Они не обеспечивают визуализацию событий в определенном интервале времени до и после компрометации. ◦ Эти средства не позволяют быстро искать уникальные индикаторы компрометации без обновления всех данных.

Таблица 5. Контроль или сдерживание эпидемий

Непрерывный подход	Модель защиты на определенный момент времени
• Простое сдерживание. Подозреваете, что файл является вредоносным? Не нужно ждать. Используйте SHA256 (алгоритм безопасного хеширования), чтобы несколькими нажатиями кнопки мыши немедленно заблокировать файл на всех конечных устройствах, в отдельной их группе или только на одном устройстве. • Расширенные возможности сдерживания. Аналогично сценариям Snort® особые средства расширенного обнаружения позволяют нейтрализовать целые семейства вредоносного ПО, не дожидаясь обновления сигнатур. • Белые и черные списки приложений. В сочетании с обширной контекстной информацией контрольные списки позволяют более эффективно определять, используются ли легальные приложения как точки доступа для злоумышленников, и блокировать предположительно опасные приложения. Эти списки расширяют данные непрерывного анализа и телеметрии. Службы безопасности могут быстро взять ситуацию под свой контроль, применяя стандартные процедуры реагирования. • Черный список IP-адресов. Аналогично контрольным спискам приложений черные списки IP-адресов можно использовать более эффективно в контексте реального события или в корпоративных политиках для контроля эпидемии и мониторинга конечных устройств на предмет поступающих с них подозрительных информационных потоков. Эта возможность особенно важна в случае взлома системы, когда нужно блокировать любые перекрестные каналы связи, используемые злоумышленником, пока выполняется план сдерживания атаки.	• Технологии защиты на определенный момент времени предоставляют очень ограниченные возможности сдерживания вредоносного или подозрительного ПО, поскольку сосредоточены на моменте обнаружения, не затрагивая более поздние этапы жизненного цикла атаки, где критически важно ее сдерживание. • Некоторые технологии обнаружения в определенный момент времени включают составление «черного» списка приложений. Это неплохой способ блокировки приложений, представляющих риск для организации, или подозрительных приложений неизвестного характера, которые должны быть блокированы в качестве меры предосторожности. Однако применение «черного» списка наиболее эффективно в сочетании с обширным набором средств анализа файлов и поведенческого обнаружения. Это позволяет выполнять основные функции обнаружения, анализа и сдерживания. Главные недостатки заключаются в том, что управление такими технологиями как основным уровнем защиты становится слишком трудоемким и что они могут пропускать атаки и не способны восстанавливать их последовательность. • Наконец, средства технической экспертизы и реагирования на инциденты, действующие в определенный момент времени, не позволяют быстро взять эпидемию под контроль, что требуется в условиях современных изощренных угроз. Они полезны в расследовании, но не способны перейти от сбора данных к сдерживанию. Для этого часто требуются трудоемкие операции, которые обычно не проводятся при более простом методе восстановления заводских настроек.

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Отпечатано в США. C11-733649-00 02/15

